# Elliptische Kurven und Kryptographie

Wolfgang M. Ruppert

Sommersemester 2003

28. Dezember 2006[1]

[1]Im Sommersemester 2003 am Mathematischen Institut der Universität Erlangen abgehaltene Vorlesung

# Inhaltsverzeichnis

## Vorbemerkung

Das vorliegende Vorlesungsskript entstand parallel zur Vorlesung. Die Beispiele wurden meist mit Maple (Version 9) gerechnet; zugehörige Funktionen finden sich im Anhang oder auf meiner Internetseite.

## Vorlesungsankündigung

## Elliptische Kurven und Kryptographie

*Elliptische Kurven* sind algebraische Kurven, die sich durch eine Gleichung der Form $y^2 = x^3 + ax + b$ beschreiben lassen. Sie tauchen auf in der *Funktionentheorie* bei der Theorie der doppeltperiodischen Funktionen, in der *Algebraischen Geometrie* als einfachste Beispiele von projektiven Varietäten mit einer Gruppenstruktur und schließlich in der *Zahlentheorie* als eine wichtige Klasse diophantischer Gleichungen, die auch beim Beweis der Fermatschen Vermutung eine entscheidende Rolle spielten.

In der *Kryptographie* geht es darum, Nachrichten/Daten/Informationen so zu verschlüsseln, dass ein Unbefugter nichts damit anfangen kann. Dies spielt inzwischen auch im Alltagsleben eine wichtige Rolle, man denke z.B. an abhörsicheres Telefonieren mit Mobiltelefonen, an Sicherheitsmaßnahmen für Bankgeschäfte per Internet und an die Sicherheit beim Einsatz von Chipkarten (z.B. Telefonkarten, Krankenversichertenkarten).

1985 wurde von Koblitz und Miller der Vorschlag gemacht, auch elliptische Kurven für kryptographische Verfahren zu benutzen. Inzwischen gibt es *ECC* (Elliptic Curve Cryptography), die Kryptographie mit elliptischen Kurven. Einer der Vorteile von elliptischen Kurven besteht darin, dass man bei gleichen Sicherheitsanforderungen mit deutlich kürzeren Schlüssellängen als bei herkömmlichen Public-Key-Kryptoverfahren wie z.B. RSA auskommt. Das macht ECC besonders interessant, wenn man wenig Speicherplatz und wenig Rechenkapazitäten hat, wie z.B. bei Smartcards.

Die 4-stündige Vorlesung setzt Grundkenntnisse der Algebra voraus, will einführen in die Theorie der elliptischen Kurven, in die Public-Key-Kryptographie und Anwendungen elliptischer Kurven in der Kryptographie behandeln.

- Aktuelle Informationen: http://www.mi.uni-erlangen.de/∼ruppert/SS03
- Zeit und Ort: Mo, Mi 8-10, ÜR 2.
- Beginn: 7.4.2003, Ende: 9.7.2003.

KAPITEL 1

# Einführung in die Kryptographie

## 1. Einfache Kryptosysteme

Die Grundsituation in der Kryptographie ist folgende: Ein Sender $A$ will eine Nachricht $T$ an einen Empfänger $B$ senden. Dabei soll verhindert werden, dass ein Unbefugter die Nachricht verstehen kann, auch wenn er bei der Übertragung an die Nachricht kommen kann. Die Nachricht $T$ wird auch Klartext, message oder plaintext genannt. $A$ hat eine Verschlüsselungsfunktion $f$, die die Nachricht $T$ in den verschlüsselten Text $f(T)$, auch Chiffretext oder ciphertext genannt, umwandelt. Die verschlüsselte Nachricht $f(T)$ sollte für Außenstehende nicht verständlich sein. Der Empfänger $B$ kennt die Entschlüsselungsfunktion $f^{-1}$ und kann sich aus $f(T)$ mit $f^{-1}(f(T)) = T$ dann die ursprüngliche Nachricht $T$ berechnen. Wichtig: $f^{-1}$ wird geheimgehalten.

**Caesar-Verschlüsselung:** Auf Gaius Julius Caesar (100–44 v.Chr.) soll folgendes Verfahren zurückgehen, wobei ein Buchstabe $x$ durch $f(x)$ ersetzt wird:

| $x$ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f(x)$ | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

Also ist $f(A) = D$, $\ldots$ $f^{-1}(A) = X$, $\ldots$. Aus dem Text *HEUTE IST MITTWOCH* wird dann *KHXWH LVW PLWWZRFK*.

**Bemerkungen:**

(1) Man kann die Buchstaben A, B, C, $\ldots$, Z mit den Zahlen von 0 bis 25 identifizieren. Die obige Verschlüsselungsfunktion lässt sich dann einfach als
$$f(x) = x + 3 \bmod 26$$
schreiben. Außerdem ist $f^{-1}(x) = x - 3 \bmod 26$ oder auch $f^{-1}(x) = x + 23 \bmod 26$.

(2) Statt obiger Verschlüsselungsfunktion kann man natürlich ebenso für jedes $t \in \{0, 1, \ldots, 25\}$ die Funktion
$$f_t(x) \equiv x + t \bmod 26$$
benutzen.

Wollen zwei Personen sicher Nachrichten übermitteln, können sie sich eine Verschlüsselungsfunktion $f$ ausdenken, die dann geheim gehalten werden muss. Hat man viele Personen, die paarweise geheim Informationen austauschen wollen, liegt gewöhnlich ein festgewähltes Verschlüsselungsverfahren zugrunde, das allgemein bekannt sein kann, das aber von einem Parameter, dem sogenannten Schlüssel $K$ abhängt, der dann natürlich auch variiert werden kann, d.h. man hat $f_K$ und $f_K^{-1}$. Alles hängt dann von der Geheimhaltung des Schlüssels $K$ ab. Bei obigem Kryptosystem gibt es also 26 mögliche Schlüssel.

Den Versuch, die Verschlüsselungsfunktion $f_K$, die Entschlüsselungsfunktion $f_K^{-1}$, den Schlüssel $K$, oder aus $f(T)$ den Text $T$ zu gewinnen, wird als Kryptanalyse bezeichnet.

Bei unserem ersten Kryptosystem gibt es nur 26 Schlüssel. Weiß man also, dass dieses Verschlüsselungsverfahren zugrunde liegt, so kann man alle Möglichkeiten durchprobieren.

Man kann nun natürlich auch mehr bzw. andere Zeichen zugrundelegen. Die Menge der verwendeten Zeichen wird als Alphabet bezeichnet.

**Beispiele:**

(1) Wir haben in unserem ersten Kryptosystem das Alphabet A, B, C, ..., Z verwendet und eine Bijektion mit $\mathbf{Z}/(26)$ benutzt.
(2) Ein etwas größeres Alphabet erhält man, wenn man noch die Kleinbuchstaben a, b, c, ..., z, Leerzeichen, Interpunktionszeichen . , ! ? hinzunimmt.
(3) Ein ascii-Zeichensatz besteht aus 255 Zeichen, die durch $0, \ldots, 255 = 2^8 - 1$ repräsentiert werden. (In C-Programmen kann man damit arbeiten.) So ist $\phi(A) = 65$, $\phi(B) = 66$, ..., $\phi(Z) = 90$, $\phi(a) = 97$, ..., $\phi(z) = 122$, $\phi$(Return/Wagenrücklauf) = 10, $\phi$(Leerzeichen) = 32, etc.

Wichtig ist, dass man sich für ein Kryptosystem auf ein bestimmtes Alphabet einigen muss.

Hat das zugrundeliegende Alphabet $N$ Zeichen, identifiziert man diese mit den Zahlen $0, 1, \ldots, N-1$, so bilden die Funktionen

$$f_t(x) = x + t \bmod N$$

geeignete Verschlüsselungsfunktionen, wodurch unser erstes Kryptosystem verallgemeinert wird.

**Beispiel:** (Caesar - Verschlüsselung für Dateien)

(1) Gegeben sei eine Datei. Sie besteht aus einer Folge von Bytes $c_1 c_2 c_3 \ldots$, wobei wir ein Byte $c_i$ mit einer Zahl zwischen 0 und 256 identifizieren können.
(2) Als Schlüssel wählen wir eine ganze Zahl $t$. Die Verschlüsselungsfunktion wird

$$f_t(x) = x + t \bmod 256.$$

(3) Die Ausgabedatei soll aus der Bytefolge $f_t(c_1) f_t(c_2) f_t(c_3) \ldots$ bestehen.
(4) Die Entschlüsselungsfunktion ist dann $f_{-t}$.

Was kann ein Unbefugter machen, der eine Datei erwischt, die mit Kryptosystem 1a verschlüsselt wurde? Er kann auf die Datei $f_{-t}$ für $t = 0, 1, 2, \ldots, 255$ anwenden und untersuchen, ob die entstehende Datei sinnvoll ist. Es gibt aber noch andere Möglichkeiten.

**Häufigkeitsanalyse von Buchstaben:** Im Deutschen kommen die Buchstaben nicht gleich häufig vor. Statistische Untersuchungen haben folgende Häufigkeitsverteilung gezeigt (aus A. Beutelspacher, Kryptologie, Vieweg 1991):

| Buchstabe | E | N | I | S | R | A | T |
|---|---|---|---|---|---|---|---|
| Häufigkeit in % | 17.40 | 9.78 | 7.55 | 7.27 | 7.00 | 6.51 | 6.15 |

Natürlich kann man nicht erwarten, dass sich jeder Text so verhält. Aber es ist immerhin ein Anhaltspunkt.

So ohne weiteres lässt sich dies nicht auf unser Kryptosystem 1a übertragen, da im allgemeinen in den Plaintextdateien auch andere Zeichen außer A,B,C,...,Z vorkommen.

**Häufigkeitsanalyse von Zeichen in TeX-Dateien:** Wir haben 10 TeX-Dateien untersucht. Häufigstes Zeichen war Zeichen Nr. 32 (Leerzeichen), dann Zeichen Nr. 101 (e).

**Anwendung:** Angenommen, wir finden eine Datei, die mit einer Funktion $f_t(x) \equiv x + t \bmod 256$ verschlüsselt wurde. Als häufigstes Zeichen finden wir Nr. 65 (A). War die Ausgangsdatei eine TeX-Datei mit Nr. 32 als häufigstem Zeichen, so erfüllt die Verschlüsselungsfunktion

$$f_t(32) = 32 + t = 65 \bmod 256,$$

also ist $t = 33$ und wir versuchen die Datei mit $f_{-33}$ zu entschlüsseln. Was passiert, wenn die Datei keine TeX-Datei ist?

Ein offensichtlicher Nachteil der Caesar-Verschlüsselung ist, dass sie leicht durch Häufigkeitsanalyse der Buchstaben gebrochen werden kann. Der Grund ist, dass die Verschlüsselungsfunktionen auf einzelne Buchstaben angewendet werden. Das wird nun verallgemeinert. Wir fassen jeweils $k$ Zeichen zu einem Block bzw. einer Nachrichteneinheit zusammen, d.h. wir schreiben den Text $T$ als Folge $T_1 T_2 T_3 T_4 \ldots$, wobei $T_i$ aus $k$ Zeichen/Buchstaben des Alphabets besteht. Die Verschlüsselungsfunktion soll jetzt auf der Menge der Blöcke bzw. Nachrichteneinheiten wirken. Man spricht dann von einer **Blockchiffrierung**.

**Beispiel:**

- Wir legen ein Alphabet mit $N$ Zeichen zugrunde, das wir mit $\{0, 1, \ldots, N-1\}$ bzw. $\mathbf{Z}/N\mathbf{Z}$ identifizieren.
- Der Plaintext wird in Blöcke/Plaintexteinheiten der Länge $k = 2$ zerlegt. Die möglichen Plaintexteinheiten bilden eine Menge $M$, die man dann mit $(\mathbf{Z}/N\mathbf{Z})^2$ identifizieren kann.
- Die Verschlüsselungsfunktionen $f_K$ operieren auf den Plaintexteinheiten, $f_K : M \to M$, und werden durch
$$f_{(A,b)} : (\mathbf{Z}/N\mathbf{Z})^2 \to (\mathbf{Z}/N\mathbf{Z})^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} + b \bmod N,$$
definiert mit $A \in M_2(\mathbf{Z}/N\mathbf{Z})$ und $b \in (\mathbf{Z}/N\mathbf{Z})^2$. Damit die Verschlüsselungsabbildung bijektiv ist, muss $A \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ gelten, was äquivalent mit $\mathrm{ggT}(\det A, N) = 1$ ist.
- Alles hängt von der Geheimhaltung des Schlüssels $K$ ab, da man aus der Kenntnis von $f_K$ sofort $f_K^{-1}$ berechnen kann. In obigem Beispiel ist
$$f_{(A,b)}^{-1} : (\mathbf{Z}/N\mathbf{Z})^2 \to (\mathbf{Z}/N\mathbf{Z})^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \widetilde{A} \begin{pmatrix} x \\ y \end{pmatrix} - \widetilde{A}b,$$
wo $\widetilde{A}$ eine Matrix ist mit $\widetilde{A}A \equiv 1 \bmod N$.
- Die Anzahl der möglichen Schlüssel beträgt dann
$$\#\mathrm{GL}_2(\mathbf{Z}/(N)) \cdot N^2 = N^6 \prod_{p|N} (1 - \frac{1}{p})(1 - \frac{1}{p^2}),$$
was für $N = 26$ die Zahl 106299648 ergibt.)
- Wenn die Anzahl der Zeichen des Ausgangstextes nicht gerade ist, muss man sich darauf einigen, wie man mit dem letzten Zeichen verfährt.

**Beispiel:** Wir verwenden das letzte Kryptosystem mit dem gewöhnlichen Alphabet A,..., Z (und die Bijektion mit 0,..., 25) und der Verschlüsselungsabbildung
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 5 & 8 \\ 23 & 15 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 17 \\ 14 \end{pmatrix}.$$
Das Buchstabenpaar ZA ergibt den Vektor $\begin{pmatrix} 25 \\ 0 \end{pmatrix}$, der auf $\begin{pmatrix} 12 \\ 17 \end{pmatrix}$ abgebildet wird, was dem Buchstabenpaar MR entspricht. Die Umkehrabbildung ist
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 23 & 12 \\ 15 & 25 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 13 \\ 19 \end{pmatrix}.$$

Bei den letzten beiden Kryptosystem operierte die Verschlüsselungsfunktion auf Buchstabenpaaren. Um das Kryptosystem zu brechen, kann man daher die Häufigkeit von Buchstabenpaaren untersuchen.

**Häufigkeitsanalyse von Buchstabenpaaren:** Die häufigsten Buchstabenpaare im Deutschen sind folgende (aus A. Beutelspacher, Kryptologie, Vieweg 1991):

| en | er | ch | te | de | nd | ei | ie | in | es |
|---|---|---|---|---|---|---|---|---|---|
| 3.88 | 3.75 | 2.75 | 2.26 | 2.00 | 1.99 | 1.88 | 1.79 | 1.67 | 1.52 |

Allerdings halten sich natürlich nicht alle Texte an solche Verteilungen.

Man kann jetzt leicht weitere Kryptosysteme konstruieren:

**Beispiel:** Man lege ein Alphabet mit $N$ Zeichen zugrunde, fasse jeweils $k$ Zeichen $x_1 x_2 \ldots x_k$ zu einer Nachrichteneinheit zusammen, bilde daraus einen Vektor mit Koeffizienten aus $\mathbf{Z}/(N)$ und definiere die Verschlüsselungsabbildung durch
$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \mapsto A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \bmod N$$

mit einer Matrix $A \in \mathrm{GL}_k(\mathbf{Z}/N\mathbf{Z})$ und $b_1, \ldots, b_k \in \mathbf{Z}/N\mathbf{Z}$.

**Aktuelle Blockchiffrierungen:**

(1) DES (Data Encryption Standard). Es gibt ein Programm 'des', das bei Aufruf von 'des -e datei datei.aus' nach Eingabe eines Passworts 'datei' mit DES verschlüsselt und in die Datei 'datei.aus' schreibt. Entschlüsselt wird mit 'des -d datei.aus datei.ein'.
(2) IDEA (International Data Encryption Algorithm) mit Plaintextblocklänge 64 Bit, Schlüssellänge 128 Bit. Im Softwarepaket PGP wird diese Verschlüsselung verwendet bei Aufruf von 'pgp -c datei': nach Eingabe eines (frei wählbaren) Passworts erhält man die verschlüsselte Datei 'datei.pgp'. Entschlüsselt wird mit 'pgp -d datei.pgp'.
(3) AES (Advanced Encryption Standard). Dies soll ein neuer Standard werden.

**Anmerkungen:**

(1) Erfahrungsgemäß ist ein Kryptosystem dann am sichersten, wenn der Algorithmus allgemein bekannt ist und von vielen Leuten getestet wurde.
(2) Es gibt verschiedene Arten kryptanalytischer Angriffe, so z.B.
   - Ciphertext-only-Angriff: Man hat nur einen verschlüsselten Text zur Verfügung und will diesen entschlüsseln.
   - Known-plaintext-Angriff: Man kennt den Ausgangstext (oder Teile davon) und den verschlüsselten Text.
   - Chosen-plaintext-Angriff: Man kann Ausgangstexte wählen und sehen, wie sie verschlüsselt werden.
(3) Verwendet man eines der vorgestellten Kryptosysteme, so muss man natürlich vorher auf anderem Wege, der aber trotzdem sicher sein muss, den Schlüssel ausgetauscht haben. Dies ist vor allem bei einer großen Zahl von Teilnehmern problematisch.

## 2. Eine Grundidee der Public-Key-Kryptographie

Wir betrachten nun eine neue Situation: Angenommen, wir finden eine Familie von (bijektiven) Funktionen $f_K : M \to M$, mit folgenden Eigenschaften:

**Eigenschaft 1:** Kennt man $K$, so lässt sich für alle $x \in M$ der Wert $f_K(x)$ schnell berechnen.
**Eigenschaft 2:** Auch wenn man $K$ und damit $f_K$ kennt, kann man zu $y \in M$ das Urbild $f_K^{-1}(y)$ praktisch - d.h. in angemessener Zeit - nicht berechnen.
**Eigenschaft 3:** Man kann Parameter $K$ so finden/konstruieren, dass man dazu einfach $K'$ berechnen kann mit $f_K^{-1} = f_{K'}$.

Die Idee, eine solche Situation kryptographisch zu nutzen, geht wohl auf Diffie und Hellman (1976) zurück: Wir denken uns ein System mit vielen Teilnehmern $A$, die verschlüsselt Nachrichten austauschen wollen.

- Jeder Teilnehmer $A$ wählt sich eine Verschlüsselungsfunktion $f_{K_A}$ und die zugehörige Entschlüsselungsfunktion $f_{K_A}^{-1} = f_{K'_A}$, was nach Eigenschaft 3 möglich ist.
- In einer Liste (Telefonbuch) werden die Daten $(A, K_A)$ öffentlich zugänglich gemacht. $K_A$ (und damit $f_{K_A}$) ist also allgemein bekannt, man nennt dies den öffentlichen Schlüssel - public key - von $A$. Allerdings ist $K'_A$ nur $A$ selbst bekannt; man nennt $K'_A$ daher den privaten Schlüssel - private key - von $A$.
- Will ein Teilnehmer $B$ eine Nachricht $T = t_1 t_2 t_3 t_4 \ldots$ vertraulich an $A$ senden, besorgt er sich aus der Liste (Telefonbuch) den öffentlichen Schlüssel $K_A$ von $A$, berechnet dann $f_{K_A}(t_i)$ und schickt
$$f_{K_A}(t_1) f_{K_A}(t_2) f_{K_A}(t_3) \ldots$$
an $A$. Der Teilnehmer $A$ kann sich daraus mit seinem privaten Schlüssel $K'_A$ wegen $f_{K'_A}(f_{K_A}(t_i)) = f_{K_A}^{-1}(f_{K_A}(t_i)) = t_i$ sofort die Nachricht $T$ bestimmen.
Sollte ein nichtbefugter Teilnehmer $C$ irgendwie an die verschlüsselte Nachricht $f_{K_A}(t_i)$ kommen, kann er dennoch nicht viel damit anfangen: er kann zwar $f_{K_A}$ benutzen, er kann sich aber nach Eigenschaft 2 das Urbild $t_i$ nicht berechnen. Die Geheimhaltung ist also gewährleistet.

- Ein großer Vorteil eines solchen Kryptosystems ist, dass man kein Problem mit dem Schlüsselaustausch hat, da die Schlüssel $K_A$ öffentlich zugänglich sind. Außerdem können leicht neue Teilnehmer $C$ dazu kommen; sie müssen nur ihre Daten $(C, f_{K_C})$ in die öffentliche Liste (Telefonbuch) eintragen lassen.
- Ein solches Kryptosystem wird **Public-Key-Kryptosystem** genannt.

Natürlich stellt sich nun die Frage, ob man tatsächlich Funktionen $f_K$ mit den oben geforderten Eigenschaften finden kann.

## 3. Schnelle zahlentheoretische Algorithmen

Sei $b \geq 2$ eine festgewählte natürliche Zahl. Dann lässt sich jede natürliche Zahl $n$ eindeutig schreiben als

$$n = \sum_{i=0}^{k-1} n_i \cdot b^i \quad \text{mit} \quad n_i \in \{0, 1, \ldots, b-1\}.$$

Man schreibt auch $n = (n_{k-1}n_{k-2}\ldots n_1 n_0)_b$ und spricht von der $b$-adischen Darstellung von $n$, im Fall $b = 10$ hat man die Dezimaldarstellung, im Fall $b = 2$ die Binärdarstellung. Ist $n_{k-1} \neq 0$, so sagt man, $n$ hat $k$ Stellen bzgl. der Basis $b$. Ist $n$ zur Basis $b$ $k$-stellig, so gilt $b^{k-1} \leq n < b^k$, also $k - 1 \leq \frac{\ln n}{\ln b} < k$ und somit

$$k = [\frac{\ln n}{\ln b}] + 1,$$

insbesondere $k = O(\ln n)$. Die Stellenzahl von $n$ wächst wie $\ln n$.

Analysiert man, wie man natürliche Zahlen mit der Hand addiert, multipliziert und dividiert, so erhält man folgendes Ergebnis:

Satz. *Die Schrittzahl bzw. Laufzeit zur Addition, $k$-stelliger natürlichen Zahlen lässt sich durch $O(k)$ abschätzen, die Laufzeit für Multiplikation und Division durch $O(k^2)$. Anders formuliert: Addition, Multiplikation, Division natürlicher Zahlen $\leq n$ kann in $O(\ln n)$ bzw. $O(\ln^2 n)$ Schritten erfolgen.*

**Bemerkung:** Ein Algorithmus, ein Berechnungsverfahren, wobei natürliche Zahlen $\leq n$ eingehen, hat polynomiale Laufzeit, wenn sich die Schrittzahl durch $O((\ln n)^k)$ mit einer natürlichen Zahl $k$ abschätzen lässt. Wenn wir von 'schnellen' Verfahren sprechen, meinen wir solche mit einer einer polynomialen Laufzeit.

Im Folgenden geben wir ein paar wichtige zahlentheoretische Algorithmen mit einer polynomialen Laufzeit an.

### 3.1. Der euklidische Algorithmus.

Er berechnet den ggT zweier ganzer Zahlen.

Satz (Euklidischer Algorithmus). *Seien $a_0, a_1$ ganze Zahlen $\neq 0$. Man definiert rekursiv ganze Zahlen $a_i$ und $q_i$ durch die Vorschrift: Solange $a_{i+1} \neq 0$ gilt, teilt man $a_i$ durch $a_{i+1}$ und erhält den Quotienten $q_i$ und den Rest $a_{i+2}$. Explizit:*

$$\begin{aligned}
a_0 &= q_0 a_1 + a_2 \quad \textit{mit} \quad 0 < a_2 < |a_1|,\\
a_1 &= q_1 a_2 + a_3 \quad \textit{mit} \quad 0 < a_3 < a_2,\\
&\vdots \quad\quad \vdots\\
a_i &= q_i a_{i+1} + a_{i+2} \quad \textit{mit} \quad 0 < a_{i+2} < a_{i+1},\\
&\vdots \quad\quad \vdots\\
a_{n-2} &= q_{n-2} a_{n-1} + a_n \quad \textit{mit} \quad 0 < a_n < a_{n-1},\\
a_{n-1} &= q_{n-1} a_n + 0.
\end{aligned}$$

*Dann gilt* $\mathrm{ggT}(a_0, a_1) = a_n$.

**Beispiele:** Mit dem euklidischen Algorithmus erhalten wir in 79 Schritten

$$\mathrm{ggT}(17^{60} + 20882693916, 13^{40} + 14609017703) = 25937424629.$$

Die Schnelligkeit des euklidischen Algorithmus wird aus folgendem Satz ersichtlich:

SATZ. *Um den ggT zweier natürlicher Zahl $a > b$ zu berechnen, braucht man mit dem euklidischen Algorithmus*

$$\leq 4.785 \log_{10} a$$

*Divisionen mit Rest.*

**3.2. Der erweiterte euklidische Algorithmus.** Er berechnet zu Zahlen $a, b \in \mathbf{Z}$ ganze Zahlen $x, y \in \mathbf{Z}$ mit $\mathrm{ggT}(a, b) = xa + yb$:

SATZ (Erweiterter euklidischer Algorithmus). *Zu $a_0, a_1 \in \mathbf{Z}$, $(a_0, a_1) \neq (0, 0)$, führe man den euklidischen Algorithmus durch mit Quotienten $q_i$:*

$$\begin{aligned}
a_0 &= q_0 a_1 + a_2, \quad 0 < a_2 < |a_1| \\
a_1 &= q_1 a_2 + a_3, \quad 0 < a_3 < a_2 \\
a_2 &= q_2 a_3 + a_4, \quad 0 < a_4 < a_3 \\
\vdots &= \vdots \\
a_{n-2} &= q_{n-2} a_{n-1} + a_n, \quad 0 < a_n < a_{n-1} \\
a_{n-1} &= q_{n-1} a_n + 0.
\end{aligned}$$

*Setzt man $x_0 = 1$, $y_0 = 0$, $x_1 = 0$, $y_1 = 1$, definiert man für $i \geq 2$ rekursiv*

$$x_i = x_{i-2} - q_{i-2} x_{i-1}, \quad y_i = y_{i-2} - q_{i-2} y_{i-1},$$

*so gilt*

$$a_i = x_i a_0 + y_i a_1$$

*und insbesondere*

$$\mathrm{ggT}(a_0, a_1) = a_n = x_n a_0 + y_n a_1.$$

**3.3. Kongruenzen.** Addition und Multiplikation im Ring $\mathbf{Z}/N\mathbf{Z}$ entspricht der Addition und Multiplikation in $\mathbf{Z}$, wobei eventuell noch Division (mit Rest) durch $N$ erfolgt um einen eindeutigen Repräsentanten modulo $N$ zu erhalten.

SATZ. *Genau dann ist die Kongruenz $ax \equiv 1 \bmod N$ lösbar, wenn $\mathrm{ggT}(a, N) = 1$ gilt. Ist $\mathrm{ggT}(a, N) = 1$, so findet man mit dem erweiterten euklidischen Algorithmus $x, y \in \mathbf{Z}$ mit $ax + Ny = 1$, also ist $ax \equiv 1 \bmod N$.*

*Beweis:* Sei $d = \mathrm{ggT}(a, N)$. Gibt es eine Lösung der Kongruenz, d.h. hat man $ax \equiv 1 \bmod N$, so folgt $0 \equiv ax \equiv 1 \bmod d$ und damit $d = 1$. Sei umgekehrt $d = 1$. Mit dem erweiterten euklidischen Algorithmus findet man $x, y$ mit $ax + Ny = 1$ und damit $ax \equiv 1 \bmod N$. ■

**Bemerkungen:**

(1) Gilt $ab \equiv 1 \bmod N$, so schreibt man auch $b \equiv \frac{1}{a} \bmod N$.
(2) Will man mit Maple eine Lösung der Gleichung $ax \equiv 1 \bmod N$ finden, so berechnet man einfach '1/a mod N'.

**3.4. Die square-and-multiply-Methode zum schnellen Potenzieren.** Während man keine Methode kennt, um Fakultäten $d! = 1 \cdot 2 \cdot \cdots \cdot d$ oder $d! \bmod N$ für große $d$ und $N$ schnell zu berechnen, kann man mit nachfolgender Methode schnell potenzieren:

**Square-and-multiply-Methode:** Wir wollen für $a \in \mathbf{Z}$, $d, N \in \mathbf{N}$ die Potenz $a^d \bmod N$ berechnen.

- Ist
$$d = d_0 + d_1 \cdot 2 + \cdots + d_r \cdot 2^r \text{ mit } d_i \in \{0, 1\}$$
die Binärentwicklung von $d$, so gilt
$$a^d \equiv \prod_{j=0}^{r} (a^{2^j})^{d_j} \bmod N$$
und $r = \lfloor \log_2 d \rfloor$, falls $d_r \neq 0$ ist.
- Definiert man für $i = 0, 1, 2, \ldots, r$
$$c_i = \lfloor \frac{d}{2^i} \rfloor = d_i + d_{i+1} \cdot 2 + \cdots + d_r \cdot 2^{r-i}, \quad x_i \equiv a^{2^i} \bmod N, \quad y_i \equiv \prod_{j=0}^{i} (a^{2^j})^{d_j} \bmod N,$$
so sieht man sofort, dass $c_i$, $d_i$, $x_i$ und $y_i$ durch folgende Rekursionsformeln gegeben werden
$$c_0 = d, \quad d_0 \equiv c_0 \bmod 2, \quad x_0 = a, \quad y_0 = a^{d_0}$$
und
$$c_i = \lfloor \frac{c_{i-1}}{2} \rfloor, \quad d_i \equiv c_i \bmod 2, \quad x_i \equiv x_{i-1}^2 \bmod N, \quad y_i \equiv y_{i-1} x_i^{d_i} \bmod N.$$
Man hat dann
$$y_r \equiv a^d \bmod N.$$
- Man überlegt sich schnell, dass man mit den obigen Rekursionsformeln (wegen $d_i \in \{0, 1\}$)
$$\lfloor \log_2 d \rfloor \leq \log_2 d < 3.33 \log_{10} d$$
Quadratbildungen und höchstens soviele Multiplikationen modulo $N$ braucht. Die ist ein schnelles Verfahren.
- Wir geben noch folgenden einfachen expliziten Algorithmus an:
**Algorithmus:** Für $N, d \in \mathbf{N}$ und $a \in \mathbf{Z}$ soll $a^d \bmod N$ berechnet werden.
(1) Setze $c := d$, $x := a$. Setze $y := 1$, falls $c \equiv 0 \bmod 2$, sonst $y := a$.
(2) Ist $c \leq 1$, gib $y$ als Ergebnis aus und beende das Verfahren.
(3) Setze $c := \lfloor \frac{c}{2} \rfloor$, $x := x^2 \bmod N$.
(4) Ist $c \equiv 1 \bmod 2$, setze $y := xy \bmod N$.
(5) Gehe zurück zu Schritt 2.
Man kann den Algorithmus auch leicht modifizieren um in einer multiplikativ bzw. additiv geschriebenen Gruppe $G$ und $a \in G$, $d \in \mathbf{N}$ die Potenz $a^d$ bzw. das Produkt $d \cdot a$ zu berechnen.

**Beispiel:** Berechnung von $2^{19487190} \bmod 19487191$:

| $i$ | $c_i$ | $d_i$ | $x_i$ | $y_i$ |
|---|---|---|---|---|
| 0 | 19487190 | 0 | 2 | 1 |
| 1 | 9743595 | 1 | 4 | 4 |
| 2 | 4871797 | 1 | 16 | 64 |
| 3 | 2435898 | 0 | 256 | 64 |
| 4 | 1217949 | 1 | 65536 | 4194304 |
| 5 | 608974 | 0 | 7785276 | 4194304 |
| 6 | 304487 | 1 | 18895842 | 12707193 |
| 7 | 152243 | 1 | 15484497 | 5384192 |
| 8 | 76121 | 1 | 9279458 | 12472249 |
| 9 | 38060 | 0 | 17081390 | 12472249 |
| 10 | 19030 | 0 | 7339882 | 12472249 |
| 11 | 9515 | 1 | 8253526 | 16737979 |
| 12 | 4757 | 1 | 19392852 | 2885849 |
| 13 | 2378 | 0 | 13687825 | 2885849 |
| 14 | 1189 | 1 | 14850112 | 2726202 |
| 15 | 594 | 0 | 3820594 | 2726202 |
| 16 | 297 | 1 | 19119904 | 11781179 |
| 17 | 148 | 0 | 9404267 | 11781179 |
| 18 | 74 | 0 | 18378282 | 11781179 |
| 19 | 37 | 1 | 17930990 | 17521259 |
| 20 | 18 | 0 | 10378067 | 17521259 |
| 21 | 9 | 1 | 12051623 | 11407692 |
| 22 | 4 | 0 | 16255176 | 11407692 |
| 23 | 2 | 0 | 7096585 | 11407692 |
| 24 | 1 | 1 | 10960476 | 1 |

Ergebnis: $2^{19487190} \equiv 1 \bmod 19487191$.

**3.5. Erzeugung großer wahrscheinlicher Primzahlen.** Der folgende Satz spielt in der Zahlentheorie eine wichtige Rolle:

SATZ (Kleiner Satz von Fermat). *Ist $p$ und Primzahl und $a$ eine ganze Zahl mit* $\mathrm{ggT}(a,p)=1$*, so gilt*

$$a^{p-1} \equiv 1 \bmod p.$$

FOLGERUNG. *Ist $N \geq 2$ eine ungerade natürliche Zahl und gilt*

$$2^{N-1} \not\equiv 1 \bmod N,$$

*so ist $N$ zusammengesetzt.*

Leider gilt die Umkehrung nicht. So sind die Zahlen

$$341 = 11 \cdot 31, \quad 561 = 3 \cdot 11 \cdot 17, \quad 645 = 3 \cdot 5 \cdot 43$$

zusammengesetzte Zahlen $N$ mit $2^{N-1} \equiv 1 \bmod N$. (Dies sind auch die einzigen $< 1000$.) Aber es gibt erfahrungsgemäß nur recht wenige solcher Zahlen.
Man sagt, eine ungerade zusammengesetzte natürliche Zahl $N$ ist eine Fermatsche Pseudoprimzahl zur Basis 2, wenn gilt

$$2^{N-1} \equiv 1 \bmod N.$$

(Es gibt 168 Primzahlen $< 1000$, aber nur 3 Fermatsche Pseudoprimzahlen zur Basis 2.) Erfüllt also eine Zahl $N$ die Gleichung $2^{N-1} \equiv 1 \bmod N$, so ist es recht wahrscheinlich, dass $N$ eine Primzahl ist.

Auf diese Weise kann man sich schnell große Zahlen $N$ verschaffen, die wahrscheinlich Primzahlen sind.

**Beispiel:** Die 10 größten 1000-stelligen Zahlen $N$ mit $2^{N-1} \equiv 1 \bmod N$ sind

$$10^{1000}-1769, \quad 10^{1000}-6567, \quad 10^{1000}-9861, \quad 10^{1000}-11237, \quad 10^{1000}-18873,$$
$$10^{1000}-21969, \quad 10^{1000}-22071, \quad 10^{1000}-26981, \quad 10^{1000}-29861, \quad 10^{1000}-31821.$$

Sie sind sehr wahrscheinlich prim.

Neben dem Fermattest (zur Basis 2) $2^{N-1} \equiv 1 \bmod N$ gibt es eine Reihe weiterer sogenannter Primzahltests, die als Ergebnis ausgeben:

'$N$ ist zusammengesetzt' oder '$N$ ist wahrscheinlich prim'.

In der Praxis ist man meist mit wahrscheinlichen Primzahlen zufrieden.

## 4. Rechnerisch schwierige zahlentheoretische Probleme

**4.1. Die Primfaktorzerlegung natürlicher Zahlen.** (The integer factorization problem) Der Fundamentalsatz der Arithmetik besagt, dass jede natürliche Zahl $N$ eine eindeutige Primfaktorzerlegung

$$N = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

besitzt.

**Beispiel:** Die folgenden Primfaktorzerlegungen wurden mit Maple erstellt.

$$\begin{aligned}
10^{29}+1 &= 11 \cdot 59 \cdot 154083204930662557781201849,\\
10^{29}+2 &= 2 \cdot 3 \cdot 7 \cdot 17041 \cdot 445847 \cdot 313378923550840603,\\
10^{29}+3 &= 31 \cdot 10928153 \cdot 295183134022089846821,\\
10^{29}+4 &= 2^2 \cdot 41 \cdot 16183 \cdot 53731 \cdot 701248902272927557,\\
10^{29}+5 &= 3 \cdot 5 \cdot 19 \cdot 347 \cdot 577 \cdot 1752467013532462655147,\\
10^{29}+6 &= 2 \cdot 17 \cdot 353 \cdot 833194467588735210798 2003,\\
10^{29}+7 &= 53 \cdot 827 \cdot 228149026944400082133 6497,\\
10^{29}+8 &= 2^3 \cdot 3^3 \cdot 103 \cdot 1361 \cdot 2647 \cdot 53047 \cdot 23519935674229,\\
10^{29}+9 &= 7 \cdot 13 \cdot 23 \cdot 6526241 \cdot 12047047 \cdot 607696954219,\\
10^{29}+10 &= 2 \cdot 5 \cdot 73 \cdot 137 \cdot 7841 \cdot 127522001020150503761.
\end{aligned}$$

Es gibt zwar einige Faktorisierungsmethoden, z.B. Morrison-Brillhart, Pollardsche $\rho$-Methode, Quadratisches Sieb, Zahlkörpersieb, aber keine Methode ist wirklich schnell.

Die Schwierigkeit der Faktorzerlegung kann man auch daran erkennen, dass die Firma RSA Data Security, Inc. für die Faktorisierung sogenannter RSA Challenge Numbers Geldpreise ausgesetzt sind. Die kleinste derartige Zahl ist zur Zeit RSA-576 (mit 576 Bits bzw. 174 Dezimalstellen):

$$\begin{aligned}\text{RSA-576} \;=\; & 188198812920607963838697239461650439807163563379417382700763356422988\backslash\\ & 8597152346654853190606065047430453173880113033967161996923212057340318\backslash 7\\ & 9550656996221305168759307650257059.\end{aligned}$$

Wer als erster eine Faktorisierung einreicht, erhält \$10000.
Die größte RSA Challenge Number ist zur Zeit RSA-2048 (2048 Bits und 617 Dezimalstellen):

$$\begin{aligned}\text{RSA-2048} \;=\; & 25195908475657893494027183240048398571429282126204032027777137836043\backslash 66\\ & 2020707595556264018525880784406918290641249515082189298559149176184502\backslash\\ & 8084891200728449926873928072877767359714183472702618963750149718246911\backslash\\ & 6507761337985909570009733045974880842840179742910064245869181719511874\backslash\\ & 6121515172654632282216869987549182422433637259085141865462043576798423\backslash\\ & 3871847744479207399342365848238242811981638150106748104516603773060562\backslash\\ & 0161967625613384414360383390441495263443219011465754445417842402092461\backslash\\ & 6515723350778707749817125772467962926386356373289912154831438167899885\backslash\\ & 0404453640235273819513786365643912120103971228221207203 57\end{aligned}$$

Durch Faktorisierung dieser Zahl kann \$200000 verdienen.

**4.2. Berechnung diskreter Logarithmen.** (The discrete logarithm problem) Ist $p$ eine Primzahl, $g$ eine natürliche Zahl mit $2 \le g \le p-2$, so kann man $g^n \bmod p$ mit der square-and-multiply-Methode schnell berechnen. Ist $a$ eine weitere natürliche Zahl und gilt

$$g^x \equiv a \bmod p$$

für eine natürliche Zahl $x$, so heißt $x$ diskreter Logarithmus von $a$ zur Basis $g$ (in $\mathbf{Z}/p\mathbf{Z} \simeq \mathbf{F}_p$). Die Berechnung diskreter Logarithmen ist praktisch ein schwieriges Problem. Es ist bis jetzt kein allgemein funktionierender schneller Algorithmus bekannt. In Maple gibt es die Funktion 'numtheory[mlog]($a$,$g$,$p$)'.

**Beispiel:** Es gilt für $p = 10^{10} + 19$

$$2^{5181957398} \equiv 3 \bmod p,$$

also ist 5181957398 der diskrete Logarithmus von 3 zur Basis 2 in $\mathbf{Z}/p\mathbf{Z} \simeq \mathbf{F}_p$. Die Gleichung $3^x \equiv 2 \bmod p$ hat dagegen keine Lösung.

Das folgende Beispiel soll die Schwierigkeit der Logarithmenberechnung illustrieren.

**Beispiel:** Am 17. April 2001 gaben Antoine Joux und Reynald Lercier bekannt, dass sie in 10 Wochen folgende diskrete Logarithmen mit einer 120-stelligen Primzahl berechnet haben:

$$\begin{aligned} p \;&=\; \lfloor 10^{119}\pi \rfloor + 207819 =\\ &=\; 3141592653589793238462643383279502884197169399375105820974944\backslash\backslash\\ &\quad 5923078164062862089986280348253421170679821480865132843848 3,\\ g \;&=\; 2,\\ y \;&=\; \lfloor 10^{119}e \rfloor =\\ &=\; 2718281828459045235360287471352662497757247093699959574966968\backslash\backslash\\ &\quad 7627724076630353547594571382178525166427427466391932003059 92.\end{aligned}$$

Dann gilt

$$y \equiv g^{z_0} \bmod p \quad \text{und} \quad y+1 \equiv g^{z_1} \bmod p$$

mit

$$\begin{aligned} z_0 &= 26211228068581138763600862203819182737039076852065697424303\backslash\backslash \\ &\quad 38038219347876743601868144980494084037374164145286473076508 2, \\ z_1 &= 39657965519539238631090956325038481900751981791165229696297\backslash\backslash \\ &\quad 42152064583290471091218956225132952799490844975060704685793 7. \end{aligned}$$

## 5. Schlüsselaustausch nach Diffie-Hellmann

Diffie und Hellman haben 1976 das folgende Verfahren vorgeschlagen, es war das erste Public-Key-Verfahren:

**Schlüsselaustausch nach Diffie-Hellman.** Wir nehmen an, $A$ und $B$ wollen einen Schlüssel austauschen, z.B. um damit ein klassisches Kryptosystem zu benutzen. Dazu eignet sich jede hinreichend große Zahl. $A$ und $B$ einigen sich öffentlich auf einen Körper $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, d.h. auf eine (große) Primzahl und auf ein Element $g \in \mathbf{F}_p^*$, d.h. auf eine natürliche Zahl $g$ mit $2 \leq g \leq p-1$.

- $A$ wählt sich eine Zufallszahl $a$ zwischen 1 und $p-1$ und veröffentlicht $g^a \in \mathbf{F}_p$.
- $B$ wählt sich eine Zufallszahl $b$ zwischen 1 und $p-1$ und veröffentlicht $g^b \in \mathbf{F}_p$.
- Der gemeinsame Schlüssel soll nun $g^{ab}$ sein, den sich $A$ durch $(g^b)^a$ und $B$ durch $(g^a)^b$ berechnen kann.

Ein Außenstehender $C$ kennt dann die Zahlen $g$, $g^a$ und $g^b$. Kann $C$ daraus den Schlüssel $g^{ab}$ berechnen?

(1) Kann $C$ den diskreten Logarithmus von $g^a$ bzgl. $g$ berechnen, so kann er natürlich sofort den Schlüssel $g^{ab}$ berechnen. Das ist/sollte aber sehr schwer sein.
(2) Es ist nicht bekannt, ob man aus der Kenntnis von $g$, $g^a$ und $g^b$ den Wert $g^{ab}$ berechnen kann ohne Berechnung von diskreten Logarithmen. (Diffie-Hellman-Problem)

**Beispiel:** Um die Zahlen nicht zu groß zu machen, wählen wir (zufällig)

$$p = 97325968347859674398576349088 1 \quad \text{und} \quad g = 2.$$

Die 6 Personen Anita, Bert, Carola, Dietmar, Eva und Frieder wählen jeweils zufällig eine Zahl $e$ und berechnen damit $g^e \bmod p$ als ihren öffentlichen Schlüssel:

| | $e$ | $g^e \bmod p$ |
|---|---|---|
| Anita | 32709874385967438957638497563 4 | 81591592082290961258985427759 8 |
| Bert | 49857689327652873645094376893 6 | 73981134643962446308354915804 6 |
| Carola | 46589326590436478216925763760 3 | 48506923592120131564372748341 3 |
| Dietmar | 97634908756098347659837405968 7 | 91439306029763249772961207846 4 |
| Eva | 73648756238456650978609782823 2 | 78035220693009499732799602676 8 |
| Frieder | 27345632874965847544833789737 6 | 98873961440510704674604019073 |

Der gemeinsame Schlüssel von Anita und Bert ist dann

$$60033888387677128832055139624 0 \equiv (g^{e_{\text{Anita}}})^{e_{\text{Bert}}} \equiv (g^{e_{\text{Bert}}})^{e_{\text{Anita}}} \bmod p,$$

## 6. RSA-Verschlüsselung

Das wohl bekannteste Public-Key-Verschlüsselungsverfahren geht auf Rivest, Shamir und Adleman (1977) zurück - daher die Bezeichnung RSA. Wir beginnen mit der Mathematik.

LEMMA. *Seien $p$ und $q$ verschiedene ungerade Primzahlen, $N = pq$ und $e$ eine natürliche Zahl mit* $\mathrm{ggT}(e,(p-1)(q-1)) = 1$. *Dann ist*

$$f : \mathbf{Z}/N\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}, \quad x \mapsto x^e$$

*bijektiv. Wählt man eine natürliche Zahl $d$ mit $de \equiv 1 \bmod (p-1)(q-1)$, die man mit dem erweiterten euklidischen Algorithmus finden kann, so ist die Umkehrabbildung gegeben durch $f^{-1}(x) = x^d$.*

*Beweis:* Wegen $\mathrm{ggT}(e,(p-1)(q-1))=1$ gibt es ein $d$ mit $de\equiv 1 \bmod (p-1)(q-1)$. Wir schreiben $de=1+\ell(p-1)(q-1)$. Sei $x\in\mathbf{Z}$ beliebig. Wir müssen zeigen, dass $x^{de}\equiv x \bmod pq$ gilt. Wir zeigen zunächst, dass $x^{de}\equiv x \bmod p$ gilt. Ist $x\equiv 0 \bmod p$, so gilt natürlich $x^{de}\equiv x \bmod p$. Ist $x\not\equiv 0 \bmod p$, so gilt mit dem kleinen Satz von Fermat $x^{p-1}\equiv 1 \bmod p$, also folgt

$$x^{de}=x^{1+\ell(p-1)(q-1)}=x\cdot(x^{p-1})^{\ell(q-1)}\equiv x \bmod p.$$

Damit haben wir $p|x^{de}-x$. Analog folgt $q|x^{de}-x$, was sofort $pq|x^{de}-x$ und damit $x^{de}\equiv x \bmod pq$ impliziert. ■

**Überlegung:** Wir wollen sehen, ob die im Lemma auftretenden Abbildungen $f:\mathbf{Z}/N\mathbf{Z}\to\mathbf{Z}/N\mathbf{Z}, x\mapsto x^e$ (mit $N=pq$) die oben geforderten Eigenschaften für eine Public-Key-Verschlüsselung erfüllen.

(1) Mit der square-and-multiply-Methode kann man bei gegebenem $N$ und $e$ zu $x$ schnell den Wert $x^e \bmod N$ berechnen. (Eigenschaft 1)

(2) Sind $N$ und $e$ bekannt und weiß man, dass

$$f:\mathbf{Z}/N\mathbf{Z}\xrightarrow{x\mapsto x^e}\mathbf{Z}/N\mathbf{Z}$$

bijektiv ist und $N$ aus zwei verschiedenen Primteilern besteht, so kennt man heute nur einen Weg um die Umkehrabbildung $f^{-1}$ zu bestimmen, nämlich über die Faktorisierung von $N$ und das Berechnen eines $e$ mit $de\equiv 1 \bmod (p-1)(q-1)$, wie im Lemma. Also: Kann man $N$ nicht faktorisieren, so kann man auch die Umkehrabbildung nicht bestimmen. Nun ist es aber im allgemeinen sehr schwierig bzw. praktisch unmöglich, die Faktorzerlegung einer geeignet gewählten großen Zahl der Form $N=pq$ zu finden. (Damit ist Eigenschaft 2 erfüllt.)

(3) Es ist leicht, sich (zufällige) große (wahrscheinliche) Primzahlen $p$ und $q$ zu verschaffen, sodass $N=pq$ mit keinem der gängigen Faktorisierungsverfahren praktisch zu faktorisieren ist. Wählt man dann $e$ teilerfremd zu $(p-1)(q-1)$, so kann man dazu mit dem erweiterten euklidischen Algorithmus schnell ein $d$ mit $de\equiv 1 \bmod (p-1)(q-1)$ berechnen. Dies zeigt Eigenschaft 3.

Wir wollen jetzt damit ein Public-Key-Kryptosystem konstruieren.

**Kryptosystem RSA:**

(1) **Schlüsselerzeugung:** Jeder Teilnehmer $A$ wählt sich zwei verschiedene große (wahrscheinliche) Primzahlen $p$ und $q$ und setzt $N_A=pq$. (Die Wahl von $p$ und $q$ sollte so sein, dass sich $N_A$ mit den gängigen Faktorisierungsmethoden praktisch nicht faktorisieren lässt.) Dann wählt $A$ eine Zahl $e_A$ mit $\mathrm{ggT}(e_A,(p-1)(q-1))=1$ und berechnet sich mit dem erweiterten euklidischen Algorithmus ein $d_A$ mit $d_Ae_A\equiv 1 \bmod (p-1)(q-1)$. Der Teilnehmer $A$ gibt $(N_A,e_A)$ als seinen öffentlichen Schlüssel bekannt und hebt sich $(N_A,d_A)$ als seinen privaten/geheimen Schlüssel auf.

(2) **Verschlüsselung:**

(a) Man legt ein Alphabet mit $n$ Zeichen zugrunde, z.B. $\{A,B,C,\ldots,Z\}$ mit $n=26$, wobei jedes Zeichen mit einem Wert zwischen 0 und $n-1$ identifiziert wird.

(b) $B$ will eine Nachricht $T$ verschlüsselt an $A$ senden und besorgt sich zunächst den öffentlichen Schlüssel $(N_A,e_A)$ von $A$. Die Plaintext-Blocklänge $k$ wird so gewählt, dass gilt

$$n^k<N_A<n^{k+1}.$$

Ein Plaintextblock aus den $k$ Zeichen $a_0a_1a_2\ldots a_{k-1}$ (mit $a_i\in\{0,1,\ldots,n-1\}$) liefert durch

$$a_0a_1\ldots a_{k-1}\leftrightarrow a_0+a_1\cdot n+a_2\cdot n^2+\cdots+a_{k-1}\cdot n^{k-1}=a$$

eine Zahl $a$ mit $0\le a\le n^k-1<N_A$. Nun berechnet $B$

$$b\equiv a^{e_A} \bmod N_A.$$

Wegen $0\le b<N_A<n^{k+1}$ gibt es eine eindeutige Darstellung

$$b=b_0+b_1n+b_2n^2+\cdots+b_{k-1}n^{k-1}+b_kn^k \quad \text{mit} \quad b_i\in\{0,1,\ldots,n-1\}.$$

$b_0b_1\dots b_{k-1}b_k$ wird jetzt der zugehörige Ciphertextblock (mit Blocklänge $k+1$) und an $A$ geschickt.

(c) $A$ empfängt den Ciphertextblock $b_0b_1\dots b_{k-1}b_k$ und berechnet damit

$$b = b_0 + b_1 n + b_2 n^2 + \cdots + b_{k-1}n^{k-1} + b_k n^k,$$

dann mit seinem privaten Schlüssel $(N_A, d_A)$

$$c \equiv b^{d_A} \bmod N_A.$$

Wegen $0 \le c < N_A < n^{k+1}$ kann man entwickeln

$$c = c_0 + c_1 n + \cdots + c_{k-1}n^{k-1} + c_k n^k \quad \text{mit} \quad c_i \in \{0, 1, \dots, n-1\}.$$

Ist alles richtig gelaufen, so gilt $c \equiv b^{d_A} \equiv a^{e_A d_A} \equiv a \bmod N_A$, d.h. $c = a$. Dann ist $c_k = 0$ und $c_0c_1\dots c_{k-1} = a_0a_1\dots a_{k-1}$ der gewünschte Plaintextblock.

**Beispiel:** Wir legen als Alphabet A,...,Z mit $n = 26$ zugrunde und wollen den Text 'ZAHLENTHEORIE' mit dem öffentlichen RSA-Schlüssel $(N, e) = (438751, 7)$ verschlüsseln. Wegen

$$26^3 = 17576 < 438751 < 456976 = 26^4$$

wird die Plaintextblocklänge $k = 3$. Wir beginnen mit dem ersten Plaintextblock ZAH:

$$\begin{aligned} \text{ZAH} \quad \leftrightarrow \quad & (25,0,7)_{26} \mapsto 25 + 0\cdot 26 + 7\cdot 26^2 = 4757 \xrightarrow{a\mapsto a^7 \bmod 438751} 208791 = \\ & = 208791 = 11 + 22\cdot 26 + 22\cdot 26^2 + 11\cdot 26^3 \mapsto (11,22,22,11)_{26} \leftrightarrow \text{LWWL}. \end{aligned}$$

Der erste Ciphertextblock ist also LWWL. Analog ergibt sich der Rest:

| | | |
|---|---|---|
| ZAH | $25 + 0\cdot 26 + 7\cdot 26^2 = 4757 \mapsto 208791 = 11 + 22\cdot 26 + 22\cdot 26^2 + 11\cdot 26^3$ | LWWL |
| LEN | $11 + 4\cdot 26 + 13\cdot 26^2 = 8903 \mapsto 63882 = 0 + 13\cdot 26 + 16\cdot 26^2 + 3\cdot 26^3$ | ANQD |
| THE | $19 + 7\cdot 26 + 4\cdot 26^2 = 2905 \mapsto 65932 = 22 + 13\cdot 26 + 19\cdot 26^2 + 3\cdot 26^3$ | WNTD |
| ORI | $14 + 17\cdot 26 + 8\cdot 26^2 = 5864 \mapsto 365771 = 3 + 2\cdot 26 + 21\cdot 26^2 + 20\cdot 26^3$ | DCVU |
| E | $4 + 0\cdot 26 + 0\cdot 26^2 = 4 \mapsto 16384 = 4 + 6\cdot 26 + 24\cdot 26^2 + 0\cdot 26^3$ | EGYA |

Die verschlüsselte Text ist also LWWLANQDWNTDDCVUEGYA.

Angenommen, wir erhalten die Nachricht MPABPEDNVFNFGYAOEGYA und wissen, dass sie mit dem obigen Schlüssel $(N, e) = (438751, 7)$ verschlüsselt wurde. Wir wollen den zugehörigen Plaintext finden. Zunächst faktorisieren wir $N$ und erhalten $N = 541\cdot 811$, also o.E. $p = 541$, $q = 811$. Mit dem erweiterten euklidischen Algorithmus berechnen wir $d = 249943$ mit der Eigenschaft $de \equiv 1 \bmod (p-1)(q-1)$. Nun gehen wir analog zu oben vor, wobei die Abbildung $b \mapsto b^{249943} \bmod 438751$ verwendet wird:

$$\begin{aligned} &\text{MPAB} \leftrightarrow 12 + 15\cdot 26 + 0\cdot 26^2 + 1\cdot 26^3 = 17978 \mapsto 16676 = 10 + 17\cdot 26 + 24\cdot 26^2 \leftrightarrow \text{KRY} \\ &\text{PEDN} \leftrightarrow 15 + 4\cdot 26 + 3\cdot 26^2 + 13\cdot 26^3 = 230635 \mapsto 9973 = 15 + 19\cdot 26 + 14\cdot 26^2 \leftrightarrow \text{PTO} \\ &\text{VFNF} \leftrightarrow 21 + 5\cdot 26 + 13\cdot 26^2 + 5\cdot 26^3 = 96819 \mapsto 448 = 6 + 17\cdot 26 + 0\cdot 26^2 \leftrightarrow \text{GRA} \\ &\text{GYAO} \leftrightarrow 6 + 24\cdot 26 + 0\cdot 26^2 + 14\cdot 26^3 = 246694 \mapsto 5605 = 15 + 7\cdot 26 + 8\cdot 26^2 \leftrightarrow \text{PHI} \\ &\text{EGYA} \leftrightarrow 4 + 6\cdot 26 + 24\cdot 26^2 + 0\cdot 26^3 = 16384 \mapsto 4 = 4 + 0\cdot 26 + 0\cdot 26^2 \leftrightarrow \text{EAA} \end{aligned}$$

Der Ausgangstext war also KRYPTOGRAPHIEAA. Natürlich wird das Ende AA wohl wegfallen sollen. (Man muss sich also überlegen, was man macht, wenn die Anzahl der Zeichen im Plaintext nicht $\equiv 0 \bmod k$ ist.)

**Bemerkung:** Die Sicherheit von RSA beruht darauf, dass man eine große Zahl $N = pq$ (bei geeigneter Wahl von $p$ und $q$) praktisch nicht faktorisieren kann. Es ist klar, dass das Fortschreiten der Computertechnologie und die Entwicklung neuer Faktorisierungsalgorithmen die Verwendung immer größerer Schlüssel $N$ notwendig macht.

KAPITEL 2

# Affine und projektive ebene Kurven

Wir legen im folgenden einen Körper $K$ zugrunde, dessen algebraischer Abschluss mit $\overline{K}$ bezeichnet wird. Insbesondere werden bei uns folgende Körper eine Rolle spielen:

- Der Körper $\mathbf{Q}$ der rationalen Zahlen.
- Die Körper $\mathbf{R}$ und $\mathbf{C}$ der reellen bzw. komplexen Zahlen.
- Endliche Körper $\mathbf{F}_p \simeq \mathbf{Z}/p\mathbf{Z}$ von Primzahlordnung $p$.
- Endliche Körper $\mathbf{F}_q$ mit Primzahlpotenzordnung $q = p^n$. Von besonderem praktischen Interesse ist hier der Fall $q = 2^n$.

## 1. Affine Räume

DEFINITION. Der $n$-dimensionale affine Raum über $K$ wird definiert durch

$$\mathbf{A}^n = \mathbf{A}^n(\overline{K}) = \{(x_1, \ldots, x_n) : x_i \in \overline{K}\}.$$

Die Elemente von $\mathbf{A}^n$ werden Punkte genannt.

$$\mathbf{A}^n(K) = \{((x_1, \ldots, x_n) \in \mathbf{A}^n : x_i \in K\}$$

heißt die Menge der $K$-rationalen Punkte von $\mathbf{A}^n$. Der 1-dimensionale affine Raum $\mathbf{A}^1$ wird auch als affine Gerade, $\mathbf{A}^2$ als affine Ebene bezeichnet.

**Beispiel:** Sei $K = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ der endliche Körper mit $p$ Elementen, dessen Elemente wir uns durch die Zahlen $0, 1, 2, \ldots, p-1$ repräsentiert denken können. Dann ist

$$\mathbf{A}^n(\mathbf{F}_p) = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in \mathbf{F}_p\}, \quad \text{also} \quad \#\mathbf{A}^n(\mathbf{F}_p) = p^n.$$

In der Linearen Algebra und Analytischen Geometrie werden affine Teilräume affiner Räume untersucht. Für uns ist hauptsächlich der 2-dimensionale Fall interessant, den wir kurz wiederholen:

**Geraden in $\mathbf{A}^2$:**

(1) Eine Gerade in $\mathbf{A}^2$ ist eine Teilmenge der Gestalt

$$G = \{(x, y) \in \mathbf{A}^2 : a + bx + cy = 0\}$$

mit $a, b, c \in \overline{K}$ und $(b, c) \neq 0$.

(2) Zwei Geraden

$$G_1 = \{(x, y) \in \mathbf{A}^2 : a_1 + b_1 x + c_1 y = 0\} \quad \text{und} \quad G_2 = \{(x, y) \in \mathbf{A}^2 : a_2 + b_2 x + c_2 y = 0\}$$

können in folgenden Beziehungen stehen:

(a) Sind $(b_1, c_1)$ und $(b_2, c_2)$ linear unabhängig, so gilt

$$G_1 \cap G_2 = \{(x_0, y_0)\}, \text{ wobei } (x_0, y_0) \text{ durch } \begin{pmatrix} b_1 & c_1 \\ b_2 & c_2 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} -a_1 \\ -a_2 \end{pmatrix}$$

eindeutig bestimmt ist. ($G_1$ und $G_2$ schneiden sich in einem Punkt.)

(b) Sind $(b_1, c_1)$ und $(b_2, c_2)$ linear abhängig, aber $(a_1, b_1, c_2)$ und $(a_2, b_2, c_2)$ linear unabhängig, so gilt

$$G_1 \cap G_2 = \emptyset.$$

($G_1$ und $G_2$ sind parallel.)

Version vom 28.4.2003 - 25.12.2006

(c) Sind $(a_1, b_1, c_1)$ und $(a_2, b_2, c_2)$ linear abhängig, so gilt

$$G_1 = G_2.$$

(3) Eine Gerade $G = \{(x, y) \in \mathbf{A}^2 : a + bx + cy = 0\}$ lässt sich in parametrisierter Form darstellen, d.h. man findet $\alpha, \beta, \gamma, \delta \in \overline{K}$ mit $(\beta, \gamma) \neq 0$, sodass gilt:

$$G = \{(\alpha + \beta t, \gamma + \delta t) \in \mathbf{A}^2 : t \in \overline{K}\}.$$

Explizit kann man sofort folgende Parametrisierungen angeben:

$$G = \begin{cases} \{(x, -\frac{a}{c} - \frac{b}{c}x) : x \in \overline{K}\} & \text{für } c \neq 0, \\ \{(-\frac{a}{b} - \frac{c}{b}y, y) : y \in \overline{K}\} & \text{für } b \neq 0. \end{cases}$$

(4) Zu zwei verschiedenen Punkten $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in \mathbf{A}^2$ gibt es genau eine Gerade $G = \{(x, y) \in \mathbf{A}^2 : a + bx + cy = 0\}$, die beide Punkte enthält. $(a, b, c)$ wird bis auf eine Konstante bestimmt durch die Gleichung

$$\begin{pmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0.$$

**Affiner Koordinatenwechsel:** Ein affiner Koordinatenwechsel wird gegeben durch eine Abbildung

$$\phi : \mathbf{A}^n \to \mathbf{A}^n, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

mit $A = (a_{ij}) \in \mathrm{GL}_n(\overline{K})$ und $b_i \in \overline{K}$. Ist $A \in \mathrm{GL}_n(K)$ und $b_i \in K$, so sagt man, der Koordinatenwechsel ist über $K$ definiert.

Leicht beweist man nun folgendes Lemma:

LEMMA. *Sind $P_1, P_2, P_3$ drei Punkte in $\mathbf{A}^2$, die nicht auf einer Geraden liegen, so gibt es einen Koordinatenwechsel $\phi : \mathbf{A}^2 \to \mathbf{A}^2$ mit*

$$\phi(P_1) = (0, 0), \quad \phi(P_2) = (1, 0), \quad \phi(P_3) = (0, 1).$$

## 2. Ebene affine Kurven

DEFINITION. Eine ebene affine Kurve $C$ über $K$ wird durch ein Polynom $f(x, y) \in K[x, y] \setminus K$ gegeben. (Man sagt auch, dass $C$ durch die Gleichung $f(x, y) = 0$ definiert wird.) Das zugehörige geometrische Objekt ist die Nullstellenmenge

$$C(\overline{K}) = \{(x, y) \in \mathbf{A}^2 : f(x, y) = 0\}.$$

Die Menge

$$C(K) = \{(x, y) \in \mathbf{A}^2(K) : f(x, y) = 0\}$$

heißt die Menge der $K$-rationalen Punkte von $C$. Etwas allgemeiner betrachtet man für einen Oberkörper $L$ von $K$ die Menge der $L$-rationalen Punkte von $C$:

$$C(L) = \{(x, y) \in \mathbf{A}^2(L) : f(x, y) = 0\}.$$

Ist $c \in K^*$, so unterscheiden wir nicht zwischen der durch $f(x, y) = 0$ und der durch $cf(x, y) = 0$ definierten Kurve.

**Beispiele:**

(1) Sind $a, b, c \in K$ mit $(b, c) \neq (0, 0)$ so definiert $a + bx + cy$ eine Kurve $G$ mit

$$G(\overline{K}) = \{(x, y) \in \mathbf{A}^2 : a + bx + cy = 0\},$$

d.h. $G(\overline{K})$ ist eine affine Gerade. Da $G(\overline{K})$ den Vektor $(a, b, c)$ und damit die Gleichung $a+bx+cy$ bis auf eine Konstante bestimmt, nennen wir auch $G$ einfach affine Gerade.

(2) $y = x^2$ definiert eine Parabel, $y^2 = x^3$ die sogenannte Neilsche Parabel.

(3) $f = x^2 - y^2 = (x-y)(x+y)$ definiert eine ebene Kurve $C$ über $\mathbf{R}$ mit
$$C(\mathbf{R}) = \{(x,y) \in \mathbf{R}^2 : (x-y)(x+y) = 0\} = \{(x,y) \in \mathbf{R}^2 : y = x\} \cup \{(x,y) \in \mathbf{R}^2 : y = -x\}.$$
$C$ besteht also aus den beiden Geraden $y = x$ und $y = -x$.

(4) Auch $f = x^2 + y^2$ definiert eine ebene Kurve über $\mathbf{R}$. Allerdings ist
$$C(\mathbf{R}) = \{(0,0)\}$$
nur ein Punkt. Über dem algebraischen Abschluss ist
$$C(\mathbf{C}) = \{(x,y) \in \mathbf{C}^2 : y = ix \text{ oder } y = -ix\},$$
d.h. $C(\mathbf{C})$ besteht aus den beiden Geraden $y = ix$ und $y = -ix$.

(5) Wir betrachten die durch $f = 1 + 2x^3 + 3y^3$ über $\mathbf{F}_5$ definierte Kurve $C$. Durch Ausprobieren aller 25 Punkte von $\mathbf{A}^2(\mathbf{F}_5)$ findet man
$$C(\mathbf{F}_5) = \{(0,2),(1,4),(2,1),(3,0),(4,3)\},$$
insbesondere ist $\#C(\mathbf{F}_5) = 5$.

DEFINITION. Sei $C$ eine durch $f(x,y) \in K[x,y]$ über $K$ definierte Kurve.

(1) Ist $f(x,y)$ in $K[x,y]$ irreduzibel, so nennt man $C$ irreduzibel über $K$.
(2) Ist $f(x,y)$ im Polynomring $\overline{K}[x,y]$ irreduzibel, so nennt man $C$ absolut irreduzibel.

**Beispiele:**

(1) Geraden sind absolut irreduzible Kurven.
(2) $y^2 = x^3$ definiert eine absolut irreduzible Kurve.
(3) $f = x^2+y^2 \in \mathbf{R}[x,y]$ definiert eine über $\mathbf{R}$ irreduzible Kurve, die aber wegen $f = (y-ix)(y+ix)$ nicht absolut irreduzibel ist.

Ein Grundproblem der Zahlentheorie ist folgendes: Bestimme für eine über $\mathbf{Q}$ definierte Kurve $C$ die Menge der $\mathbf{Q}$-rationalen Punkte $C(\mathbf{Q})$ von $C$.

**Beispiel:** Sei $p$ eine Primzahl und $C$ die durch die Gleichung $x^p + y^p = 1$ definierte Kurve über $\mathbf{Q}$. Dann ist
$$C(\mathbf{Q}) = \begin{cases} \{(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}) : t \in \mathbf{Q}\} & \text{für } p = 2, \\ \{(0,1),(1,0)\} & \text{für } p > 2. \end{cases}$$
(Dies besagt die Fermatsche Vermutung.)

**Affiner Koordinatenwechsel:** Sei $C$ durch eine Gleichung $f(x_1,x_2) = 0$ definiert. Ist
$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$
ein affiner Koordinatenwechsel über $K$, so definiert
$$\widetilde{f}(y_1,y_2) = f(a_{11}y_1 + a_{12}y_2 + b_1, a_{21}y_1 + a_{22}y_2 + b_2)$$
eine Kurve $\widetilde{C}$. Man sagt $\widetilde{C}$ ist affin äquivalent zu $C$. Offensichtlich definiert der Koordinatenwechsel eine Bijektion zwischen $C(\overline{K})$ und $\widetilde{C}(\overline{K})$. Ist der Koordinatenwechsel über $K$ definiert, so gibt es eine Bijektion zwischen $C(K)$ und $\widetilde{C}(K)$.

**Bemerkung:** Geometrische Eigenschaften, wie sie im folgenden beschrieben werden, ändern sich nicht bei Koordinatenwechsel. Dies muss man natürlich eigentlich zeigen. Wir werden dies aber meist nicht tun.

Wir wollen nun Kurven lokal um eine Punkt näher betrachten.

**Überlegung:** Sei $C$ eine ebene Kurve gegeben durch eine Gleichung $f(x,y) = 0$ und $P = (x_0,y_0) \in C(\overline{K})$. Wir bilden die Taylorreihenentwicklung von $f$ in $(x_0,y_0)$:
$$f = a_1(x-x_0) + a_2(y-y_0) + a_3(x-x_0)^2 + a_4(x-x_0)(y-y_0) + a_5(y-y_0)^2 + \dots$$

Es folgt

$$\begin{aligned}\frac{\partial f}{\partial x} &= a_1 + 2a_3(x-x_0) + a_4(y-y_0) + \dots,\\ \frac{\partial f}{\partial y} &= a_2 + a_4(x-x_0) + 2a_5(y-y_0) + \dots\end{aligned}$$

und damit

$$\frac{\partial f}{\partial x}(P) = a_1, \quad \frac{\partial f}{\partial y}(P) = a_2.$$

Ist $(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) = (a_1, a_2) \neq (0,0)$, so ist

$$a_1(x-x_0) + a_2(y-y_0) = \frac{\partial f}{\partial x}(P)(x-x_0) + \frac{\partial f}{\partial y}(P)(y-y_0)$$

die lineare Approximation von $f$ in $P$.

DEFINITION. Sei eine Kurve $C$ gegeben durch ein Polynom $f(x,y)$ und $P = (x_0, y_0) \in C(\overline{K})$.

(1) Die Kurve $C$ heißt singulär im Punkt $P$ bzw. hat eine Singularität im Punkt $P$, wenn gilt

$$(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) = (0,0).$$

(2) Ist $(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) \neq (0,0)$, so heißt $P$ nichtsingulärer oder glatter Punkt der Kurve $C$, und

$$\frac{\partial f}{\partial x}(P)(x-x_0) + \frac{\partial f}{\partial y}(P)(y-y_0) = 0$$

heißt die Tangente von $C$ im Punkt $P$.

**Beispiele:**

(1) Sei $C$ gegeben durch $f = x^2 + y^2 - 1 = 0$ und $P = (\frac{3}{5}, \frac{4}{5}) \in C(\mathbf{Q})$. Es ist $\frac{\partial f}{\partial x} = 2x$ und $\frac{\partial f}{\partial y} = 2y$, also

$$(\frac{\partial f}{\partial x}(P), (\frac{\partial f}{\partial y}(P)) = (2x(P), 2y(P)) = (\frac{6}{5}, \frac{8}{5}).$$

Daher ist $C$ in $P$ nichtsingulär mit Tangente

$$\frac{6}{5}(x - \frac{3}{5}) + \frac{8}{5}(y - \frac{4}{5}) = 0 \quad \text{bzw.} \quad 3x + 4y = 5.$$

(2) Sei $C$ gegeben durch $f = y^2 - x^3 = 0$. Offensichtlich ist $C$ singulär in $P = (0,0)$.

**Bemerkung:** Bei Koordinatenwechsel gehen Singularitäten in Singularitäten und Tangenten in Tangenten über.

LEMMA. *Ist $f(x,y) = \sum_{i=0}^{m} a_i x^i y^{m-i} \in K[x,y]$ ein homogenes Polynom vom Grad $m$, dann gibt es $\alpha_i, \beta_i \in \overline{K}$ mit*

$$f(x,y) = \prod_{i=1}^{m} (\alpha_i x + \beta_i y).$$

*Beweis:* Ist $f(x,y) = 0$, so ist nichts zu zeigen. Sei nun $d$ mit $a_d \neq 0$, $a_{d+1} = a_{d+2} = \dots = 0$. Es gibt $\lambda_i \in \overline{K}$ mit

$$a_0 + a_1 t + \dots + a_{d-1} t^{d-1} + a_d t^d = a_d(t-\lambda_1)\dots(t-\lambda_d).$$

Dann ist

$$\begin{aligned} f(x,y) &= a_0 y^m + a_1 x y^{m-1} + \dots + a_{d-1} x^{d-1} y^{m-d+1} + a_d x^d y^{m-d} = \\ &= y^m (a_0 + a_1(\frac{x}{y}) + \dots + a_{d-1}(\frac{x}{y})^{d-1} + a_d(\frac{x}{y})^d) = \\ &= a_d y^m (\frac{x}{y} - \lambda_1)\dots(\frac{x}{y} - \lambda_d) = \\ &= a_d y^{m-d}(x - \lambda_1 y)\dots(x - \lambda_d y), \end{aligned}$$

was die Behauptung beweist. ■

**Bemerkung:** Sei $C$ eine durch $f(x,y)=0$ definierte ebene Kurve und $P \in \mathbf{A}^2$ ein Punkt. Nach Koordinatenwechsel können wir o.E. $P=(0,0)$ annehmen. Ist $f(x,y)=\sum_{i,j} a_{ij}x^iy^j$, so ist $f_\ell = \sum_{i+j=\ell} a_{ij}x^iy^j$ der homogene Anteil vom Grad $\ell$. Dann kann man schreiben

$$f = f_m + f_{m+1} + f_{m+2} + \dots \quad \text{mit} \quad f_m \neq 0.$$

$m$ heißt die Multiplizität von $C$ in $P$. Wir unterscheiden einige Fälle:

- $m=0$: Dann ist $P \notin C(\overline{K})$.
- $m=1$: Dann ist $P$ glatter Punkt von $C$. Der lineare Anteil $f_1 = a_{10}x + a_{01}y$ liefert die Tangente $a_{10}x + a_{01}y = 0$ von $C$ in $P$.
- $m \geq 2$: Dann ist $C$ singulär in $P$. Man kann faktorisieren

$$f_m(x,y) = \prod_{i=1}^{m} (\alpha_i x + \beta_i y) \quad \text{mit} \quad \alpha_i, \beta_i \in \overline{K} \quad \text{und} \quad (\alpha_i, \beta_i) \neq 0.$$

  Die Geraden $\alpha_i x + \beta_i y = 0$ nennt man Tangentenrichtungen von $C$ in $P$ oder manchmal auch einfach Tangenten von $C$ in $P$.

**Beispiel:** Wir betrachten die Kurve $C$ mit der Gleichung $y^2 = x^2 + x^3$ bzw. $f(x,y) = x^2 - y^2 + x^3 = 0$ über $\mathbf{R}$ und den Punkt $P=(0,0)$. Die Taylorreihenentwicklung von $f(x,y)$ in $(0,0)$ ist

$$f(x,y) = (x^2 - y^2) + x^3,$$

daher ist die Multiplizität von $C$ in $P$ einfach 2 und $y=x$ und $y=-x$ sind die Tangentenrichtungen.

Wir wollen nun Schnitte von Kurven betrachten. Für praktische Anwendungen erinnern wir an ein Hilfsmittel aus der Algebra, die Resultanten:

**Resultanten:** Seien $f(x,y), g(x,y) \in K[x,y]$ von 0 verschiedene Polynome, die wir in der Form

$$f(x,y) = a_m(x)y^m + a_{m-1}(x)y^{m-1} + \dots + a_0(x), \quad g(x,y) = b_n(x)y^n + b_{n-1}(x)y^{n-1} + \dots + b_0(x)$$

schreiben können mit $m = \operatorname{grad}_y(f)$ und $n = \operatorname{grad}_y(g)$. Dann ist die Resultante $R_y(x)$ von $f(x,y)$ und $g(x,y)$ bzgl. $y$ definiert durch die Determinante

$$R_y(x) = \det \begin{pmatrix} a_m(x) & \dots & \dots & a_0(x) & & \\ & \ddots & & & \ddots & \\ & & a_m(x) & \dots & \dots & a_0(x) \\ b_n(x) & \dots & \dots & b_0(x) & & \\ & \ddots & & & \ddots & \\ & & b_n(x) & \dots & \dots & b_0(x) \end{pmatrix} \in K[x].$$

(Die Matrix hat $m+n$ Zeilen und Spalten, wobei zunächst $n$ Zeilen mit den Koeffizienten von $f(x,y)$, dann $m$ Zeilen mit den Koeffizienten von $g(x,y)$ eingetragen werden.) Wir geben zwei wichtige Eigenschaften an:

(1) Es gibt Polynome $A(x,y), B(x,y) \in K[x,y]$ mit

$$A(x,y)f(x,y) + B(x,y)g(x,y) = R_y(x).$$

(2) Ist $R_y(x) = 0$, so haben $f(x,y)$ und $g(x,y)$ einen gemeinsamen Teiler $h(x,y) \in K[x,y]$ mit $\operatorname{grad}_y h(x,y) \geq 1$.

Natürlich kann man analog auch die Resultante bzgl. $x$ bilden, die dann ein Polynom $R_x(y)$ in $y$ ist.

**Bemerkung:** Die Maple-Funktion 'resultant($f$,$g$,$y$)' berechnet die Resultante von $f$ und $g$ bzgl. der Variablen $y$.

Wir erhalten jetzt einfach folgenden Satz:

SATZ. *Seien $C$ und $D$ durch $f(x,y)$ bzw. $g(x,y)$ definierte Kurven über $K$. Sind $R_y(x)$ und $R_x(y)$ die Resultanten von $f(x,y)$ und $g(x,y)$ bzgl. $y$ bzw. $x$, so gilt:*

(1)
$$C(\overline{K}) \cap D(\overline{K}) \subseteq \{(x_0,y_0) \in \mathbf{A}^2 : R_y(x_0) = R_x(y_0) = 0\}.$$

(2) *Sind $f(x,y)$ und $g(x,y)$ teilerfremd, so sind die Resultanten $R_y$ und $R_x$ von 0 verschiedene Polynome einer Variablen. Insbesondere folgt*
$$\#C(\overline{K}) \cap D(\overline{K}) \leq \operatorname{grad}_x R_y \cdot \operatorname{grad}_y R_x.$$

*Beweis:* Es gibt Polynome $A(x,y), B(x,y), U(x,y), V(x,y) \in K[x,y]$ mit
$$A(x,y)f(x,y) + B(x,y)g(x,y) = R_y(x) \quad \text{und} \quad U(x,y)f(x,y) + V(x,y)g(x,y) = R_x(y).$$
Ist $(x_0,y_0) \in C(\overline{K}) \cap D(\overline{K})$, so folgt mit $f(x_0,y_0) = g(x_0,y_0) = 0$ sofort $R_y(x_0) = R_x(y_0) = 0$ und damit die erste Behauptung. Haben $f(x,y)$ und $g(x,y)$ keinen gemeinsamen Teiler, so sind beide Resultanten $R_y$ und $R_x$ von 0 verschieden, was sofort die zweite Behauptung liefert. ■

Wir geben eine Anwendung für die Singularitäten einer ebenen Kurve:

SATZ. *Sei $C$ gegeben durch ein Polynom $f(x,y) \in K[x,y]$. Die Menge der Singularitäten von $C$ ist*
$$\{P \in \mathbf{A}^2(\overline{K}) : f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0\}.$$
*Ist $C$ absolut irreduzibel, so hat $C$ nur endlich viele Singularitäten.*

*Beweis:* Da eine Singularität $P$ von $C$ durch die Gleichungen $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$ charakterisiert werden, ist klar, dass die angegebene Menge genau die Singularitäten beschreibt. Wir betrachten jetzt den Fall, dass $f(x,y)$ irreduzibel über $\overline{K}$ ist. Wir unterscheiden ein paar Fälle:

- *Fall 1:* $\frac{\partial f}{\partial y} \neq 0$. Wir schreiben
$$f(x,y) = a_0(x) + a_1(x)y + \cdots + a_m(x)y^m \quad \text{mit} \quad a_m(x) \neq 0.$$
Dann ist
$$\frac{\partial f}{\partial y}(x,y) = a_1(x) + \cdots + m a_m(x) y^{m-1}.$$
Da $f(x,y)$ irreduzibel ist, haben $f(x,y)$ und $\frac{\partial f}{\partial y}(x,y)$ keinen gemeinsamen Teiler. Also sind die beiden zugehörigen Resultanten $R_y(x)$ und $R_x(y)$ von 0 verschieden. Demnach haben $f(x,y) = 0$ und $\frac{\partial f}{\partial y}(x,y) = 0$ nur endlich viele Schnittpunkte, weswegen es auch nur endlich viele Singularitäten geben kann.
- *Fall 2:* $\frac{\partial f}{\partial x} \neq 0$. Diesen Fall behandelt man genauso wie Fall 1.
- *Fall 3:* $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$. Sei
$$f = \sum_{i,j} a_{ij} x^i y^j.$$
Dann ist
$$\frac{\partial f}{\partial x} = \sum_{i,j} i a_{ij} x^{i-1} y^j \quad \text{und} \quad \frac{\partial f}{\partial y} = \sum_{i,j} j a_{ij} x^i y^{j-1}$$
und damit $i a_{ij} = 0$ und $j a_{ij} = 0$. In Charakteristik 0 ist dies nicht möglich, da mindestens ein Indexpaar $(i,j)$ mit $i > 0$ oder $j > 0$ existiert. Also ist die Charakteristik $p$. Im Fall $a_{ij} \neq 0$ gilt dann $i \equiv j \equiv 0 \bmod p$. Wählen wir $b_{ij} \in \overline{K}$ mit $b_{ij}^p = a_{pi,pj}$, so folgt
$$f = \sum_{i,j} a_{pi,pj} x^{pi} y^{pj} = \sum_{i,j} (b_{ij} x^i y^j)^p = (\sum_{i,j} b_{ij} x^i y^j)^p,$$
was der Irreduzibilität von $f$ über $\overline{K}$ widerspricht. Also kann dieser Fall überhaupt nicht eintreten. ■

**Beispiele:**

(1) Wir betrachten $C$ mit $y^2 = x^3$. Die Kurve wird gegeben durch das Polynom $f = y^2 - x^3$. Dann gilt
$$f = y^2 - x^3, \quad \frac{\partial f}{\partial x} = -3x^2, \quad \frac{\partial f}{\partial y} = 2y.$$
Man sieht dann sofort, dass die einzige Singularität der Punkt $P = (0,0)$ ist. (Man unterscheide zunächst zwischen Charakteristik $\neq 2$ und $\neq 3$.)
(2) $f = x^2$ definiert eine Kurve $C$, die wegen $\frac{\partial f}{\partial x} = 2x$ und $\frac{\partial f}{\partial y} = 0$ für alle Punkte der Form $(0, y)$ singulär ist. D.h. alle Kurvenpunkte sind singulär.

**Schnittvielfachheiten:** Sind $C$ und $D$ affine Kurven, so kann man eine Schnittvielfachheit $(C \cdot D)_P$ von $C$ und $D$ in einem Punkt $P \in \mathbf{A}^2$ definieren. Der Einfachkeit halber werden wir uns zunächst auf Schnitte von Kurven mit Geraden beschränken. Sei also $C$ gegeben durch ein Polynom $f(x, y)$ und die Gerade $G$ durch $a + bx + cy$. Wir setzen voraus, dass $a + bx + cy$ das Polynom $f(x, y)$ nicht teilt. Wir wählen eine Parametrisierung $x = \alpha + \beta t$, $y = \gamma + \delta t$ der Geraden $G$. Sei $P = (x_0, y_0) \in \mathbf{A}^2$.

(1) Ist $P \notin G(\overline{K})$, so setzen wir $(C \cdot G)_P = 0$.
(2) Ist $P \in G(\overline{K})$, so gibt es $t_0 \in \overline{K}$ mit $x_0 = \alpha + \beta t_0$, $y_0 = \gamma + \delta t_0$. Wir setzen die Geradenparametrisierung $x = \alpha + \beta t$, $y = \gamma + \delta t$ in die Gleichung $f(x, y)$ der Kurve $C$ ein und erhalten ein Polynom in $g(t) = f(\alpha + \beta t, \gamma + \delta t) \in \overline{K}[t]$. Wäre $g(t)$ identisch 0, so wäre $G(\overline{K}) \subseteq C(\overline{K})$ und damit nach unseren Vorüberlegungen $a + bx + cy$ ein Teiler von $f(x, y)$. Da das ausgeschlossen war, ist $g(t) \neq 0$, also kann man faktorisieren:
$$g(t) = f(\alpha + \beta t, \gamma + \delta t) = (t - t_0)^m h(t) \quad \text{mit} \quad h(t) \in \overline{K}[t] \quad \text{und} \quad h(t_0) \neq 0.$$
Als Schnittmultiplizität nehmen wir die Vielfachkeit der Nullstelle $t_0$, also
$$(C \cdot G)_P = m.$$
(Natürlich müsste man nun eigentlich noch zeigen, dass die Schnittmultiplizität unabhängig von der gewählten Geradenparametrisierung ist.)

**Beispiel:** Wir betrachten die durch $y = x^2$ bzw. $f(x, y) = y - x^2 = 0$ definierte Kurve $C$.

(1) Zunächst betrachten wir die Gerade $G$ mit der Gleichung $y = x$. Als Parametrisierung wählen wir $x = t$, $y = t$. Einsetzen in die Kurvengleichung liefert
$$f(t, t) = t - t^2 = -t(t - 1).$$
Also erhält man für $t = 0$ und $t = 1$ jeweils Schnittpunkte mit Schnittmultiplizität 1, nämlich $P_1 = (0, 0)$ und $P_2 = (1, 1)$.
(2) Nun betrachten wir die Gerade $G$ mit der Gleichung $y = 0$. Als Parametrisierung wählen wir $x = t$, $y = 0$. Einsetzen liefert
$$f(t, 0) = -t^2.$$
Daher ist $P = (0, 0)$ Schnittpunkt und $(C \cdot G)_P = 2$.

Satz. *Sei $C$ eine durch $f(x, y)$ definierte ebene affine Kurve, $P$ ein Punkt von $C$ der Multiplizität $m \geq 1$, sowie $G$ eine Gerade durch $P$, gegeben durch $a + bx + cy$. Wir setzen voraus, dass $a + bx + cy$ das Polynom $f(x, y)$ nicht teilt. Dann gilt:*
$$(C \cdot G)_P \begin{cases} = m & \textit{falls } G \textit{ keine Tangente bzw. Tangentenrichtung ist,} \\ \geq m + 1 & \textit{falls } G \textit{ Tangente bzw. Tangentenrichtung ist.} \end{cases}$$

*Beweis:* Wir können o.E. $P = (0, 0)$ annehmen. Wir schreiben
$$f(x, y) = f_m(x, y) + f_{m+1}(x, y) + \ldots,$$
wobei $f_\ell(x, y)$ homogen vom Grad $\ell$ ist. Wir faktorisieren
$$f_m(x, y) = \prod_{i=1}^{m} (\lambda_i x + \mu_i y) \quad \text{mit} \quad \lambda_i, \mu_i \in \overline{K}.$$

Die Gerade $G$ können wir in der Form $x = \alpha t$, $y = \beta t$ parametrisieren. Die Schnittmultiplizität $(C \cdot G)_P$ ist die Vielfachheit der Nulltstelle $t = 0$ in $f(\alpha t, \beta t)$. Daher berechnen wir

$$\begin{aligned} f(\alpha t, \beta t) &= f_m(\alpha t, \beta t) + f_{m+1}(\alpha t, \beta t) + \cdots = t^m f_m(\alpha, \beta) + t^{m+1} f_{m+1}(\alpha, \beta) + \cdots = \\ &= t^m \left( f_m(\alpha, \beta) + t f_{m+1}(\alpha, \beta) + \dots \right) = \\ &= t^m \left( \prod_{i=1}^{m} (\lambda_i \alpha + \mu_i \beta) + t f_{m+1}(\alpha, \beta) + \dots \right). \end{aligned}$$

*Fall 1:* Stimmt $G$ mit einer Tangentenrichtung $\lambda_i x + \mu_i y = 0$ überein, so gilt $\lambda_i \alpha + \mu_i \beta = 0$, also ist die Schnittmultiplizität $(C \cdot G)_P \geq m + 1$.
*Fall 2:* Stimmt $G$ mit keiner Tangentenrichtung überein, so gilt $\lambda_i \alpha + \mu_i \beta \neq 0$ für alle $i$, also folgt sofort $(C \cdot G)_P = m$, was alles beweist. ■

DEFINITION. Ein nichtsingulärer Punkt $P$ einer ebenen affinen Kurve $C$ heißt Wendepunkt, falls die Tangente $T$ die Kurve $C$ mit Multiplizität $\geq 3$ in $P$ schneidet. Die Tangente nennt man dann eine Wendetangente von $C$.

**Beispiel:** Wir betrachten $C$ mit der Gleichung $y = x^n$ mit $n \geq 3$ über $\mathbf{R}$. Der Punkt $P = (0, 0)$ ist ein nichtsingulärer Kurvenpunkt mit Tangente $T$, gegeben durch $y = 0$. Die Schnittmultiplizität ist $(C \cdot T)_P = n \geq 3$, also ist $P$ ein Wendepunkt der Kurve und $T$ eine Wendetangente.

## 3. Projektive Räume

Projektive Räume sollen affine Räume vervollständigen bzw. kompaktifizieren.

DEFINITION. Auf $\mathbf{A}^{n+1} \setminus \{0\}$ wird wie folgt eine Äquivalenzrelation definiert:

$$(a_0, \dots, a_n) \sim (b_0, \dots, b_n) \quad \Longleftrightarrow \quad a_0 = \lambda b_0, \dots a_n = \lambda b_n \text{ für ein } \lambda \in \overline{K}^*.$$

Die Äquivalenzklasse von $(a_0, \dots, a_n)$ wird mit $(a_0 : \cdots : a_n)$ bezeichnet. Die Menge der Äquivalenzklassen heißt $n$-dimensionaler projektiver Raum $\mathbf{P}^n = \mathbf{P}^n(\overline{K})$. Also

$$\mathbf{P}^n = \{(a_0 : \cdots : a_n) : (a_0, \dots, a_n) \in \overline{K}^{n+1} \setminus \{0\}\}.$$

Wie im affinen Fall definiert man die Menge der $K$-rationalen Punkte von $\mathbf{P}^n$ durch

$$\mathbf{P}^n(K) = \{(a_0 : \cdots : a_n) \in \mathbf{P}^n : a_i \in K\}.$$

**Beispiele:**

(1) $\mathbf{P}^1 = \{(1 : a) : a \in \overline{K}\} \cup \{(0 : 1)\}$.
(2) $\mathbf{P}^2 = \{(1 : x : y) : (x, y) \in \mathbf{A}^2\} \cup \{(0 : 1 : x) : x \in \mathbf{A}^1\} \cup \{(0 : 0 : 1)\}$.

**Bemerkung:** Aus $(a_0 : a_1 : \cdots : a_n) \in \mathbf{P}^n(K)$ folgt noch nicht $a_i \in K$, wie das Beispiel

$$(\sqrt{2} : \frac{1}{\sqrt{2}}) = (2 : 1) \in \mathbf{P}^1(\mathbf{Q}) \text{ mit } \sqrt{2} \notin \mathbf{Q}$$

zeigt.

**Überdeckung von $\mathbf{P}^n$ durch affine Räume $\mathbf{A}^n$:** Definiere

$$\phi_i : \mathbf{A}^n \to \mathbf{P}^n, \quad (a_1, \dots, a_n) \mapsto (a_1 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_n).$$

$\phi_i$ ist injektiv. Sei

$$H_i = \{(b_0 : \cdots : b_n) \in \mathbf{P}^n : b_i = 0\} \text{ und } U_i = \{(b_0 : \cdots : b_n) \in \mathbf{P}^n : b_i \neq 0\}.$$

Dann gilt $\phi_i(\mathbf{A}^n) = U_i$ mit der Umkehrabbildung

$$\phi_i^{-1} : U_i \to \mathbf{A}^n, \quad (b_0 : \cdots : b_n) \mapsto (\frac{b_0}{b_i}, \cdots : \frac{b_{i-1}}{b_i}, \frac{b_{i+1}}{b_i}, \dots, \frac{b_n}{b_i}).$$

Also $U_i \simeq \mathbf{A}^n$ und $H_i \simeq \mathbf{P}^{n-1}$. Der projektive Raum $\mathbf{P}^n$ wird überdeckt von den affinen Mengen $U_0, \dots, U_n$.

**Einbettung von $\mathbf{A}^n$ in $\mathbf{P}^n$:** Mit obiger Abbildung $\phi_0$ denken wir uns manchmal $\mathbf{A}^n$ eingebettet in $\mathbf{P}^n$:

$$\mathbf{A}^n \hookrightarrow \mathbf{P}^n, \quad (x_1, \ldots, x_n) \mapsto (1 : x_1 : \cdots : x_n).$$

Damit ist

$$\mathbf{P}^n \setminus \mathbf{A}^n = H_0 = \{(0 : x_1 : \cdots : x_n) \in \mathbf{P}^n\} \simeq \mathbf{P}^{n-1}.$$

$H_0$ wird auch die unendlich ferne Hyperebene, im Fall $n = 1$ der unendlich ferne Punkt, im Fall $n = 2$ die unendlich ferne Gerade $G_\infty$ genannt.

Definition. Eine projektive Transformation (oder ein projektiver Koordinatenwechsel) ist eine Abbildung $\phi : \mathbf{P}^n \to \mathbf{P}^n$, sodass eine Matrix $A \in \mathrm{GL}_{n+1}(\overline{K})$ existiert mit

$$\phi(x_0 : \cdots : x_n) = (y_0 : \cdots : y_n) \iff A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix} \text{ für ein } \lambda \in \overline{K}^*.$$

$\phi$ ist offensichtlich bijektiv, $\phi^{-1}$ ist eine projektive Transformation, die durch die Matrix $A^{-1}$ beschrieben wird.
Zwei Mengen $V, W \subseteq \mathbf{P}^n$ heißen projektiv äquivalent, wenn es eine projektive Transformation $\phi$ gibt mit $W = \phi(V)$. Die Mengen $V, W$ heißen projektiv äquivalent über $K$, wenn die Matrix $A$ in $\mathrm{GL}_{n+1}(K)$ gewählt werden kann.

Definition. Eine Gerade in $\mathbf{P}^2$ ist eine Teilmenge der Gestalt

$$G = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$$

mit $a_0, a_1, a_2 \in \overline{K}$ und $(a_0, a_1, a_2) \neq 0$.

**Der affine Teil von Geraden im $\mathbf{P}^2$:** Wir denken uns $\mathbf{A}^2 \simeq \{(1 : x : y) : x, y \in \overline{K}\} \subseteq \mathbf{P}^2$. Sei $G$ gegeben durch $a_0x_0 + a_1x_1 + a_2x_2 = 0$. Dann ist

$$G \cap \mathbf{A}^2 = \{(1 : x : y) \in \mathbf{P}^2 : a_0 + a_1x + a_2y = 0\} \text{ und } G \cap G_\infty = \{(0 : z_1 : z_2) \in \mathbf{P}^2 : a_1z_1 + a_2z_2 = 0\}.$$

- Ist $(a_1, a_2) \neq (0, 0)$, so ist $G \cap \mathbf{A}^2$ also die affine Gerade $a_0 + a_1x + a_2y = 0$, und $G \cap G_\infty = \{(0 : a_2 : -a_1)\}$ besteht aus einem Punkt.
- Ist $(a_1, a_2) = (0, 0)$, so ist $G \cap \mathbf{A}^2 = \emptyset$ und $G = G_\infty$.

Bis auf die unendlich ferne Gerade $G_\infty$ sieht man also alle Geraden von $\mathbf{P}^2$ als affine Geraden im endlichen Teil $\mathbf{A}^2$. Man überlegt sich nun schnell, dass die Zuordnung

$$\{\text{Geraden in } \mathbf{P}^2\} \setminus \{G_\infty\} \to \{\text{Geraden in } \mathbf{A}^2\}, \quad G \mapsto G \cap \mathbf{A}^2$$

eine Bijektion ist.

**Welche Punkte haben affine Geraden im Unendlichen?** Nach der letzten Bemerkung können wir jede affine Gerade uns denken als $G \cap \mathbf{A}^2$ mit einer projektiven Geraden $G$. Was ist dann $G \cap G_\infty$?

- Die affine Gerade $y = ax + b$ ist der endliche Teil der projektiven Geraden $bx_0 + ax_1 - x_2 = 0$. Der Schnitt mit $G_\infty = \{x_0 = 0\}$ ergibt den Punkt $(0 : 1 : a)$. (Variiert man $b$, so erhält man parallele Geraden, die sich im Unendlichen im Punkt $(0 : 1 : a)$ schneiden.)
- Die affine Gerade $x = c$ ist der endliche Teil der projektiven Geraden $cx_0 - x_1 = 0$. Der Schnitt mit $G_\infty$ ergibt den Punkt $(0 : 0 : 1)$. (Verschiedene Werte von $c$ ergeben parallele Geraden im Endlichen.)

Wir sehen insbesondere: Schneiden sich zwei Geraden auf der unendlich fernen Geraden, so sind ihre affinen Teile parallele Geraden.

**Weitere Betrachtungen zu Geraden in der projektiven Ebene $\mathbf{P}^2$:**

(1) Zwei Geraden

$$\begin{aligned} G_1 &= \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}, \\ G_2 &= \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : b_0x_0 + b_1x_1 + b_2x_2 = 0\} \end{aligned}$$

können in folgenden Beziehungen stehen:

(a) Sind $(a_0, a_1, a_2)$ und $(b_0, b_1, b_2)$ linear unabhängig, so gilt

$$G_1 \cap G_2 = \{(p_0 : p_1 : p_2)\}, \text{ wobei } (p_0, p_1, p_2) \text{ durch } \begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

bis auf eine multiplikative Konstante eindeutig bestimmt ist. ($G_1$ und $G_2$ schneiden sich in einem Punkt.)

(b) Sind $(a_0, a_1, a_2)$ und $(b_0, b_1, b_2)$ linear abhängig, so gilt offensichtlich

$$G_1 = G_2.$$

($G_1$ und $G_2$ sind identisch.)

(2) Sind $P = (p_0 : p_1 : p_2)$ und $Q = (q_0 : q_1 : q_2)$ zwei verschiedene Punkte in $\mathbf{P}^2$, so gibt es genau eine Gerade $G$, die $P$ und $Q$ enthält, nämlich $G = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$, wobei $(a_0, a_1, a_2)$ eine nichttriviale Lösung der Gleichung

$$\begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

ist. (Je zwei nichttriviale Lösungen unterscheiden sich nur um eine multiplikative Konstante.)

(3) Sind $P = (p_0 : p_1 : p_2)$ und $Q = (q_0 : q_1 : q_2)$ zwei verschiedene Punkte in $\mathbf{P}^2$, so kann man die durch $P$ und $Q$ gehende Gerade $G$ auch in parametrisierter Form angeben:

$$G = \{(p_0u + q_0v : p_1u + q_1v : p_2u + q_2v) \in \mathbf{P}^2 : (u : v) \in \mathbf{P}^1\}.$$

(4) Da $a_0x_0 + a_1x_1 + a_2x_2 = 0$ und $b_0x_0 + b_1x_1 + b_2x_2 = 0$ genau dann die gleiche Gerade in $\mathbf{P}^2$ definieren, wenn gilt $(a_0 : a_1 : a_2) = (b_0 : b_1 : b_2)$, so ist klar, dass die Zuordnung

$$\mathbf{P}^2 \to \{\text{Geraden in } \mathbf{P}^2\}, \quad (a_0 : a_1 : a_2) \mapsto \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$$

eine Bijektion ist. Man sagt: Die Geraden in $\mathbf{P}^2$ bilden wieder einen $\mathbf{P}^2$.

(5) Drei Punkte $P = (p_0 : p_1 : p_2)$, $Q = (q_0 : q_1 : q_2)$, $R = (r_0 : r_1 : r_2)$ der projektiven Ebene $\mathbf{P}^2$ liegen genau dann auf einer Geraden, wenn gilt

$$\det \begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \\ r_0 & r_1 & r_2 \end{pmatrix} = 0.$$

Eine zugehörige Gerade $G$ mit der Gleichung $a_0x_0 + a_1x_1 + a_2x_2 = 0$ ergibt sich dann aus der Bedingung

$$\begin{pmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \\ r_0 & r_1 & r_2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = 0.$$

LEMMA. *Seien $P, Q, R \in \mathbf{P}^2$ drei verschiedene Punkte der projektiven Ebene. Liegen $P, Q, R$ nicht auf einer Geraden, so gibt es einen projektiven Koordinatenwechsel mit*

$$\phi(P) = (1 : 0 : 0), \quad \phi(Q) = (0 : 1 : 0), \quad \phi(R) = (0 : 0 : 1).$$

*Sind $P, Q, R, S \in \mathbf{P}^2$ vier Punkte der projektiven Ebene, von denen keine drei auf einer Geraden liegen, so gibt es einen projektiven Koordinatenwechsel mit*

$$\phi(P) = (1 : 0 : 0), \quad \phi(Q) = (0 : 1 : 0), \quad \phi(R) = (0 : 0 : 1), \quad \phi(S) = (1 : 1 : 1).$$

*Beweis:* Sei $P = (p_0 : p_1 : p_2)$, $Q = (q_0 : q_1 : q_2)$, $R = (r_0 : r_1 : r_2)$. Da $P$, $Q$, $R$ nicht auf einer Geraden liegen, ist $\psi$ mit

$$\psi \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} p_0 & q_0 & r_0 \\ p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

ein projektiver Koordinatenwechsel mit

$$\psi((1 : 0 : 0)) = P, \quad \psi((0 : 1 : 0)) = Q, \quad \psi((0 : 0 : 1)) = R.$$

Mit $\phi = \psi^{-1}$ folgt dann die erste Aussage. Für die zweite Behauptung können wir nun o.E.

$$P = (1:0:0), \quad Q = (0:1:0), \quad R = (0:0:1), \quad S = (s_0 : s_1 : s_2)$$

annehmen. $P$ und $Q$ liegen auf der Geraden $x_2 = 0$, $P$ und $R$ auf der Geraden $x_1 = 0$, $Q$ und $R$ auf der Geraden $x_0 = 0$. Da $S$ auf keiner der Geraden liegen soll, ist $s_0, s_1, s_2 \neq 0$. Dann ist

$$\rho \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} s_0 & 0 & 0 \\ 0 & s_1 & 0 \\ 0 & 0 & s_2 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

ein projektiver Koordinatenwechsel mit

$$\rho((1:0:0)) = (1:0:0), \quad \rho((0:1:0)) = (0:1:0), \quad \rho((0:0:1)) = (0:0:1), \quad \rho((1:1:1)) = S,$$

sodass $\rho^{-1}$ ein geeigneter Koordinantenwechsel ist. ■

## 4. Ebene projektive Kurven

Ein Polynom $f(x_0, x_1, \ldots, x_n) \in K[x_0, x_1, \ldots, x_n]$ ist homogen vom Grad $d$, wenn alle auftretenden Monome Grad $d$ haben, d.h. wenn es sich in der Form

$$f = \sum_{i_0 + \cdots + i_n = d} a_{i_0 \ldots i_n} x_0^{i_0} \ldots x_n^{i_n}$$

schreiben lässt. Dann ist

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n) \quad \text{für alle} \quad \lambda \in K$$

und es gilt die Eulersche Relation

$$df(x_0, \ldots, x_n) = \sum_{i=0}^{n} \frac{\partial f}{\partial x_i} x_i.$$

**Bemerkung:** Sei $P = (a_0 : a_1 : a_2) = (b_0 : b_1 : b_2) \in \mathbf{P}^2$ und $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ homogen vom Grad $d$. Dann gibt es ein $\lambda \in \overline{K}^*$ mit $b_i = \lambda a_i$ und daher

$$f(b_0, b_1, b_2) = \lambda^d f(a_0, a_1, a_2).$$

Man kann also nicht den Wert von $f$ in $P$ (natürlich) definieren. Sinnvoll, d.h. repräsentantenunabhängig, ist aber die Aussage '$f(P) = 0$' oder '$f(P) \neq 0$'. Man definiert nun:

Definition. Eine ebene projektive Kurve $C$ über $K$ vom Grad $d$ wird durch ein homogenes Polynom $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ vom Grad $d$ gegeben. (Man sagt auch, dass $C$ durch die Gleichung $f(x_0, x_1, x_2) = 0$ definiert wird.) Das zugehörige geometrische Objekt ist die Nullstellenmenge

$$C(\overline{K}) = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : f(x_0, x_1, x_2) = 0\}.$$

Die Menge

$$C(K) = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2(K) : f(x_0, x_1, x_2) = 0\}$$

heißt die Menge der $K$-rationalen Punkte von $C$. Etwas allgemeiner betrachtet man für einen Oberkörper $L$ von $K$ die Menge der $L$-rationalen Punkte von $C$:

$$C(L) = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2(L) : f(x_0, x_1, x_2) = 0\}.$$

Ist $c \in K^*$, so unterscheidet man nicht zwischen der durch $f(x_0, x_1, x_2) = 0$ und der durch $cf(x_0, x_1, x_2) = 0$ definierten Kurve. Die Kurve $C$ heißt irreduzibel über $K$, wenn $f(x_0, x_1, x_2)$ als Polynom über $K$ irreduzibel ist, $C$ heißt absolut irreduzibel, wenn $f(x_0, x_1, x_2)$ als Polynom über $\overline{K}$ irreduzibel ist.

**Beispiele:**

(1) Eine Gerade in $\mathbf{P}^2$, gegeben als $G = \{(x_0 : x_1 : x_2) \in \mathbf{P}^2 : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$ können wir mit einer projektiven ebenen Kurve vom Grad 1, gegeben durch das Polynom $a_0x_0 + a_1x_1 + a_2x_2$, identifizieren.

(2) Ebene projektive Kurven vom Grad 2 nennt man Quadriken, Kurven vom Grad 3 heißen Kubiken.

(3) Wir betrachten die durch $f(x_0,x_1,x_2)=x_0x_2-x_1^2$ definierte Quadrik $Q$. Wir wollen sehen, wie $Q$ in den affinen Teilen $U_i$ aussieht:

$$\begin{aligned} Q(\overline{K})\cap U_0 &= Q(\overline{K})\cap\{(1:x:y):(x,y)\in\mathbf{A}^2\}=\{(1:x:y):y=x^2\},\\ Q(\overline{K})\cap U_1 &= Q(\overline{K})\cap\{(u:1:v):(u,v)\in\mathbf{A}^2\}=\{(u:1:v):uv=1\},\\ Q(\overline{K})\cap U_2 &= Q(\overline{K})\cap\{(r:s:1):(r,s)\in\mathbf{A}^2\}=\{(r:s:1):r=s^2\}. \end{aligned}$$

Die projektive Quadrik sieht also in den affinen Teilen wie eine Parabel oder wie eine Hyperbel aus.

Sei die ebene projektive Kurve $C$ gegeben durch das Polynom $f(x_0,x_1,x_2)$. Mit der Identifikation $\mathbf{A}^2\simeq\{(1:x:y)\}\subseteq\mathbf{P}^2$ erhalten wir

$$\begin{aligned} C(\overline{K})\cap\mathbf{A}^2 &= \{(1:x:y)\in\mathbf{P}^2:f(1,x,y)=0\}\simeq\{(x,y)\in\mathbf{A}^2:f(1,x,y)=0\} \quad \text{und}\\ C(\overline{K})\cap G_\infty &= \{(0:z_1:z_2):f(0,z_1,z_2)=0\}. \end{aligned}$$

Ist $f(1,x,y)$ ein nichtkonstantes Polynom, so entspricht der affine Teil von $C$ also der affinen Kurve $f(1,x,y)=0$. Ist $f(1,x,y)$ konstant, so ist $f=cx_0^d$ und mengenmäßig $C(\overline{K})=G_\infty$.

DEFINITION. Sei $f\in K[x_1,\dots,x_n]$ ein Polynom vom Grad $d$. Dann ist die Homogenisierung

$$\widetilde{f}(x_0,\dots,x_n)=x_0^d f(\frac{x_1}{x_0},\dots,\frac{x_n}{x_0})$$

ein homogenes Polynom vom Grad $d$.

DEFINITION. Sei $C$ eine affine ebene Kurve gegeben durch ein Polynom $f(x,y)\in K[x,y]$ vom Grad $d$. Ist dann

$$\widetilde{f}(x_0,x_1,x_2)=x_0^d f(\frac{x_1}{x_0},\frac{x_2}{x_0})$$

die Homogenisierung von $f$, so heißt die durch $\widetilde{f}(x_0,x_1,x_2)$ definierte projektive ebene Kurve der projektive Abschluss $\overline{C}$ von $C$.

**Beispiel:** Wir betrachten die Parabel $C$ mit der Gleichung $f=y-x^2=0$ in $\mathbf{A}^2$. Die Homogenisierung von $f(x,y)$ ist $\widetilde{f}(x_0,x_1,x_2)=x_0^2f(\frac{x_1}{x_0},\frac{x_2}{x_0})=x_0x_2-x_1^2$. Der projektive Abschluss von $C$ ist also $\overline{C}$, gegeben durch $\widetilde{f}=x_0x_2-x_1^2$.

**Überlegung:** Sei eine ebene affine Kurve $C$ gegeben durch das Polynom $f(x,y)\in K[x,y]$. Wir schreiben

$$f(x,y)=\sum_{\ell=0}^{d}f_\ell(x,y),\quad f_\ell(x,y)\text{ homogen vom Grad }\ell,\quad f_d(x,y)\neq 0.$$

Dann definiert die Homogenisierung

$$\widetilde{f}(x_0,x_1,x_2)=\sum_{\ell=0}^{d}x_0^{d-\ell}f_\ell(x_1,x_2)=x_0^df_0(x_1,x_2)+x_0^{d-1}f_1(x_1,x_2)+\cdots+x_0f_{d-1}(x_1,x_2)+f_d(x_1,x_2)$$

den projektiven Abschluss $\overline{C}$ von $C$. Faktorisieren wir

$$f_d(x_1,x_2)=\prod_{i=1}^{d}(\lambda_ix_1-\mu_ix_2),$$

so gilt

$$\begin{aligned} \mathbf{A}^2\cap\overline{C}(\overline{K}) &= \{(x,y)\in\mathbf{A}^2:\widetilde{f}(1,x,y)=0\}=\{(x,y)\in\mathbf{A}^2:f(x,y)=0\}=C(\overline{K}),\\ G_\infty\cap\overline{C}(\overline{K}) &= \{(0:z_1:z_2)\in\mathbf{P}^2:\widetilde{f}(0,z_1,z_2)=0\}=\{(0:z_1:z_2)\in\mathbf{P}^2:f_d(z_1,z_2)=0\}=\\ &= \{(0:\mu_1:\lambda_1),\dots,(0:\mu_d:\lambda_d)\}, \end{aligned}$$

wobei nicht alle Punkte $(0:\mu_i:\lambda_i)$ notwendig verschieden sind. Offensichtlich kann man sich jede projektive ebene Kurve als projektiven Abschluss einer affinen ebenen Kurve vorstellen.

**Lokale Betrachtung:** Sei die projektve ebene Kurve $C$ vom Grad $d$ gegeben durch das Polynom $F(x_0, x_1, x_2)$. Wir schreiben

$$F(x_0, x_1, x_2) = \sum_{\ell=0}^{d} x_0^{d-\ell} f_\ell(x_1, x_2) \quad \text{und} \quad f(x, y) = F(1, x, y) = \sum_{\ell=0}^{d} f_\ell(x, y)$$

und erhalten

$$\begin{aligned}
\frac{\partial F}{\partial x_1}(1, x, y) &= \frac{\partial f}{\partial x}(x, y), \\
\frac{\partial F}{\partial x_2}(1, x, y) &= \frac{\partial f}{\partial y}(x, y), \\
\frac{\partial F}{\partial x_0}(1, x, y) &= dF(1, x, y) - x\frac{\partial F}{\partial x_1}(1, x, y) - y\frac{\partial F}{\partial x_2}(1, x, y) = df(x, y) - x\frac{\partial f}{\partial x}(x, y) - y\frac{\partial f}{\partial y}(x, y).
\end{aligned}$$

Sei weiter $P = (p_0 : p_1 : p_2) \in C(\overline{K})$ ein Punkt der projektiven Kurve. Wir betrachten den Fall $p_0 \neq 0$, d.h. $P = (1, \frac{p_1}{p_0}, \frac{p_2}{p_0})$. Wegen $F(P) = F(p_0, p_1, p_2) = p_0^d f(\frac{p_1}{p_0}, \frac{p_2}{p_0}) = 0$ gilt

$$\frac{\partial F}{\partial x_0}(P) = \frac{\partial F}{\partial x_1}(P) = \frac{\partial F}{\partial x_2}(P) = 0 \quad \Longleftrightarrow \quad \frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) = \frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) = 0$$

und

$$\begin{aligned}
& \frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0})(x - \frac{p_1}{p_0}) + \frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0})(y - \frac{p_2}{p_0}) = \\
= \; & x\frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) + y\frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) - \left(\frac{p_1}{p_0}\frac{\partial f}{\partial x}(\frac{p_1}{p_0}, \frac{p_2}{p_0}) + \frac{p_2}{p_0}\frac{\partial f}{\partial y}(\frac{p_1}{p_0}, \frac{p_2}{p_0})\right) = \\
= \; & x\frac{\partial F}{\partial x_1}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) + y\frac{\partial F}{\partial x_2}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) - \left(dF(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) - \frac{\partial F}{\partial x_0}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0})\right) = \\
= \; & \frac{\partial F}{\partial x_0}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) + x\frac{\partial F}{\partial x_1}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) + y\frac{\partial F}{\partial x_2}(1, \frac{p_1}{p_0}, \frac{p_2}{p_0}) = \\
= \; & \frac{1}{p_0^{d-1}}\left(\frac{\partial F}{\partial x_0}(p_0, p_1, p_2) + x\frac{\partial F}{\partial x_1}(p_0, p_1, p_2) + y\frac{\partial F}{\partial x_2}(p_0, p_1, p_2)\right)
\end{aligned}$$

hat (bis auf eine Konstante) die Homogenisierung (vom Grad 1)

$$x_0\frac{\partial F}{\partial x_0}(p_0, p_1, p_2) + x_1\frac{\partial F}{\partial x_1}(p_0, p_1, p_2) + x_2\frac{\partial F}{\partial x_2}(p_0, p_1, p_2).$$

Daher gilt: $P$ ist auf dem affinen Teil der Kurve genau dann singulär, wenn gilt

$$\frac{\partial F}{\partial x_0}(P) = \frac{\partial F}{\partial x_1}(P) = \frac{\partial F}{\partial x_2}(P) = 0.$$

Ist $P$ ein glatter Punkt, so ist der projektive Abschluss der Tangente die Gerade

$$\frac{\partial F}{\partial x_0}(P)x_0 + \frac{\partial F}{\partial x_1}(P)x_1 + \frac{\partial F}{\partial x_2}(P)x_2 = 0.$$

Man definiert nun:

DEFINITION. Ist die projektive ebene Kurve $C$ gegeben durch das Polynom $f(x_0, x_1, x_2)$, so heißt $P \in C(\overline{K})$ ein singulärer Punkt, wenn gilt

$$\frac{\partial f}{\partial x_0}(P) = \frac{\partial f}{\partial x_1}(P) = \frac{\partial f}{\partial x_2}(P) = 0.$$

Im andern Fall heißt $P$ nichtsingulärer oder glatter Punkt, die Gerade

$$\frac{\partial f}{\partial x_0}(P)x_0 + \frac{\partial f}{\partial x_1}(P)x_1 + \frac{\partial f}{\partial x_2}(P)x_2 = 0$$

heißt die Tangente an $C$ in $P$.

Mit der vorangegangenen lokalen Betrachtung sieht man, dass man Singularitäten in affinen Teilen untersuchen kann. Natürlich muss man sich überlegen, dass diese Begriffe mit Koordinatenwechsel verträglich sind.

Wir wollen jetzt noch Schnitte von Kurven mit Geraden in $\mathbf{P}^2$ betrachten. Die Schnittvielfachkeit $(C\cdot G)_P$ in einem Punkt wird lokal definiert, indem man den Punkt in einem affinen Teil anschaut.

SATZ. *Sei $G$ eine Gerade, $C$ eine Kurve vom Grad $d$ in $\mathbf{P}^2$ mit $G(\overline{K}) \not\subseteq C(\overline{K})$. Dann gilt*

$$\sum_{P\in C(\overline{K})\cap G(\overline{K})} (C\cdot G)_P = d,$$

*d.h. $C$ schneidet $G$ in genau $d$ Punkten, wenn man mit Multiplizitäten zählt.*

*Beweis:* $C$ sei durch das Polynom $f(x_0,x_1,x_2)$ gegeben, nach Koordinatenwechsel können wir die Gerade $G$ in der Gestalt $x_2=\alpha x_0+\beta x_1$ annehmen. Dann wird

$$f(x_0,x_1,\alpha x_0+\beta x_1) = cx_0^{n_0}\prod_i (x_1-\alpha_i x_0)^{n_i} \quad \text{mit} \quad \sum_i n_i = d.$$

Ist $n_0>0$, so ist $(0:1:\beta)$ ein Schnittpunkt mit Schnittmultiplizität $n_0$. (Im affinen Teil $x_1=1$ mit den affinen Koordinaten $u=x_0, v=x_2$ lautet die Kurvengleichung $f(u,1,v)$, die parametrisierte Geradengleichung $u=t$, $v=\alpha t+\beta$ und

$$f(t,1,\alpha t+\beta) = ct^{n_0}\prod_i (1-\alpha_i t)^{n_i},$$

sodass die Schnittmultiplizität $n_0$ ist.) Die anderen Schnittpunkte liegen im affinen Teil $x_0=1$. Wählt man affine Koordinaten $x_1=x$, $x_2=y$, so lautet die Kurvengleichung $f(1,x,y)$ und die parametrisierte Geradengleichung $x=t$, $y=\alpha+\beta t$. Einsetzen in die Kurvengleichung ergibt

$$f(1,t,\alpha+\beta t) = c\prod_i (t-\alpha_i)^{n_i}.$$

Daraus sieht man sofort, dass $(x,y)=(\alpha_i,\alpha+\beta\alpha_i)\simeq(1:\alpha_i:\alpha+\beta\alpha_i)$ ein Schnittpunkt mit Multiplizität $n_i$ ist. ■

**Beispiel:** Wir betrachten die ebene Kurve $C$ mit der affinen Gleichung $y=x^2$ bzw. der projektiven Gleichung $f=x_0x_2-x_1^2=0$. Wir wollen den Schnitt mit den Geraden der Form $x=c$ bzw. $x_1=cx_0$ bestimmen. Einsetzen ergibt

$$f(x_0,cx_0,x_2) = x_0x_2-c^2x_0^2 = x_0(x_2-c^2x_0).$$

Es gibt genau zwei Schnittpunkte, nämlich

$$(1:c:c^2)\simeq(c,c^2) \quad \text{und} \quad (0:0:1),$$

beide mit Schnittmultiplizität 1.

**Bemerkung:** Der Satz ist ein Spezialfall des Satzes von Bézout, der besagt, dass sich ebene projektive Kurven $C$ und $D$ in genau $\mathrm{grad}C\cdot\mathrm{grad}D$ Punkten schneiden, wenn man mit Multiplizitäten zählt und wenn es nur endlich viele Schnittpunkte gibt.

Für die Wendepunkte erhalten wir folgenden Satz:

SATZ. *(Die Charakteristik von $K$ sei 0.) Sei $C=\{f(x_0,x_1,x_2)=0\}$ eine ebene Kurve, definiert durch ein Polynom $f(x_0,x_1,x_2)$. Ist*

$$H(f) = \det\left(\frac{\partial^2 f}{\partial x_i\partial x_j}\right)_{0\le i,j\le 2},$$

*so definiert das Polynom $H(f)$ die sogenannte Hessesche Kurve $H_C$ zu $C$. Ist $P$ ein glatter Punkt von $C$, so ist $P$ genau dann ein Wendepunkt, wenn $P\in H_C(\overline{K})$ gilt.*

Natürlich muss man zeigen, dass die Hessesche Kurve unabhängig vom Koordinatensystem definiert ist.

KAPITEL 3

# Geometrische Addition auf ebenen Kubiken

## 1. Eine geometrisch definierte Verknüpfung auf nichtsingulären ebenen Kubiken

Eine über einem Körper $K$ definierte ebene projektive Kubik $C$ wird gegeben durch ein homogenes Polynom

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + a_3x_0x_1^2 + a_4x_0x_1x_2 + a_5x_0x_2^2 + a_6x_1^3 + a_7x_1^2x_2 + a_8x_1x_2^2 + a_9x_2^3$$

mit $a_0, \ldots, a_9 \in K$. (Mitunter gibt man auch nur eine affine Darstellung $f(1, x, y) = a_0 + a_1x + a_2y + \cdots + a_9y^3$ an.)

LEMMA. *Eine nichtsinguläre ebene projektive Kubik ist absolut irreduzibel.*

*Beweis:* Sei $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ das die Kubik beschreibene Polynom. Wäre die Kubik reduzibel über $\overline{K}$, so gäbe es Polynome

$$g = g_0x_0 + g_1x_1 + g_2x_2 \quad \text{und} \quad q = q_0x_0^2 + q_1x_0x_1 + q_2x_0x_2 + q_3x_1^2 + q_4x_1x_2 + q_5x_2^2$$

mit $g_0, g_1, g_2, q_0, q_1, \ldots, q_5 \in \overline{K}$. Ist $P$ ein Punkt im Durchschnitt der Geraden $g = 0$ und der Quadrik $q = 0$, den es nach unseren Überlegungen immer gibt, macht man einen Koordinantenwechsel, sodass $P = (1 : 0 : 0)$ gilt, so folgt

$$\begin{aligned} f(1, x, y) &= g(1, x, y)q(1, x, y) = (g_1x + g_2y)(q_1x + q_2y + q_3x^2 + q_4xy + q_5y^2) = \\ &= g_1q_1x^2 + (g_1q_2 + g_2q_1)xy + g_2q_2y^2 + \ldots, \end{aligned}$$

insbesondere ist $P$ ein singulärer Punkt von $C$, ein Widerspruch zur Voraussetzung. Daher ist die Annahme falsch, $f(x_0, x_1, x_2)$ ist absolut irreduzibel. ■

**Bemerkung:** Allgemein kann man zeigen, dass jede nichtsinguläre ebene projektive Kurve absolut irreduzibel ist. Für affine Kurven gilt das nicht, wie man beispielsweise an $f = x(x - 1)$ sehen kann.

Ist $C$ eine nichtsinguläre ebene projektive Kubik und $G$ eine Gerade, so schneidet $C$ die Gerade $G$ in genau drei Punkten $P, Q, R \in \mathbf{P}^2$, wenn man mit Vielfachheiten zählt. Wir schreiben dann auch

$$C \cdot G = P + Q + R.$$

Wir werden jetzt damit eine Abbildung $\varphi : C(K) \times C(K) \to C(K)$ mit $\varphi(P, Q) = R$ konstruieren.

**Die Verknüpfung $\varphi : C(K) \times C(K) \to C(K)$:** Sei $C$ eine nichtsinguläre ebene projektive Kubik, gegeben durch ein Polynom homogenes kubisches Polynom $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$. Seien $P = (p_0 : p_1 : p_2), Q = (q_0 : q_1 : q_2) \in C(K)$, o.E. $p_0, p_1, p_2, q_0, q_1, q_2 \in K$.

- Ist $P \neq Q$, d.h. $p_0q_1 \neq p_1q_0$ oder $p_0q_2 \neq p_2q_0$ oder $p_1q_2 \neq p_2q_1$, so wird die Gerade $G$ durch $P$ und $Q$

  $$G = \{(p_0u + q_0v : p_1u + q_1v : p_2u + q_2v) \in \mathbf{P}^2 : (u : v) \in \mathbf{P}^1\}.$$

  Einsetzen der angegebenen Parametrisierung in $f(x_0, x_1, x_2)$ ergibt

  $$g(u, v) = f(p_0u + q_0v, p_1u + q_1v, p_2u + q_2v) \in K[u, v].$$

  Wegen $g(0, v) = v^3f(q_0, q_1, q_2) = 0$ und $g(u, 0) = u^3f(p_0, p_1, p_2)$ erhalten wir

  $$g(u, v) = f(p_0u + q_0v, p_1u + q_1v, p_2u + q_2v) = uv(c_uu + c_vv) \quad \text{mit} \quad c_u, c_v \in K.$$

Dann liefert $(u:v)=(c_v:-c_u)$ den 3. Schnittpunkt der Geraden mit der Kurve $C$, also

$$R=(p_0c_v-q_0c_u:p_1c_v-q_1c_u:p_2c_v-q_2c_u)\in C(K).$$

- Ist $P=Q$, so schneidet die Tangente $T$ an $C$ in $P$ die Kurve $C$ in $P$ mindestens zweifach. Die Tangentengleichung lautet

$$f_0x_0+f_1x_1+f_2x_2=0$$

mit

$$f_0=\frac{\partial f}{\partial x_0}(p_0,p_1,p_2),\quad f_1=\frac{\partial f}{\partial x_1}(p_0,p_1,p_2),\quad f_2=\frac{\partial f}{\partial x_2}(p_0,p_1,p_2).$$

Ist $p_0\neq 0$, so ist $(f_1,f_2)\neq(0,0)$ wegen $f_0p_0+f_1p_1+f_2p_2=0$ und $(f_0,f_1,f_2)\neq(0,0,0)$. Also ist $\widetilde{P}=(0:f_2:-f_1)$ ein von $P$ verschiedener Punkt der Tangente. Wählt man im Allgemeinfall ein $\widetilde{P}$ mit

$$\widetilde{P}=(\widetilde{p}_0:\widetilde{p}_1:\widetilde{p}_2)=\begin{cases}(0:f_2:-f_1) & \text{im Fall } p_0\neq 0,\\ (f_2:0:-f_0) & \text{im Fall } p_1\neq 0,\\ (f_1:-f_0:0) & \text{im Fall } p_0\neq 0,\end{cases}$$

so ist $\widetilde{P}$ ein von $P$ verschiedener Punkt der Tangente. Die Tangente hat dann die Parametrisierung

$$x_0=p_0u+\widetilde{p}_0v,\quad x_1=p_1u+\widetilde{p}_1v,\quad x_2=p_2u+\widetilde{p}_2v.$$

Einsetzen in $f(x_0,x_1,x_2)$ liefert

$$g(u,v)=f(p_0u+\widetilde{p}_0v,p_1u+\widetilde{p}_1v,p_2u+\widetilde{p}_2v)\in K[u,v].$$

Für $v=0$ ergibt sich der Punkt $P$. Da die Schnittmultiplizität hier $\geq 2$ ist, erhält man die Darstellung

$$g(u,v)=v^2(c_uu+c_vv)\quad\text{mit}\quad c_u,c_v\in K.$$

Dann liefert $(u:v)=(c_v:-c_u)$ den weiteren Schnittpunkt der Tangenten mit der Kurve:

$$R=(p_0c_v-\widetilde{p}_0c_u:p_1c_v-\widetilde{p}_1c_u:p_2c_v-\widetilde{p}_2c_u)\in C(K).$$

- Wir definieren nun $\varphi(P,Q)=R$ und erhalten damit eine Abbildung $\varphi: C(K)\times C(K)\to C(K)$.
- Ist $L$ ein Oberkörper von $K$, so ist natürlich $C$ auch über $L$ definiert. Also erhalten wir ebenso eine Abbildung

$$C(L)\times C(L)\to C(L),\quad (P,Q)\mapsto\varphi(P,Q).$$

**Bemerkungen:**

(1) Sind $P,Q\in C(K)$, so gibt es also eine Gerade $G$, die $C$ (richtig gezählt) in $P$, $Q$ und $\varphi(P,Q)$ schneidet:

$$G\cdot C=P+Q+\varphi(P,Q).$$

(2) Die angegebene Konstruktion von $\varphi$ ist so explizit, dass man dazu leicht ein Maple-Programm schreiben kann. Damit wurden die nachfolgenden Beispiele gerechnet.

**Beispiele:** Wir betrachten $C$ über $\mathbf{Q}$ mit

$$f=+690x_0^3-1101x_0^2x_1+98x_0^2x_2+369x_0x_1^2-70x_0x_1x_2-56x_0x_2^2+42x_1^2x_2+28x_1x_2^2$$

und den Punkten

$$P_1=(1:1:1),\quad P_2=(2:3:5),\quad P_3=(7:11:13).$$

Dann findet man

$$\begin{aligned}\varphi(P_1,P_1) &= (170772:309106:3342573),\\ \varphi(P_1,P_2) &= (21:-10:-72),\\ \varphi(P_1,P_3) &= (12:-38:-63),\\ \varphi(P_2,P_2) &= (2943570:7080290:-41523597),\\ \varphi(P_2,P_3) &= (45:122:-378),\\ \varphi(P_3,P_3) &= (226415420:655306190:-1297615533).\end{aligned}$$

**Beispiel:** Wir betrachten $f = x^3 + 2y^3 + 3z^3$ und $P_1 = (1 : 1 : -1) \in C(\mathbf{Q})$. Wir berechnen rekursiv

$$\begin{aligned}
P_2 = \varphi(P_1, P_1) &= (5 : -4 : 1),\\
P_3 = \varphi(P_2, P_2) &= (655 : -488 : -253),\\
P_4 = \varphi(P_3, P_3) &= (120418942015 : -160841972528 : 129900299507),\\
P_5 = \varphi(P_4, P_4) &= (1793984047837470883062951691301324725262602495 :\\
&\quad 7768161632610794601560668923553327607916253 12 :\\
&\quad -1307858335918621966586468212651205223746821453),\\
\varphi(P_1, P_3) &= (26309 : 3449 : -18269),\\
\varphi(P_2, P_4) &= (483407899445154725 : -125896480637499244 : -331181768668393439).
\end{aligned}$$

**Beispiel:** Wir betrachten die Kurve $C$ mit der affinen Gleichung $y^2 = x^3 - 2$. Projektiv wird $C$ beschrieben durch $f = x_0x_2^2 - x_1^3 + 2x_0^3$. Man sieht sofort $P_1 = (1 : 3 : 5) \in C(\mathbf{Q})$. Rekursiv findet man

$$\begin{aligned}
P_2 = \varphi(P_1, P_1) &= (1000 : 1290 : 383),\\
P_3 = \varphi(P_2, P_2) &= (449455096000 : 17931469268460 : 113259286337279),\\
P_4 = \varphi(P_3, P_3) &= (5223934923525719974563641453744978655831227509874752000 :\\
&\quad 5211832184344999670739436225745738739162239573438365188 0 :\\
&\quad -1644557217519796256439143766866676956618981555872010593281),\\
\varphi(P_1, P_3) &= (2029190552145716973931 : 3890813344569928273593 : -4559771683571581358275).
\end{aligned}$$

**Beispiel:** Wir betrachten $C$ mit der Gleichung $f = x_0^3 + 2x_1^3 + 3x_2^3$ über $K = \mathbf{F}_5$. Durch Ausprobieren findet man

$$C(\mathbf{F}_5) = \{(1 : 0 : 2), (1 : 1 : 4), (1 : 2 : 1), (1 : 3 : 0), (1 : 4 : 3), (0 : 1 : 1)\}.$$

Bezeichnet man die Punkte in der angegebenen Reihenfolge mit $P_1, \ldots, P_6$, so erhält man $\varphi(P_i, P_j) = P_k$ mit

| | $j=1$ | $j=2$ | $j=3$ | $j=4$ | $j=5$ | $j=6$ |
|---|---|---|---|---|---|---|
| $i=1$ | $k=1$ | $k=3$ | $k=2$ | $k=6$ | $k=5$ | $k=4$ |
| $i=2$ | $k=3$ | $k=6$ | $k=1$ | $k=5$ | $k=4$ | $k=2$ |
| $i=3$ | $k=2$ | $k=1$ | $k=4$ | $k=3$ | $k=6$ | $k=5$ |
| $i=4$ | $k=6$ | $k=5$ | $k=3$ | $k=4$ | $k=2$ | $k=1$ |
| $i=5$ | $k=5$ | $k=4$ | $k=6$ | $k=2$ | $k=1$ | $k=3$ |
| $i=6$ | $k=4$ | $k=2$ | $k=5$ | $k=1$ | $k=3$ | $k=6$ |

**Formeln für $\varphi$:** Rechnet man mit Unbestimmten Koeffizienten $a_0, \ldots, a_9$, $p_0, p_1, p_2$, $q_0, q_1, q_2$, so erhält man im Fall $P \neq Q$ die Größen $c_u$ und $c_v$ aus

$$uv(c_uu + c_vv) = f(p_0u + q_0v, p_1u + q_1v, p_2u + q_2v) = a_0(p_0u + q_0v)^3 + a_1(p_0u + q_0v)^2(p_1u + q_1v) + \ldots$$

durch Koeffizientenvergleich (bei $u^2v$ bzw. $uv^2$). Explizit erhält man für $c_u$ und $c_v$:

```
c_u := 3*a6*p1^2*q1+a1*p0^2*q1+a7*p1^2*q2+a5*q0*p2^2+a2*p0^2*q2+3*a0*p0^2*q0+
a8*q1*p2^2+a3*q0*p1^2+3*q2*p2^2*a9+2*a5*p0*p2*q2+a4*p0*p1*q2+a4*p0*q1*p2+2*a3*
p0*p1*q1+2*a7*p1*q1*p2+2*a1*p0*q0*p1+2*a2*p0*q0*p2+2*a8*p1*p2*q2+a4*q0*p1*p2;
c_v := a2*q0^2*p2+a1*q0^2*p1+a3*p0*q1^2+3*a6*p1*q1^2+a7*q1^2*p2+3*q2^2*p2*a9+
a8*p1*q2^2+3*a0*p0*q0^2+2*a7*p1*q1*q2+2*a5*q0*p2*q2+2*a2*p0*q0*q2+2*a8*q1*p2*
q2+2*a3*q0*p1*q1+a4*p0*q1*q2+2*a1*p0*q0*q1+a4*q0*p1*q2+a4*q0*q1*p2+a5*p0*q2^2;
```

Mit $r_0 = p_0c_v - q_0c_u$, $r_1 = p_1c_v - q_1c_u$, $r_2 = p_2c_v - q_2c_u$ erhält man

```
r0 := -p0*a1*q0^2*p1-3*q0*q2*p2^2*a9-q0*a8*q1*p2^2-a5*q0^2*p2^2-a3*q0^2*p1^2-2
*q0*a8*p1*p2*q2-a4*q0^2*p1*p2-3*q0*a6*p1^2*q1-q0*a7*p1^2*q2-p0*a2*q0^2*p2-2*q0
*a7*p1*q1*p2+a1*p0^2*q0*q1+a4*p0^2*q1*q2+2*p0*a7*p1*q1*q2+3*p0*a6*p1*q1^2+p0*
a7*q1^2*p2+3*p0*q2^2*p2*a9+p0*a8*p1*q2^2+a2*p0^2*q0*q2+a3*p0^2*q1^2+a5*p0^2*q2
^2+2*p0*a8*q1*p2*q2;
r1 := p1*a2*q0^2*p2+2*p1*a5*q0*p2*q2+2*p1*a2*p0*q0*q2+a3*q0*p1^2*q1+a4*q0*p1^2
```

```
*q2-2*q1*a5*p0*p2*q2-2*q1*a2*p0*q0*p2+a8*p1^2*q2^2-a1*p0^2*q1^2+3*p1*q2^2*p2*
a9+3*p1*a0*p0*q0^2-p1*a3*p0*q1^2-p1*a7*q1^2*p2+a1*q0^2*p1^2+a7*p1^2*q1*q2+p1*
a5*p0*q2^2-a4*p0*q1^2*p2-q1*a5*q0*p2^2-q1*a2*p0^2*q2-3*q1*a0*p0^2*q0-3*q1*q2*
p2^2*a9-a8*q1^2*p2^2;
r2 := -3*q2*a6*p1^2*q1-q2*a1*p0^2*q1-3*q2*a0*p0^2*q0-q2*a3*q0*p1^2+a4*q0*q1*p2
^2+p2*a1*q0^2*p1+p2*a3*p0*q1^2+3*p2*a6*p1*q1^2-p2*a8*p1*q2^2+3*p2*a0*p0*q0^2-
a4*p0*p1*q2^2+2*p2*a1*p0*q0*q1+a8*q1*p2^2*q2+a2*q0^2*p2^2+a7*q1^2*p2^2-2*q2*a3
*p0*p1*q1-2*q2*a1*p0*q0*p1-p2*a5*p0*q2^2-a7*p1^2*q2^2+2*p2*a3*q0*p1*q1+a5*q0*
p2^2*q2-a2*p0^2*q2^2;
```

Also gilt $\varphi((p_0 : p_1 : p_2), (q_0 : q_1 : q_2)) = (r_0 : r_1 : r_2)$ mit obigen Formeln für $r_0, r_1, r_2$. Im Fall $P = Q$ erhält man durch Unterscheiden der Fälle $p_0 \neq 0$, $p_1 \neq 0$, $p_2 \neq 0$ analog Formeln für $\varphi(P, P)$. Diese sind allerdings etwas länglich, sodass wir auf deren Wiedergabe hier verzichten.

**Formeln für $\varphi$ im Fall $f = Ax_0^3 + Bx_1^3 + Cx_2^3$:** Man sieht leicht, dass die durch $f = Ax_0^3 + Bx_1^3 + Cx_2^3$ definierte Kurve genau dann singulär ist, wenn im Grundkörper $3ABC = 0$ gilt. Die Formeln für $\varphi$ haben nun eine deutlich einfachere Gestalt: Im Fall $P \neq Q$ erhalten wir

$$\begin{aligned} r_0 &= 3p_1q_1(p_0q_1 - p_1q_0)B + 3p_2q_2(p_0q_2 - p_2q_0)C, \\ r_1 &= 3p_2q_2(p_1q_2 - q_1p_2)C + 3p_0q_0(p_1q_0 - p_0q_1)A, \\ r_2 &= 3p_0q_0(p_2q_0 - p_0q_2)A + 3p_1q_1(p_2q_1 - p_1q_2)B, \end{aligned}$$

Der Fall $P = Q$, $p_0 \neq 0$

$$\begin{aligned} r_0 &= -27p_0BC(Bp_1^3 + Cp_2^3)(Bp_1^3 - Cp_2^3) = -27p_0BC \cdot (-Ap_0^3)(Bp_1^3 - Cp_2^3), \\ r_1 &= -27p_1BC(Bp_1^3 + Cp_2^3)(Bp_1^3 + 2Cp_2^3) = -27p_1BC \cdot (-Ap_0^3)(Cp_2^3 - Ap_0^3), \\ r_2 &= 27p_2BC(Bp_1^3 + Cp_2^3)(2B_1^3 + Cp_2^3) = -27p_2BC \cdot (-Ap_0^3)(Ap_0^3 - Bp_1^3) \end{aligned}$$

und damit

$$R = \varphi(P, P) = (r_0 : r_1 : r_2) = (p_0(Bp_1^3 - Cp_2^3) : p_1(Cp_2^3 - Ap_0^3) : p_2(Ap_0^3 - Bp_1^3)).$$

Man sieht schnell, dass diese Formeln allgemein im Fall $P = Q$ gelten.

**Eigenschaften von $\varphi$:**

(1) Offensichtlich ist $\varphi(P, Q) = \varphi(Q, P)$.
(2) Gilt $\varphi(P_1, P_2) = P_3$, so gibt es eine Gerade $G$ mit $G \cdot C = P_1 + P_2 + P_3$, was auch die anderen Gleichungen
$$\varphi(P_1, P_3) = P_2 \quad \text{und} \quad \varphi(P_2, P_3) = P_1$$
impliziert.
(3) Aus der letzten Eigenschaft folgt sofort
$$\varphi(P, \varphi(P, Q)) = Q.$$

**Bemerkung:** Kann $\varphi$ eine Gruppenstruktur auf $C(K)$ definieren? Angenommen, dies wäre der Fall. Aus $\varphi(P, \varphi(P, P)) = P$ würde folgen, dass $\varphi(P, P)$ das neutrale Element $O$ der Gruppe wäre, für alle $P \in C(K)$. D.h. jede Tangente an einen Punkt $P \in C(K)$ ginge durch $O$. Dass dies im Allgemeinen nicht der Fall ist, sieht man durch Betrachten obiger Beispiele. Also definiert $\varphi$ im Allgemeinen keine Gruppenstruktur.

## 2. Einführung einer Gruppenstruktur

Sei $C$ eine nichtsinguläre ebene Kubik, definiert über einem Körper $K$ und $O \in C(K)$ ein Punkt der Kurve. Wir definieren eine Verknüpfung $\oplus : C(K) \times C(K) \to C(K)$ durch

$$P \oplus Q = \varphi(\varphi(P, Q), O).$$

Satz. *Ist $C$ eine nichtsinguläre ebene projektive Kubik über einem Körper $K$ und $O \in C(K)$, so ist $(C(K), \oplus)$ eine abelsche Gruppe mit neutralem Element $O$. (Invers zu $P$ ist $\varphi(P, \varphi(O, O))$.)*

*Beweisskizze:*

(1) Die Kommutativität $P \oplus Q = Q \oplus P$ ist klar.
(2) Die Eigenschaft $\varphi(P, \varphi(P, Q)) = Q$ impliziert
$$P \oplus O = \varphi(\varphi(P, O), O) = \varphi(O, \varphi(O, P)) = P,$$
d.h. $O$ ist das neutrale Element der Gruppenstruktur.
(3) Wieder folgt mit der Eigenschaft $\varphi(P, \varphi(P, Q) = Q$
$$P \oplus \varphi(P, \varphi(O, O)) = \varphi(\varphi(P, \varphi(P, \varphi(O, O))), O) = \varphi(\varphi(O, O), O) = O,$$
d.h. $\varphi(P, \varphi(O, O))$ ist invers zu $P$.
(4) Wir wollen die Assoziativität $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ zeigen. Wir wählen Geraden $L_1$, $L_2$, $L_3$, $M_1$, $M_2$, $M_3$, sodass wir erhalten:
$$L_1 \cdot C = P + Q + S', \quad M_1 \cdot C = O + S' + S, \quad L_2 \cdot C = S + R + T',$$
$$M_2 \cdot C = Q + R + U', \quad L_3 \cdot C = O + U' + U, \quad M_3 \cdot C = P + U + T''.$$
Dann ist $P \oplus Q = S$, $Q \oplus R = U$ und
$$(P \oplus Q) \oplus R = S \oplus R = \varphi(T', O), \quad P \oplus (Q \oplus R) = P \oplus U = \varphi(T'', O).$$
Es genügt also zu zeigen, dass $T' = T''$ gilt. Ist $L_i = \{\ell_i = 0\}$ und $M_i = \{m_i = 0\}$, so schneidet die Kubik $\ell_1\ell_2\ell_3 = 0$ die Kurve $C$ richtig gezählt in den 9 Punkten $P, Q, S', S, R, T', O, U', U$, die Kubik $m_1m_2m_3 = 0$ die Kurve $C$ in den Punkten $O, S', S, Q, R, U', P, U, T''$. Acht Punkte sind also gemeinsam. Nun kann man zeigen, dass auch der neunte gleich sein muss, d.h. $T' = T''$. Wir werden dies aber hier nicht tun, da wir die Behauptung noch auf andere Weise zeigen werden. Ein Beweis findet sich bei W. Fulton, Algebraic Curves, Benjamin 1969. ■

**Beispiel:** Die Kurve $C$, die durch $x_0^3 = x_1^3 + x_2^3$ definiert wird, die wir auch affin durch $x^3 + y^3 = 1$ beschreiben, ist nichtsingulär, falls die Charakteristik von $K$ von 3 verschieden ist. In Charakteristik 3 ist $C$ die dreifach gezählte Gerade $x_0 = x_1 + x_2$.

(1) Durch Probieren findet man folgende Punkte auf $C$:
$$(1 : 1 : 0) \simeq (1, 0), \quad (1 : 0 : 1) \simeq (0, 1), \quad (0 : 1 : -1).$$
Tatsächlich kann man zeigen, dass für $K = \mathbf{Q}$ gilt
$$C(\mathbf{Q}) = \{((1, 0), (0, 1), (0 : 1 : -1)\},$$
also ist $C(\mathbf{Q})$ eine zyklische Gruppe der Ordnung 3.
(2) Wir betrachten $C$ über $K = \mathbf{F}_7$. Durch Ausprobieren findet man
$$C(\mathbf{F}_7) = \{(0 : 1 : 3), (0 : 1 : 5), (0 : 1 : 6), (0, 1), (0, 2), (0, 4), (1, 0), (2, 0), (4, 0)\}.$$
Als Nullpunkt wählen wir $O = (1, 0)$. Als abelsche Gruppe mit 9 Elementen ist $C(\mathbf{F}_7)$ also isomorph zu $\mathbf{Z}/(9)$ oder $\mathbf{Z}/(3) \oplus \mathbf{Z}/(3)$.
Die Tangente in $(0, 1)$ ist $y = 1$, sie schneidet $C$ dreifach in $(0, 1)$, also
$$\varphi((0, 1), (0, 1)) = (0, 1).$$
Die Verbindungsgerade von $(0, 1)$ und $(1, 0)$ ist $y = -x+1$ bzw. projektiv $x_2 = x_0 - x_1$, eingesetzt in $x_0^3 - x_1^3 - x_2^3$ ergibt dies
$$3x_0x_1(x_0 - x_1),$$
die drei Schnittpunkte mit $C$ sind also
$$(0 : 1 : -1), \quad (1 : 0 : 1) \simeq (0, 1), \quad (1 : 1 : 0) \simeq (1, 0),$$
d.h. $\varphi((0, 1), (1, 0)) = (0 : 1 : -1)$ und damit
$$(0, 1) \oplus (0, 1) = \varphi(\varphi((0, 1), (0, 1)), (1, 0)) = \varphi((0, 1), (1, 0)) = (0 : 1 : -1).$$
Weiter erhält man damit
$$(0, 1) \oplus (0 : 1 : -1) = \varphi(\varphi((0, 1), (0 : 1 : -1)), (1, 0)) = \varphi((1, 0), (1, 0)) = (1, 0),$$
d.h. $(0, 1) \oplus (0, 1) \oplus (0, 1) = O$.
Die Tangente in $(0, 2)$ ist $y = 2$, wiederum eine Wendetangente, also $\varphi((0, 2), (0, 2)) = (0, 2)$.

Die Verbindungsgerade von $(0,2)$ und $(1,0)$ ist $y = -2x + 2$ bzw. $x_2 = 2x_0 - 2x_1$, die drei Schnittpunkte mit $C$

$$(0:1:5), \quad (0,2), \quad (1,0),$$

also

$$(0,2) \oplus (0,2) = (0:1:5).$$

Damit erhält man

$$(0,2) \oplus (0:1:5) = \varphi((1,0),(1,0)) = (1,0),$$

d.h. $(0,2) \oplus (0,2) \oplus (0,2) = O$. Da $(0,2)$ nicht in der von $(0,1)$ erzeugten Untergruppe liegt, folgt

$$C(\mathbf{F}_7) \simeq \mathbf{Z}/(3) \oplus \mathbf{Z}/(3).$$

(3) Wir betrachten nun $C(\mathbf{F}_p)$ für $p \neq 3$. Durch Probieren findet man

| $p$ | 2 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\#C(\mathbf{F}_p)$ | 3 | 6 | 9 | 12 | 9 | 18 | 27 | 24 | 30 | 36 | 27 | 42 | 36 | 48 | 54 | 60 |

Was fällt auf?

(a) Es gilt $\#C(\mathbf{F}_p) \equiv 0 \bmod 3$. Dies erklärt sich leicht daraus, dass

$$\{((1,0),(0,1),(0:1:-1)\}$$

eine Untergruppe von $C(\mathbf{F}_p)$ ist.

(b) Für $p \equiv 2 \bmod 3$ gilt $\#C(\mathbf{F}_p) = p + 1$.
*Beweis:* $\mathbf{F}_p^*$ ist eine zyklische Gruppe der Ordnung $p-1$, die keine Untergruppe der Ordnung 3 enthält. Daher ist der Gruppenhomomorphismus $\mathbf{F}_p^* \xrightarrow{x \mapsto x^3} \mathbf{F}_p^*$ injektiv, also auch surjektiv. Insbesondere ist

$$\mathbf{F}_p \to \mathbf{F}_p, \quad x \mapsto x^3$$

bijektiv. Zu jedem $y \in \mathbf{F}_p$ gibt es also genau ein $x \in \mathbf{F}_p$ mit $x^3 = 1 - y^3$, d.h. $\{(x,y) \in \mathbf{A}^2(\mathbf{F}_p) : x^3 + y^3 = 1\}$ hat genau $p$ Elemente. Weiter gibt es genau ein $z \in \mathbf{F}_p$ mit $1 + z^3 = 0$, nämlich $z = -1$, d.h. $(0:1:-1)$ ist der einzige Punkt in $C(\mathbf{F}_p)$ mit $x_0 = 0$, woraus schließlich folgt $\#C(\mathbf{F}_p) = p + 1$.

(c) Wir betrachten nun den Fall $p \equiv 1 \bmod 3$. Numerisch findet man:

| $p$ | 7 | 13 | 19 | 31 | 37 | 43 | 61 | 67 | 73 | 79 | 97 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\frac{\#C(\mathbf{F}_p)-(p+1)}{\sqrt{p}}$ | 0.38 | -1.39 | 1.61 | 0.72 | -1.81 | -1.22 | 0.13 | -0.61 | 0.82 | -1.91 | 1.93 |

Gilt $|\#C(\mathbf{F}_p) - (p+1)| \leq 2\sqrt{p}$?

**Problem:** Sei $C$ eine über $K$ definierte nichtsinguläre ebene Kubik. Kann man feststellen, ob $C(K) \neq \emptyset$ gilt? Ist $C(K) \neq \emptyset$, so können wir durch Wahl eines Punktes $O \in C(K)$ die Menge $C(K)$ zu einer Gruppe machen. Wir geben zwei Resultate an:

(1) Wir werden später sehen, dass für endliche Körper $K = \mathbf{F}_q$ immer $C(K) \neq \emptyset$ gilt.
(2) Die Kurve $C = \{3x_0^3 + 4x_1^3 + 5x_2^3 = 0\}$ gibt ein Beispiel, für das $C(\mathbf{Q}) = \emptyset$ gilt.

Der folgende Satz besagt, dass die Struktur von $C(K)$ als abstrakte Gruppe nicht von der Auswahl des Punktes $O \in C$ abhängt.

Satz. *Sei $C$ eine über $K$ definierte nichtsinguläre ebene Kubik und $O, O' \in C(K)$. Dann definieren*

$$\begin{aligned} P \oplus Q &= \varphi(\varphi(P,Q),O) \\ P \oplus' Q &= \varphi(\varphi(P,Q),O') \end{aligned}$$

*Gruppenstrukturen auf $C(K)$ mit neutralem Element $O$ bzw. $O'$. Die Abbildung*

$$\lambda : C(K) \to C(K), \quad P \mapsto P \oplus O' = \varphi(\varphi(P,O'),O)$$

*definiert einen Gruppenisomorphismus, d.h.*

$$\lambda(P \oplus Q) = \lambda(P) \oplus' \lambda(Q) \quad \text{und} \quad \lambda(O) = O'.$$

*Beweis:*

(1) Wir definieren $\mu : C(K) \to C(K)$ durch $\mu(P) = P \oplus' O = \varphi(\varphi(P, O'), O)$. Für $P \in C(K)$ gilt $\lambda(P) = P \oplus O' = \varphi(\varphi(P, O'), O)$, was die Gleichung $\varphi(\lambda(P), O) = \varphi(P, O')$ liefert. Es folgt

$$P = \varphi(\varphi(\lambda(P), O), O') = \lambda(P) \oplus' O = \mu(\lambda(P)),$$

also $\mu \circ \lambda = \mathrm{id}_{C(K)}$. Analog folgt $\lambda \circ \mu = \mathrm{id}_{C(K)}$, was die Bijektivität von $\lambda$ beweist.

(2) Es gilt $\lambda(O) = O \oplus O' = O'$, da $O$ neutrales Element bzgl. $\oplus$ ist.

(3) Für $R, S \in C(K)$ folgt aus $R \oplus' S = \varphi(\varphi(R, S), O')$ die Gleichung $\varphi(R \oplus' S, O') = \varphi(R, S)$ und damit

$$(R \oplus' S) \oplus O' = \varphi(\varphi(R \oplus' S, O'), O) = \varphi(\varphi(R, S), O) = R \oplus S.$$

Mit $R = \lambda(P)$, $S = \lambda(Q)$ ergibt sich

$$\begin{aligned}(\lambda(P) \oplus' \lambda(Q)) \oplus O' &= \lambda(P) \oplus \lambda(Q) = (P \oplus O') \oplus (Q \oplus O') = ((P \oplus Q) \oplus O') \oplus O' = \\ &= \lambda(P \oplus Q) \oplus O',\end{aligned}$$

also

$$\lambda(P \oplus Q) = \lambda(P) \oplus' \lambda(Q).$$

Damit ist $\lambda$ auch ein Gruppenhomomorphismus. ■

LEMMA. *Ist $C$ eine nichtsinguläre ebene Kubik und ist der Nullpunkt der Gruppenstruktur $O$ ein Wendepunkt, d.h. $\varphi(O, O) = O$, so gilt:*

(1) *$P \oplus \varphi(P, O) = O$, d.h. der dritte Punkt auf der Geraden durch $P$ und $O$ ist der zu $P$ inverse Punkt.*

(2) *$P \oplus Q \oplus R = O$ gilt genau dann, wenn $R = \varphi(P, Q)$ gilt, d.h. wenn $P, Q, R$ die (richtig gezählten) Schnittpunkte von $C$ mit einer Geraden sind.*

(3) *$P$ ist genau dann ein Wendepunkt dann, wenn $P \oplus P \oplus P = O$ gilt.*

*Beweis:*

(1) $P \oplus \varphi(P, O) = \varphi(\varphi(P, \varphi(P, O)), O) = \varphi(O, O) = O$.

(2) Es gelte $R = \varphi(P, Q)$. Dann folgt mit 1.

$$O = R \oplus \varphi(R, O) = R \oplus \varphi(\varphi(P, Q), O) = R \oplus (P \oplus Q) = P \oplus Q \oplus R.$$

Es gelte nun umgekehrt $P \oplus Q \oplus R = O$. Mit 1. gilt $\varphi(R, O) \oplus R = O$ und daher $P \oplus Q = \varphi(R, O)$, also $\varphi(\varphi(P, Q), O) = \varphi(R, O)$. Dies impliziert $R = \varphi(P, Q)$, wie behauptet.

(3) $P$ ist genau dann ein Wendepunkt, wenn $P = \varphi(P, P)$ gilt. Die Behauptung folgt nun sofort aus 2. ■

**Bemerkung:** Wir werden im Folgenden einfach + statt $\oplus$ schreiben.

## 3. Ein Diffie-Hellman-Schlüsselaustausch mit ebenen Kubiken

Ist $C$ eine nichtsinguläre projektive ebene Kubik, die über einem endlichen Körper $\mathbf{F}_q$ definiert ist, und $O \in C(\mathbf{F}_q)$ ein $\mathbf{F}_q$-rationaler Punkt, so definiert

$$P \oplus Q = \varphi(\varphi(P, Q), O)$$

eine Gruppenstruktur auf $C(K)$ mit $O$ als neutralem Element. Ist $P \in C(\mathbf{F}_q)$ ein Punkt und $k \in \mathbf{N}_0$, so kann man mit der square-and-multiply-Methode schnell $k \cdot P \in C(\mathbf{F}_q)$ berechnen. Zur Erinnerung geben wir den Algorithmus kurz an:

(1) Setze $\ell := k$, $X := P$ und $Y := \begin{cases} O & \text{im Fall } \ell \equiv 0 \bmod 2, \\ P & \text{im Fall } \ell \equiv 1 \bmod 2 \end{cases}$.

(2) Ist $\ell \leq 1$, so gilt $Y = k \cdot P$ und man hört auf.

(3) Setze $\ell := \lfloor \frac{\ell}{2} \rfloor$ und $X := 2 \cdot X = X + X$.

(4) Ist $\ell \equiv 1 \bmod 2$, setze $Y := Y + X$.

(5) Gehe zurück zu Schritt 2.

**Diffie-Hellman-Schlüsselaustausch mit nichtsingulären ebenen projektiven Kubiken:** Man einigt sich auf eine (große) Primzahl $p$, auf eine über $\mathbf{F}_p$ definierte nichtsinguläre ebene projektive Kubik $C$, auf zwei Punkte $O, P \in C(\mathbf{F}_p)$. Durch die Wahl von $O$ wird $C(\mathbf{F}_p)$ zu einer abelschen Gruppe mit neutralem Element $O$. Wollen zwei Teilnehmer $A$ und $B$ einen gemeinsamen Schlüssel vereinbaren, wählen beide geheim zufällige natürliche Zahlen $a$ bzw. $b$ und berechnen $P_A = a \cdot P$ bzw. $P_B = b \cdot P$. Die Punkte $P_A$ und $P_B$ sind die öffentlichen Schlüssel von $A$ und $B$. Der gemeinsame Schlüssel wird $ab \cdot P = a \cdot P_B = b \cdot P_A$.

**Beispiel:** Wir wählen

$p = 47852364786523784652783582764827365 67, \quad f = 7x_0^3 + 9x_1^3 - 2x_2^3, \quad O = (1:1:2), \quad P = (1:3:5).$

$f = 0$ definiert dann eine über $\mathbf{F}_p$ definierte nichtsinguläre Kubik $C$, wobei $O, P \in C(\mathbf{F}_p)$ gilt.

$$\begin{aligned} a &= 1157116440786795754977461575171865783, \\ b &= 34781967937222209195210847359391237 63, \\ a \cdot P &= (1 : 852295116230234362319206474379103249 : 110324652561041098880149102074906 1563), \\ b \cdot P &= (1 : 284068152328947494646419014017652547 0 : 34994803324344526043070145224939 18433), \\ ab \cdot P &= (1 : 315124826187665631254671591109377443 8 : 24552382673688114518109488361554 0668). \end{aligned}$$

Wählt $A$ die Zahl $a$, $B$ die Zahl $b$, so ist $P_A = a \cdot P$ der öffentliche Schlüssel von $A$, $P_B = b \cdot P$ der öffentliche Schlüssel von $B$. Der gemeinsame Schlüssel ist $ab \cdot P = a \cdot P_B = b \cdot P_A$.

## 4. Addition auf singulären Kubiken

Was passiert, wenn $C$ eine singuläre über $K$ definierte Kubik ist?

Ist $C$ reduzibel, so enthält $C(\overline{K})$ eine Gerade, also kann man die geometrische Verknüpfung $\varphi$ nicht sinnvoll definieren.

LEMMA. *Eine absolut irreduzible singuläre ebene projektive Kubik besitzt genau eine Singularität.*

*Beweis:* Nach Voraussetzung hat die Kurve $C$ mindestens einen singulären Punkt. Angenommen, es gäbe zwei Singularitäten $P, Q \in C(\overline{K})$, $P \neq Q$. Sei $G$ die Gerade durch $P$ und $Q$. Da $C$ absolut irreduzibel ist, schneidet $G$ die Kurve $C$ richtig gezählt in genau 3 Punkten. Nun schneidet aber die Gerade in einer Singularität mit Vielfachheit $\geq 2$, was den Widerspruch $3 \geq 2 + 2$ ergibt. Es folgt die Behauptung. ■

Sei $C$ nun eine absolut irreduzible singuläre ebene Kubik mit dem singulären Punkt $S$.

(1) Ist $P \in C(\overline{K})$, $P \neq S$ und $G$ die Gerade durch $P$ und $S$, so gilt $C \cdot G = P + S + S$. Man müsste also setzen $\varphi(P, S) = S$, was aber nicht sehr sinnvoll erscheint. Außerdem ist überhaupt nicht klar, wie man $\varphi(S, S)$ definieren sollte.

(2) Sind $P, Q \in C(\overline{K}) \setminus \{S\}$, ist $G$ die Gerade durch $P$ und $Q$ (bzw. die Tangente im Fall $P = Q$), so gibt es einen Punkt $R \in C(\overline{K})$ mit $C \cdot G = P + Q + R$. Dann muss $R \neq S$ gelten. Setzt man $C_{ns}(\overline{K}) = C(\overline{K}) \setminus \{S\}$, so erhält man also eine geometrisch definierte Verknüpfung

$$\varphi : C_{ns}(\overline{K}) \times C_{ns}(\overline{K}) \to C_{ns}(\overline{K}).$$

Wie im nichtsingulären Fall ergibt sich dann folgender Satz:

SATZ. *Sei $C$ eine über $K$ definierte singuläre absolut irreduzible ebene Kubik und $O \in C_{ns}(K)$. Dann bildet $(C_{ns}(K), O, \oplus)$ mit der Verknüpfung $P \oplus Q = \varphi(\varphi(P, Q), O)$ eine abelsche Gruppe.*

**Frage:** Was kann man über die Gruppenstruktur von $C_{ns}(K)$ sagen?

Wie schauen über $K$ definierte singuläre absolut irreduzible ebene Kubiken aus? Sei $C$ gegeben durch $f(x_0, x_1, x_2) = 0$ und $S$ die einzige Singularität. Wir nehmen an, dass $S \in C(K)$ gilt, was meist der Fall ist. Nach Koordinatenwechsel über $K$ können wir dann $S = (1:0:0) \simeq (0,0)$ annehmen und wird

$$f(1, x, y) = (b_0 x^2 + b_1 xy + b_2 y^2) + (c_0 x^3 + c_1 x^2 y + c_2 xy^2 + c_3 y^3).$$

Man unterscheidet geometrisch zwei Fälle:

(1) Zerfällt $b_0x^2 + b_1xy + b_2y^2$ über $\overline{K}$ in zwei verschiedene Linearfaktoren, so hat $C$ in $S$ einen gewöhnlichen Doppelpunkt.
(2) Ist $b_0x^2 + b_1xy + b_2y^2$ ein Quadrat in $\overline{K}[x, y]$, so hat $C$ in $S$ eine Spitze.

LEMMA. *Sei $C$ eine über $K$ definierte irreduzible singuläre ebene Kubik mit Spitze. Ist die Charakteristik von $K \neq 3$, so ist $C$ über $K$ projektiv äquivalent zu $y^2 = x^3$. Ist $char(K) = 3$, so ist $C$ über $K$ projektiv äquivalent zu $y^2 = x^3$ oder $y^2 = x^3 + x^2y$.*

*Beweis:* Wir nehmen die Bezeichnungen wie oben. Schon in $K[x, y]$ kann man schreiben $b_0x^2 + b_1xy + b_2y^2 = \beta(\gamma x + \delta y)^2$, jedenfalls wenn die Charakteristik $\neq 2$ ist, nach Koordinatenwechsel kann man also

$$f = by^2 + (c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3)$$

annehmen. Hier ist $b \neq 0$ und $c_0 \neq 0$. Substituiert man, $x = -\frac{b}{c_0}x'$ und $y = -\frac{b}{c_0}y'$, so erreicht man

$$f = (x^3 + c_1x^2y + c_2xy^2 + c_3y^3) - y^2.$$

Sei jetzt $char(K) \neq 3$. Durch $x = x' - \frac{1}{3}c_1y$ erreicht man $c_1 = 0$, also

$$f = x^3 + c_2xy^2 + c_3y^3 - y^2 = x^3 - y^2(1 - c_2x - c_3y),$$

woraus man durch $x'_0 = x_0 - c_2x_1 - c_3x_2$ sofort $f = x^3 - y^2$ erhält.
Sei jetzt $char(K) = 3$. Mit der letzten Substitution können wir sofort

$$f = x^3 + c_1x^2y - y^2$$

erreichen. Ist $c_1 = 0$, so haben wir den ersten Fall. Ist $c_1 \neq 0$, so substitutieren wir $x = \frac{1}{c_1^2}x'$, $y = \frac{1}{c_1^3}y'$ und erhalten $f = x^3 + x^2y - y^2$ wie gewünscht. ■

**Bemerkung:** Für $char(K) = 3$ sind die singulären Kubiken $y^2 = x^3$ und $y^2 = x^3 + x^2y$ nicht projektiv äquivalent: Bei der Kurve $y^2 = x^3$ sind alle Tangenten Wendetangenten. Bei der Kurve $y^2 = x^3 + x^2y$ ist $x_0 = 0$ Tangente in $(0 : 0 : 1)$, die die Kurve aber in dem weiteren Punkt $(0 : 1 : -1)$ schneidet.

LEMMA. *Sei $C$ eine über $K$ definierte irreduzible singuläre ebene Kubik mit gewöhnlichem Doppelpunkt. Dann ist $C$ über $\overline{K}$ projektiv äquivalent zu $xy+x^3+y^3 = 0$. Ist $char(K) \neq 2$, so kann man als Normalform auch $y^2 = x^2 + x^3$ nehmen.*

*Beweis:* Nach Koordinatenwechsel über $\overline{K}$ können wir schreiben

$$f = xy + (c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3) = xy(1 + c_1x + c_2y) + c_0x^3 + c_3y^3.$$

Mit $x'_0 = x_0 + c_1x_1 + c_2x_2$ können wir

$$f = xy + c_0x^3 + c_3y^3$$

erreichen. Wir substituieren $x = ux'$, $y = vy'$ und erhalten

$$f = xy + \frac{c_0u^2}{v}x^3 + \frac{c_3v^2}{u}y^3,$$

wählt man $v = c_0u^2$, so erhält man

$$f = xy + x^3 + c_0^2c_3u^3y^3.$$

Wählt man schließlich $u \in \overline{K}$ mit $c_0^2c_3u^3 = 1$, so erhält man $f = xy + x^3 + y^3$. Also sind alle Kubiken mit einem gewöhnlichen Doppelpunkt projektiv äquivalent über $\overline{K}$. Für $char(K) \neq 2$ ist $y^2 = x^2 + x^3$ eine solche, also kann man diese als Normalform nehmen. ■

**Beispiel:** Die Kubik $C$ mit $y^2 = x^3$ bzw. $x_0x_2^2 = x_1^3$ hat genau eine Singularität, nämlich $(1 : 0 : 0) \simeq (0, 0)$. Es gibt nur einen Punkt im Unendlichen, nämlich $(0 : 0 : 1)$. Wir wählen $O = (0 : 0 : 1)$.
Sei $(x, y) \in C_{ns} \setminus \{O\}$. Setzt man $t = \frac{x}{y}$, so wird

$$t^2 = \frac{x^2}{y^2} = \frac{1}{x} \quad \text{und} \quad t^3 = \frac{x^3}{y^3} = \frac{1}{y},$$

d.h. $(x,y)=(\frac{1}{t^2},\frac{1}{t^3})$. Damit ist also

$$C=\{(\frac{1}{t^2},\frac{1}{t^3}),t\in\overline{K}\setminus\{0\}\}\cup\{(0,0),O\}.$$

Nun ist

$$\varphi((\frac{1}{a^2},\frac{1}{a^3}),(\frac{1}{b^2},\frac{1}{b^3}))=(\frac{1}{(a+b)^2},-\frac{1}{(a+b)^3}),$$

denn

$$\begin{vmatrix} 1 & \frac{1}{a^2} & \frac{1}{a^3} \\ 1 & \frac{1}{b^2} & \frac{1}{b^3} \\ 1 & \frac{1}{(a+b)^2} & -\frac{1}{(a+b)^3} \end{vmatrix}=0,$$

und

$$\varphi(O,(\frac{1}{(a+b)^2},-\frac{1}{(a+b)^3}))=(\frac{1}{(a+b)^2},\frac{1}{(a+b)^3}),$$

woraus sich sofort

$$(\frac{1}{a^2},\frac{1}{a^3})\oplus(\frac{1}{b^2},\frac{1}{b^3})=(\frac{1}{(a+b)^2},\frac{1}{(a+b)^3})$$

ergibt, d.h.

$$K^+\to C_{ns},\quad t\mapsto(\frac{1}{t^2},\frac{1}{t^3})$$

ist ein Gruppenhomomorphismus. Beachtet man

$$(\frac{1}{t^2},\frac{1}{t^3})\simeq(1:\frac{1}{t^2}:\frac{1}{t^3})=(t^3:t:1),$$

so sieht man, dass $t=0$ den Punkt $O=(0:0:1)$ liefert. Wir formulieren das Ergebnis als Satz:

SATZ. *Sei $C$ durch $y^2=x^3$ gegeben und $O=(0:0:1)$ als Nullpunkt gewählt. Dann ist*

$$K^+\to C_{ns}(K),\quad t\mapsto(\frac{1}{t^2},\frac{1}{t^3})$$

*ein Gruppenisomorphismus mit Umkehrabbildung*

$$C_{ns}(K)\to K^+,\quad (x,y)\mapsto\frac{x}{y}.$$

Analog zeigt man folgenden Satz:

SATZ. *Sei $C$ durch $y^2=x^2+x^3$ gegeben mit $O=(0:0:1)$ und $char(K)\neq 2$. Dann ist*

$$C_{ns}(\overline{K})\to\overline{K}^*,\quad (x,y)\mapsto\frac{y-x}{y+x}$$

*ein Gruppenisomorphismus (mit Umkehrabbildung $t\mapsto(\frac{4t}{(1-t)^2},\frac{4t(1+t)}{(1-t)^3})$.)*

**Beispiel:** Die Kurve $y^2=x^2+x^3$ hat 3 Wendepunkte, nämlich $(0:0:1)$ und $(-\frac{4}{3},\pm\sqrt{-\frac{16}{27}})$, die Kurve $y^2=x^3$ hat nur $(0:0:1)$ als Wendepunkt. Dies entspricht der Tatsache, dass $\overline{K}^*$ drei Elemente besitzt, die von 3 annulliert werden, dass $\overline{K}^+$ aber nur ein Element besitzt, das von 3 annulliert wird.

## 5. Ein Verschlüsselungsverfahren mit ebenen Kubiken

**Vorbemerkung:** Das 'exklusive Oder' (XOR) lässt sich zu einer Operation $\oplus:\mathbf{N}_0\times\mathbf{N}_0\to\mathbf{N}_0$ (bitweise) wie folgt fortsetzen: Für natürliche Zahlen $x,y\in\mathbf{N}_0$ bildet man die Binärdarstellungen

$$x=\sum_i x_i\cdot 2^i,\quad y=\sum_i y_i\cdot 2^i\quad\text{mit}\quad x_i,y_i\in\{0,1\}$$

und setzt dann

$$x\oplus y=\sum_i z_i\cdot 2^i\quad\text{mit}\quad z_i\equiv x_i+y_i \bmod 2\quad\text{und}\quad z_i\in\{0,1\}.$$

Beispielsweise gilt

$$17\oplus 39=(010001)_2\oplus(100111)_2=(110110)_2=54.$$

Mit der Definition sieht man sofort, dass

$$(x \oplus y) \oplus y = x$$

gilt.

Das folgende Verfahren ist eine vereinfachte Version von PSEC (Provably Secure Elliptic Curve Encryption Scheme).

**Ein Verschlüsselungsverfahren mit ebenen Kubiken:**

(1) **Schlüsselerzeugung:**
   (a) Man legt eine nichtsinguläre ebene Kubik $C$ über $\mathbf{F}_p$ zugrunde, zusammen mit zwei Punkten $O, P \in C(\mathbf{F}_p)$. Durch Wahl von $O$ als neutrales Element wird $C(\mathbf{F}_p)$ zu einer abelschen Gruppe mit der geometrischen Addition $Q \oplus R = \varphi(\varphi(Q, R), O)$.
   (b) Jeder Teilnehmer $A$ wählt sich eine Zahl $k_A$ mit $0 \leq k_A \lessapprox p$ als geheimen Schlüssel, berechnet $K_A = k_A \cdot P \in C(\mathbf{F}_p)$ und macht $K_A$ als seinen öffentlichen Schlüssel öffentlich zugänglich.

(2) **Verschlüsselung:** Will $B$ eine Nachricht verschlüsselt an $A$ schicken, besorgt er sich den öffentlichen Schlüssel von $A$, teilt die Nachricht in Blöcke, sodass ein Nachrichtenblock einer Zahl $m$ mit $0 \leq m \leq p-1$ entspricht. Dann berechnet $B$ die Punkte

$$Q = m \cdot P \quad \text{und} \quad R = m \cdot K_A$$

in $C(\mathbf{F}_p)$, schreibt

$$Q = (1 : x_Q : y_Q), \quad R = (1 : x_R : y_R),$$

berechnet

$$s = m \oplus x_R$$

und schickt das Tripel

$$(x_Q, y_Q, s)$$

an $A$.

(3) **Entschlüsselung:** $A$ empfängt $(x_Q, y_Q, s)$, berechnet

$$S = k_A \cdot (1 : x_Q : y_Q) \in C(\mathbf{F}_p),$$

schreibt $S = (1 : x_S : y_S)$ und berechnet

$$\widetilde{m} = s \oplus x_S.$$

Ist alles in Ordnung, so ist $\widetilde{m}$ der ursprüngliche Nachrichtenblock $m$.

**Bemerkungen:**

(1) Warum gilt $\widetilde{m} = m$? Wenn alles richtig zugegangen ist, so gilt

$$(1 : x_S : y_S) = S = k_A \cdot (1 : x_Q : y_Q) = k_A Q = k_A m P = m k_A P = m K_A = R = (1 : x_R : y_R),$$

also $x_S = x_R$, was sofort zu

$$\widetilde{m} = s \oplus x_S = (m \oplus x_R) \oplus x_S = m$$

führt.

(2) Wie sicher ist das Verfahren?
   (a) Kann man diskrete Logarithmen in $C(\mathbf{F}_p)$ berechnen, gibt es keine Sicherheit. Im Allgemeinen wird das aber bei entsprechender Parameterwahl praktisch nicht durchführbar sein.
   (b) Da $s = m \oplus x_R$ bekannt ist, ist die Kenntnis von $m$ gleichwertig mit der Kenntnis von $x_R$, also der Kenntnis von $R$. Nun kennt man $Q = mP$ und $K_A = k_A P$ und sucht $R = m k_A P$, was wieder ein typisches Diffie-Hellman-Problem ist, für das man nur den Weg über die diskreten Logarithmen kennt.

**Beispiel:** Wir wählen

$p = 47852364786523784652783582764827365 67, \quad f = 7x_0^3 + 9x_1^3 - 2x_2^3, \quad O = (1:1:2), \quad P = (1:3:5).$

$f = 0$ definiert dann über $\mathbf{F}_p$ eine nichtsinguläre Kubik $C$, wobei $O, P \in C(\mathbf{F}_p)$ gilt. Durch Wahl von $O$ wird $C(\mathbf{F}_p)$ zu einer abelschen Gruppe. Wir wählen zufällig

$$k_A = 158219317979738066999302138270193 9848$$

und berechnen

$$\begin{aligned} K_A &= k_A \cdot P = \\ &= (1 : 48386385420527847958745134002519595 : 176525337558359981869381032468431 0030). \end{aligned}$$

Wir wollen

$$m = 12345678901234567890123456789012345 67$$

mit dem öffentlichen Schlüssel $K_A$ verschlüsseln und berechnen dazu

$$\begin{aligned} Q &= m \cdot P = \\ &= (1 : 28935049493486862851224388711673858 64 : 24936018158030236987801616708216031 00), \\ R &= m \cdot K_A = \\ &= (1 : 24451820241875075594662261474373782 76 : 18964679905063693965183171766576102 45). \end{aligned}$$

Mit

$$\begin{aligned} x_Q &= 28935049493486862851224388711673858 64, \\ y_Q &= 24936018158030236987801616708216031 00, \\ x_R &= 24451820241875075594662261474373782 76, \\ s = m \oplus x_R &= 16363884052018682555381868822708678 11 \end{aligned}$$

wird die verschlüsselte Nachricht $(x_Q, y_Q, s)$.

KAPITEL 4

# Elliptische Kurven in Weierstraßscher Normalform

## 1. Ebene Kubiken mit $K$-rationalem Wendepunkt

Wir wollen eine Normalform für ebene kubische Kurven herleiten. Wir beginnen mit einem allgemeinen Lemma.

LEMMA. *Sei $C$ eine über dem Körper $K$ durch ein homogenes Polynom $f(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ definierte ebene projektive Kurve und $P = (p_0 : p_1 : p_2) \in C(K)$ ein nichtsingulärer $K$-rationaler Punkt der Kurve mit $p_0, p_1, p_2 \in K$. Setzt man*

$$f_0 = \frac{\partial f}{\partial x_0}(p_0, p_1, p_2), \quad f_1 = \frac{\partial f}{\partial x_1}(p_0, p_1, p_2), \quad f_2 = \frac{\partial f}{\partial x_2}(p_0, p_1, p_2),$$

*und wählt man ein $T$ mit*

$$T = (t_{ij})_{0 \le i,j \le 2} = \begin{cases} \begin{pmatrix} 0 & 0 & p_0 \\ 1 & f_2 & p_1 \\ 0 & -f_1 & p_2 \end{pmatrix} & \text{im Fall } p_0 \neq 0, f_1 \neq 0, \\ \begin{pmatrix} 0 & 0 & p_0 \\ 0 & f_2 & p_1 \\ 1 & -f_1 & p_2 \end{pmatrix} & \text{im Fall } p_0 \neq 0, f_2 \neq 0, \\ \begin{pmatrix} 1 & f_2 & p_0 \\ 0 & 0 & p_1 \\ 0 & -f_0 & p_2 \end{pmatrix} & \text{im Fall } p_1 \neq 0, f_0 \neq 0, \\ \begin{pmatrix} 0 & f_2 & p_0 \\ 0 & 0 & p_1 \\ 1 & -f_0 & p_2 \end{pmatrix} & \text{im Fall } p_1 \neq 0, f_2 \neq 0, \\ \begin{pmatrix} 1 & f_1 & p_0 \\ 0 & -f_0 & p_1 \\ 0 & 0 & p_2 \end{pmatrix} & \text{im Fall } p_2 \neq 0, f_0 \neq 0, \\ \begin{pmatrix} 0 & f_1 & p_0 \\ 1 & -f_0 & p_1 \\ 0 & 0 & p_2 \end{pmatrix} & \text{im Fall } p_2 \neq 0, f_1 \neq 0, \end{cases}$$

*so definiert*

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = T \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

*eine über $K$ definierte projektive Transformation mit folgenden Eigenschaften: Bzgl. der Koordinaten $y_0, y_1, y_2$ wird $C$ durch das Polynom*

$$g(y_0, y_1, y_2) = f(t_{00}y_0 + t_{01}y_1 + t_{02}y_2, t_{10}y_0 + t_{11}y_1 + t_{12}y_2, t_{20}y_0 + t_{21}y_1 + t_{22}y_2)$$

*beschrieben, der Punkt $P$ erhält die Koordinanten $(0 : 0 : 1)$, die Tangente an $C$ in $P$ die Gleichung $y_0 = 0$.*

*Beweis:* Aus Symmetriegründen können wir uns auf den Fall $p_0 \neq 0$ beschränken. Da $P$ nichtsingulär ist, folgt $(f_0, f_1, f_2) \neq 0$. Die Gleichung für die Tangente in $P$ lautet $f_0x_0 + f_1x_1 + f_2x_2 = 0$. Da $P$ auf der Tangente liegt, folgt $f_0p_0 + f_1p_1 + f_2p_2 = 0$. Im Fall $p_0 \neq 0$ folgt dann aber sofort $(f_1, f_2) \neq 0$. Wieder können wir uns aus Symmetriegründen auf den Fall $f_1 \neq 0$ beschränken. Als zugehöriges $T$ wählen wir

$$T = \begin{pmatrix} 0 & 0 & p_0 \\ 1 & f_2 & p_1 \\ 0 & -f_1 & p_2 \end{pmatrix},$$

was sofort $\det T = -f_1p_0 \neq 0$ zeigt, d.h.

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & p_0 \\ 1 & f_2 & p_1 \\ 0 & -f_1 & p_2 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

liefert tatsächlich eine projektive Transformation. Man sieht sofort, dass $(x_0 : x_1 : x_2) = (p_0 : p_1 : p_2)$ nun dem Punkt $(y_0 : y_1 : y_2) = (0 : 0 : 1)$ entspricht. Die Tangentengleichung wird zu

$$\begin{aligned} f_0x_0 + f_1x_1 + f_2x_2 &= f_0(p_0y_2) + f_1(y_0 + f_2y_1 + p_1y_2) + f_2(-f_1y_1 + p_2y_2) = \\ &= f_1y_0 + (f_1f_2 - f_2f_1)y_1 + (f_0p_0 + f_1p_1 + f_2p_2)y_2 = f_1y_0, \end{aligned}$$

also zu $y_0 = 0$, wie behauptet. Genauso folgt die Behauptung in den anderen Fällen. ■

Eine einfache Folgerung ist nun:

LEMMA. *Sei $C$ eine über dem Körper $K$ definierte ebene projektive kubische Kurve mit einem $K$-rationalen Wendepunkt $P$. Führt man einen (über $K$ definierten) Koordinatenwechsel durch, sodass der Punkt $P$ die Koordinaten $(0 : 0 : 1)$, die Wendetangente die Gleichung $x_0 = 0$ erhält, so wird $C$ beschrieben durch ein Polynom*

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + a_3x_0x_1^2 + a_4x_0x_1x_2 + a_5x_0x_2^2 + a_6x_1^3 \quad \text{mit } a_i \in K.$$

*Beweis:* Mit dem vorangegangenen Lemma können wir einen Koordinatenwechsel wie gewünscht durchführen. Die Gleichung der Kurve $C$ schreiben wir nun

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + a_3x_0x_1^2 + a_4x_0x_1x_2 + a_5x_0x_2^2 + a_6x_1^3 + a_7x_1^2x_2 + a_8x_1x_2^2 + a_9x_2^3.$$

Die Kurve $C$ schneidet die Gerade $x_0 = 0$ im Punkt $(x_0 : x_1 : x_2) = (0 : 0 : 1)$ 3-fach. Also wird bei Einsetzen von $x_0 = 0$ der Punkt $(x_1 : x_2) = (0 : 1)$ 3-fach ausgeschnitten, d.h.

$$f(0, x_1, x_2) = a_6x_1^3 + a_7x_1^2x_2 + a_8x_1x_2^2 + a_9x_2^3 = a_6x_1^3,$$

was sofort

$$a_7 = a_8 = a_9 = 0$$

und damit die Behauptung impliziert. ■

SATZ. *Ist $C$ eine über $K$ definierte irreduzible ebene projektive Kubik mit einem $K$-rationalen Wendepunkt $P$, so gibt es einen (über $K$ definierten) Koordinatenwechsel, sodass $C$ durch eine affine Gleichung*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K,$$

*beschrieben wird. Der Wendepunkt ist dann $P = (0 : 0 : 1)$, die Wendetangente hat die Gleichung $x_0 = 0$.*

*Beweis:* Wir können schreiben

$$f = b_0x_0^3 + b_1x_0^2x_1 + b_2x_0^2x_2 + b_3x_0x_1^2 + b_4x_0x_1x_2 + b_5x_0x_2^2 + b_6x_1^3.$$

Im affinen Teil $x_2 \neq 0$ mit Koordinaten $(x_0 : x_1 : x_2) = (u : v : 1)$ wird

$$f(u, v, 1) = b_0u^3 + b_1u^2v + b_2u^2 + b_3uv^2 + b_4uv + b_5u + b_6v^3.$$

Da $C$ nichtsingulär in $(0 : 0 : 1)$ ist, muss $b_5 \neq 0$ gelten. Da $C$ irreduzibel ist, muss $b_6 \neq 0$ gelten. Definieren wir einen neuen Koordinatenwechsel durch

$$x_0 = -\frac{b_6}{b_5}y_0, \quad x_1 = y_1, \quad x_2 = y_2,$$

so wird

$$\begin{aligned}-\frac{1}{b_6}f &= -\frac{b_0}{b_6}(-\frac{b_6}{b_5}y_0)^3 - \frac{b_1}{b_6}(-\frac{b_6}{b_5}y_0)^2y_1 - \frac{b_2}{b_6}(-\frac{b_6}{b_5}y_0)^2y_2 - \frac{b_3}{b_6}(-\frac{b_6}{b_5}y_0)y_1^2 - \frac{b_4}{b_6}(-\frac{b_6}{b_5}y_0)y_1y_2 + \\ &\quad -\frac{b_5}{b_6}(-\frac{b_6}{b_5}y_0)y_2^2 - \frac{b_6}{b_6}y_1^3 = \\ &= \frac{b_0b_6^2}{b_5^3}y_0^3 - \frac{b_1b_6}{b_5^2}y_0^2y_1 - \frac{b_2b_6}{b_5^2}y_0^2y_2 + \frac{b_3}{b_5}y_0y_1^2 + \frac{b_4}{b_5}y_0y_1y_2 + y_0y_1^2 - y_2^3.\end{aligned}$$

Schreibt man wieder $x_i$ statt $y_i$ und definiert man $c_i$ durch Koeffizientenvergleich, so wird $C$ beschrieben durch ein Polynom

$$\begin{aligned}g &= c_0x_0^3 + c_1x_0^2x_1 + c_2x_0^2x_2 + c_3x_0x_1^2 + c_4x_0x_1x_2 + x_0x_2^2 - x_1^3 = \\ &= (x_0x_2^2 + c_4x_0x_1x_2 + c_2x_0^2x_2) - (x_1^3 - c_3x_0x_1^2 - c_1x_0^2x_1 - c_0x_0^3).\end{aligned}$$

Durch Umbenennung erhalten wir

$$g = (x_0x_2^2 + a_1x_0x_1x_2 + a_3x_0^2x_2) - (x_1^3 + a_2x_0x_1^2 + a_4x_0^2x_1 + a_6x_0^3),$$

was affin zu

$$g(1, x, y) = (y^2 + a_1xy + a_3y) - (x^3 + a_2x^2 + a_4x + a_6)$$

wird. Das war zu zeigen. ■

## 2. Elliptische Kurven in Weierstraßscher Normalform

DEFINITION. Eine elliptische Kurve $E$ über einem Körper $K$ wird in Weierstraßscher Normalform durch eine nichtsinguläre ebene projektive Kubik mit affiner Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{mit} \quad a_i \in K$$

gegeben. Die zugehörige homogene Gleichung ist

$$x_0x_2^2 + a_1x_0x_1x_2 + a_3x_0^2x_2 = x_1^3 + a_2x_0x_1^2 + a_4x_0^2x_1 + a_6x_0^3.$$

$E$ hat genau einen Punkt im Unendlichen, nämlich den Wendepunkt $O = (0 : 0 : 1)$ mit Wendetangente $x_0 = 0$. Wir haben dann

$$E(K) = \{(x, y) \in K \times K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

Durch Auswahl von $O$ als neutrales Element wird $E(K)$ zu einer abelschen Gruppe mit Verknüpfung $\oplus$.

Die angegebene Gleichung kann auch eine singuläre Kurve definieren. Hier gilt der Satz:

SATZ. *Die ebene projektive kubische Kurve $C$ werde durch die affine Gleichung*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \textit{mit} \quad a_i \in K$$

*definiert. Dann gilt:*

$$C \textit{ ist singulär} \quad \Longleftrightarrow \quad \Delta = 0,$$

*wobei*

$$\begin{aligned}\Delta &= 288a_4a_2a_6 + a_1^5a_4a_3 + 144a_2a_1a_6a_3 - 64a_4^3 - 96a_4^2a_1a_3 + 72a_1^2a_6a_4 + 16a_2^2a_4^2 - 432a_6^2 \\ &\quad -27a_3^4 + a_1^4a_4^2 - 30a_4a_1^2a_3^2 + 8a_2a_4^2a_1^2 - a_1^6a_6 + 72a_2a_4a_3^2 - 216a_6a_3^2 - 64a_2^3a_6 + a_3^3a_1^3 \\ &\quad -16a_2^3a_3^2 + 36a_2a_3^3a_1 + 8a_2a_4a_3a_1^3 - a_2a_3^2a_1^4 + 16a_2^2a_4a_3a_1 - 8a_2^2a_3^2a_1^2 + 36a_6a_3a_1^3 \\ &\quad -48a_2^2a_6a_1^2 - 12a_1^4a_2a_6\end{aligned}$$

*ist.*

Die Gruppenstruktur auf der elliptischen Kurve lässt sich nun explizit wie folgt beschreiben:

SATZ. *Eine elliptische Kurve $E$ sei gegeben durch die Gleichung*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Die Gruppenstruktur $(E(K), +)$ ergibt sich dann wie folgt: Zunächst gilt für $(x_0, y_0) \in E(K)$*

$$-(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$

*Sei nun $P_i = (x_i, y_i)$ und $P_3 = P_1 \oplus P_2$.*
*Ist $x_1 = x_2$ und $y_1 + y_2 + a_1x_2 + a_3 = 0$, so gilt $P_1 \oplus P_2 = O$. Definiere sonst*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \quad \text{falls } x_1 \neq x_2,$$

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \text{falls } x_1 = x_2.$$

*Dann gilt*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

DEFINITION. Zwei über $K$ definierte elliptische Kurven $E$ und $E'$ mit Weierstraßgleichungen

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{und} \quad y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

heißen isomorph über $K$, wenn es einen über $K$ definierten Koordinatenwechsel gibt, der $E$ in $E'$ überführt, wobei $(0 : 0 : 1)$ festbleibt.

LEMMA. (1) *Ein über $K$ definierter Koordinatenwechsel von $\mathbf{P}^2$, der den Punkt $(0 : 0 : 1)$ festlässt und die Gerade $x_0 = 0$ in sich überführt, hat die Gestalt*

$$x = vx' + r, \quad y = wy' + sx' + t \quad \text{mit} \quad v, w \in K^*, r, s, t \in K.$$

(2) *Soll der Koordinatenwechsel außerdem eine Weierstraßgleichung in eine Weierstraßgleichung überführen, so gibt es $u \in K^*$, $r, s, t \in K$ mit*

$$x = u^2x' + r, \quad y = u^3y' + sx' + t.$$

*Beweis:*

(1) Für einen Koordinatenwechsel, der den Punkt $(0 : 0 : 1)$ festlässt, können wir ansetzen

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} u_0 & v_0 & 0 \\ u_1 & v_1 & 0 \\ u_2 & v_2 & w_2 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}.$$

Die Gerade $x_0 = 0$ wird zu

$$x_0 = u_0y_0 + v_0y_1,$$

also muss $v_0 = 0$ gelten. Schreiben wir

$$x = \frac{x_1}{x_0}, \quad y = \frac{x_2}{x_0}, \quad x' = \frac{y_1}{y_0}, \quad y' = \frac{y_2}{y_0},$$

so erhalten wir die Darstellung

$$x = vx' + r, \quad y = wy' + sx' + t,$$

wobei natürlich $vw \neq 0$ gelten muss.

(2) Setzt man in

$$f = (y^2 + a_1xy + a_3y) - (x^3 + a_2x^2 + a_4x + a_6)$$

den Koordinatenwechsel ein, so erhält man

$$f = \ldots w^2y'^2 - v^3x'^3 \ldots$$

Die Koeffizienten bei $y'^2$ und $-x'^3$ müssen gleich sein, also erhalten wir die Bedingung $w^2 = v^3$. Setzt man nun $u = \frac{w}{v}$, so gilt

$$u^2 = \frac{w^2}{v^2} = \frac{v^3}{v^2} = v \quad \text{und} \quad u^3 = \frac{w^3}{v^3} = \frac{w^3}{w^2} = w,$$

woraus dann die Behauptung folgt. ■

SATZ. *Seien $E$ und $E'$ zwei über $K$ definierte elliptische Kurven mit Weierstraßgleichungen*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{und} \quad y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6.$$

*sind genau dann isomorph über $K$, wenn es $u \in K^*$, $r, s, t \in K$ gibt mit*

$$\begin{aligned} ua'_1 &= a_1 + 2s, \\ u^2a'_2 &= a_2 + 3r - s^2 - sa_1, \\ u^3a'_3 &= a_3 + 2t + ra_1, \\ u^4a'_4 &= a_4 + 3r^2 - 2st - (rs + t)a_1 + 2ra_2 - sa_3, \\ u^6a'_6 &= a_6 + r^3 - t^2 - rta_1 + r^2a_2 - ta_3 + ra_4. \end{aligned}$$

*In diesem Fall definiert*

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t$$

*einen zugehörigen Isomorphismus.*

*Beweis:* Wir setzen den Koordinatenwechsel an als

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t.$$

Mit dem Ansatz

$$(y^2 + a_1xy + a_3y) - (x^3 + a_2x^2 + a_4x + a_6) = u^6\left((y'^2 + a'_1x'y' + a'_3y') - (x'^3 + a'_2x'^2 + a'_4x' + a'_6)\right)$$

erhält man durch Koeffizientenvergleich

$$\begin{aligned} ua'_1 &= a_1 + 2s, \\ u^2a'_2 &= a_2 + 3r - s^2 - sa_1, \\ u^3a'_3 &= a_3 + 2t + ra_1, \\ u^4a'_4 &= a_4 + 3r^2 - 2st - (rs + t)a_1 + 2ra_2 - sa_3, \\ u^6a'_6 &= a_6 + r^3 - t^2 - rta_1 + r^2a_2 - ta_3 + ra_4, \end{aligned}$$

woraus die Behauptung folgt. ■

Abhängig von der Charakteristik kann man jetzt noch einfachere Normalformen finden.

## 3. Elliptische Kurven in Charakteristik $\neq 2, 3$

SATZ. *Sei $K$ ein Körper der Charakteristik $\neq 2, 3$. Ist $E$ eine elliptische Kurve über $K$, so lässt sich $E$ durch eine Gleichung*

$$y^2 = x^3 + ax + b \quad \textit{mit} \quad a, b \in K$$

*beschreiben.*

*Beweis:* Wir können $E$ zunächst durch eine Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

mit $a_i \in K$ beschreiben. Durch einen Koordinatenwechsel

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t$$

erhalten wir eine neue Kurvengleichung

$$y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6$$

mit

$$\begin{aligned} ua'_1 &= a_1 + 2s, \\ u^2a'_2 &= a_2 + 3r - s^2 - sa_1, \\ u^3a'_3 &= a_3 + 2t + ra_1, \\ u^4a'_4 &= a_4 + 3r^2 - 2st - (rs + t)a_1 + 2ra_2 - sa_3, \\ u^6a'_6 &= a_6 + r^3 - t^2 - rta_1 + r^2a_2 - ta_3 + ra_4. \end{aligned}$$

Definiert man nacheinander $s, r, t$ durch

$$s = -\frac{1}{2}a_1, \quad r = -\frac{1}{3}(a_2 - s^2 - sa_1), \quad t = -\frac{1}{2}(a_3 + ra_2),$$

so folgt

$$a_1' = 0, \quad a_2' = 0, \quad a_3' = 0$$

und die neue Gleichung hat die gewünschte Form. ■

LEMMA. *Durch $y^2 = x^3 + ax + b$ wird genau dann eine nichtsinguläre projektive Kurve definiert, wenn gilt $4a^3 + 27b^2 \neq 0$. Im Fall $4a^3 + 27b^2 = 0$ ist*

$$\begin{cases} (-\frac{3b}{2a}, 0) & \text{für } a \neq 0, \\ (0,0) & \text{für } a = 0 \end{cases}$$

*die (einzige) Singularität der Kurve.*

*Beweis:* Die homogene Gleichung lautet $f = x_0x_2^2 - x_1^3 - ax_0^2x_1 - bx_0^3$. Der einzige Punkt im Unendlichen ($x_0 = 0$) ist $(0:0:1)$. Wählt man affine Koordinaten $(x_0 : x_1 : x_2) = (u : v : 1)$, so gilt

$$f(u, v, 1) = u - v^3 - au^2v - bu^3,$$

der Punkt $(u, v) = (0, 0)$ ist also nichtsingulär. (Er ist sogar ein Wendepunkt mit Wendetangente $u = 0$ bzw. $x_0 = 0$.) Wir können uns also auf den endlichen Teil beschränken. Wir schreiben

$$f = y^2 - x^3 - ax - b, \quad \frac{\partial f}{\partial x} = -3x^2 - a, \quad \frac{\partial f}{\partial y} = 2y.$$

Genau dann ist also $(x, y)$ ein singulärer Kurvenpunkt, wenn gilt

$$y = 0, \quad x^3 + ax + b = 0, \quad 3x^2 + a = 0.$$

Nun liefert Polynomdivision die Darstellung

$$x^3 + ax + b = \frac{1}{3}x(3x^2 + a) + (\frac{2}{3}ax + b).$$

$(x, 0)$ ist also genau dann singulär, wenn gilt

$$3x^2 + a = 0 \quad \text{und} \quad \frac{2}{3}ax + b = 0.$$

Im Fall $a = 0$ ist dies genau dann der Fall, wenn $b = 0$ und $x = 0$ gilt. Wir können also nun $a \neq 0$ voraussetzen. Dann gilt:

$$\begin{aligned} (x,0) \text{ singulär} \quad &\iff \quad 3x^2 + a = 0, \quad \frac{2}{3}ax + b = 0 \quad \iff \\ &\iff \quad x = -\frac{3b}{2a}, \quad 0 = 3x^2 + a = 3\frac{9b^2}{4a^2} + a \quad \iff \\ &\iff \quad x = -\frac{3b}{2a}, \quad 4a^3 + 27b^2 = 0, \end{aligned}$$

was die Behauptung beweist. ■

Elliptische Kurven über einem Körper $K$ der Charakteristik $\neq 2, 3$ werden also durch eine Gleichung

$$y^2 = x^3 + ax + b \quad \text{mit} \quad a, b \in K \quad \text{und} \quad 4a^3 + 27b^2 \neq 0$$

beschrieben. Wir schreiben für die Kurve dann auch manchmal $E_{a,b}$.

Wir geben jetzt nochmals eine explizite Form der Addition auf $E_{a,b}(K)$ an:

SATZ. *Für die Addition auf $E_{a,b}(K)$ mit neutralem Element $O = (0:0:1)$ gilt:*

- *Für alle $P \in E_{a,b}(K)$ ist $P + O = O + P = P$.*
- *Gilt für $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E_{a,b}(K)$ die Beziehung $x_1 = x_2$ und $y_1 + y_2 = 0$, so ist $P_1 + P_2 = O$.*

- *Setze*

$$m = \begin{cases} \frac{y_1-y_2}{x_1-x_2} & \text{falls } x_1 \neq x_2, \\ \frac{3x_1^2+a}{2y_1} & \text{falls } x_1 = x_2, y_1 = y_2 \neq 0. \end{cases}$$

*Dann ist* $P_1 + P_2 = P_3$ *mit*

$$x_3 = m^2 - x_1 - x_2 \quad \text{und} \quad y_3 = -m(x_3 - x_1) - y_1.$$

*Außerdem gilt für* $(x, y) \in E_{a,b}(K)$

$$-(x, y) = (x, -y).$$

*Beweis:* $O = (0 : 0 : 1)$ ist ein Wendepunkt der Kurve, also gilt $\varphi(O, O) = O$. Die Wendetangente ist die unendlich ferne Gerade $x_0 = 0$. Die andern Geraden durch $O$ haben die Gestalt $x = c$ mit $c \in \overline{K}$. Dann folgt für $(x, y) \in E_{a,b}(K)$ leicht $\varphi((x, y), O) = (x, -y)$. Seien jetzt Punkte $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E_{a,b}(K)$ gegeben, d.h. $y_i^2 = x_i^3 + ax_i + b$.

(1) Wir betrachten den Fall $P_1 \neq P_2$ und unterscheiden zwei Fälle:
   (a) $x_1 = x_2$. Wegen $P_1 \neq P_2$ gilt dann $y_1 = -y_2$ mit $y_1, y_2 \neq 0$. Die Gerade durch $P_1$ und $P_2$ ist $x = x_1$, also folgt $\varphi(P_1, P_2) = O$ und damit $P_1 \oplus P_2 = \varphi(\varphi(P_1, P_2), O) = \varphi(O, O) = O$.
   (b) $x_1 \neq x_2$. Die Gerade durch $P_1$ und $P_2$ ist

$$y = m(x - x_1) + y_1 \quad \text{mit} \quad m = \frac{y_1 - y_2}{x_1 - x_2}.$$

Setzt man dies in $x^3 + ax + b - y^2$ ein, erhält man ein kubisches Polynom in $x$, dessen Nullstellen die Schnittpunkte der Geraden mit der Kurve liefern, also $(x-x_1)(x-x_2)(x-x_3)$:

$$x^3 + ax + b - (m(x - x_1) + y_1)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Durch Koeffizientenvergleich bei $x^2$ erhält man

$$x_1 + x_2 + x_3 = m^2$$

und damit

$$\varphi(P_1, P_2) = (x_3, y_3) \quad \text{mit} \quad x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_3 - x_1) + x_1.$$

Dann gilt

$$P_1 \oplus P_2 = \varphi(\varphi(P_1, P_2), O) = \varphi((x_3, y_3), O) = (x_3, -y_3) = (m^2 - x_1 - x_2, -m(x_3 - x_1) - x_1).$$

(2) Wir behandeln jetzt den Fall $P_1 = (x_1, y_1) = P_2$ und unterscheiden wieder zwei Möglichkeiten.
   (a) Ist $y_1 = 0$, so ist die Tangentengleichung $x = x_1$, die Tangente geht durch $O$, also $\varphi(P_1, P_2) = O$ und damit $P_1 \oplus P_2 = \varphi(\varphi(P_1, P_2), O) = \varphi(O, O) = O$.
   (b) Sei jetzt $y_1 \neq 0$. Die Tangentengleichung ergibt sich mit $f = x^3 + ax + b - y^2$ und $\frac{\partial f}{\partial x} = 3x^2 + a$, $\frac{\partial f}{\partial y} = -2y$ zu

$$(3x_1^2 + a)(x - x_1) - 2y_1(y - y_1) = 0, \quad \text{d.h.} \quad y = \frac{3x_1^2 + a}{2y_1}(x - x_1) + y_1.$$

Setzt man

$$m = \frac{3x_1^2 + a}{2y_1},$$

so ist man in der gleichen Situation wie oben und man erhält die angegebenen Formeln. ■

SATZ. *Genau dann sind zwei Kurven* $E_{a,b}$ *und* $E_{a',b'}$ *isomorph über* $K$*, wenn es* $u \in K^*$ *gibt mit*

$$u^4 a' = a, \quad u^6 b' = b.$$

*Ein zugehöriger Isomorphismus wird durch den Koordinatenwechsel* $x = u^2 x'$, $y = u^3 y'$ *definiert.*

*Beweis:* Wir wenden die zuvor gezeigten allgemeinen Formeln an und erhalten mit

$$a_1 = a_2 = a_3 = 0, a_4 = a, a_6 = b, a_1' = a_2' = a_3' = 0, a_4' = a', a_6' = b$$

die Bedingungen

$$\begin{aligned} 0 = ua_1' &= a_1 + 2s = 2s, \\ 0 = u^2a_2' &= a_2 + 3r - s^2 - sa_1 = 3r - s^2, \\ 0 = u^3a_3' &= a_3 + 2t + ra_1 = 2t, \\ u^4a' = u^4a_4' &= a_4 + 3r^2 - 2st - (rs + t)a_1 + 2ra_2 - sa_3 = a + 3r^2 - 2st, \\ u^6b' = u^6a_6' &= a_6 + r^3 - t^2 - rta_1 + r^2a_2 - ta_3 + ra_4 = b + r^3 - t^2 + ra, \end{aligned}$$

was nacheinander $s = 0$, $r = 0$, $t = 0$ und dann $u^4a' = a$, $u^6b' = b$ liefert. Ein zugehöriger Koordinatenwechsel ist $x = u^2x'$, $y = u^3y'$. ■

SATZ. *Sind $E_{a,b} : y^2 = x^3 + ax + b$ und $E_{a',b'} : y^2 = x^3 + a'x + b'$ über $K$ isomorphe elliptische Kurven, d.h. gibt es ein $u \in K^*$ mit $a' = u^4a$, $b' = u^6b$, so liefert*

$$E_{a,b}(K) \to E_{a'.b'}(K), \quad (x, y) \mapsto (u^2x, u^3y)$$

*einen Gruppenisomorphismus.*

*Beweis:* Ist $(x, y) \in E_{a,b}(K)$, so gilt $y^2 = x^3 + ax + b$ und damit $(u^3y)^2 = (u^2x)^3 + au^4(u^2x) + bu^6$, d.h. $(u^2x, u^3y) \in E_{a',b'}(K)$. Die angegebene Abbildung ist also sinnvoll definiert. Die Bijektivität ist klar, da die Umkehrabbildung die gleiche Gestalt hat, aber mit dem Parameter $\frac{1}{u}$. Mit den expliziten Formeln für die Addition sieht man, dass die Abbildung ein Gruppenhomomorphismus ist. ■

**Beispiel:** Wir betrachten alle elliptischen Kurven über $K = \mathbf{F}_5$. Es ist

$$\{(u^4, u^6) : u \in K^*\} = \{(1, 1), (1, 4)\} = \{(1, 1), (1, -1)\}.$$

Wollen wir also die Kurven $y^2 = x^3 + ax + b$ bis auf Isomorphie klassifizieren, so können wir $0 \le a \le 4$ und $0 \le b \le 2$ voraussetzen. Durch die Bedingung $4a^3 + 27b^2 \neq 0$ werden die Fälle $(0, 0)$, $(2, 2)$, $(3, 1)$ ausgeschlossen. Die Isomorphieklassen elliptischer Kurven über $\mathbf{F}_5$ werden also durch die Kurven $y^2 = x^3 + ax + b$ mit

$$(a, b) \in \{(0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (3, 0), (3, 2), (4, 0), (4, 1), (4, 2)\}$$

repräsentiert.

| $(a, b)$ | (0,1) | (0,2) | (1,0) | (1,1) | (1,2) | (2,0) | (2,1) | (3,0) | (3,2) | (4,0) | (4,1) | (4,2) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\#E_{a,b}(\mathbf{F}_5)$ | 6 | 6 | 4 | 9 | 4 | 2 | 7 | 10 | 5 | 8 | 8 | 3 |

DEFINITION. Sei $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über $K$. Dann heißt

$$j = j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

die $j$-Invariante von $E$. ($1728 = 12^3$.)

**Beispiele:** Genau die Kurven $y^2 = x^3 + b$ (mit $b \neq 0$) haben $j$-Invariante 0, genau die Kurven $y^2 = x^3 + ax$ (mit $a \neq 0$) haben $j$-Invariante 1728.

SATZ. *Seien $E$ und $E'$ elliptische Kurven über einem Körper $K$. Genau dann sind $E$ und $E'$ über dem algebraischen Abschluss $\overline{K}$ isomorph, wenn gilt $j(E) = j(E')$.*

*Beweis:* Sei $E : y^2 = x^3 + ax + b$ und $E' : y^2 = x^3 + a'x + b'$.

(1) Sind $E$ und $E'$ isomorph über $K$, so gibt es ein $u \in K^*$ mit $a' = u^4a$, $b' = u^6b$, woraus sofort

$$j(E') = 1728\frac{4a'^3}{4a'^3 + 27b'^2} = 1728\frac{4u^{12}a^3}{4u^{12}a^3 + 27u^{12}b^2} = 1728\frac{4a^3}{4a^3 + 27b^2} = j(E)$$

folgt.

(2) Sei nun $j(E) = j(E')$.
- Ist $j(E) = 0 = j(E')$, so ist $a = a' = 0$. Wählt man ein $u \in \overline{K}^*$ mit $u^6 = \frac{b'}{b}$, so hat man $a' = u^4 a$, $b' = u^6 b$, $E$ und $E'$ sind also isomorph über $\overline{K}$.
- Ist $j(E) = 1728 = j(E')$, so ist $b = b' = 0$. Die Wahl von $u \in \overline{K}^*$ mit $u^4 = \frac{a'}{a}$ führt wegen $a' = u^4 a$, $b' = u^6 b$ zu einem Isomorphismus von $E$ und $E'$ über $\overline{K}$.
- Sei jetzt $j(E) = j(E') \neq 0, 1728$. Dann sind $a, a', b, b' \neq 0$. Die Gleichung $j(E) = j(E')$ führt zu $a^3(4a'^3 + 27b'^2) = a'^3(4a^3 + 27b^2)$, was sofort

$$a^3 b'^2 = a'^3 b^2$$

ergibt. Wählt man $u \in \overline{K}^*$ mit

$$u^2 = \frac{ab'}{a'b},$$

so folgt unter Verwendung obiger Gleichung

$$u^4 = \frac{a^2 b'^2}{a'^2 b^2} = \frac{a^3 b'^2}{a a'^2 b^2} = \frac{a'^3 b^2}{a a'^2 b^2} = \frac{a'}{a}$$

und

$$u^6 = \frac{a^3 b'^3}{a'^3 b^3} = \frac{a^3 b'^2 b'}{a'^3 b^2 b} = \frac{b'}{b},$$

was die Isomorphie von $E$ und $E'$ über $\overline{K}$ zeigt. ■

SATZ. *Sei $K$ ein Körper der Charakteristik $\neq 2, 3$. Folgende Kurven ergeben ein Repräsentantensystem aller elliptischen Kurven über $K$ bis auf $K$-Isomorphie:*
- *$j = 0$: $y^2 = x^3 + b$, wobei $b$ ein Repräsentantensystem von $K^*/K^{*6}$ durchläuft.*
- *$j = 1728$: $y^2 = x^3 + ax$, wobei $a$ ein Repräsentantensystem von $K^*/K^{*4}$ durchläuft.*
- *$j \neq 0, 1728$: $y^2 = x^3 - 3cu^2 x + 2cu^3$ mit $c = \frac{j}{j-1728}$, wobei $u$ ein Repräsentantensystem von $K^*/K^{*2}$ durchläuft.*

*Beweis:* Wir betrachten den Fall $j \neq 0, 1728$.
- Zunächst rechnet man nach, dass jede Kurve $y^2 = x^3 - 3cu^2 x + 2cu^3$ wirklich $j$-Invariante $j$ hat.
- Ist $E$ eine elliptische Kurve über $K$ mit der Gleichung $y^2 = x^3 + ax + b$ und $j$-Invariante $j$, so gibt es also ein $\lambda \in \overline{K}^*$ mit

$$a = -3c\lambda^4 \quad \text{und} \quad b = 2c\lambda^6.$$

Also folgt $\lambda^4, \lambda^6 \in K$ und damit $\lambda^2 \in K$. Setzt man $u = \lambda^2 \in K$, so hat $E$ die gewünschte Form.
- Sei $E$ gegeben durch $y^2 = x^3 - 3cu^2 x + 2cu^3$ und $E'$ durch $y^2 = x^3 - 3cu'^2 x + 2cu'^3$. Dann gilt:

$$\begin{aligned} E \simeq_K E' &\iff -3cu^2 \cdot v^4 = -3cu'^2, \quad 2cu^3 \cdot v^6 = 2cu'^3 \text{ für ein } v \in K \\ &\iff u'^2 = u^2 \cdot v^4, u'^3 = u^3 \cdot v^6 \text{ für ein } v \in K \\ &\iff u' = u \cdot v^2 \text{ für ein } v \in K^*, \end{aligned}$$

woraus sofort die Behauptung folgt.

Die Fälle $j = 0$ und $j = 1728$ funktionieren analog. ■

**Beispiele:** Sei $K$ ein Körper der Charakteristik $\neq 2, 3$.

(1) Ist $K$ algebraisch abgeschlossen, so ist $K^* = K^{*2} = K^{*4} = K^{*6}$, zu jedem $j \in K$ gibt es also bis auf Isomorphie genau eine elliptische Kurve mit $j$-Invariante $j$.

(2) Für $K = \mathbf{R}$ sind $K^{*2} = K^{*4} = K^{*6} = \mathbf{R}_{>0}$ die positiven reellen Zahlen, als Repräsentanten von $K^*/K^{*2\ell}$ kann man also 1 und $-1$ wählen. Zu jedem $j \in \mathbf{R}$ gibt es also genau zwei elliptische Kurven über $\mathbf{R}$ mit $j$-Invariante $j$.

**Beispiel:** Wir wollen nochmals alle elliptischen Kurven $E$ über $\mathbf{F}_5$ angeben zusammen mit $j = j(E)$ und $N = E(\mathbf{F}_5)$.

$$\begin{aligned}
j = 0: &\quad y^2 = x^3 + 1 \quad (N = 6), \quad y^2 = x^3 + 2 \quad (N = 6)\\
j = 1: &\quad y^2 = x^3 + x + 2 \quad (N = 4), \quad y^2 = x^3 + 4x + 1 \quad (N = 8)\\
j = 2: &\quad y^2 = x^3 + x + 1 \quad (N = 9), \quad y^2 = x^3 + 4x + 2 \quad (N = 3)\\
j = 3: &\quad y^2 = x^3 + x \quad (N = 4), \quad y^2 = x^3 + 2x \quad (N = 2),\\
&\quad y^2 = x^3 + 3x \quad (N = 10), \quad y^2 = x^3 + 4x \quad (N = 8)\\
j = 4: &\quad y^2 = x^3 + 2x + 1 \quad (N = 7), \quad y^2 = x^3 + 3x + 2 \quad (N = 5)
\end{aligned}$$

Wir wollen eine Formel für die Anzahl elliptischer Kurven über $\mathbf{F}_p$ angeben. Wir beginnen mit einem Lemma.

LEMMA. *Sei $G$ eine multiplikativ geschriebene zyklische Gruppe der Ordnung $d$. Dann gilt:*

(1) *Für $\ell \in \mathbf{N}$ ist $G^\ell = G^{\mathrm{ggT}(d,\ell)}$.*
(2) *Ist $d = d_1 d_2$, so ist der Kern der Abbildung $G \to G^{d_1}$, $x \mapsto x^{d_1}$ die Untergruppe $G^{d_2}$, insbesondere*
$$G/G^{d_2} \simeq G^{d_1}.$$
(3) *Mit $d = d_1 d_2$ ist $G^{d_2}$ die (eindeutig bestimmte zyklische) Untergruppe der Ordnung $d_1$.*
(4) *Für $\ell \in \mathbf{N}$ gilt*
$$\#G/G^\ell = \mathrm{ggT}(d, \ell).$$

*Beweis:* Übung. ■

SATZ. *Sei $p$ eine Primzahl $\geq 5$. Die Anzahl der $\mathbf{F}_p$-Isomorphieklassen elliptischer Kurven über $\mathbf{F}_p$ ist*

$$2p + \begin{cases} 6 & \text{für } p \equiv 1 \bmod 12,\\ 2 & \text{für } p \equiv 5 \bmod 12,\\ 4 & \text{für } p \equiv 7 \bmod 12,\\ 0 & \text{für } p \equiv 11 \bmod 12. \end{cases}$$

*Beweis:* Sei $K_p$ die Anzahl der $\mathbf{F}_p$-Isomorphieklassen elliptischer Kurven über $\mathbf{F}_p$. Für $j \neq 0, 1728$ gibt es $\#\mathbf{F}_p^*/\mathbf{F}_p^{*2}$ Isomorphieklassen, für $j = 0$ gibt es $\#\mathbf{F}_p^*/\mathbf{F}_p^{*6}$ Isomorphieklassen, für $j = 1728$ gibt es $\#\mathbf{F}_p^*/\mathbf{F}_p^{*4}$ Isomorphieklassen. Da $j$ alle Zahlen von $\mathbf{F}_p$ durchlaufen kann und da $\mathbf{F}_p^*$ zyklisch von Ordnung $p-1$ ist, folgt

$$\begin{aligned}
K_p &= (p-2) \cdot \#\mathbf{F}_p^*/\mathbf{F}_p^{*2} + \#\mathbf{F}_p^*/\mathbf{F}_p^{*4} + \#\mathbf{F}_p^*/\mathbf{F}_p^{*6} =\\
&= (p-2)\mathrm{ggT}(p-1,2) + \mathrm{ggT}(p-1,4) + \mathrm{ggT}(p-1,6) =\\
&= 2(p-2) + \mathrm{ggT}(p-1,4) + \mathrm{ggT}(p-1,6) = 2p + \mathrm{ggT}(p-1,4) + \mathrm{ggT}(p-1,6) - 2.
\end{aligned}$$

Da $\mathrm{ggT}(p-1,4) + \mathrm{ggT}(p-1,6)$ nur von der Restklasse von $p$ modulo 12 abhängt, erhält man die Behauptung durch Überprüfen der angegebenen Fälle. ■

**Verfahren:** Zu $j \in \mathbf{F}_p$ soll ein Repräsentantensystem aller elliptischer Kurven über $\mathbf{F}_p$ mit $j$-Invariante $j$ gegeben werden.

(1) $j = 0$:
   (a) $p \equiv 1 \bmod 6$: Suche durch Probieren von $u = 2, 3, \ldots$ ein $u$ mit
   $$u^{(p-1)/2} \neq 1, \quad u^{(p-1)/3} \neq 1.$$
   Dann ist
   $$y^2 = x^3 + 1, \quad y^2 = x^3 + u, \quad y^2 = x^3 + u^2, \quad y^2 = x^3 + u^3, \quad y^2 = x^3 + u^4, \quad y^2 = x^3 + u^5$$
   ein Repräsentantensystem.

(b) $p \equiv 5 \bmod 6$: Bestimme ein $u$ mit

$$u^{(p-1)/2} \neq 1.$$

Dann wird ein Repräsentantensystem gegeben durch

$$y^2 = x^3 + 1, \quad y^2 = x^3 + u.$$

(2) $j = 1728$: Bestimme $u = 2, 3, \ldots$ mit

$$u^{(p-1)/2} \neq 1.$$

(a) $p \equiv 1 \bmod 4$:

$$y^2 = x^3 + x, \quad y^2 = x^3 + ux, \quad y^2 * x^3 + u^2 x, \quad y^2 * x^3 + u^3 x.$$

(b) $p \equiv 3 \bmod 4$:

$$y^2 = x^3 + x, \quad y^2 = x^3 + ux.$$

(3) $j \neq 0, 1728$: Bestimme $u$ mit

$$u^{(p-1)/2} \neq 1.$$

Berechne

$$c = \frac{j}{j - 1728}, \quad a = -3c, \quad b = 2c.$$

Dann ist

$$y^2 = x^3 + ax + b, \quad y^2 = x^3 + au^2 x + bu^3$$

ein Repräsentantensystem.

*Beweis:* Sei $g$ ein Erzeuger der Gruppe $\mathbf{F}_p^*$. Wir schreiben $u = g^m$ mit $0 \leq m \leq p-2$. Aus

$$1 \neq u^{(p-1)/2} = u^{m(p-1)/2}$$

folgt $p - 1 \nmid m\frac{p-1}{2}$, also $2 \nmid m$. Analog folgt im Fall $u^{(p-1)/3} \neq 1$, dass $3 \nmid m$ gilt. Wir betrachten den Fall $p \equiv 1 \bmod 6$ und $j = 0$: Nun gilt

$$\begin{aligned}
\frac{u^i}{u^j} \in \mathbf{F}_p^{*6} &\iff u^{i-j} = g^{6n} \text{ für ein } n \\
&\iff g^{m(i-j)} = g^{6n} \text{ für ein } n \\
&\iff m(i-j) \equiv 6n \bmod (p-1) \text{ für ein } n \\
&\implies m(i-j) \equiv 0 \bmod 6 \\
&\implies (i-j) \equiv 0 \bmod 6 \\
&\implies i \equiv j \bmod 6.
\end{aligned}$$

Dies zeigt, dass $1, u, u^2, u^3, u^4, u^5$ tatsächlich $\mathbf{F}_p^*/\mathbf{F}_p^{*6}$ repräsentieren. ■

## 4. Diskriminante und $j$-Invariante für die allgemeine Gleichung

Wir wollen jetzt sehen, wie man ausgehend von den Formeln für elliptische Kurven der Form $y^2 = x^3 + ax + b$ zu Formeln für Kurven der Form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ kommt. Dabei setzen wir zunächst wieder Charakteristik $\neq 2, 3$ voraus.

Wir erinnern zunächst an die allgemeinen Transformationsformeln: Zwei elliptische Kurven

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{und} \quad y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

sind genau dann isomorph über $K$, wenn es $u \in K^*$ und $r, s, t \in K$ gibt mit

$$\begin{aligned}
ua_1' &= a_1 + 2s, \\
u^2a_2' &= a_2 + 3r - s^2 - sa_1, \\
u^3a_3' &= a_3 + 2t + ra_1, \\
u^4a_4' &= a_4 + 3r^2 - 2st - (rs + t)a_1 + 2ra_2 - sa_3, \\
u^6a_6' &= a_6 + r^3 - t^2 - rta_1 + r^2a_2 - ta_3 + ra_4.
\end{aligned}$$

Wir beginnen mit einer elliptischen Kurve $E$ mit der Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

(in Charakteristik $\neq 2, 3$). Wählt man

$$s = -\frac{1}{2}a_1, \quad r = -\frac{1}{12}a_1^2 - \frac{1}{3}a_2, \quad t = \frac{1}{24}a_1^3 + \frac{1}{6}a_1a_2 - \frac{1}{2}a_3, \quad u = 1,$$

so ist die Kurve $E_{a,b}$ mit der Gleichung $y^2 = x^3 + ax + b$ und

$$\begin{aligned} a &= \frac{1}{48}(-16a_2^2 - a_1^4 - 8a_1^2a_2 + 48a_4 + 24a_1a_3), \\ b &= \frac{1}{864}(864a_6 + 12a_1^4a_2 + a_1^6 - 288a_4a_2 + 216a_3^2 + 64a_2^3 - 36a_1^3a_3 + 48a_1^2a_2^2 - 144a_1a_2a_3 - 72a_4a_1^2) \end{aligned}$$

über $K$ zu $E$ isomorph.
Man rechnet nun leicht nach, dass für das früher definierte

$$\begin{aligned} \Delta = {} & 288a_4a_2a_6 + a_1^5a_4a_3 + 144a_2a_1a_6a_3 - 64a_4^3 - 96a_4^2a_1a_3 + 72a_1^2a_6a_4 + 16a_2^2a_4^2 - 432a_6^2 \\ & -27a_3^4 + a_1^4a_4^2 - 30a_4a_1^2a_3^2 + 8a_2a_4^2a_1^2 - a_1^6a_6 + 72a_2a_4a_3^2 - 216a_6a_3^2 - 64a_2^3a_6 + a_3^3a_1^3 \\ & -16a_2^3a_3^2 + 36a_2a_3^3a_1 + 8a_2a_4a_3a_1^3 - a_2a_3^2a_1^4 + 16a_2^2a_4a_3a_1 - 8a_2^2a_3^2a_1^2 + 36a_6a_3a_1^3 \\ & -48a_2^2a_6a_1^2 - 12a_1^4a_2a_6 \end{aligned}$$

die Beziehung

$$4a^3 + 27b^2 = -\frac{1}{16}\Delta$$

gilt. Damit ist klar, dass gilt:

$$E \text{ nichtsingulär} \quad \Longleftrightarrow \quad \Delta \neq 0.$$

Außerdem verifiziert durch Einsetzen in die Formel mit Maple, dass bei einem allgemeinen Koordinatenwechsel (wie oben) die Beziehung

$$\Delta' = \frac{1}{u^{12}}\Delta$$

gilt, wobei $\Delta'$ mit den Koeffizienten von $y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$ gebildet wurde.

Wir betrachten jetzt die $j$-Invariante. Setzt man

$$A = 16a_2^2 + a_1^4 + 8a_1^2a_2 - 48a_4 - 24a_1a_3,$$

so gilt zunächst

$$a = -\frac{1}{48}A$$

und damit dann

$$j = 1728\frac{4a^3}{4a^3 + 27b^2} = \frac{A^3}{\Delta}.$$

Nun stellt man fest, dass bei einem allgemeinen Koordinatenwechsel

$$A' = \frac{1}{u^4}A$$

gilt, was sofort

$$j' = j$$

liefert. D.h. die durch $j = \frac{A^3}{\Delta}$ definierte Invariante ändert sich nicht bei Koordinatenwechsel und stimmt mit der für die Gleichung $y^2 = x^3 + ax + b$ definierten $j$-Invariante überein.

Wir müssen jetzt noch zeigen, dass die allgemeinen Formeln auch in Charakteristik 2 und 3 sinnvoll sind. Wir beschränken uns auf Charakteristik 2.

## 5. Elliptische Kurven in Charakteristik 2

Wir setzen jetzt einen Körper der Charakteristik 2 voraus. Für die allgemeine Gleichung $y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$ ergeben die obigen Formeln

$$\begin{aligned} \Delta &= a_3^3a_1^3 + a_1^5a_4a_3 + a_1^6a_6 + a_3^4 + a_2a_3^2a_1^4 + a_1^4a_4^2, \\ A &= a_1^4, \\ j &= \frac{a_1^{12}}{\Delta}. \end{aligned}$$

Unsere allgemeinen Transformationsformeln zeigen, dass zwei Kurven

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{und} \quad y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

(in Charakteristik 2) genau dann isomorph über $K$ sind, wenn es $u \in K^*$, $r, s, t \in K$ gibt mit

$$\begin{aligned} ua_1' &= a_1, \\ u^2a_2' &= a_2 + r + s^2 + sa_1, \\ u^3a_3' &= a_3 + ra_1, \\ u^4a_4' &= a_4 + r^2 + (rs + t)a_1 + sa_3, \\ u^6a_6' &= a_6 + r^3 + t^2 + rta_1 + r^2a_2 + ta_3 + ra_4. \end{aligned}$$

wobei der zugehörige Koordinatenwechsel durch

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t$$

definiert wird.

**5.1. Der Fall: $a_1 \neq 0$.** Wir wählen nacheinander

$$u = a_1, \quad r = \frac{a_3}{a_1}, \quad s = 0, \quad t = \frac{a_4 + r^2}{a_1}$$

und erhalten dann

$$a_1' = 1, \quad a_3' = 0, \quad a_4' = 0.$$

Wir können also die Gleichung (nach Umbenennung) schreiben als

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

Wann ist diese Kurve singulär? Wir schreiben $f = (y^2 + xy) - (x^3 + a_2x^2 + a_6)$ und erhalten

$$\frac{\partial f}{\partial x} = y + x^2, \quad \frac{\partial f}{\partial y} = x,$$

also kommt als Singularität nur $(x, y) = (0, 0)$ in Frage. Dieser Punkt liegt genau dann auf der Kurve, wenn $a_6 = 0$ gilt. Tatsächlich gilt $\Delta = a_6$, d.h. $\Delta = 0$ beschreibt das Vorkommen von Singularitäten. Weiter gilt nun $j = \frac{1}{a_6}$. Wir können also die Kurvengleichung auch durch

$$y^2 + xy = x^3 + ax^2 + \frac{1}{j}$$

beschreiben mit $a \in K$.
Zwei Kurven

$$y^2 + xy = x^3 + ax^2 + \frac{1}{j} \quad \text{und} \quad y^2 + xy = x^3 + a'x^2 + \frac{1}{j}$$

sind genau dann isomorph, wenn es $u \in K^*$, $r, s, t \in K$ gibt mit

$$\begin{aligned} u &= 1, \\ u^2a' &= a + r + s^2 + s, \\ 0 &= r, \\ 0 &= r^2 + rs + t, \\ u^6\frac{1}{j} &= \frac{1}{j} + r^3 + t^2 + rt + r^2a, \end{aligned}$$

was äquivalent zu

$$u = 1, \quad r = 0, \quad t = 0, \quad a' = a + s^2 + s$$

ist. Wir fassen das Erreichte zusammen:

SATZ. *Sei $K$ ein Körper der Charakteristik 2 und $j \in K, j \neq 0$.*

(1) *Ist $E$ eine elliptische Kurve über $K$ mit $j(E) = j$, so lässt sich $E$ durch eine Gleichung*

$$y^2 + xy = x^3 + ax^2 + \frac{1}{j} \quad \text{mit} \quad a \in K$$

*beschreiben.*

(2) *Zwei Kurven*

$$y^2 + xy = x^3 + ax^2 + \frac{1}{j} \quad \text{und} \quad y^2 + xy = x^3 + a'x^2 + \frac{1}{j}$$

*genau dann isomorph über $K$, wenn $s \in K$ existiert mit $a' = a + s + s^2$.*

**Beispiel:** Zu $K = \mathbf{F}_2$, $j = 1$ gibt es die zwei elliptischen Kurven $y^2+xy = x^3+1$ und $y^2+xy = x^3+x^2+1$.

**Bemerkung:** Für einen Körper der Charakteristik 2 ist $s \mapsto s^2 - s$ ein Gruppenhomomorphismus der additiven Gruppe des Körpers, der Kern ist $\{0, 1\}$. Für $K = \mathbf{F}_{2^m}$ ist also $\{s^2-s : s \in K\}$ eine Untergruppe vom Index 2. Damit folgt sofort der Satz:

FOLGERUNG. *Ist $K = \mathbf{F}_{2^m}$ und $c \in K \setminus \{s^s - s : s \in K\}$, so sind*

$$y^2 + xy = x^3 + \frac{1}{j} \quad \text{und} \quad y^2 + xy = x^3 + cx^2 + \frac{1}{j}$$

*Repräsentanten der $K$-Isomorphieklassen elliptischer Kurven über $K$ mit $j$-Invariante $j \neq 0$.*

**5.2. Der Fall $a_1 = 0$.** Die Transformationsformeln lauten nun

$$\begin{aligned} ua_1' &= 0, \quad \text{also} \quad a_1' = 0, \\ u^2a_2' &= a_2 + r + s^2, \\ u^3a_3' &= a_3, \\ u^4a_4' &= a_4 + r^2 + sa_3, \\ u^6a_6' &= a_6 + r^3 + t^2 + r^2a_2 + ta_3 + ra_4. \end{aligned}$$

Durch Wahl von $u = 1$, $r = a_2$, $s = t = 0$ lässt sich also die Gleichung $y^2 + a_3'y = x^3 + a_4'x + a_6'$ erreichen. D.h. jede Kurve mit $a_1 = 0$ ist isomorph zu einer Kurve mit der Gleichung

$$y^2 + a_3y = x^3 + a_4x + a_6.$$

Wann ist eine Kurve mit dieser Gleichung singulär? Wir setzen $f = (y^2 + a_3y) - (x^3 + a_4x + a_6)$ und erhalten

$$\frac{\partial f}{\partial x} = x^2 + a_4, \quad \frac{\partial f}{\partial y} = a_3.$$

Ist $a_3 \neq 0$, so gibt es keine Singularität. Ist $a_3 = 0$, wählt erhält man aus den Gleichungen $x_0^2 = a_4$, $y_0^2 = x_0^3 + a_4x_0 + a_6 = a_6$ eine Singularität $(x_0, y_0)$. Da $\Delta = a_3^4$ gilt, sieht man, dass auch in diesem Fall $\Delta \neq 0$ die Bedingung für Nichtsingularität ist.

Wir erhalten nun folgenden Satz:

SATZ. *Eine elliptische Kurve in Charakteristik 2 mit $j$-Invariante 0 lässt sich durch eine Gleichung*

$$y^2 + a_3y = x^3 + a_4x + a_6$$

*beschreiben. Zwei Kurven (mit $j$-Invariante 0)*

$$y^2 + a_3y = x^3 + a_4x + a_6 \text{ und } y^2 + a_3'y = x^3 + a_4'x + a_6'$$

*sind genau dann isomorph über $K$, wenn $u, s, t \in K$ existieren mit*

$$\begin{aligned} u^3 a_3' &= a_3, \\ u^4 a_4' &= a_4 + s a_3 + s^4, \\ u^6 a_6' &= a_6 + s^2 a_4 + t a_3 + s^6 + t^2, \end{aligned}$$

**Beispiel:** Über $\mathbf{F}_2$ gibt es genau 3 Isomorphieklassen elliptischer Kurven mit $j = 0$. Repräsentanten sind:

$$y^2 + y = x^3, \quad y^2 + y = x^3 + x, \quad y^2 + y = x^3 + x + 1.$$

FOLGERUNG. *Eine elliptische Kurve $E$ in Charakteristik 2 mit $j$-Invariante 0 ist über dem algebraischen Abschluss isomorph zu*

$$y^2 + y = x^3.$$

KAPITEL 5

# Punkte auf elliptischen Kurven über $\mathbf{F}_p$

Wir betrachten im Folgenden elliptische Kurven über Körpern $\mathbf{F}_p$, wo $p$ eine Primzahl $\geq 5$ ist. $E$ lässt sich durch eine Gleichung $y^2 = x^3 + ax + b$ beschreiben. Die Menge

$$E(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = x^3 + ax + b\} \cup \{O\}$$

wird durch die früher definierte Addition zu einer abelschen Gruppe mit $O = (0 : 0 : 1)$ als neutralem Element.
Wie findet man einen nichttrivialen Punkt $(x_0, y_0) \in E(\mathbf{F}_p)$? Gibt man sich $x_0 \in \mathbf{F}_p$ vor, so muss man untersuchen, ob die Gleichung

$$Y^2 = x_0^3 + ax_0 + b$$

in $\mathbf{F}_p$ lösbar ist, d.h. man muss

- untersuchen, ob $x_0^3 + ax_0 + b$ ein Quadrat in $\mathbf{F}_p$ ist, und
- gegebenenfalls eine Quadratwurzel von $x_0^3 + ax_0 + b$ in $\mathbf{F}_p$ bestimmen.

## 1. Das Legendre-Symbol

Wir erinnern an eine wichtige Eigenschaft der multiplikativen Gruppe eines endlichen Körpers:

LEMMA. *Ist $K$ ein endlicher Körper, so ist die multiplikative Gruppe $K^*$ zyklisch.*

*Beweis:* Der Hauptsatz über endliche abelsche Gruppe besagt, dass $d_1, d_2, \ldots, d_r \in \mathbf{N}$ existieren mit

$$K^* \simeq Z_{d_1} \oplus Z_{d_2} \oplus \cdots \oplus Z_{d_r} \quad \text{und} \quad d_1 | d_2 | \ldots | d_r.$$

Im Fall $\#K^* = 1$, also $K \simeq \mathbf{F}_2$, ist nichts zu zeigen. Daher können wir o.E. $d_1 \geq 2$ voraussetzen. Dann gibt es in $K^*$ eine zu

$$Z_{d_1} \oplus Z_{d_1} \oplus \cdots \oplus Z_{d_1}$$

isomorphe Untergruppe, also erhält man $d_1^r$ Elemente von $K$, die Nullstellen des Polynoms $x^{d_1} - 1$ sind. In einem Körper hat aber ein Polynom vom Grad $d_1$ höchstens $d_1$ Nullstellen. Dies impliziert $r = 1$ und damit $K^* \simeq Z_{d_1}$, was die Behauptung liefert. ■

Im Folgenden bezeichnet $p$ eine ungerade Primzahl. Wir interessieren uns für die Quadrate in $\mathbf{F}_p$, d.h. für die Menge

$$Q = \{a^2 \in \mathbf{F}_p^* : a \in \mathbf{F}_p^*\}.$$

Wir erinnern an ein früher erwähntes Lemma über endliche zyklische Gruppen:

LEMMA. *Ist $G$ eine (multiplikativ geschriebene) zyklische Gruppe der Ordnung $d$ und $d = d_1 d_2$, so gilt für $x \in G$:*

$$x \in G^{d_1} \quad \Longleftrightarrow \quad x^{d_2} = 1.$$

Das Lemma impliziert sofort folgendes Satz:

SATZ. *Sei $p$ eine ungerade Primzahl. Dann gilt für $a \in \mathbf{F}_p^*$:*

$$a \text{ ist Quadrat in } \mathbf{F}_p^* \quad \Longleftrightarrow \quad a^{\frac{p-1}{2}} = 1.$$

**Bemerkung:** Da wir mit der square-and-multiply-Methode für $a \in \mathbf{Z}$ schnell $a^{\frac{p-1}{2}} \bmod p$ berechnen können, können wir schnell testen, ob $a \in \mathbf{F}_p^*$ ein Quadrat ist oder nicht.

**Beispiel:** $p = 10^{1000} + 453$ ist (wahrscheinlich) prim. Nun ist

$$1009^{\frac{p-1}{2}} \equiv 1 \bmod p, \quad 1013^{\frac{p-1}{2}} \equiv -1 \bmod p,$$

d.h. 1009 ist Quadrat modulo $p$, 1013 ist kein Quadrat modulo $p$.

**Bemerkung:** Ist $a \in \mathbf{F}_p^*$ mit $a^{\frac{p-1}{2}} \neq 1$, so ist

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1,$$

also bleibt nur die Möglichkeit

$$a^{\frac{p-1}{2}} = -1.$$

Für $a \in \mathbf{F}_p$ gibt es also drei Möglichkeiten:

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & a \in \mathbf{F}_p^{*2}, \\ -1 & a \in \mathbf{F}_p^* \setminus \mathbf{F}_p^{*2}, \\ 0 & a = 0. \end{cases}$$

Die historische Entwicklung war nicht so direkt:

DEFINITION. Für eine ungerade Primzahl $p$ und eine ganze Zahl $a$ definiert man das Legendre-Sysmbol durch

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } b \in \mathbf{Z} \text{ existiert mit } a \equiv b^2 \bmod p \text{ und } \mathrm{ggT}(a,p) = 1 \text{ ist}, \\ -1, & \text{falls kein } b \in \mathbf{Z} \text{ existiert mit } a \equiv b^2 \bmod p, \\ 0, & \text{falls } a \equiv 0 \bmod p. \end{cases}$$

Ist $\left(\frac{a}{p}\right) = 1$, so nennt man $a$ einen quadratischen Rest modulo $p$ oder auch ein Quadrat modulo $p$, ist $\left(\frac{a}{p}\right) = -1$, so nennt man $a$ einen quadratischen Nichtrest modulo $p$.

Aus der Definition ersieht man, dass aus $a \equiv a' \bmod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$, also kann man das Legendre-Symbol $\left(\frac{\cdot}{p}\right)$ auch als Funktion auf $\mathbf{F}_p$ auffassen.

**Beispiel:** Das frühere Beispiel kann man jetzt mit $p = 10^{1000} + 453$ so schreiben:

$$\left(\frac{1009}{p}\right) = 1, \quad \left(\frac{1013}{p}\right) = -1.$$

Wir fassen einige Eigenschaften des Legendre-Symbols, die sich direkt aus unseren obigen Überlegungen ergeben, nochmals zusammen:

SATZ. *Das Legendre-Symbol hat folgende Eigenschaften:*

(1)
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$
*d.h.*
$$\mathbf{F}_p^* \to \{\pm 1\}, \quad a \mapsto \left(\frac{a}{p}\right)$$
*ist ein Gruppenhomomorphismus.*

(2) *Es gibt genau so viele Quadrate wie Nichtquadrate in $\mathbf{F}_p^*$, d.h.*
$$\#\{a^2 \in \mathbf{F}_p^* : a \in \mathbf{F}_p^*\} = \frac{p-1}{2}.$$

(3) *(Euler)*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

*(Mit der square-and-multiply-Methode kann man dann $\left(\frac{a}{p}\right)$ schnell berechnen.)*

Unter Benutzung der Eulerschen Formeln haben wir zwei gmp-Funktionen legendre1 und legendre2 geschrieben, die im Anhang zu finden sind.

Der folgende Satz ist ein wichtiger Satz der Zahlentheorie, für den Gauß mehrere Beweise geliefert hat:

SATZ (Quadratisches Reziprozitätsgesetz). (1) *Für ungerade Primzahlen $p$ und $q$ gilt:*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4, \\ -\left(\frac{q}{p}\right), & \text{falls } p \equiv q \equiv -1 \bmod 4. \end{cases}$$

*In geschlossener Form schreibt sich dies als*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}.$$

(2) *(Ergänzungssätze zum quadratischen Reziprozitätsgesetz)*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4, \\ -1, & \text{falls } p \equiv 3 \bmod 4, \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv 1, 7 \bmod 8, \\ -1, & \text{falls } p \equiv 3, 5 \bmod 8. \end{cases}$$

*In geschlossener Form lassen sich die Gleichungen so schreiben:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

**Beispiel:** Für $p = 10^{1000} + 453$ berechnen wir mit Hilfe des quadratischen Reziprozitätsgesetzes und der vorangegangenen Formeln:

$$\begin{aligned} \left(\frac{1009}{p}\right) &= \left(\frac{p}{1009}\right) = \left(\frac{p \bmod 1009}{1009}\right) = \left(\frac{417}{p}\right) = \left(\frac{3 \cdot 139}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{139}{1009}\right) = \\ &= \left(\frac{1009}{3}\right)\left(\frac{1009}{139}\right) = \left(\frac{1009 \bmod 3}{3}\right)\left(\frac{1009 \bmod 139}{139}\right) = \left(\frac{1}{3}\right)\left(\frac{36}{139}\right) = 1. \end{aligned}$$

Mit dem quadratischen Reziprozitätsgesetz kann man das Legendre-Symbol $\left(\frac{a}{p}\right)$ auf die Berechnung von Legendre-Symbolen $\left(\frac{a'}{p'}\right)$ mit Primzahlen $p' < p$ zurückführen. Praktisch undurchführbar wird das aber, wenn man notwendige Primfaktorzerlegungen nicht bestimmen kann. Umgehen kann man das durch Einführung des Jacobi-Symbols:

DEFINITION. Für $m, n \in \mathbf{Z}$, $n \geq 1$, $n \equiv 1 \bmod 2$ wird das Jacobi-Symbol durch

$$(\frac{m}{n}) = \prod_i (\frac{m}{p_i})^{e_i} \text{ mit der Primfaktorzerlegung } n = \prod_i p_i^{e_i}$$

definiert, wo $(\frac{m}{p_i})$ das Legendre-Symbol ist. (Das Jacobi-Symbol verallgemeinert also das Legendre-Symbol.)

**Achtung:** Das Jacobi-Symbol $\left(\frac{a}{n}\right)$ wird über das Legendre-Symbol definiert, nicht über die Lösbarkeit einer Gleichung $x^2 \equiv a \bmod n$.

Folgende Eigenschaften ergeben sich aus den entsprechenden Eigenschaften für des Legendre-Symbol:

SATZ. *Für das Jacobi-Symbol gilt:*

(1)

$$(\frac{m}{n}) = (\frac{m \bmod n}{n}).$$

(2) *Das Jacobi-Symbol ist multiplikativ:*

$$(\frac{m_1 m_2}{n}) = (\frac{m_1}{n})(\frac{m_2}{n}).$$

(3) *Es gilt das quadratische Reziprozitätsgesetz:*

$$(\frac{m}{n}) = \begin{cases} (\frac{n}{m}) & \textit{falls } m \equiv 1 \bmod 4 \textit{ oder } n \equiv 1 \bmod 4, \\ -(\frac{n}{m}) & \textit{falls } m \equiv n \equiv -1 \bmod 4. \end{cases}$$

(4)

$$(\frac{-1}{n}) = \begin{cases} 1 & \textit{für } n \equiv 1 \bmod 4, \\ -1 & \textit{für } n \equiv 3 \bmod 4, \end{cases} \qquad (\frac{2}{n}) = \begin{cases} 1 & \textit{für } n \equiv 1, 7 \bmod 8, \\ -1 & \textit{für } n \equiv 3, 5 \bmod 8. \end{cases}$$

Mit den Eigenschaften des Satzes kann man das Jacobi-Symbol und damit das Legendre-Symbol schnell berechnen.

**Beispiel:** Sei $p = 10^{1000} + 453$. Dann ist

$$\begin{aligned} \left(\frac{1009}{p}\right) &= \left(\frac{p \bmod 1009}{1009}\right) = \left(\frac{417}{1009}\right) = \left(\frac{1009 \bmod 417}{417}\right) = \left(\frac{175}{417}\right) = \\ &= \left(\frac{417 \bmod 175}{175}\right) = \left(\frac{67}{175}\right) = -\left(\frac{175 \bmod 67}{67}\right) = -\left(\frac{41}{67}\right) = \\ &= -\left(\frac{67 \bmod 41}{41}\right) = -\left(\frac{26}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{13}{41}\right) = -1 \cdot \left(\frac{41 \bmod 13}{13}\right) = \\ &= -\left(\frac{2}{13}\right) = 1. \end{aligned}$$

Das Beispiel verallgemeinert sich wie folgt:

**Verfahren zur Berechnung des Jacobi-Symbols $\left(\frac{m}{n}\right)$:** Wir wollen für $m \in \mathbf{Z}$ und $n \in \mathbf{N}$ das Symbol $\left(\frac{m}{n}\right)$ berechnen:

(1) Setze $m = m \bmod n$.

(2) Schreibe $m = 2^e u$ mit $u \equiv 1 \bmod 2$. Dann ist

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^e (-1)^{\frac{u-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{u}\right).$$

Beginne jetzt mit $\left(\frac{n}{u}\right)$ von vorne.

(Man beachte, dass man bei dieser Berechnungsmethode keine ungeraden Zahlen zu faktorisieren braucht.)

**Bemerkung:** In Maple gibt es die zugehörigen Funktionen 'numtheory[legendre]' und 'numtheory[jacobi]'.

## 2. Eine Formel für $\#E(\mathbf{F}_p)$

Mit Kenntnis des Legendre-Symbols können wir jetzt eine einfache Formel für die Anzahl der Punkte $\#E(\mathbf{F}_p)$ einer über $\mathbf{F}_p$ definierten elliptischen Kurve angeben.

Sei $E$ über $\mathbf{F}_p$ durch $y^2 = x^3 + ax + b$ gegeben. Zunächst gibt es den unendlich fernen Punkt $O = (0 : 0 : 1)$. Sei jetzt $x \in \mathbf{F}_p$.

- Es gibt 2 Punkte der Gestalt $(x, *) \in E(\mathbf{F}_p)$, wenn $x^2 + ax + b$ ein Quadrat $\neq 0$ in $\mathbf{F}_p$ ist, d.h. wenn $(\frac{x^3+ax+b}{p}) = 1$ ist.
- Es gibt einen Punkt der Gestalt $(x, *) \in E(\mathbf{F}_p)$, wenn $x^2+ax+b = 0$ ist, d.h. wenn $(\frac{x^3+ax+b}{p}) = 0$ ist.
- Es gibt keinen Punkt der Gestalt $(x, *) \in E(\mathbf{F}_p)$, wenn $x^3 + ax + b$ kein Quadrat in $\mathbf{F}_p$ ist, d.h. wenn $(\frac{x^3+ax+b}{p}) = -1$ ist.

Man sieht nun sofort: Es gibt genau

$$1 + (\frac{x^3 + ax + b}{p})$$

Punkte der Gestalt $(x, *)$ in $E(\mathbf{F}_p)$. Damit erhalten wir insgesamt

$$\#E(\mathbf{F}_p) = 1 + \sum_{x \in \mathbf{F}_p} (1 + (\frac{x^3 + ax + b}{p})) = p + 1 + \sum_{x \in \mathbf{F}_p} (\frac{x^3 + ax + b}{p}).$$

Wir formulieren das Ergebnis als Satz:

SATZ. *Wird $E_{a,b}$ über $\mathbf{F}_p$ durch $y^2 = x^3 + ax + b$ definiert, so gilt*

$$\#E(\mathbf{F}_p) = p + 1 + \sum_{x \in \mathbf{F}_p} (\frac{x^3 + ax + b}{p}).$$

Die Anzahl der Schritte ist also $O(p)$, wobei bei jedem Schritt ein Legendre-Symbol zu berechnen ist. Ist $p$ nicht zu groß, kann man $\#E(\mathbf{F}_p)$ mit dieser Formel bequem berechnen. Es ist aber klar, dass man auf diese Weise $\#E(\mathbf{F}_p)$ für größere $p$'s nicht berechnen kann.

Wir geben sofort eine Anwendung der Formel:

SATZ. *Sei $p \geq 5$ eine Primzahl und $u \in \mathbf{F}_p^*$ kein Quadrat, d.h. $\left(\frac{u}{p}\right) = -1$. Sind $a, b \in \mathbf{F}_p$ mit $4a^3 + 27b^2 \neq 0$, so gilt:*

(1) *$E_{a,b}$ und $E_{u^2a,u^3b}$ sind elliptische Kurven mit*

$$j(E_{a,b}) = j(E_{u^2a,u^3b}).$$

(2) *Für die Anzahl der $\mathbf{F}_p$-rationalen Punkte gilt:*

$$\#E_{a,b}(\mathbf{F}_p) + \#E_{u^2a,u^3b}(\mathbf{F}_p) = 2(p+1).$$

*Beweis:* Die erste Aussage wurde bereits früher erörtert bzw. lässt sich unmittelbar durch Einsetzen in die Formel $j(E_{a,b}) = 1728\frac{4a^3}{4a^3+27b^2}$ bestätigen. Nun gilt mit der Formel des letzten Satzes, da mit $x$ auch $ux$ ganz $\mathbf{F}_p$ durchläuft:

$$\begin{aligned}
\#E_{a,b}(\mathbf{F}_p) + \#E_{u^2a,u^3b}(\mathbf{F}_p) &= p + 1 + \sum_{x \in \mathbf{F}_p} \left(\frac{x^3 + ax + b}{p}\right) + p + 1 + \sum_{x \in \mathbf{F}_p} \left(\frac{x^3 + u^2ax + u^3b}{p}\right) = \\
&= 2p + 2 + \sum_{x \in \mathbf{F}_p} \left(\frac{x^3 + ax + b}{p}\right) + \sum_{x \in \mathbf{F}_p} \left(\frac{(ux)^3 + u^2a(ux) + u^3b}{p}\right) = \\
&= 2p + 2 + \sum_{x \in \mathbf{F}_p} \left(\left(\frac{x^3 + ax + b}{p}\right) + \left(\frac{u^3(x^3 + ax + b)}{p}\right)\right) = \\
&= 2p + 2 + (1 + \left(\frac{u^3}{p}\right)) \sum_{x \in \mathbf{F}_p} \left(\frac{x^3 + ax + b}{p}\right) = 2p + 2,
\end{aligned}$$

da $\left(\frac{u^3}{p}\right) = \left(\frac{u}{p}\right)^3 = (-1)^3 = -1$ gilt. ■

## 3. Der Satz von Hasse

Durch $y^2 = x^3 + ax + b$ werde eine elliptische Kurve $E$ über $\mathbf{F}_p$ definiert. Was kann man dann über $\#E(\mathbf{F}_p)$ sagen?

- Aus der Formel

$$\#E(\mathbf{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right)$$

sieht man sofort, dass

$$1 \leq \#E(\mathbf{F}_p) \leq 2p + 1$$

gilt.

- Die folgende Überlegung ist reine Spekulation: Die Hälfte aller Zahlen in $\mathbf{F}_p^*$ ist ein Quadrat. Sind die Werte von $x \mapsto x^3+ax+b$ also zufällig verteilt, so sollte ungefähr für die Hälfte aller $x$ gelten $\left(\frac{x^3+ax+b}{p}\right) = 1$, für die andere Hälfte aber $\left(\frac{x^3+ax+b}{p}\right) = -1$, sodass man insgesamt auf $\#E(\mathbf{F}_p) \approx p$ kommen würde.

Tatsächlich gilt der folgende wichtige Satz, dessen Beweis die bisher zur Verfügung stehenden elementaren Mittel allerdings übersteigt:

Satz (Hasse). *Für eine elliptische Kurve $E$ über $\mathbf{F}_p$ gilt*

$$p+1-2\sqrt{p} < \#E(\mathbf{F}_p) < p+1+2\sqrt{p}.$$

**Bemerkung:** Alle durch den Satz von Hasse zugelassenen Zahlen für $\#E(\mathbf{F}_p)$ kommen auch vor.

## 4. Quadratwurzeln modulo $p$

Mit dem Legendre-Symbol $\left(\frac{a}{p}\right)$ kann man entscheiden, ob die Gleichung $x^2 \equiv a \bmod p$ lösbar ist oder nicht. Wir geben jetzt ein Verfahren an, wie man im Fall der Lösbarkeit explizit eine Lösung konstruieren kann. Gleichzeitig mit der Darstellung des Verfahrens folgt die Begründung, die mit elementarer Gruppentheorie arbeitet und die folgenden Eigenschaften benutzt:

- $\mathbf{F}_p^*$ ist eine zyklische Gruppe der Ordnung $p-1$.
- Ist $G$ eine zyklische Gruppe der Ordnung $2^n$ und haben $g_1, g_2 \in G$ die gleiche Ordnung, so gilt
$$\operatorname{ord}(g_1 g_2) < \operatorname{ord}(g_1) = \operatorname{ord}(g_2).$$

**Algorithmus zur Berechnung von Quadratwurzeln modulo $p$:** Sei $p \geq 3$ eine Primzahl und $a \in \mathbf{F}_p^*$.

(1) Zerlege $p-1 = 2^e q$ mit $q \equiv 1 \bmod 2$ und $e \geq 1$. Da $\mathbf{F}_p^*$ zyklisch ist, gibt es genau eine Untergruppe $G \subseteq \mathbf{F}_p^*$ mit $\#G = 2^e$; $G$ ist dann ebenfalls zyklisch. Ist $n \in \mathbf{F}_p^*$, so ist $z = n^q \in G$. Genau dann erzeugt $z$ die Gruppe $G$, wenn $z$ kein Quadrat ist, was gleichwertig damit ist, dass $n$ kein Quadrat ist, d.h. dass $\left(\frac{n}{p}\right) = -1$ gilt. Dies ist leicht nachzuprüfen. Durch Probieren zufälliger $n$'s erhält man so schnell einen Erzeuger $z$ von $G$. Insbesondere $\operatorname{ord}(z) = 2^e$.

(2) Wir wollen rekursiv Folgen $x_i$ und $b_i$ konstruieren mit
$$x_i \in \mathbf{F}_p^*, \quad b_i \in G, \quad \operatorname{ord}(b_i) = 2^{e_i}, \quad ab_i = x_i^2.$$

(3) Wir beginnen mit $i = 0$,
$$b_0 = a^q \quad \text{und} \quad x_0 = a^{\frac{q+1}{2}},$$
denn dann gilt $b_0 \in G$ und $ab_0 = x_0^2$.

(4) Wir bestimmen $e_i$ mit $\operatorname{ord}(b_i) = 2^{e_i}$ durch Probieren: $e_i$ ist minimal mit der Eigenschaft $b_i^{2^{e_i}} = 1$, wobei $0 \leq e_i \leq e$ gilt.
   (a) Ist $e_i = 0$, also $b_i = 1$, so ist $x = x_i$ eine Lösung der Gleichung $x^2 = a$ und wir sind fertig.
   (b) Gilt $e_i = e$, so ist $b_i$ ein Erzeuger von $G$, also kein Quadrat, sodass wegen $ab_i = x_i^2$ auch $a$ kein Quadrat ist. Wir können dann aufhören.

(5) Wir haben nun $1 \leq e_i \leq e-1$ und können daher definieren
$$x_{i+1} = x_i z^{2^{e-e_i-1}} \in \mathbf{F}_p^* \quad \text{und} \quad b_{i+1} = b_i z^{2^{e-e_i}} \in G.$$
Dann gilt nämlich wie verlangt
$$ab_{i+1} = ab_i z^{2^{e-e_i}} = x_i^2 (z^{2^{e-e_i-1}})^2 = x_{i+1}^2.$$
Außerdem erhalten wir mit der Vorbemerkung und
$$\operatorname{ord}(b_i) = 2^{e_i} = \operatorname{ord}(z^{2^{e-e_i}})$$
die Beziehung
$$\operatorname{ord}(b_{i+1}) < \operatorname{ord}(b_i).$$
Wir gehen jetzt zurück zu 4.

(6) Es ist klar, dass das Verfahren wegen

$$\operatorname{ord}(b_0) = 2^e \quad \text{oder} \quad \operatorname{ord}(b_{i+1}) < \operatorname{ord}(b_i) < 2^e$$

nach endlich vielen Schritten aufhört.

**Beispiel:** Wir wählen $p = 1033$ und $a = 1009$ und wollen die Gleichung $x^2 \equiv a \bmod p$ untersuchen. Zunächst ist $p - 1 = 2^3 \cdot 129$, also $e = 3$, $q = 129$. Wegen $\left(\frac{5}{p}\right) = -1$ wählen wir $z \equiv 5^q \bmod p$, also $z = 802$. Dann ist

$$b_0 \equiv a^q \equiv 355 \bmod p \quad \text{und} \quad x_0 \equiv a^{\frac{q+1}{2}} \equiv 515 \bmod p.$$

Durch Probieren findet man $\operatorname{ord}(b_0) = 4$, also $e_0 = 2$. Mit

$$x_1 \equiv x_0 z^{2^{e-e_0-1}} = x_0 z \equiv 863 \bmod p \quad \text{und} \quad b_1 \equiv b_0 z^{2^{e-e_0}} \equiv b_0 z^2 \equiv 1 \bmod p$$

ergibt sich als Lösung der Gleichung $x = 863$. Natürlich ist dann auch $x = 146 = 1009 - 863$ eine Lösung.

**Bemerkung:** Bei obigem Verfahren muss man nicht wissen, ob $a$ tatsächlich ein Quadrat modulo $p$ ist.

Wir haben zu dem Verfahren eine Maple-Funktion sqrtmodp geschrieben. Maple hat eine eigene Funktion 'Roots$(x^2 - a)$ mod $p$'.

**Beispiel:** Für $p = 10^{100} + 267$ und $a = 10^{10} + 19$ erhält man sofort als Ergebnis der Gleichung $x^2 \equiv a \bmod p$:

```
581921505931718571869399326765058282618577252140381151420286130779371\
16973646563174669798144909160 71
```

Sowohl die Berechnung des Legendre-Symbols als auch das Quadratwurzelziehen modulo $p$ geht also sehr schnell.

**Beispiele:** Wir wenden den beschriebenen Algorithmus etwas allgemeiner an.

(1) Sei $p$ eine Primzahl mit $p \equiv 3 \bmod 4$ und $a \in \mathbf{F}_p^*$. Wir schreiben $p = 3 + 4m$ und erhalten $p - 1 = 2 + 4m = 2(1 + 2m)$, also $e = 1$ und $q = 1 + 2m = \frac{p-1}{2}$. Dann ist $G = \{1, -1\}$. Zu Beginn erhält man

$$b_0 = a^q = a^{\frac{p-1}{2}}, \quad x_0 = a^{\frac{q+1}{2}} = a^{\frac{p+1}{4}}.$$

Ist $b_0 = a^{\frac{p-1}{2}} = -1$, so ist $a$ kein Quadrat. Im andern Fall ist $x_0 = a^{\frac{p+1}{4}}$ eine Lösung der Gleichung $x_0^2 = a$.

(2) Sei $p$ eine Primzahl mit $p \equiv 5 \bmod 8$ und $a \in \mathbf{F}_p^*$. Wir schreiben $p = 5 + 8m$ und erhalten $p - 1 = 4 + 8m = 2^2(1 + 2m)$, also $e = 2$ und $q = 1 + 2m = \frac{p-1}{4}$. Die Gruppe $G \subseteq \mathbf{F}_p^*$ hat also 4 Elemente. Wegen $p \equiv 5 \bmod 8$ besagt ein Ergänzungssatz zum quadratischen Reziprozitätsgesetz, dass 2 kein Quadrat in $\mathbf{F}_p$ ist, d.h. $2^{\frac{p-1}{2}} = -1$. Wir wählen daher $z = 2^q = 2^{\frac{p-1}{4}}$. Dann ist $G = \{1, -1, z, z^3\}$ und $z^2 = -1$. Wir beginnen mit

$$b_0 = a^q = a^{\frac{p-1}{4}} \in G, \quad x_0 = a^{\frac{q+1}{2}} = a^{\frac{p+3}{8}}.$$

Wir unterscheiden drei Fälle:

(a) Ist $b_0 \in \{z, z^3\}$, so ist $a^{\frac{p-1}{2}} = b_0^2 = z^2 = -1$, also ist $a$ kein Quadrat in $\mathbf{F}_p$.

(b) Ist $b_0 = a^{\frac{p-1}{4}} = -1$, so ist $e_0 = 1$, also berechnen wir weiter

$$x_1 = x_0 z^{2^{e-e_0-1}} = x_0 z = a^{\frac{p+3}{8}} \cdot 2^{\frac{p-1}{4}}, \quad b_1 = b_0 z^{2^{e-e_0}} = b_0 z^2 = (-1)(-1) = 1,$$

also löst $x_1 = a^{\frac{p+3}{8}} \cdot 2^{\frac{p-1}{4}}$ die Gleichung $x_1^2 = a$.

(c) Ist $b_0 = a^{\frac{p-1}{4}} = 1$, so ist $x_0 = a^{\frac{p+3}{8}}$ eine Lösung der Gleichung $x_0^2 = a$.

Wir formulieren die Ergebnisse nochmals als Satz:

SATZ. *Sei $p$ eine Primzahl mit $p \equiv 3, 5, 7 \bmod 8$ und $a \in \mathbf{F}_p^2$ ein Quadrat, d.h. $a^{\frac{p-1}{2}} = 1$. Setzt man*

$$x = \begin{cases} a^{\frac{p+1}{4}} & \text{im Fall } p \equiv 3 \bmod 4, \\ a^{\frac{p+3}{8}} & \text{im Fall } p \equiv 5 \bmod 8 \text{ und } a^{\frac{p-1}{4}} = 1, \\ 2^{\frac{p-1}{4}} \cdot a^{\frac{p+3}{8}} & \text{im Fall } p \equiv 5 \bmod 8 \text{ und } a^{\frac{p-1}{4}} = -1, \end{cases}$$

*so gilt $x^2 = a$.*

## 5. Wie findet man einen Punkt in $E(\mathbf{F}_p)$?

Da wir nun gut Quadratwurzeln in $\mathbf{F}_p$ berechnen können, bietet sich folgendes probabilistische Verfahren an:
Sei $p$ eine ungerade Primzahl und $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbf{F}_p$.

(1) Wähle einen Startwert $x$ mit $0 \leq x \leq p - 1$.
(2) Berechne $x^3 + ax + b \bmod p$ und bestimme mit sqrtmodp, ob $y^2 = x^3 + a + x + b$ eine Lösung in $y$ hat.
(3) Hat $y^2 = x^3 + ax + b$ keine Lösung, setze $x := x + 1$ und gehe zu 2.
(4) Hat $y^2 = x^3 + ax + b$ eine Lösung, gib $(x, y)$ als Element von $E(\mathbf{F}_p)$ aus.

**Bemerkungen:**

(1) Wir haben dies als Maple-Funktion 'nxtpkt' programmiert.
(2) Wir überlegen naiv: die Hälfte aller Zahlen in $\mathbf{F}_p$ ist ein Quadrat, also sollte die Wahrscheinlichkeit, dass bei Vorgabe von $x$ die Gleichung $y^2 = x^3 + ax + b$ lösbar ist, ungefähr $\frac{1}{2}$ sein.

**Beispiele:** Wir haben zufällig elliptische Kurven gewählt und jeweils die ersten 10 Punkte bestimmt.

```
p=1009 (mit 10 Bits), a=963, b=881
1. Punkt: (0,440)
2. Punkt: (1,182)
3. Punkt: (8,4)
4. Punkt: (9,79)
5. Punkt: (10,307)
6. Punkt: (16,397)
7. Punkt: (18,43)
8. Punkt: (19,233)
9. Punkt: (20,54)
10. Punkt: (24,22)

p=1009, a=1003, b=999
1. Punkt: (0,303)
2. Punkt: (1,127)
3. Punkt: (2,457)
4. Punkt: (3,469)
5. Punkt: (4,78)
6. Punkt: (8,59)
7. Punkt: (11,341)
8. Punkt: (19,88)
9. Punkt: (20,118)
10. Punkt: (30,24)

p=10107427073962545517 (mit 64 Bits), a=3765701151230258868, b=5201686601578086531
1. Punkt: (0,4483156386101202728)
2. Punkt: (1,2744395708872277769)
3. Punkt: (4,3539021309230092863)
4. Punkt: (5,1513862121212883004)
5. Punkt: (8,4644377451977508570)
```

```
6. Punkt: (10,1729928990208888334)
7. Punkt: (11,188383560677094847)
8. Punkt: (13,1021841824971689384)
9. Punkt: (14,98660670316312194)
10. Punkt: (16,713643828735543401)

p=14077923117271886293 (mit 64 Bits), a=13817682715159570458, b=12803114839482524872
1. Punkt: (0,2837149296616859043)
2. Punkt: (1,4306418036842977213)
3. Punkt: (27,4813638594860221832)
4. Punkt: (30,477462003285670986)
5. Punkt: (36,1060704451214994465)
6. Punkt: (38,3446164586180115639)
7. Punkt: (40,5586410975462824893)
8. Punkt: (44,2277852371585410465)
9. Punkt: (46,1770456462980584890)
10. Punkt: (48,5729656515183883004)
```

**Bemerkung:** Ist $E$ eine durch $y^2 = x^3 + ax + b$ über $\mathbf{F}_p$ definierte elliptische Kurve und $P = (x, y) \in E(\mathbf{F}_p)$, so gibt es (im Allgemeinen) zwei Punkte mit $x$-Koordinate $x$, nämlich $(x, y)$ und $(x, -y) = (x, p - y)$. Will man $P$ in möglichst kurzer Form angeben, kann man die $x$-Koordinate angeben und dann mitteilen, welcher der beiden $y$-Werte zu $P$ gehört.

## 6. Einbettung von Text in eine elliptische Kurve

Hat man einen Text gegeben, so muss man natürlich den Worten irgendwie Punkte einer elliptischen Kurve zuordnen. Wie kann man das machen? Wir skizzieren ein probabilistisches Verfahren:

*1. Schritt:* Wir legen ein Alphabet mit $N$ Zeichen zugrunde, einigen uns auf eine Plaintextblocklänge $\ell$. Die Zeichen des Alphabets identifizieren wir mit den Zahlen $0, 1, 2, \ldots, N-1$. Durch die Zuordnung

$$\begin{aligned} w = (a_0 a_1 a_2 \ldots a_\ell) \quad &\mapsto \quad a_0 N^{\ell-1} + a_1 N^{\ell-2} + \cdots + a_{\ell-2} N + a_{\ell-1} = \\ &((\ldots(((a_0 N + a_1)N + a_2)N + a_3)\ldots)N + a_{\ell-2})N + a_{\ell-1} = x_w \end{aligned}$$

erhalten wir eine Bijektion zwischen den Plaintextblöcken $w$ und den Zahlen $0 \le x_w < N^\ell$.

*Überlegung:* Ist $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbf{F}_p$, so gibt es leider nicht zu jedem $x_0$ einen Kurvenpunkt $(x_0, y_0) \in E(\mathbf{F}_p)$. Man kann aber den nächsten Kurvenpunkt $(x_1, y_1) \in E(\mathbf{F}_p)$ (schnell) bestimmen. Ist eine natürliche Zahl $k$ vorgegeben, so sollte die Wahrscheinlichkeit, dass $x_0 \le x_1 < x_0 + k$ nicht gilt, in der Größenordnung von $(\frac{1}{2})^k$ sein. (Beispiel: Für $k = 50$ ist $(\frac{1}{2})^{50} < 10^{-15}$.)

*2. Schritt:* Wir wählen eine Zahl $k$, sodass die Wahrscheinlichkeit für das Scheitern des Verfahrens sehr gering ist. Wir wählen eine elliptische Kurve $E$ über $\mathbf{F}_p$ mit einer Primzahl

$$p > kN^\ell.$$

*3. Schritt:* Sei nun eine Zahl $x_w$ mit $0 \le x_w < N^\ell$ entsprechend einem Plaintextblock $w$ gegeben. Wir bestimmen den/einen ersten Punkt $P_w$ mit Koordinate $\ge kx_w$, d.h.

$$P_w = (kx_w + j, *) \in E(\mathbf{F}_p)$$

mit kleinstmöglichem $j \ge 0$. ($-P_w$ hat natürlich die gleiche $x$-Koordinate wie $P_w$.) Wir haben damit eine Zuordnung

$$\text{Plaintextblock } w \mapsto x_w \mapsto P_w.$$

*4. Schritt:* Wie erhält man aus einem Kurvenpunkt $P = (x, y) \in E(\mathbf{F}_p)$ den Plaintextblock $w$ zurück? Es gilt $x = kx_w + j$. Hat das Verfahren funktioniert, so ist $0 \le j < k$ und damit

$$x_w = \lfloor \frac{x}{k} \rfloor.$$

**Beispiel:** Wir wählen das Alphabet $\{A, B, C, \ldots, Z\}$, die übliche Bijektion mit $\{0, 1, 2, \ldots, 25\}$, also $N = 26$, Plaintextblocklänge $\ell = 2$. Weiter wählen wir $k = 10$. Dann erfüllt $p = 6833$ die Bedingung $p > kN^2 = 6760$. Sei $E$ über $\mathbf{F}_p$ gegeben durch $y^2 = x^3 + 5984x + 1180$. Wir setzen nach dem skizzierten Verfahren den Text KRYPTOSYSTEM in eine Folge von Punkten aus $E(\mathbf{F}_p)$ um:

| $w$ | $x_w$ | $kx_w$ | $P_w$ |
|---|---|---|---|
| KR | $(10, 17)_{26} = 277$ | 2770 | (2771,353) |
| YP | $(24, 15)_{26} = 639$ | 6390 | (6390,2797) |
| TO | $(19, 14)_{26} = 508$ | 5080 | (5080,238) |
| SY | $(18, 24)_{26} = 492$ | 4920 | (4920,1540) |
| ST | $(18, 19)_{26} = 487$ | 4870 | (4872,3315) |
| EM | $(4, 12)_{26} = 116$ | 1160 | (1160,2122) |

## 7. ElGamal-Verschlüsselung

**7.1. Das klassische ElGamal-Verschlüsselungsverfahren.** Die Sicherheit des nachfolgenden Verfahrens beruht auf der Schwierigkeit, diskrete Logarithmen in $\mathbf{F}_p^*$ zu berechnen.

**ElGamal-Verschlüsselung:**

(1) **Schlüsselerzeugung:**
   (a) Man wählt eine Primzahl $p$ und eine Zahl $g$ mit $2 \leq g \leq p-2$. Die Zahlen können systemweit benutzt werden. $g$ sollte eine möglichst große Untergruppe von $(\mathbf{Z}/p\mathbf{Z})^*$ erzeugen.
   (b) Jeder Teilnehmer $A$ wählt sich geheim eine Zahl $e_A$ mit $2 \leq e_A \leq p-2$ und berechnet $f_A \equiv g^{e_A} \bmod p$. Der öffentliche Schlüssel von $A$ ist $f_A$, der geheime Schlüssel $e_A$.

(2) **Verschlüsselung:**
   (a) Will $B$ eine Nachricht geheim an $A$ schicken, besorgt er sich zunächst den öffentlichen Schlüssel $f_A$ von $A$ und wandelt dann die Nachricht (nach einem vereinbarten Schema) in eine Folge von Zahlen $a_i$ mit $0 \leq a_i \leq p-1$ um.
   (b) Zu jedem $a_i$ wählt $B$ eine Zufallszahl $z_i$ und berechnet
   $$b_i \equiv g^{z_i} \bmod p, \quad c_i \equiv a_i f_A^{z_i} \bmod p.$$
   Die Folge $(b_i, c_i)$ wird an $A$ geschickt.

(3) **Entschlüsselung:** $A$ empfängt $(b_i, c_i)$ und berechnet sich damit die Ausgangsnachricht:
$$b_i^{p-1-e_A} c_i \equiv g^{z_i(p-1-e_A)} a_i f_A^{z_i} \equiv g^{z_i(p-1-e_A)} a_i g^{e_A z_i} \equiv g^{z_i(p-1)} a_i \equiv a_i \bmod p.$$
(Dabei wurde $g^{p-1} \equiv 1 \bmod p$ benutzt.)

Ist jetzt $C$ ein Außenstehender, der $(p, g, f_A)$ und $(b_i, c_i)$ kennt und an $a_i$ interessiert ist, so ist wegen $c_i \equiv a_i f_A^{z_i} \bmod p$ die Kenntnis von $a_i$ äquivalent zur Kenntnis von $f_A^{z_i}$. Der Exponent $z_i$ ist aber nur durch die Gleichung $b_i \equiv g^{z_i} \bmod p$ definiert, $C$ muss also den diskreten Logarithmus von $b_i$ zur Basis $g$ berechnen um an $a_i$ zu kommen. Außerdem sollte $C$ nicht in der Lage sein, die Zufallszahl $z_i$ zu erraten. Das Verfahren ist also sicher, solange man diskrete Logarithmen in $\mathbf{F}_p^*$ zur Basis $g$ nicht berechnen kann und solange man nicht an die Zahlen $z_i$ kommt.

**Beispiel:** Wir wollen den Anfang des Texts *HEUTEISTMITTWOCH* mit ElGamal verschlüsseln. Zugrunde liegt ein Alphabet mit 26 Zeichen, wo A,...,Z den Zahlen 0,...,25 entspricht. Der öffentliche Schlüssel sei
$$p = 4294967291, \quad g = 2, \quad f = 833399135,$$
wobei wegen $26^6 < p < 26^7$ die Plaintextblocklänge 6 und die Ciphertextblocklänge 7 gewählt wird.

$$\begin{aligned}
\text{HEUTEI} &\simeq a_1 = (7, 4, 20, 19, 4, 8)_{26} = 85362012 \\
&\mapsto (b_1, c_1) = (3867087628, 2520398330) = ((12, 13, 12, 8, 23, 21, 14)_{26}, (8, 4, 3, 9, 25, 23, 8)_{26}) \\
&\simeq (\text{MNMIXVO,IEDJZXI}) \\
\text{STMITT} &\simeq a_2 = (18, 19, 12, 8, 19, 19)_{26} = 222764145 \\
&\mapsto (b_2, c_2) = (52451333, 2758899076) = ((0, 4, 10, 20, 6, 18, 25)_{26}, (8, 24, 5, 7, 17, 16, 24)_{26}) \\
&\simeq (\text{AEKUGSZ,IYFHRQY})
\end{aligned}$$

*HEUTEISTMITT...* wird also verschlüsselt zu *MNMIXVOIEDJZXIAEKUGSZIYFHRQY...* (Der private Schlüssel ist $e = 1572453532$.)

**Bemerkungen:**

(1) Die verschlüsselte Datei wird ungefähr doppelt so groß wie die ursprüngliche Datei, da aus einer Zahl $a_i$ beim Verschlüsseln ein Paar $(b_i, c_i)$ wird.
(2) Für das ElGamal-Kryptosystem braucht man einen Zufallszahlengenerator.
(3) Je nach Wirken des Zufallszahlengenerators kann dann eine Datei bei zwei Verschlüsselungen mit dem gleichen öffentlichen Schlüssel verschiedene verschlüsselte Dateien liefern.

**7.2. ElGamal für elliptische Kurven.** Wir übertragen jetzt das klassische ElGamal-Verschlüsselungsverfahren auf elliptische Kurven.

**ElGamal-Verschlüsselung mit elliptischen Kurven:**

(1) **Schlüsselerzeugung:**
   (a) Man einigt sich auf eine Primzahl $p$, eine elliptische Kurve $E$ über $\mathbf{F}_p$, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$, einen Punkt $P \in E(\mathbf{F}_p)$.
   (b) Jeder Teilnehmer $A$ wählt sich geheim eine natürliche Zahl $k_A$ und berechnet $Q_A = k_A P \in E(\mathbf{F}_p)$. Der öffentliche Schlüssel von $A$ ist $Q_A$, der geheime Schlüssel ist $k_A$.
(2) **Verschlüsselung:**
   (a) Will $B$ eine Nachricht geheim an $A$ schicken, besorgt er sich den öffentlichen Schlüssel $Q_A$ von $A$ und übersetzt die Nachricht nach einem festgelegten Verfahren in eine Folge von Punkten $M_i \in E(\mathbf{F}_p)$.
   (b) Für jeden Punkt $M_i$ wählt $B$ eine Zufallszahl $z_i$ und berechnet nacheinander

$$R_i = (r_{i1}, r_{i2}) = z_i P, \quad S_i = M_i + z_i Q_A = (s_{i1}, s_{i2}).$$

   Die verschlüsselte Nachricht ist dann die Folge $(r_{i1}, r_{i2}, s_{i1}, s_{i2})$.
(3) **Entschlüsselung:** $A$ empfängt $(r_{i1}, r_{i2}, s_{i1}, s_{i2})$, also $R_i$ und $S_i$ und berechnet

$$S_i - k_A R_i = M_i + z_i Q_A - k_A z_i P = M_i + z_i k_A P - k_A z_i P = M_i,$$

   erhält also die ursprüngliche Nachricht $M_i$.

**Überlegung:** Wie kann ein Außenstehender $C$ an die Nachricht $M_i$ kommen, wenn er außer $P$ und $Q_A$ auch die Punkte $R_i$ und $S_i$ kennt? Die Kenntnis von $M_i$ ist äquivalent mit der Kenntnis von $z_i Q_A = k_A z_i P = k_A R_i$. Hier gibt es zwei Möglichkeiten: Man muss an $z_i$ oder an $k_A$ kommen:

- $k_A$ ist der diskrete Logarithmus $\log_P Q_A$, was praktisch nicht zu berechnen sein sollte bei geeigneter Parameterwahl.
- $z_i$ ist der diskrete Logarithmus $\log_P R_i$, der auch praktisch nicht zu berechnen sein sollte.
- Eine andere Möglichkeit ergibt sich, wenn $C$ die Zufallszahl $z_i$ erraten kann, z.B. bei schlechter Wahl des Zufallszahlengenerators.

Das Verschlüsselungssystem ist also sicher, wenn man die entsprechenden diskreten Logarithmen praktisch nicht berechnen kann und wenn die verwendeten Zufallszahlen gut sind.

**Beispiel:** Wir legen das Alphabet A,B,C,...,Z zugrunde, nehmen die elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbf{F}_p$ mit

$$p = 6833, \quad a = 5984, \quad b = 1180,$$

den Basispunkt $P = (1, 2631)$ und den geheimen Schlüssel $k_A = 2465$. Der öffentliche Schlüssel ist dann

$$Q_A = k_A P = (4748, 2021).$$

Will man MATHEMATISCHESINSTITUT in eine Folge von Punkten $M_i \in E(\mathbf{F}_p)$ übersetzen, so erhält man mit (Streckungsfaktor) $k = 10$, $R_i = z_i P$, $S_i = M_i + z_i Q_A$ folgende Tabelle:

| Text | $x$ | $kx$ | $M_i = (kx + \dots, \dots)$ | $z_i$ | $(R_i, S_i)$ |
|---|---|---|---|---|---|
| MA | 312 | 3120 | (3122,1761) | 620 | ((3267,5160),(3,284)) |
| TH | 501 | 5010 | (5011,781) | 4499 | ((3671,2133),(5595,603)) |
| EM | 116 | 1160 | (1160,2122) | 2364 | ((388,4477),(714,1004)) |
| AT | 19 | 190 | (190,2571) | 6310 | ((6711,2378),(357,1247)) |
| IS | 226 | 2260 | (2260,17) | 4272 | ((1752,3678),(2120,2940)) |
| CH | 59 | 590 | (590,3399) | 4483 | ((292,808),(4840,1010)) |
| ES | 122 | 1220 | (1220,1007) | 1219 | ((6708,4580),(5292,143)) |
| IN | 221 | 2210 | (2211,556) | 6794 | ((687,171),(3327,5675)) |
| ST | 487 | 4870 | (4872,3315) | 3035 | ((1211,2731),(2260,17)) |
| IT | 227 | 2270 | (2270,2994) | 3508 | ((2714,2389),(357,1247)) |
| UT | 539 | 5390 | (5392,959) | 2765 | ((6818,2527),(1333,6617)) |

**Bemerkung:** Vom Prinzip her wird die verschlüsselte Datei mindestens vierfache Länge der Ausgangsdatei haben. Da allerdings die $y$-Koordinate von $R_i$ und $S_i$ durch die $x$-Koordinate bis auf zwei Möglichkeiten bestimmt ist, könnte man die $y$-Koordinaten durch 0 oder 1 ersetzen und damit regeln, welcher $y$-Wert zu nehmen ist.

## 8. Das Menezes-Vanstone-Kryptosystem

Ein Nachteil der ElGamal-Verschlüsselung mit elliptischen Kurven ist, dass man die Nachricht in Punkte auf elliptischen Kurven übersetzen muss. Das folgende Verfahren vermeidet dies.

**Menezes-Vanstone-Verschlüsselung:**

(1) **Schlüsselerzeugung:**
   (a) Man einigt sich auf eine Primzahl $p$, eine elliptische Kurve $E$ über $\mathbf{F}_p$, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$, und einen Punkt $P \in E(\mathbf{F}_p)$.
   (b) Jeder Teilnehmer $A$ wählt sich geheim eine natürliche Zahl $k_A$ und berechnet $Q_A = k_A P \in E(\mathbf{F}_p)$. Der öffentliche Schlüssel von $A$ ist $Q_A$, der geheime Schlüssel ist $k_A$.

(2) **Verschlüsselung:**
   (a) Will $B$ eine Nachricht geheim an $A$ schicken, besorgt er sich den öffentlichen Schlüssel $Q_A$ von $A$ und übersetzt die Nachricht nach einem festgelegten Schema in eine Folge von Paaren $(m_{i1}, m_{i2})$ mit $0 \le m_{i1}, m_{i2} \le p-1$. ($(m_{i1}, m_{i2})$ ist im Allgemeinen kein Kurvenpunkt!)
   (b) Für jedes Paar $(m_{i1}, m_{i2})$ wählt $B$ eine Zufallszahl $z_i$ und berechnet nacheinander

$$R_i = (r_{i1}, r_{i2}) = z_i P, \quad z_i Q_A = (s_{i1}, s_{i2}), \quad (t_{i1}, t_{i2}) = (m_{i1} s_{i1}, m_{i2} s_{i2}) \bmod p.$$

   Die verschlüsselte Nachricht ist dann die Folge $(r_{i1}, r_{i2}, t_{i1}, t_{i2})$.

(3) **Entschlüsselung:** $A$ empfängt $(r_{i1}, r_{i2}, t_{i1}, t_{i2})$ und berechnet

$$k_A(r_{i1}, r_{i_2}) = k_A R_i = k_A z_i P = z_i Q_A = (s_{i1}, s_{i2})$$

und damit

$$m_{i1} = \frac{t_{i1}}{s_{i1}} \bmod p, \quad m_{i2} = \frac{t_{i2}}{s_{i2}} \bmod p,$$

was die ursprüngliche Nachricht $(m_{i1}, m_{i2})$ liefert.

**Bemerkungen:** Wir nehmen an, ein Außenstehender $C$ kommt an

$$P, \quad Q_A, \quad R_i, \quad (t_{i1}, t_{i2}).$$

Die Kenntnis von $(m_{i1}, m_{i2})$ ist dann gleichwertig mit der Kenntis von $(s_{i1}, s_{i2}) = S_i$. Nun ist

$$(s_{i1}, s_{i2}) = z_i Q_A = z_i k_A P = k_A R_i.$$

Dies ist wieder ein Diffie-Hellman-Problem. Nach heutigem Erkenntnisstand ist das Verfahren sicher, wenn man keine diskreten Logarithmen berechnen kann und wenn die Zufallszahlen $z_i$ nicht erraten werden können.

**Beispiel:** Wir legen $p = 4652938753$ und die Kurve $y^2 = x^3 + 5x + 7$ über $\mathbf{F}_p$ zugrunde, zusammen mit dem Punkt $P = (0, 591709564) \in E(\mathbf{F}_p)$. Als Schlüssel wählen wir

$$k_A = 3424624531(\text{privat}) \quad \text{und} \quad Q_A = k_A P = (264355494, 700888650)(\text{öffentlich}).$$

Wir wollen den Text *ELLIPTISCHEKURVENUNDKRYPTOGRAPHIE* verschlüsseln, wobei das Alphabet A,...,Z zugrundeliegt. Wegen $26^6 < p < 26^7$ wählen wir die Blocklänge 6 für den Ausgangstext, 7 für den verschlüsselten Text. Wir übersetzen den Text zunächst in eine Zahlenfolge:

$$\begin{aligned}
\text{ELLIPT} &\simeq (4, 11, 11, 8, 15, 19)_{26} = 52751393,\\
\text{ISCHEK} &\simeq (8, 18, 2, 7, 4, 10)_{26} = 103316574,\\
\text{URVENU} &\simeq (20, 17, 21, 4, 13, 20)_{26} = 245768270,\\
\text{NDKRYP} &\simeq (13, 3, 10, 17, 24, 15)_{26} = 156016707,\\
\text{TOGRAP} &\simeq (19, 14, 6, 17, 0, 15)_{26} = 232260771,\\
\text{HIEXXX} &\simeq (7, 8, 4, 23, 23, 23)_{26} = 86911913.
\end{aligned}$$

Wir bilden Paare $M_i = (m_{i1}, m_{i2})$

$$M_1 = (52751393, 103316574), M_2 = (245768270, 156016707), M_3 = (232260771, 86911913)$$

und wählen Zufallszahlen

$$z_1 = 4002242467, \quad z_2 = 57919244, \quad z_3 = 3968544655.$$

Nun berechnen wir $R_i = (r_{i1}, r_{i2}) = z_i P$ und $S_i = (s_{i1}, s_{i2}) = z_i Q_A$ und damit $T_i = (t_{i1}, t_{i2}) = (m_{i1} s_{i1} \bmod p, m_{i2} s_{i2} \bmod p)$:

$$R_1 = (4364887320, 558058698), S_1 = (740115200, 700601605), T_1 = (1297802303, 4109560319),$$

$$R_2 = (2347187003, 2404883447), S_2 = (4622669484, 29804611), T_2 = (4272531842, 554172861),$$

$$R_3 = (1457809017, 2603232813), S_3 = (823369772, 2862097214), T_3 = (3414885003, 4151065152)$$

Die verschlüsselte Zahlenfolge besteht aus $(r_{i1}, r_{i2}, t_{i1}, t_{i2})$, also

$$\begin{aligned}
&(4364887320, 558058698, 1297802303, 4109560319, 2347187003, 2404883447,\\
&4272531842, 554172861, 1457809017, 2603232813, 3414885003, 4151065152).
\end{aligned}$$

Wandelt man dies mit Blocklänge 7 in Text um, erhält man als Verschlüsselung

```
ODJRPXOBUZFEQCEFFZLXFNHWYPGHHPOJADFHUKPRXF
NVPOZJUBUQSCIVESSDEFPILCQYCZLBKUNAXNLJUAYA.
```

**Bemerkungen:**

(1) Sei $E$ mit der Gleichung $y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbf{F}_p$, $P \in E(\mathbf{F}_p)$ und $Q = kP \in E(\mathbf{F}_p)$. Dies definiert ein Menezes-Vanstone-Kryptosystem. Sei $(r_1, r_2, t_1, t_2)$ die Verschlüsselung von $(m_1, m_2)$ mit $m_1, m_2 \in \mathbf{F}_p^*$, d.h. es gibt eine Zahl $z$ mit

$$(r_1, r_2) = zP, \quad (\frac{t_1}{m_1}, \frac{t_2}{m_2}) = zQ.$$

Sei weiter $f(x, y) = x^3 + ax + b - y^2 \in \mathbf{F}_p[x, y]$.

(a)
$$f(\frac{t_1}{m_1}, \frac{t_2}{m_2}) = 0.$$

(b) Für $n_1, n_2 \in \mathbf{F}_p^*$ gilt:
$$f(\frac{t_1}{n_1}, \frac{t_2}{n_2}) \neq 0 \quad \Longrightarrow \quad (m_1, m_2) \neq (n_1, n_2).$$

(c)
$$\frac{\#\{(n_1, n_2) \in \mathbf{F}_p^* \times \mathbf{F}_p^* : f(\frac{t_1}{n_1}, \frac{t_2}{n_2}) = 0\}}{\#\{(n_1, n_2) \in \mathbf{F}_p^* \times \mathbf{F}_p^*\}} \approx \frac{1}{p}.$$

Dies bedeutet, vermutet man $(n_1, n_2)$ als die verschlüsselte Nachricht, so testet man, ob $f(\frac{t_1}{n_1}, \frac{t_2}{n_2}) = 0$ gilt. Ist dies der Fall, so ist $(n_1, n_2)$ sehr wahrscheinlich die verschlüsselte Nachricht. Andernfalls ist $(n_1, n_2)$ sicher nicht die Ausgangsnachricht.

(2) Das beschriebene Phänomen tritt nicht bei der ElGamal-Verschlüsselung auf. Durch die Verwendung von Zufallszahlen kann man nicht testen, ob eine vermutetete Nachricht wirklich verschlüsselt wurde.

(3) Die Verwendung der Zufallszahlen hat also bei der Menezes-Vanstone-Verschlüsselung nicht die gleiche Funktion wie bei der ElGamal-Verschlüsselung. Dies ist sicher ein Schwachpunkt der Menezes-Vanstone-Verschlüsselung. (Klaus Kiefer, A Weakness of the Menezes-Vanstone Cryptosystem)

KAPITEL 6

# Diskrete Logarithmen

## 1. Einführung

Ist $G$ eine (multiplikativ geschriebene) endliche abelsche Gruppe, in der man das Produkt zweier Elemente $a \cdot b$ schnell berechnen kann, so kann man auch die Potenz $a^k$ für $k \in \mathbf{N}_0$ mit der square-and-multiply-Methode schnell berechnen. Andererseits ist kein allgemeiner Algorithmus bekannt, der zu $a, b \in G$ schnell $x \in \mathbf{N}_0$ liefert mit $a^x = b$ bzw. liefert, dass ein solches $x$ nicht existiert. $x$ wird auch als diskreter Logarithmus $\log_a b$ bezeichnet, das Problem der Berechnung diskreter Logarithmen heißt auch *discrete logarithm problem (DLP).*

Das von Diffie und Hellman 1976 vorgeschlagene Schlüsselaustauschverfahren beruht auf der Schwierigkeit, diskrete Logarithmen in der multiplikativen Gruppe $\mathbf{F}_p^*$ zu berechnen, wenn $p$ eine hinreichend große Primzahl ist. Andere kryptographische Anwendungen folgten, z.B. die ElGamal-Verschlüsselung.

Natürlich kann man dann fragen, ob sich auch andere Gruppen kryptographisch nutzen lassen.

Die Verwendung von elliptischen Kurven in der Kryptographie wurde erstmals 1985 von Neal Koblitz und Victor Miller (unabhängig voneinander) vorgeschlagen. Man sah dabei folgende Vorteile:

- Man hat für festes $p$ eine große Auswahl an Gruppen $E_{a,b}(\mathbf{F}_p)$ zur Verfügung, während es nur eine Gruppe $\mathbf{F}_p^*$ gibt.
- Man kannte keine schnellen Algorithmen zur Berechnung diskreter Logarithmen in $E_{a,b}(\mathbf{F}_p)$, es sei denn, die Gruppenordnung $\#E_{a,b}(\mathbf{F}_p)$ ist das Produkt kleiner Primzahlen.

Im Folgenden sollen einige allgemeine Verfahren zur Berechnung diskreter Logarithmen behandelt werden.

Das folgende Beispiel zeigt, dass die Logarithmenberechnung nicht immer schwierig sein muss.

**Beispiel:** Logarithmenberechnung in der additiven Gruppe $\mathbf{Z}/N\mathbf{Z}$. Das Logarithmenproblem lautet: Bestimme zu $a, b \in \mathbf{Z}/N\mathbf{Z}$ eine Zahl $x$ mit $ax = b$. Interpretiert man $a$ und $b$ als ganze Zahlen, so lautet die Aufgabe: Bestimme $x \in \mathbf{Z}$ mit $ax \equiv b \bmod N$. Oder: Bestimme $x, y \in \mathbf{Z}$ mit

$$ax + Ny = b.$$

Dies ist gleichwertig mit

$$\frac{a}{\mathrm{ggT}(a,N)}x + \frac{N}{\mathrm{ggT}(a,N)}y = \frac{b}{\mathrm{ggT}(a,N)}.$$

Das Problem ist genau dann lösbar, wenn $\mathrm{ggT}(a,N)|b$ gilt. In diesem Fall erhält man schnell eine Lösung mit dem erweiterten euklidischen Algorithmus.

## 2. Naive Logarithmenberechnung

Ist $G$ eine (multiplikativ geschriebene) endliche abelsche Gruppe, sind $a, b \in G$, so definiert man rekursiv

$$a_n = a \cdot a_{n-1} \quad \text{mit dem Startwert} \quad a_0 = 1,$$

und testet bei jedem Schritt:

- Gilt $a_n = b$? Dann ist $n = \log_a b$ der gesuchte Logarithmus und man hört auf.
- Gilt $a_n = 1$ und $n > 0$? Dann ist $n = \mathrm{ord}\,(a)$, der diskrete Logarithmus existiert nicht.

Version vom 15.6.2003 - 25.12.2006

Für eine durch $y^2 = x^3+ax+b$ definierte elliptische Kurve $E$ über $\mathbf{F}_p$ sieht das Verfahren so aus: Gegeben sind $P, Q \in E(\mathbf{F}_p)$. Wir suchen $n$ mit $nP = Q$, d.h. $n = \log_P Q$.
Setze $P_1 = P$ und berechne rekursiv $P_n = nP = P_{n-1} + P$ für $n = 1, 2, 3, \ldots$ und teste bei jedem Schritt:

- Gilt $P_n = Q$? Dann ist $n$ der gesuchte Logarithmus und man hört auf.
- Gilt $P_n = O$? Dann ist $n = ord(P)$, der Logarithmus existiert nicht.

Da $\#E(\mathbf{F}_p)$ ungefähr $p$ ist, lässt sich die Anzahl der Schritte bei diesem Verfahren durch $O(p)$ abschätzen.

**Beispiele:** Wir wählen jeweils eine Kurve $E$ über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$ und einen Punkt $P \in E(\mathbf{F}_p)$. Dann werden 10 zufällige Zahlen $z$ gewählt, damit $Q = zP \in E(\mathbf{F}_p)$ berechnet, und anschließend das naive Logarithmenberechnungsverfahren zur Berechnung von $\log_P Q$ angewendet.
Wir betrachten zunächst

$$p = 65521, \quad a = 101, \quad b = 1009, \quad P = (0, 9215) \in E(\mathbf{F}_p)$$

mit der 16-Bit-Primzahl $p$.

| $Q$ | $\log_P Q$ | Rechenzeit |
|---|---|---|
| (51470, 62096) | 15618 | 3 sec |
| (30224, 28207) | 28326 | 6 sec |
| (19403, 33652) | 42906 | 9 sec |
| (56732, 32249) | 44578 | 9 sec |
| (48022, 64593) | 33192 | 7 sec |
| (43696, 57893) | 65273 | 13 sec |
| (5513, 30615) | 31232 | 6 sec |
| (37127, 50326) | 60168 | 12 sec |
| (19702, 25) | 27897 | 6 sec |
| (19922, 51249) | 54418 | 11 sec |

Für die nächsten Beispiele wählen wir

$$p = 16777213, \quad a = 101, \quad b = 1009, \quad P = (1, 8113953) \in E(\mathbf{F}_p),$$

wobei $p$ eine 24-Bit-Primzahl ist.

| $Q$ | $\log_P Q$ | Rechenzeit |
|---|---|---|
| (9478999, 10420091) | 11769382 | 3024 sec |
| (11278304, 15869150) | 8240777 | 2114 sec |
| (10187249, 11595350) | 13643584 | 3502 sec |
| (2364903, 5284327) | 14609794 | 3753 sec |
| (14757305, 12479563) | 106614 | 27 sec |
| (14982699, 3951843) | 15386075 | 3953 sec |
| (12224894, 12034646) | 4036623 | 1038 sec |
| (9533585, 4553761) | 10049138 | 2584 sec |
| (3461448, 1000293) | 6030423 | 1551 sec |
| (8667988, 5399237) | 6660374 | 1714 sec |

**Bemerkungen:**

(1) Die Schrittzahl bei der dargestellten naiven Logarithmenberechnungsmethode lässt sich durch $O(\#G)$ abschätzen.
(2) Um das Verfahren durchzuführen, muss man die Gruppenordnung $\#G$ nicht kennen.

## 3. Die baby-step-giant-step-Methode nach Shanks

Wir beginnen mit einem Lemma:

LEMMA. *Ist $m \in \mathbf{N}$, so lässt sich jede ganze Zahl $x$ mit $0 \le x \le m^2 - 1$ in der Form*

$$x = mj - i \quad \text{mit} \quad 1 \le i, j \le m$$

*schreiben.*

Sei $G$ eine additiv geschriebene endliche abelsche Gruppe und seien $P, Q \in G$. Wir wollen die Gleichung $xP = Q$ untersuchen. Wir überlegen:

- Gibt es ein $x \in \mathbf{Z}$ mit $xP = Q$, so kann man auch $0 \leq x \leq \operatorname{ord}(P) - 1$ und damit auch $0 \leq x \leq \#G - 1$ annehmen. Ist $m \in \mathbf{N}$ mit $m^2 \geq \operatorname{ord}(P)$ oder $m^2 \geq \#G$, so gibt es nach dem vorangegangenen Lemma natürliche Zahlen $i, j$ mit

  $$1 \leq i, j \leq m \quad \text{und} \quad x = mj - i.$$

  Dann folgt $(mj - i)P = Q$, also

  $$iP + Q = j(mP).$$

- Wir bilden jetzt zwei Listen

  $B = [iP + Q : i = 1, \ldots, m]$ (baby steps) und $G = [j(mP) : j = 1, \ldots, m]$ (giant steps).

  Finden wir $i, j$ mit $B[i] = G[j]$, so folgt $iP + Q = j(mP)$, also $(jm - i)P = Q$ und damit $\log_P Q = mj - i$. Gibt es kein Paar $(i, j)$ mit $B[i] = G[j]$, so existiert der diskrete Logarithmus $\log_P Q$ nicht.

**Beispiel:** Wir betrachten die Gruppe $\mathbf{F}_p^*$ mit $p = 101$ und wollen die Gleichung $2^x = 3$ betrachten. Wir wählen $m = 10$ wegen $11^2 \geq \#\mathbf{F}_p^*$. Wir beginnen mit den baby-steps:

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^i \cdot 3 \bmod p$ | 6 | 12 | 24 | 48 | 96 | 91 | 81 | 61 | 21 | 42 |

Nun folgen die giant-steps:

| $j$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^{mj} \bmod p$ | 14 | 95 | 17 | 36 | 100 | 87 | 6 | 84 | 65 | 1 |

Wir sehen, dass für $i = 1$ und $j = 7$ die Einträge gleich sind, also ist $x = mj - i = 10 \cdot 7 - 1 = 69$ unsere gesuchte Lösung.

**Hauptproblem:** Wie findet man ein gemeinsames Element der beiden Listen, d.h. wie findet man ein Indexpaar $(i, j)$ mit $B[i] = G[j]$?

Der naive Ansatz, alle $i$ durchlaufen zu lassen, dann bei festem $i$ für alle $j = 1, \ldots, m$ zu probieren, ob $B[i] = G[j]$ gilt, führt auf eine Schrittzahl in der Größenordnung von $m^2$, was im Fall $m^2 \geq \#G$ mindestens wie $\#G$ wächst. Dies hat dann der naiven Logarithmenberechnung nichts voraus. Deshalb muss man anders vorgehen. Eine Möglichkeit ist folgende:

(1) Wähle eine injektive Abbildung $h : G \to \mathbf{Z}$.
(2) Berechne $B[i] = iP + Q$ für $i = 1, \ldots, m$ und speichere die Werte.
(3) Sortiere $B[1], \ldots, B[m]$, d.h. bestimme eine Permutation $s$ mit $\{s_1, \ldots, s_m\} = \{1, \ldots, m\}$, sodass gilt

  $$h(B[s_1]) \leq h(B[s_2]) \leq \cdots \leq h(B[s_m]).$$

  Es gibt dazu verschiedene Sortierverfahren, z.B. insertionsort, heapsort, quicksort. Bei heapsort weiß man, dass das Sortierverfahren deterministisch ist mit einer Schrittzahl von $O(m \ln m)$.
(4) Nun berechnet man für $j = 1, 2, 3, \ldots, m$ den Wert $G_j = j(mP)$ und schaut mit binary search nach, ob ein $k$ existiert mit

  $$h(G_j) = h(B[s_k]).$$

  Wenn ja, dann gilt $(jm - s_k)P = Q$, d.h. $\log_P Q = jm - s_k$, und man ist fertig. Bei festem $j$ braucht diese Suche $O(\ln m)$ Schritte, also ist man insgesamt nach $O(m \ln m)$ Schritten fertig.

**Anwendung auf elliptische Kurven:** Wir legen als Gruppe die Gruppe der $\mathbf{F}_p$-rationalen Punkte $E(\mathbf{F}_p)$ einer über $\mathbf{F}_p$ definierten elliptischen Kurve zugrunde. Ist $P = (x, y) \in E(\mathbf{F}_p)$, so können wir $x$ und $y$ durch ganze Zahlen $x, y \in \mathbf{Z}$ mit $0 \leq x, y \leq p-1$ repräsentieren und dann definieren $h(P) = xp + y$. Dann gilt $0 \leq h(P) \leq p^2 - 1$. Setzen wir noch $h(O) = p^2$, so ist $h$ auf ganz $E(\mathbf{F}_p)$ definiert.
Wegen

$$\#E(\mathbf{F}_p) \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2$$

können wir $m$ mit $\sqrt{p}+1 \le m$ wählen, also beispielsweise $m = \lceil \sqrt{p} \rceil + 1$, wenn nichts Genaueres über die Gruppenordnung $\#E(\mathbf{F}_p)$ oder die Punktordnung $\operatorname{ord}(P)$ bekannt ist.

**Beispiel:** Wir betrachten eine elliptische Kurve $E$ über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$ und $P, Q \in E(\mathbf{F}_p)$ mit

$$p = 1009, \quad a = 11, \quad b = 101, \quad P = (1, 380), \quad Q = (101, 357).$$

Hier wird nun $m = 33$. Wir sortieren $B[i] = iP + Q$ nach der Größe von $h(B[i])$.

| $h(B[i])$ | $i$ | $B[i]$ |
|---|---|---|
| 37098 | 31 | (36,774) |
| 58953 | 33 | (58,431) |
| 63866 | 25 | (63,299) |
| 123554 | 17 | (122,456) |
| 187102 | 29 | (185,437) |
| 219675 | 8 | (217,722) |
| 221535 | 15 | (219,564) |
| 235967 | 2 | (233,870) |
| 284638 | 9 | (282,100) |
| 328910 | 16 | (325,985) |
| 334309 | 18 | (331,330) |
| 366064 | 19 | (362,806) |
| 396162 | 30 | (392,634) |
| 420153 | 6 | (416,409) |
| 464657 | 13 | (460,517) |
| 468707 | 7 | (464,531) |
| 571946 | 12 | (566,852) |
| 573087 | 24 | (567,984) |
| 581693 | 1 | (576,509) |
| 601304 | 22 | (595,949) |
| 625904 | 28 | (620,324) |
| 667137 | 14 | (661,188) |
| 669841 | 32 | (663,874) |
| 697584 | 21 | (691,365) |
| 714856 | 3 | (708,484) |
| 752721 | 20 | (746,7) |
| 763065 | 10 | (756,261) |
| 839917 | 26 | (832,429) |
| 847641 | 11 | (840,81) |
| 852401 | 23 | (844,805) |
| 863578 | 4 | (855,883) |
| 890237 | 27 | (882,299) |
| 960820 | 5 | (952,252) |

| $h(jmP)$ | $j$ | $jmP$ |
|---|---|---|
| 566271 | 1 | (561,222) |
| 978961 | 2 | (970,231) |
| 720958 | 3 | (714,532) |
| 968614 | 4 | (959,983) |
| 508288 | 5 | (503,761) |
| 346379 | 6 | (343,292) |
| 679593 | 7 | (673,536) |
| 832616 | 8 | (825,191) |
| 596949 | 9 | (591,630) |
| 613028 | 10 | (607,565) |
| 542448 | 11 | (537,615) |
| 801334 | 12 | (794,188) |
| 64277 | 13 | (63,710) |
| 486301 | 14 | (481,972) |
| 931064 | 15 | (922,766) |
| 981170 | 16 | (972,422) |
| 464657 | 17 | (460,517) |

Anschließend wird $jmP$ und $h(jmP)$ berechnet. Man sieht, dass für $i = 13$ und $j = 17$ die Punkte gleich sind, also wird $\log_P Q = jm - i = 17 \cdot 33 - 13 = 548$.

Wir haben zu dem baby-step-giant-step-Verfahren Maple-Funktionen geschrieben, wobei als Sortierverfahren insertionsort und quicksort zur Verfügung stehen.

**Beispiele:** Wir wählen als Parameter

$$p = 16777213, \quad a = 101, \quad b = 1009, \quad P = (1, 8113953),$$

wobei $p$ eine 24-Bit-Primzahl ist. Dann wird für zufällige Punkte $Q_i = z_i P \in E(\mathbf{F}_p)$ der Logarithmus $\log_P Q_i$ berechnet.

Mit insertionsort erhält man folgende Tabelle ($m = 4097$):

| $Q$ | Zeit zum Sortieren (insertionsort) | $\log_P Q$ | Gesamtzeit |
|---|---|---|---|
| (9478999,10420091) | 59 sec | 11769382 | 63 sec |
| (11278304,15869150) | 57 sec | 8240777 | 61 sec |
| (10187249,11595350) | 58 sec | 13643584 | 63 sec |
| (2364903,5284327) | 57 sec | 14609794 | 62 sec |
| (14757305,12479563) | 59 sec | 106614 | 60 sec |
| (14982699,3951843) | 58 sec | 15386075 | 63 sec |
| (12224894,12034646) | 56 sec | 4036623 | 58 sec |
| (9533585,4553761) | 57 sec | 10049138 | 61 sec |
| (3461448,1000293) | 57 sec | 6030423 | 60 sec |
| (8667988,5399237) | 57 sec | 6660374 | 60 sec |

Mit quicksort erhält man:

| $Q$ | Zeit zum Sortieren (quicksort) | $\log_P Q$ | Gesamtzeit |
|---|---|---|---|
| (9478999,10420091) | 2 sec | 11769382 | 7 sec |
| (11278304,15869150) | 3 sec | 8240777 | 6 sec |
| (10187249,11595350) | 3 sec | 13643584 | 8 sec |
| (2364903,5284327) | 3 sec | 14609794 | 8 sec |
| (14757305,12479563) | 3 sec | 106614 | 4 sec |
| (14982699,3951843) | 3 sec | 15386075 | 8 sec |
| (12224894,12034646) | 3 sec | 4036623 | 5 sec |
| (9533585,4553761) | 3 sec | 10049138 | 7 sec |
| (3461448,1000293) | 3 sec | 6030423 | 6 sec |
| (8667988,5399237) | 3 sec | 6660374 | 6 sec |

Bei den nächsten Beispielen liegen die Parameter

$$p = 4294967291, \quad a = 101, \quad b = 1009, \quad P = (0, 1908380907)$$

mit der 32-Bit-Primzahl $p$ zugrunde. Hier ist $m = 65537$.

| $Q$ | Zeit zum Sortieren | $\log_P Q$ | Gesamtzeit |
|---|---|---|---|
| (916418397,733543598) | 119 sec | 1330138194 | 230 sec |
| (43720241,1975541405) | 170 sec | 758514721 | 326 sec |
| (3124161573,2470056305) | 173 sec | 1295118070 | 359 sec |
| (4042310823,791930308) | 168 sec | 849920434 | 324 sec |
| (1709164294,708075738) | 164 sec | 1042139616 | 333 sec |
| (46377496,2639586864) | 166 sec | 1242584213 | 350 sec |
| (38146108,62404824) | 164 sec | 523799115 | 299 sec |
| (2733416605,60397255) | 164 sec | 1119605696 | 338 sec |
| (1415875191,2183064218) | 167 sec | 557109557 | 305 sec |
| (1265843209,1697688315) | 167 sec | 801016948 | 320 sec |

Als nächstes haben wir die Parameter

$$p = 1099511627689, \quad a = 101, \quad b = 1009, \quad P = (1, 358113905310), \quad m = 1048577$$

mit der 40-Bit-Primzahl $p$ gewählt. Hier legte dann die Speicherverwaltung bei Maple den Rechner lahm, sodass wir die Berechnung abgebrochen haben.

**Bemerkungen:**

(1) Wie die Beispiele zeigen, wird der Speicherplatzverwaltung schnell zum Problem.
(2) Das baby-step-giant-step-Verfahren zur Berechnung diskreter Logarithmen in $E(\mathbf{F}_p)$ zeigt, dass man theoretisch Logarithmen mit $O(p^{\frac{1}{2}+\varepsilon})$ Schritten berechnen kann. Für eine Laufzeitabschätzung muss die Speicherplatzverwaltung berücksichtig werden.

## 4. Das Silver-Pohlig-Hellman-Verfahren

Sei $E$ eine elliptische Kurve über $\mathbf{F}_p$ und $P, Q \in E(\mathbf{F}_p)$. Wir wollen die Gleichung

$$xP = Q$$

untersuchen. Wir nehmen an, wir können die Gruppenordnung bestimmen und faktorisieren:

$$N = \#E(\mathbf{F}_p) = q_1^{e_1} \dots q_r^{e_r}$$

mit paarweise verschiedenen Primzahlen $q_i$. Wir schreiben $d_i = q_i^{e_i}$ und haben dann

$$N = d_1 \dots d_r \quad \text{und} \quad \text{ggT}(\frac{N}{d_1}, \dots \frac{N}{d_r}) = 1.$$

Wir überlegen:

- Gibt es ein $x$ mit $xP = Q$, so folgt auch $x\frac{N}{d_i}P = \frac{N}{d_i}Q$.
- Wegen $d_i \cdot \frac{N}{d_i}P = O$ gilt

$$\{x \cdot \frac{N}{d_i}P : x \in \mathbf{Z}\} = \{x \cdot \frac{N}{d_i}P : 0 \le x \le d_i - 1\}.$$

- Wir können daher mit dem naiven Logarithmenberechnungsverfahren oder mit der baby-step-giant-step-Methode nach einem $x_i$ suchen mit

$$x_i \cdot \frac{N}{d_i}P = \frac{N}{d_i}Q \quad \text{und} \quad 0 \le x_i \le d_i - 1.$$

  Existiert kein solches $x_i$, so existiert auch $\log_P Q$ nicht. Die Anzahl der Schritte ist dann $O(d_i)$ bzw. $O(\sqrt{d_i})$.
- Wir nehmen jetzt an, wir haben für alle $i$ ein $x_i$ mit $x_i\frac{N}{d_i}P = \frac{N}{d_i}Q$ gefunden. Mit dem chinesischen Restsatz bestimmen wir $x$ mit $x \equiv x_i \bmod d_i$ für alle $i$. Dann gilt $x\frac{N}{d_i}P = \frac{N}{d_i}Q$ und damit

$$\frac{N}{d_i}(xP - Q) = O.$$

  Es folgt

$$\text{ord}\,(xP - Q) | \frac{N}{d_i}, \quad \text{also auch} \quad \text{ord}\,(xP - Q) | \text{ggT}(\frac{N}{d_1}, \dots, \frac{N}{d_r}) = 1,$$

  was sofort $xP = Q$, also $x = \log_P Q$, liefert.
- Wir können auf diese Weise den diskreten Logarithmus in $O(d_1 + \dots + d_r)$ bzw. $O(\sqrt{d_1} + \dots + \sqrt{d_r})$ Schritten bestimmen.

**Bemerkungen:**

(1) Das Verfahren lässt sich im Fall $d_i = q_i^{e_i}$ und $e_i \ge 2$ noch verbessern, sodass man statt $O(q_i^{e_i})$ auf eine Abschätzung $O(e_i q_i)$ kommt. Da dies aber in den meisten Beispielen praktisch bedeutungslos ist, haben wir auf eine Darstellung des Verfahrens verzichtet.

(2) Das dargestellte Verfahren ist unter dem Namen Silver-Pohlig-Hellman-Verfahren bekannt. Es funktioniert in der Praxis, wenn in der Gruppenordnung $N$ nur kleine Primteiler $q_i$ auftreten. Man sagt dann auch, die Gruppe $E(\mathbf{F}_p)$ hat 'glatte' Gruppenordnung $N$.

**Beispiel:** Wir betrachten die Kurve $E : y^2 = x^3 + ax + b$ über $\mathbf{F}_p$ mit

$$p = 10000000000000140431, \quad a = -152, \quad b = -722,$$

wobei $p$ eine 67-Bit-Primzahl ist. $E(\mathbf{F}_p)$ hat (glatte) Gruppenordnung

$$N = 10000000014721958125 = 625 \cdot 169 \cdot 17 \cdot 23 \cdot 367 \cdot 647 \cdot 2417 \cdot 4219.$$

Wir wollen $xP = Q$ für die Kurvenpunkte

$$P = (2, 19029769932505619219) \quad \text{und} \quad Q = (6800969357215589186, 74352320581165835102)$$

lösen. Nun findet man durch einfaches Probieren:

| Die Gleichung | wird gelöst von |
|---|---|
| $x \cdot (N/625)P = (N/625)Q$ | $x \equiv 2 \bmod 625$ |
| $x \cdot (N/169)P = (N/169)Q$ | $x \equiv 7 \bmod 169$ |
| $x \cdot (N/17)P = (N/17)Q$ | $x \equiv 8 \bmod 17$ |
| $x \cdot (N/23)P = (N/23)Q$ | $x \equiv 22 \bmod 23$ |
| $x \cdot (N/367)P = (N/367)Q$ | $x \equiv 47 \bmod 367$ |
| $x \cdot (N/647)P = (N/647)Q$ | $x \equiv 139 \bmod 647$ |
| $x \cdot (N/2417)P = (N/2417)Q$ | $x \equiv 922 \bmod 2417$ |
| $x \cdot (N/4219)P = (N/4219)Q$ | $x \equiv 2064 \bmod 4219$ |

woraus man mit dem chinesischen Restsatz sofort die Lösung

$$x = 19350540357117144377$$

erhält.

**Bemerkungen:**

(1) Für kryptographische Zwecke sollte man also Kurven mit glatter Gruppenordnung vermeiden. Allerdings sind solche Kurven auch eher selten.
(2) Um das Silver-Pohlig-Hellman-Verfahren anzuwenden, muss man die Gruppenordnung $\#E(\mathbf{F}_p)$ bestimmen. Wir werden dafür später verschiedene Verfahren vorstellen.

Zum Silver-Pohlig-Hellman-Verfahren haben wir Maple-Funktionen geschrieben, wobei die Einzellogarithmen naiv oder mit der baby-step-giant-step-Methode berechnet werden können.

**Beispiele:** Wir betrachten

$$p = 1099511627689, \quad a = 101, \quad b = 1009, \quad P = (1, 358113905310)$$

mit der 40-Bit-Primzahl $p$. Wir erhalten

$$N = \#E(\mathbf{F}_p) = 1099512539944 = 8 \cdot 7 \cdot 13 \cdot 17 \cdot 1093 \cdot 81283.$$

| $Q$ | $\log_P Q$ | Zeit mit log_bsgs |
|---|---|---|
| (242060913680,509513926799) | 4592482624 | 1 sec |
| (937212232944,915746821971) | 465032394855 | 1 sec |
| (432863827364,520910715678) | 821509194872 | 1 sec |
| (38989140719,153849864976) | 1031654089832 | 1 sec |
| (493068969078,130967054565) | 694013370192 | 1 sec |
| (537165663021,257072119118) | 264201051167 | 1 sec |
| (33175967216,343105923973) | 956741745903 | 1 sec |
| (702642358175,508805159346) | 69125290160 | 1 sec |
| (614632868423,1024168388237) | 593759252071 | 1 sec |
| (270134709135,222542501928) | 345832790600 | 1 sec |

| $Q$ | $\log_P Q$ | Zeit mit log_naiv |
|---|---|---|
| (242060913680,509513926799) | 4592482624 | 25 sec |
| (937212232944,915746821971) | 739910529841 | 26 sec |
| (432863827364,520910715678) | 821509194872 | 14 sec |
| (38989140719,153849864976) | 1031654089832 | 4 sec |
| (493068969078,130967054565) | 694013370192 | 5 sec |
| (537165663021,257072119118) | 539079186153 | 3 sec |
| (33175967216,343105923973) | 132107340945 | 11 sec |
| (702642358175,508805159346) | 69125290160 | 11 sec |
| (614632868423,1024168388237) | 868637387057 | 8 sec |
| (270134709135,222542501928) | 345832790600 | 15 sec |

Vergleicht man die Tabellen, sieht man, dass beim zweiten $Q$ verschiedene Logarithmen berechnet wurden. Dies liegt daran, dass die Ordnung von $P$ nicht $N$ ist. Die berechneten Logarithmen sind kongruent modulo ord $(P)$.

## 5. Die Pollardsche $\rho$-Methode

Sei $E$ eine elliptische Kurve über $\mathbf{F}_p$, von der die Gruppenordnung $N = \#E(\mathbf{F}_p)$ bekannt ist. Wir wollen für $P, Q \in E(\mathbf{F}_p)$ die Gleichung $xP = Q$ lösen bzw. untersuchen. Wir konstruieren mit $P$ und $Q$ eine 'Zufallsfolge' $X_i = a_iP + b_iQ$ von Punkten in $E(\mathbf{F}_p)$ wie folgt:

(1) Wir zerlegen $E(\mathbf{F}_p)$ in drei disjunkte Mengen

$$E(\mathbf{F}_p) = S_0 \cup S_1 \cup S_2.$$

Bei den späteren Beispielen haben wir $S_i = \{(x, y) \in E(\mathbf{F}_p) : 0 \leq x \leq p-1, x \equiv 0 \bmod 3\}$ gewählt, wobei $O$ noch in einem $S_i$ untergebracht werden muss.

(2) Wir wählen $a_0, b_0$ und berechnen $X_0 = a_0P + b_0Q$.

(3) Rekursiv wird jetzt für $i \geq 1$ definiert

$$X_i = \begin{cases} P + X_{i-1} & \text{für } X_{i-1} \in S_0, \\ 2X_{i-1} & \text{für } X_{i-1} \in S_1, \\ Q + X_{i-1} & \text{für } X_{i-1} \in S_2. \end{cases}$$

Dann gilt mit $X_i = a_iP + b_iQ$

$$a_i = \begin{cases} a_{i-1} + 1 \bmod N & \text{für } X_{i-1} \in S_0, \\ 2a_{i-1} \bmod N & \text{für } X_{i-1} \in S_1, \\ a_{i-1} & \text{für } X_{i-1} \in S_2, \end{cases} \quad \text{und} \quad b_i = \begin{cases} b_{i-1} & \text{für } X_{i-1} \in S_0, \\ 2b_{i-1} \bmod N & \text{für } X_{i-1} \in S_1, \\ b_{i-1} + 1 \bmod N & \text{für } X_{i-1} \in S_2. \end{cases}$$

(4) Die Idee ist nun: Findet man $i < j$ mit $X_i = X_j$, so folgt $a_iP + b_iQ = a_jP + b_jQ$, also

$$(b_i - b_j)Q = (a_j - a_i)P.$$

Gilt $\mathrm{ggT}(b_i - b_j, N) = 1$, so folgt

$$Q = \left(\frac{a_j - a_i}{b_i - b_j} \bmod N\right) P$$

und man ist fertig. Ist $\mathrm{ggT}(b_i - b_j, N) > 1$, so kann man eventuell die Beziehung $(b_i - b_j)Q = (a_j - a_i)P$ genauer auswerten.

**Beispiel:** Wir betrachten die elliptische Kurve $E$ mit der Gleichung $y^2 = x^3 + x + 1$ über $\mathbf{F}_{1009}$. Die Gruppenordnung ist $N = \#E(\mathbf{F}_p) = 1034 = 2 \cdot 11 \cdot 47$. Wir nehmen die Punkte

$$P = (1, 149) \quad \text{und} \quad Q = (9, 235)$$

und definieren eine Folge von Punkten

$$X_i = a_iP + b_iQ \in E(\mathbf{F}_p)$$

mit dem Startwert $X_0 = O$ nach obigem Verfahren. Die ersten 50 Folgenglieder sind dann

| $i$ | $X_i$ | $a_i$ | $b_i$ |
|---|---|---|---|
| 1 | (9,235) | 0 | 1 |
| 2 | (547,540) | 1 | 1 |
| 3 | (767,61) | 2 | 2 |
| 4 | (479,613) | 2 | 3 |
| 5 | (86,828) | 2 | 4 |
| 6 | (813,112) | 2 | 5 |
| 7 | (589,852) | 3 | 5 |
| 8 | (896,538) | 6 | 10 |
| 9 | (96,254) | 6 | 11 |
| 10 | (589,157) | 7 | 11 |
| 11 | (896,471) | 14 | 22 |
| 12 | (63,895) | 14 | 23 |
| 13 | (590,836) | 15 | 23 |
| 14 | (999,0) | 15 | 24 |
| 15 | (476,113) | 16 | 24 |
| 16 | (63,114) | 16 | 25 |
| 17 | (61,308) | 17 | 25 |
| 18 | (259,572) | 34 | 50 |
| 19 | (433,324) | 68 | 100 |
| 20 | (18,352) | 136 | 200 |
| 21 | (766,806) | 137 | 200 |
| 22 | (416,892) | 274 | 400 |
| 23 | (542,935) | 274 | 401 |
| 24 | (324,525) | 274 | 402 |
| 25 | (107,15) | 275 | 402 |

| $i$ | $X_i$ | $a_i$ | $b_i$ |
|---|---|---|---|
| 26 | (864,140) | 275 | 403 |
| 27 | (669,805) | 276 | 403 |
| 28 | (743,228) | 277 | 403 |
| 29 | (478,164) | 277 | 404 |
| 30 | (181,78) | 554 | 808 |
| 31 | (970,424) | 74 | 582 |
| 32 | (235,719) | 148 | 130 |
| 33 | (130,219) | 296 | 260 |
| 34 | (549,179) | 592 | 520 |
| 35 | (841,733) | 593 | 520 |
| 36 | (925,724) | 152 | 6 |
| 37 | (368,871) | 304 | 12 |
| 38 | (934,282) | 304 | 13 |
| 39 | (11,873) | 608 | 26 |
| 40 | (841,733) | 608 | 27 |
| 41 | (925,724) | 182 | 54 |
| 42 | (368,871) | 364 | 108 |
| 43 | (934,282) | 364 | 109 |
| 44 | (11,873) | 728 | 218 |
| 45 | (841,733) | 728 | 219 |
| 46 | (925,724) | 422 | 438 |
| 47 | (368,871) | 844 | 876 |
| 48 | (934,282) | 844 | 877 |
| 49 | (11,873) | 654 | 720 |
| 50 | (841,733) | 654 | 721 |

Nun sieht man z.B. $X_{35} = X_{40}$, was man auch als

$$593P + 520Q = 608P + 27Q$$

schreiben kann. Dies ergibt $15P = 493Q$. Nun ist 493 invertierbar modulo der Gruppenordnung: $493 \cdot 797 \equiv 1 \bmod 1034$, sodass Multiplikation mit 797 ergibt

$$Q = 581P.$$

Natürlich stellt sich die Frage, wie man praktisch Punkte $X_i$ und $X_j$ finden kann mit $X_i = X_j$, ohne Speicher- und Sortierprobleme wie bei der baby-step-giant-step-Methode zu bekommen. Im Folgenden soll etwas von der allgemeinen dahinterstehenden Theorie vorgestellt werden.

LEMMA. *Sei $M$ eine Menge mit $m$ Elementen und $x_1, x_2, \ldots, x_k$ eine zufällig gewählte Folge von Elementen aus $M$. Dann ist die Wahrscheinlichkeit, dass alle Folgenglieder verschieden sind, gleich*

$$p_{m,k} = (1 - \frac{1}{m})(1 - \frac{2}{m}) \ldots (1 - \frac{k-1}{m}).$$

*(Ziehen mit Zurücklegen.)*

*Beweis:* Insgesamt gibt es $m^k$ Möglichkeiten für $(x_1, \ldots, x_k)$. Wieviele günstige Möglichkeiten gibt es? $x_1$ kann beliebig gewählt werden, also $m$ Möglichkeiten, für $x_2$ bleiben noch $m-1$ Möglichkeiten, für $x_3$ dann noch $m-2$ Möglichkeiten, etc. Also gibt es $m(m-1)(m-2)\ldots(m-(k-1))$ günstige Möglichkeiten, woraus sich durch Division sofort die Behauptung ergibt. ■

**Beispiel:** Wir wählen $M$ mit $|M| = 365$ und eine zufällige Folge $x_1, \ldots, x_k$. Die Wahrscheinlichkeit, dass alle Folgenglieder verschieden sind, kann man dann für verschiedene Werte von $k$ der folgenden Tabelle

entnehmen:

| $k$ | 10 | 20 | 30 | 40 | 50 | 60 |
|---|---|---|---|---|---|---|
| Wahrscheinlichkeit in % | 88.3 | 58.9 | 29.4 | 10.9 | 3.0 | 0.6 |

Eine Interpretation: Hat man eine Gruppe von 30 Leuten, so ist die Wahrscheinlichkeit, dass zwei davon am gleichen Tag Geburtstag haben, größer als 70 Prozent, bei einer Gruppe von 60 Leuten erhöht sich die Wahrscheinlichkeit schon auf über 99 Prozent, etc.

**Überlegung:** Wir wollen die Wahrscheinlichkeit $p_{m,k}$ abschätzen für den Fall, dass $m$ groß gegen $k$ ist. Zunächst ist

$$\ln p_{m,k} = \sum_{i=1}^{k-1} \ln(1 - \frac{i}{m}).$$

Ist $k$ groß gegen $m$ und $1 \leq i \leq k-1$, so ist wegen $\ln(1-x) \approx -x$ (für kleine $x$) dann $\ln(1 - \frac{i}{m}) \approx -\frac{i}{m}$ und damit

$$\ln p_{m,k} \approx -\sum_{i=1}^{k-1} \frac{i}{m} = -\frac{k(k-1)}{2m},$$

d.h.

$$p_{m,k} \approx e^{-\frac{k(k-1)}{2m}}.$$

Ist z.B. $m$ groß und $k \approx 3.1\sqrt{m}$, so wird

$$p_{m,k} \approx e^{-\frac{3.1\sqrt{m}(3.1\sqrt{m}-1}{2m}} \approx e^{-3.1^2/2} \approx 0.0082.$$

Indem man kleine Werte von $m$ explizit betrachtet, kann man dann folgendes Lemma beweisen:

LEMMA. *Ist $M$ eine Menge mit $m$ Elementen und $x_1, \ldots, x_k$ eine zufällig gewählte Folge in $M$ mit*

$$k \geq 3.1\sqrt{m},$$

*so ist die Wahrscheinlichkeit, dass zwei Folgenglieder gleich sind, größer als 99 Prozent.*

**Bemerkung:** Statt 99 Prozent kann man natürlich auch eine Abschätzung für andere Werte herleiten. Für uns ist wichtig: Hat man eine zufällig gewählte Folge $x_i$, so ist es sehr wahrscheinlich, dass unter den ersten $c\sqrt{m}$ Folgenglieder zwei gleiche sind, z.B. mit $c = 3.1$.

**Anwendung:** Wir haben $E(\mathbf{F}_p) \approx p$. Ist also $X_i \in E(\mathbf{F}_p)$ eine Zufallsfolge, so ist es sehr wahrscheinlich, dass Indizes $i < j \lessapprox 3.1\sqrt{p}$ existieren mit $X_i = X_j$. Die wesentliche Frage ist nun, wie man solche Indizes findet.

Unsere Folgen $X_i \in E(\mathbf{F}_p)$ waren so konstruiert, dass eine Abbildung $f : E(\mathbf{F}_p) \to E(\mathbf{F}_p)$ existiert mit $X_i = f(X_{i-1})$ nach Wahl eines Startpunktes $X_0 \in E(\mathbf{F}_p)$.

LEMMA. *Ist $M$ eine endliche Menge, $f : M \to M$ eine Abbildung, $x_0 \in M$ und die Folge $x_i$ rekursiv definiert durch $x_i = f(x_{i-1})$ für $i \geq 1$, so gibt es ganze Zahlen $k, \ell \geq 0$ mit*

$$x_{i+\ell} = x_i \text{ für alle } i \geq k.$$

*Sind $k$ und $\ell$ minimal gewählt, so nennt man $x_0, x_1, \ldots, x_{k-1}$ die Vorperiode der Folge, $x_k, x_{k+1}, \ldots, x_{k+\ell-1}$ die Periode der Folge, die sich immer wiederholt. $\ell$ wird Periodenlänge oder auch einfach Periode genannt.*

*Beweis:* Da $M$ endlich ist, gibt es natürlich Indizes $i < j$ mit $x_i = x_j$. Seien die Indizes minimal gewählt. Wir schreiben $i = k$ und $j = k + \ell$. Dann ist $x_{k+\ell} = x_k$,

$$x_{(k+1)+\ell} = f(x_{k+\ell}) = f(x_k) = x_{k+1}, \quad x_{(k+2)+\ell} = f(x_{(k+1)+\ell}) = f(x_{k+1}) = x_{k+2}, \quad \text{etc.},$$

woraus man durch Induktion schnell die Behauptung erhält. ■

**Bemerkung:** Stellt man eine Folge wie im Lemma graphisch dar, so wird man an den griechischen Buchstaben $\rho$ erinnert, wobei die Vorperiode dem Schwanz von $\rho$, die Periode dem Kreis von $\rho$ entspricht. Daher kommt der Name des Pollardschen $\rho$-Verfahrens.

Unser nächstes Problem ist, wie man zu einer Folge $x_i$ in einer endlichen Menge $M$, die durch eine Abbildung $f : M \to M$ mittels $x_{i+1} = f(x_i)$ definiert ist, Indizes $j < k$ finden kann mit $x_j = x_k$.
Natürlich könnte man so vorgehen: Man vergleicht $x_1$ mit $x_0$, dann $x_2$ mit $x_0$ und $x_1$, dann $x_3$ mit $x_0$, $x_1$, $x_2$, etc. Ist man bei $x_k$ angelangt, so braucht man insgesamt $\binom{k+1}{2} = \frac{k(k+1)}{2}$ Vergleiche, außerdem muss man die Elemente $x_0, x_1, \ldots, x_k$ speichern. Dies ist im allgemeinen zu aufwendig.
Einen eleganten Ausweg liefert folgendes Lemma:

LEMMA. *Sei $M$ eine endliche Menge, $f : M \to M$ eine Abbildung, $x_0 \in M$ und die Folge $x_i$ definiert durch $x_{i+1} = f(x_i)$ für alle $i \geq 0$.*

(1) *Sind $j < k$ zwei Indizes mit $x_j = x_k$, so gibt es einen Index $\ell$ mit $0 < \ell < k$ und $x_\ell = x_{2\ell}$.*
(2) *Definiert man eine Folge $y_i$ durch $y_0 = x_0$ und $y_i = f(f(y_{i-1}))$, so gilt $y_i = x_{2i}$. (Insbesondere ist $x_\ell = x_{2\ell}$ gleichwertig mit $x_\ell = y_\ell$.)*

*Beweis:* 1. Aus $x_j = x_k = x_{j+(k-j)}$ folgt durch Anwendung von $f$ nacheinander

$$x_{j+1} = x_{j+1+(k-j)}, \quad x_{j+2} = x_{j+2+(k-j)}, \quad x_{j+3} = x_{j+3+(k-j)}, \quad \ldots,$$

woraus man durch Induktion sofort

$$x_{i+(k-j)} = x_i \text{ für alle } i \geq j$$

erhält. Mit dem euklidischen Algorithmus können wir schreiben

$$j = q(k-j) - r \text{ mit } 0 \leq r < k - j \text{ und } q \geq 1.$$

Wir setzen $\ell = q(k-j)$. Dann gilt

$$\ell = j + r < k \quad \text{ und } \ell = j + r \geq j.$$

Damit können wir obige Formel anwenden und erhalten

$$x_\ell = x_{q(k-j)} = x_{q(k-j)+(k-j)} = x_{q(k-j)+2(k-j)} = x_{q(k-j)+3(k-j)} = \cdots = x_{2q(k-j)} = x_{2\ell},$$

was wir zeigen wollten.
2. Wir zeigen $y_i = x_{2i}$ durch Induktion, wobei der Fall $i = 0$ aufgrund der Definition klar ist. Nun ist

$$y_{i+1} = f(f(y_i)) = f(f(x_{2i})) = f(x_{2i+1}) = x_{2i+2} = x_{2(i+1)},$$

was die Behauptung liefert. ■

**Bemerkungen:** Sei $M$ eine endliche Menge, $x_0 \in M$ und eine Folge $x_i$ rekursiv definiert durch $x_{i+1} = f(x_i)$.

(1) Um Indizes $j < k$ mit $x_j = x_k$ zu finden, kann man nach dem Lemma so vorgehen: Man berechnet parallel zu $x_i$ eine Folge $y_i$, die durch $y_0 = x_0$ und $y_{i+1} = f(f(y_i))$ definiert wird, und vergleicht $x_i$ mit $y_i$. Gilt für $\ell \geq 1$ nun $x_\ell = y_\ell$, so ist $x_\ell = x_{2\ell}$ und wir haben unser Problem gelöst. Ein großer Vorteil ist, dass man keine Speicherprobleme hat.
(2) Aus unseren wahrscheinlichkeitstheoretischen Überlegungen folgt weiter: Ist $x_0, x_1, \ldots, x_{[3.1\sqrt{m}]}$ eine Zufallsfolge, dann ist die Wahrscheinlichkeit, dass ein $\ell$ mit $1 \leq \ell \leq 3.1\sqrt{m}$ und $x_\ell = y_\ell = x_{2\ell}$ existiert, größer als 99 Prozent.

**Anwendung:** Bei vorgegebener elliptischer Kurve $E$ über $\mathbf{F}_p$ und Punkten $P, Q \in E(\mathbf{F}_p)$, nach Wahl von Startwerten $a_0, b_0$ konstruieren wir uns Folgen

$$X_i = a_i P + b_i Q \quad \text{ und } \quad Y_i = X_{2i} = c_i P + d_i Q.$$

Stoßen wir auf ein $i \geq 1$ mit $X_i = Y_i$, so erhalten wir eine Gleichung

$$a_i P + b_i Q = c_i P + d_i Q,$$

also

$$(d_i - b_i)Q = (a_i - c_i)P.$$

Wir bestimmen mit dem erweiterten euklidischen Algorithmus $u$ und $v$ mit

$$\mathrm{ggT}(d_i - b_i, \mathrm{ord}\,(P)) = u(d_i - b_i) + v\,\mathrm{ord}\,(P).$$

Es folgt

$$\mathrm{ggT}(d_i - b_i, \mathrm{ord}\,(P))Q = u(d_i - b_i)P = (u(d_i - b_i) \bmod \mathrm{ord}\,(P))P.$$

Wir setzen $g = \mathrm{ggT}(d_i - b_i, \mathrm{ord}\,(P))$, $\mathrm{ord}\,(P) = gh$ und $\ell = u(a_i - c_i) \bmod \mathrm{ord}\,(P)$. Also ist $gQ = \ell P$. Es folgt

$$O = \mathrm{ord}\,(P)Q = ghP = h\ell P,$$

was $\mathrm{ord}\,(P)|h\ell$, also $gh|\ell h$ und damit $g|\ell$ impliziert. Wir schreiben $\ell = gk$ und erhalten die Gleichung

$$gQ = gkP.$$

Es folgt $g(Q - kP) = O$. Da $P$ und $Q$ in der von $P$ erzeugten zyklischen Untergruppe liegen sollen, gibt es ein $i$ mit $Q - kP = i \cdot hP$, wobei wir o.E. $0 \leq i \leq g - 1$ annehmen können. Wir erhalten

$$Q = (k + ih)P \quad \text{für ein } i \text{ mit } 0 \leq i \leq g - 1.$$

Indem wir für jedes $i$ mit $0 \leq i \leq g - 1$ probieren, ob $Q = (k + ih)P$ gilt, können wir die Gleichung $Q = xP$ lösen.

**Beispiel:** Wir wählen eine elliptische Kurve $E$ über $\mathbf{F}_p$ und Punkte $P, Q \in E(\mathbf{F}_p)$ mit den Parametern

$$p = 1009, \quad a = 1, \quad b = 1, \quad N = \#E(\mathbf{F}_p) = 1034, \quad P = (1, 149), \quad Q = (9, 235), \quad \mathrm{ord}\,(P) = 1034.$$

| $i$ | $X_i$ | $Y_i$ | $(a_i, b_i, c_i, d_i)$ |
|---|---|---|---|
| 0 | (1,149) | (1,149) | (1,0,1,0) |
| 1 | (672,465) | (727,882) | (2,0,3,0) |
| 2 | (727,882) | (556,832) | (3,0,12,0) |
| 3 | (46,103) | (542,935) | (6,0,24,1) |
| 4 | (556,832) | (107,15) | (12,0,25,2) |
| 5 | (416,892) | (669,805) | (24,0,26,3) |
| 6 | (542,935) | (478,164) | (24,1,27,4) |
| 7 | (324,525) | (970,424) | (24,2,108,16) |
| 8 | (107,15) | (130,219) | (25,2,432,64) |
| 9 | (864,140) | (841,733) | (25,3,865,128) |
| 10 | (669,805) | (368,871) | (26,3,358,512) |
| 11 | (743,228) | (11,873) | (27,3,716,1026) |
| 12 | (478,164) | (925,724) | (27,4,398,1020) |
| 13 | (181,78) | (934,282) | (54,8,796,1007) |
| 14 | (970,424) | (841,733) | (108,16,558,981) |
| 15 | (235,719) | (368,871) | (216,32,164,822) |
| 16 | (130,219) | (11,873) | (432,64,328,612) |
| 17 | (549,179) | (925,724) | (864,128,656,192) |
| 18 | (841,733) | (934,282) | (865,128,278,385) |
| 19 | (925,724) | (841,733) | (696,256,556,771) |
| 20 | (368,871) | (368,871) | (358,512,156,1016) |

Wir erhalten dann damit die Gleichung $2 \cdot Q = 2 \cdot 64 \cdot P$ und damit $Q = 581 \cdot P$.
Nun wählen wir für das gleiche Problem einen anderen Startwert für $(a_0, b_0)$:

| $i$ | $X_i$ | $Y_i$ | $(a_i, b_i, c_i, d_i)$ |
|---|---|---|---|
| 0 | (235,719) | (235,719) | (279,443,279,443) |
| 1 | (130,219) | (549,179) | (558,886,82,738) |
| 2 | (549,179) | (925,724) | (82,738,166,442) |
| 3 | (841,733) | (934,282) | (83,738,332,885) |
| 4 | (925,724) | (841,733) | (166,442,664,737) |
| 5 | (368,871) | (368,871) | (332,884,588,880) |

Dies liefert wieder die Gleichung $2 \cdot Q = 2 \cdot 64 \cdot P$ und daraus dann $Q = 581 \cdot P$.
Wir probieren einen weiteren (zufälligen) Startwert $(a_0, b_0)$:

| $i$ | $X_i$ | $Y_i$ | $(a_i, b_i, c_i, d_i)$ |
|---|---|---|---|
| 0 | (589,157) | (589,157) | (7,11,7,11) |
| 1 | (896,471) | (63,895) | (14,22,14,23) |
| 2 | (63,895) | (999,0) | (14,23,15,24) |
| 3 | (590,836) | (63,114) | (15,23,16,25) |
| 4 | (999,0) | (259,572) | (15,24,34,50) |
| 5 | (476,113) | (18,352) | (16,24,136,200) |
| 6 | (63,114) | (416,892) | (16,25,274,400) |
| 7 | (61,308) | (324,525) | (17,25,274,402) |
| 8 | (259,572) | (864,140) | (34,50,275,403) |
| 9 | (433,324) | (743,228) | (68,100,277,403) |
| 10 | (18,352) | (181,78) | (136,200,554,808) |
| 11 | (766,806) | (235,719) | (137,200,148,130) |
| 12 | (416,892) | (549,179) | (274,400,592,520) |
| 13 | (542,935) | (925,724) | (274,401,152,6) |
| 14 | (324,525) | (934,282) | (274,402,304,13) |
| 15 | (107,15) | (841,733) | (275,402,608,27) |
| 16 | (864,140) | (368,871) | (275,403,364,108) |
| 17 | (669,805) | (11,873) | (276,403,728,218) |
| 18 | (743,228) | (925,724) | (277,403,422,438) |
| 19 | (478,164) | (934,282) | (277,404,844,877) |
| 20 | (181,78) | (841,733) | (554,808,654,721) |
| 21 | (970,424) | (368,871) | (74,582,548,816) |
| 22 | (235,719) | (11,873) | (148,130,62,600) |
| 23 | (130,219) | (925,724) | (296,260,124,168) |
| 24 | (549,179) | (934,282) | (592,520,248,337) |
| 25 | (841,733) | (841,733) | (593,520,496,675) |

Hier erhalten wir direkt das Ergebnis $Q = 1 \cdot Q = 1 \cdot 581 \cdot P = 581 \cdot P$.

Zu dem Pollardschen $\rho$-Verfahren haben wir eine Maple-Funktion geschrieben, mit der die nachfolgenden Beispiele gerechnet wurden.

**Beispiel:** (16-Bit-Primzahl)

$$p = 65521, \quad a = 101, \quad b = 1009, \quad N = 65891, \quad P = (0, 9215).$$

| $Q$ | $(a_0, b_0)$ | $i$ mit $X_i = Y_i$ | ggT | $\log_P Q$ | Zeit |
|---|---|---|---|---|---|
| (51470,62096) | (1,0) | 412 | 1 | 15618 | 0 sec |
| (30224,28207) | (1,0) | 42 | 7 | 28326 | 0 sec |
| (19403,33652) | (1,0) | 880 | 1 | 42906 | 1 sec |
| (56732,32249) | (1,0) | 711 | 1 | 44578 | 1 sec |
| (48022,64593) | (1,0) | 546 | 7 | 33192 | 0 sec |
| (43696,57893) | (1,0) | 260 | 1 | 65273 | 0 sec |
| (5513,30615) | (1,0) | 111 | 7 | 31232 | 0 sec |
| (37127,50326) | (1,0) | 329 | 1 | 60168 | 0 sec |
| (19702,25) | (1,0) | 633 | 1 | 27897 | 0 sec |
| (19922,51249) | (1,0) | 294 | 1 | 54418 | 0 sec |

| $Q$ | $(a_0, b_0)$ | $i$ mit $X_i = Y_i$ | ggT | $\log_P Q$ | Zeit |
|---|---|---|---|---|---|
| (51470,62096) | (38794,63620) | 412 | 1 | 15618 | 0 sec |
| (30224,28207) | (43664,4438) | 124 | 1 | 28326 | 0 sec |
| (19403,33652) | (9714,57851) | 440 | 7 | 42906 | 0 sec |
| (56732,32249) | (56832,15635) | 711 | 1 | 44578 | 1 sec |
| (48022,64593) | (12750,46996) | 134 | 1 | 33192 | 0 sec |
| (43696,57893) | (49760,18629) | 11 | 1 | 65273 | 0 sec |
| (5513,30615) | (60271,30301) | 708 | 1 | 31232 | 1 sec |
| (37127,50326) | (39632,60460) | 489 | 7 | 60168 | 0 sec |
| (19702,25) | (63176,47105) | 633 | 1 | 27897 | 1 sec |
| (19922,51249) | (44345,46483) | 588 | 1 | 54418 | 0 sec |

| $Q$ | $(a_0, b_0)$ | $i$ mit $X_i = Y_i$ | ggT | $\log_P Q$ | Zeit |
|---|---|---|---|---|---|
| (51470,62096) | (82,71) | 309 | 1 | 15618 | 0 sec |
| (30224,28207) | (98,64) | 172 | 7 | 28326 | 0 sec |
| (19403,33652) | (77,39) | 214 | 1 | 42906 | 0 sec |
| (56732,32249) | (86,69) | 711 | 1 | 44578 | 1 sec |
| (48022,64593) | (22,10) | 546 | 1 | 33192 | 0 sec |
| (43696,57893) | (56,64) | 130 | 1 | 65273 | 0 sec |
| (5513,30615) | (58,61) | 354 | 7 | 31232 | 0 sec |
| (37127,50326) | (75,86) | 489 | 1 | 60168 | 0 sec |
| (19702,25) | (17,62) | 633 | 1 | 27897 | 0 sec |
| (19922,51249) | (8,50) | 294 | 1 | 54418 | 0 sec |

**Beispiel:** (32-Bit-Beispiel)

$$p = 4294967291, \quad a = 101, \quad b = 1009, \quad N = 4294872714, \quad P = (0, 1908380907).$$

| $Q$ | $(a_0, b_0)$ | $i$ mit $X_i = Y_i$ | ggT | $\log_P Q$ | Zeit |
|---|---|---|---|---|---|
| (916418397,733543598) | (82,71) | 54300 | 22 | 1330138194 | 60 sec |
| (43720241,1975541405) | (98,64) | 15885 | 2 | 758514721 | 18 sec |
| (3124161573,2470056305) | (77,39) | 27624 | 2 | 1295118070 | 31 sec |
| (4042310823,791930308) | (86,69) | 44511 | 2 | 849920434 | 50 sec |
| (1709164294,708075738) | (22,10) | 33856 | 2 | 1042139616 | 38 sec |
| (46377496,2639586864) | (56,64) | 38016 | 2 | 1242584213 | 42 sec |
| (38146108,62404824) | (58,61) | 46898 | 22 | 523799115 | 52 sec |
| (2733416605,60397255) | (75,86) | 35000 | 2 | 1119605696 | 39 sec |
| (1415875191,2183064218) | (17,62) | 149772 | 2 | 557109557 | 166 sec |
| (1265843209,1697688315) | (8,50) | 45574 | 2 | 801016948 | 51 sec |

**Beispiel:** (40-Bit-Primzahl)

$$p = 1099511627689, \quad a = 101, \quad b = 1009,$$

$$N = \#E(\mathbf{F}_p) = 1099512539944, \quad P = (1, 358113905310).$$

| $Q$ | $(a_0, b_0)$ | $i$ mit $X_i = Y_i$ | ggT | $\log_P Q$ | Zeit |
|---|---|---|---|---|---|
| (242060913680,509513926799) | (82,71) | 556017 | 2 | 4592482624 | 675 sec |
| (937212232944,915746821971) | (98,64) | 813460 | 34 | 190154259869 | 985 sec |
| (432863827364,520910715678) | (77,39) | 334556 | 2 | 271752924900 | 407 sec |
| (38989140719,153849864976) | (86,69) | 1374950 | 2 | 207019684874 | 1678 sec |
| (493068969078,130967054565) | (22,10) | 560570 | 2 | 144257100220 | 682 sec |
| (537165663021,257072119118) | (56,64) | 892462 | 2 | 264201051167 | 1085 sec |
| (33175967216,343105923973) | (58,61) | 585058 | 14 | 132107340945 | 715 sec |
| (702642358175,508805159346) | (75,86) | 521703 | 2 | 69125290160 | 635 sec |
| (614632868423,1024168388237) | (17,62) | 582485 | 2 | 44002982099 | 709 sec |
| (270134709135,222542501928) | (8,50) | 247248 | 14 | 70954655614 | 302 sec |

Die erwartete Schrittzahl beim Pollardschen $\rho$-Verfahren wächst mindestens wie $\sqrt{p}$. Bei den gerechneten Beispielen war die durchschnittliche Rechenzeit 787.3 Sekunden. Damit können wir folgende 'Formel' aufstellen:

$$\text{Erwartete Rechenzeit}(p) = \frac{787.3 \text{ sec}}{\sqrt{1099511627689}}\sqrt{p}.$$

Für eine 48-Bit-Primzahl liefert dies ungefähr 210 Minuten.

**Beispiel:** Wir betrachten eine 48-Bit-Primzahl:

$$p = 281474976710597, \quad a = 101, \quad b = 1009,$$

$$N = \#E(\mathbf{F}_p) = 281474946817398 = 2 \cdot 3^3 \cdot 5212499015137, \quad P = (1, 57773631196335).$$

| $Q$ | $(a_0, b_0)$ | $i$ mit $X_i = Y_i$ | ggT | $\log_P Q$ | Zeit |
|---|---|---|---|---|---|
| (17360337544878,78373196164624) | (82,71) | 4709596 | 2 | 76047371882016 | 102 min |
| (61943345807950,185901827120755) | (98,64) | 5520501 | 18 | 23258957554047 | 120 min |
| (103510647071282,277626071480446) | (77,39) | 721950 | 2 | 81114558715678 | 16 min |
| (193586265093976,44199516399278) | (82,71) | 13525076 | 6 | 87452242006742 | 294 min |
| (226644945691654,247019338810999) | (98,64) | 11765195 | 2 | 25992862002766 | 255 min |
| (99270012496821,184425423171411) | (77,39) | 14009456 | 2 | 33048008270643 | 304 min |
| (275952684572308,239090966476837) | (86,69) | 5975016 | 6 | 58331851513985 | 129 min |
| (255160595592544,66839882443965) | (22,10) | 4063011 | 2 | 80566587888044 | 88 min |
| (251256723091911,237989087768103) | (56,64) | 5123646 | 6 | 80710949188603 | 111 min |
| (19442092480415,63997034279250) | (82,71) | 16088098 | 18 | 5865514045054 | 350 min |

Die durchschnittliche Rechenzeit betrug 176.9 min. Setzt man nun die 'Formel'

$$\text{Erwartete Rechenzeit}(p) = \frac{176.9 \text{ min}}{281474976710597}\sqrt{p}$$

an, so kommt man für eine 56-Bit-Primzahl auf über 47 Stunden, für eine 40-Bit-Primzahl auf ungefähr 11 Minuten.

**Parallelisierungsversuche:**

(1) Die Grundidee beim Pollardschen $\rho$-Verfahren zur Berechnung von $\log_P Q$ ist die Konstruktion einer 'Zufallsfolge'

$$X_i = a_i P + b_i Q.$$

Findet man Indizes $i$ und $j$ mit $X_i = X_j$, so gilt $(b_j - b_i)Q = (a_i - a_j)P$, woraus man im Allgemeinen schnell $\log_P Q$ berechnen kann. Das Problem ist das Auffinden eines Paares $(i, j)$ mit $X_i = X_j$. Würde man alle $X_i$ speichern, so erhält man schnell Speicherplatzprobleme.

(2) Für den zuvor dargestellten Ansatz wurde gezeigt, dass es im Fall $X_i = X_j$ mit $i < j$ auch einen Index $k < j$ gibt mit $X_k = X_{2k}$. Indem man gleichzeitig rekursiv $X_i$ und $X_{2i}$ berechnet, kann man $X_i$ mit $X_{2i}$ vergleichen. Dadurch braucht man praktisch keinen Speicherplatz. Die wahrscheinliche Schrittzahl wächst wie $\sqrt{p}$.

(3) Was kann man machen, wenn man viele Computer zur Verfügung hat? Eine Idee ist die folgende: Jeder Interessent $A$ konstruiert sich eine Zufallsfolge

$$X_{A,i} = a_{A,i}P + b_{A,i}Q.$$

Alle Punkte $X_{A,i}$, die einer bestimmten vereinbarten Bedingung genügen, werden zusammen mit $(a_{A,i}, b_{A,i})$ an eine zentrale Stelle geschickt. Die Bedingung sollte so sein, dass nicht zu viele Punkte bearbeitet werden müssen. Findet man nun in der Zentrale einen Punkt als $X_{A,i} = X_{B,j}$, so hat man eine Gleichung

$$a_{A,i}P + b_{A,i}Q = a_{B,j}P + b_{B,j}Q$$

und man hat die Gleichung (sehr wahrscheinlich) gelöst.

**Beispiel:** (48-Bit-Beispiel) Wir betrachten wieder

$$p = 281474976710597, \quad a = 101, \quad b = 1009, \quad N = 281474946817398, \quad P = (1, 57773631196335)$$

und wollen $\log_P Q$ für

$$Q = (17360337544878, 78373196164624)$$

bestimmen. Wir berechnen eine Folge $X_i = a_iP + b_iQ$ wie früher (mit zufälligen Startwerten $(a_0, b_0)$) und speichern nur solche, für die mit $X_i = (x_i, y_i)$ gilt $x_i \equiv 0 \bmod 10^6$.

| $X_i = a_iP + b_iQ$ | $(a_i, b_i)$ | $i$ |
|---|---|---|
| (255359918000000, 272898129801098) | (200247570835400, 93732598293465) | 2630154 |
| (217458697000000, 24331238400800) | (21044045945644, 129518387318606) | 2774121 |
| (90581218000000, 97155124760977) | (231116019237356, 15619226100092) | 3163081 |
| (129764383000000, 170706178171334) | (89699249949442, 165930853667508) | 3806029 |
| (8006601000000, 71986105205377) | (37536648454184, 274001130853930) | 4084668 |
| (63699671000000, 248645424929809) | (90580071602453, 218998243525558) | 4713900 |
| (255528056000000, 255837429239132) | (171648281030569, 250866587650667) | 7401334 |
| (212353082000000, 19243175972293) | (158280750011512, 39296637880994) | 8299703 |
| (65819608000000, 235180453382324) | (254332083823616, 65138545747939) | 11365476 |
| (272849187000000, 23264878066656) | (5440941924822, 143332806668098) | 12258831 |
| (236427185000000, 79804652720975) | (261060338770174, 181673748311596) | 12519860 |
| (218960892000000, 214530879773597) | (205546063037844, 174433859453778) | 13934843 |
| (154320388000000, 192789116502680) | (40375991461104, 56509823715670) | 14086929 |
| (196484987000000, 149271918683684) | (83881653123611, 195163063572937) | 15375271 |
| (248178801000000, 142763360811057) | (210633947370422, 41778432927670) | 16570471 |
| (213329110000000, 241731095258667) | (40698893204140, 7026680040701) | 17837490 |
| (196484987000000, 149271918683684) | (120740682511319, 68543736846167) | 18959974 |
| (248178801000000, 142763360811057) | (146344782271736, 191641975651568) | 20155174 |
| (213329110000000, 241731095258667) | (206936530064926, 122650932604617) | 21422193 |
| (196484987000000, 149271918683684) | (160677650997479, 193668039168247) | 22544677 |
| (248178801000000, 142763360811057) | (54519742049264, 120464063052832) | 23739877 |

Für $i = 15375271$ und $j = 18959974$ gilt $X_i = X_j$, also $a_iP + b_iQ = a_jP + b_jQ$, woraus man mit dem früher dargestellten Verfahren sofort

$$\log_P Q = 76047371882016$$

erhält.

**Bemerkung:** Für elliptische Kurven hat man im Allgemeinfall keine anderen Methoden zur Verfügung um diskrete Logarithmen zu berechnen also die zuvor dargestellten. Dies ist anders im Fall der Gruppe $\mathbf{F}_p^*$, wie im Folgenden dargestellt wird.

## 6. Die Index-Calculus-Methode für $\mathbf{F}_p^*$

Sei $p$ eine ungerade Primzahl und $g \in \mathbf{F}_p^*$ mit $\operatorname{ord}_{\mathbf{F}_p^*}(g) = p-1$. (Man nennt dann $g$ eine Primitivwurzel modulo $p$.) Da $\mathbf{F}_p^*$ zyklisch ist, gibt es zu jedem $a \in \mathbf{F}_p^*$ ein $x \in \mathbf{Z}$ mit $g^x = a$. Wir wollen die Gleichung $g^x = a$ lösen. Dies erfolgt in 3 Schritten.

*1. Schritt:* Wir wählen eine natürliche Zahl $n$. Seien $q_1, q_2, \ldots, q_n$ die ersten $n$ Primzahlen. Wir brauchen zunächst einige Relationen

$$\prod_{j=1}^{n} q_j^{a_{ij}} \equiv g^{b_i} \bmod p \text{ für } i = 1, 2, \ldots, m \text{ mit } m \geq n$$

und gehen dazu wie folgt vor:

(1) Wähle $b$ mit $0 \leq b \leq p-2$ (zufällig).
(2) Berechne $x \equiv g^b \bmod p$ mit $1 \leq x \leq p-1$.
(3) Faktorisiere aus $x$ alle $q_i$, $i = 1, \ldots, n$ heraus, solange es geht:

$$x = q_1^{a_1} q_2^{a_2} \ldots q_n^{a_n} \cdot \widetilde{x} \text{ mit } \widetilde{x} \in \mathbf{N} \text{ und } \operatorname{ggT}(\widetilde{x}, q_1 \ldots q_n) = 1.$$

(4) Ist $\widetilde{x} > 1$, fängt man von vorne an. Ist $\widetilde{x} = 1$, haben wir eine gewünschte Relation

$$q_1^{a_1} q_2^{a_2} \ldots q_n^{a_n} \equiv g^b \bmod p$$

gefunden.

**Beispiel:** $p = 10009$, $g = 11$ und $n = 3$. Wir suchen also Relationen

$$11^{b_i} \equiv 2^{a_{i1}} \cdot 3^{a_{i2}} \cdot 5^{a_{i3}} \bmod p.$$

Durch zufällige Wahl von $b$ finden wir:

| $b_i$ | $a_{i1}$ | $a_{i2}$ | $a_{i3}$ |
|---|---|---|---|
| 5140 | 11 | 1 | 0 |
| 3438 | 2 | 1 | 1 |
| 6876 | 4 | 2 | 2 |
| 4374 | 2 | 3 | 0 |

*2. Schritt:* Wir haben also jetzt einige Relationen

$$\prod_{j=1}^{m} q_j^{a_{ij}} \equiv g^{b_i} \text{ für } i = 1, 2, \ldots, m \text{ mit } m \geq n.$$

Schreiben wir $q_i \equiv g^{\ell_i} \bmod p$ mit $0 \leq \ell_i \leq p-2$, so werden die Relationen zu

$$\sum_{j=1}^{n} a_{ij} \ell_j \equiv b_i \bmod p-1 \text{ für } i = 1, 2, \ldots, m.$$

Dies ist ein lineares Gleichungssystem über dem Ring $\mathbf{Z}/(p-1)\mathbf{Z}$ mit den Unbekannten $\ell_1, \ldots, \ell_n$. Die folgenden elementaren Umformungen modulo $p-1$ ändern die Lösungsmenge nicht: Vertauschen zweier Gleichungen, Multiplikation einer Gleichung mit einer Zahl und Addition zu einer davon verschiedenen Gleichung, Multiplikation einer Gleichung mit einer zu $p-1$ teilerfremden Zahl. Mit diesen Operationen kann man versuchen, das Gleichungssystem auf Dreiecksgestalt zu bringen und dann wie üblich eine Lösung zu bestimmen. Reicht die Anzahl der Gleichungen nicht aus, muss man im 1. Schritt noch mehr Relationen suchen. Im günstigen Fall erhält man Zahlen $\ell_i \bmod (p-1)$ mit $g^{\ell_i} \equiv q_i \bmod p$, also $\ell_i = \log_g q_i$.

**Beispiel:** Wir betrachten unser obiges Beispiel weiter, also $p = 10009$, $g = 11$, $n = 3$. Die gefundenen Relationen liefern folgende (erweiterte) Matrix (modulo $p-1$)

$$\begin{pmatrix} 11 & 1 & 0 & 5140 \\ 2 & 1 & 1 & 3438 \\ 4 & 2 & 2 & 6876 \\ 2 & 3 & 0 & 4374 \end{pmatrix}.$$

Nach elementaren Umformungen erhalten wir die Matrix

$$\begin{pmatrix} 1 & -4 & -5 & -12050 \\ 0 & 1 & 15 & 23794 \\ 0 & 0 & 1 & 7316 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

aus der man dann sofort

$$\log_{11}(2) = \ell_1 = 1002, \quad \log_{11}(3) = \ell_2 = 4126, \quad \log_{11}(5) = \ell_3 = 7316$$

berechnet.

*3. Schritt:* Wir können jetzt die Gleichung $g^x \equiv a \bmod p$ für verschiedene $a$'s (leicht) lösen.
Wir wählen wie im 1. Schritt zufällig $b$, bis wir eine Relation

$$ag^b \equiv \prod_{j=1}^{n} q_j^{e_j} \bmod p$$

erhalten. Dann ist nämlich

$$ag^b \equiv g^{\sum_{j=1}^{n} e_j \ell_j}$$

und damit

$$\log_g(a) = b - \sum_{j=1}^{n} e_j \log_g(q_j) \equiv p-1.$$

**Beispiel:** Wir betrachten wieder $p = 10009$ mit $g = 11$, wobei wir jetzt schon

$$\log(2) = 1002, \quad \log(3) = 4126, \quad \log(5) = 7316$$

kennen. Wir berechnen einige Logarithmen:

| $a$ | $b$ | $e_1$ | $e_2$ | $e_3$ | $\log(a)$ |
|---|---|---|---|---|---|
| 101 | 6373 | 0 | 1 | 1 | 5069 |
| 1001 | 3438 | 1 | 1 | 0 | 1690 |
| 10001 | 1238 | 0 | 0 | 4 | 8010 |

**Bemerkungen:**

(1) Eine wesentliche Vorarbeit in der Index-Calculus-Methode ist der 1. Schritt. Man muss $n$, die Anzahl der Basisprimzahlen geeignet wählen. Ist $n$ zu klein, findet man schwer Relationen, ist $n$ zu groß, muss man viele Relationen erzeugen, außerdem wird das Gleichungssystem im 2. Schritt schwierig.

(2) Hat man die ersten beiden Schritte erledigt, lassen sich diskrete Logarithmen bei festem $p$ und $g$ schnell finden. Dies ist anders als bei den anderen beschriebenen Verfahren.

(3) Sei

$$L(p) = e^{\sqrt{\log p \log\log p}}.$$

Man kann zeigen, dass sich das Verfahren so implementieren lässt, dass die Laufzeit für die ersten beiden Schritte bei Wahl von $q_n \approx L(p)^{\frac{1}{2}}$ durch $L(p)^{2+o(1)}$ abgeschätzt werden kann. Dies ist eine sogenannte subexponentielle Laufzeit, denn $L(p)^2 = o(p^\varepsilon)$ für jedes $\varepsilon > 0$.

(4) Für elliptische Kurven ist keine Methode bekannt, die der Index-Calculus-Methode ähnelt.

KAPITEL 7

# Hash-Funktionen

## 1. Kryptographische Hash-Funktionen

Hash-Funktionen sind Funktionen, die beliebig lange Zeichenketten in Zeichenketten ein fest vorgegebenen Länge $n$ umwandeln. Wir geben eine mathematische Definition: Ist $\Sigma$ ein Alphabet, so ist

$$\Sigma^m = \{a_1 a_2 \dots a_m : a_i \in \Sigma\}$$

die Menge der Worte/Strings/Zeichenketten der Länge $m$ und

$$\Sigma^* = \{a_1 a_2 \dots a_m : a_i \in \Sigma, m \geq 0\} = \bigcup_{m \geq 0} \Sigma^m$$

die Menge aller möglichen Worte/Strings/Zeichenketten.
Eine **Hash-Funktion** $H$ ist zunächst eine Abbildung

$$H : \Sigma^* \to \Sigma^n,$$

sie bildet also beliebig lange Zeichenketten auf Zeichenketten fest vorgegebener Länge $n$ ab. Für unsere Zwecke wird $\Sigma = \{0, 1\}$ sein, wir deuten $\Sigma^*$ als Menge aller möglichen Bitfolgen/Bytefolgen/Nachrichten. Zur Motivation geben wir zwei Beispiele:

**Beispiele:**

(1) Will man testen, ob man beim Abschreiben von Zahlen einen Fehler gemacht hat, kann man die Quersummen bilden: sind sie verschieden, ist ein Fehler passiert.

(2) Beim Komprimieren einer Datei datei mit gzip wird eine 32-Bit-Prüfsumme (crc - cyclic redundancy code) gespeichert, die man mit 'gzip -l -v datei.gz' erhält, z.B.

```
method  crc     date  time  compressed  uncompr. ratio uncompressed_name
defla 28eac75d Jun 14 15:06     54372    165840  67.2% sam1
```

Wurde die gzip-komprimierte Datei verändert/beschädigt, erhält man bei Anwendung von gunzip (meistens) die Meldung 'invalid compressed data–crc error' und man weiß, dass etwas nicht stimmt.

Für kryptographische Anwendungen stellt man noch weitere Forderungen. Man trifft dann auch auf Namen wie Kompressionsfunktion, message digest (MD), kryptographische Prüfsumme, Fingerabdruck, message integrity check (MIC), manipulation detection code (MDC). Nun zu den Forderungen:

(1) Für jedes $a \in \Sigma^*$ soll sich der Hashwert $H(a)$ schnell und effektiv berechnen lassen.

(2) Zu (allgemeinem) $h$ im Bild von $H$ kann man praktisch kein $a \in \Sigma^*$ finden mit $h = H(a)$. (Mit dieser Eigenschaft nennt man $H$ eine Einwegfunktion.)

(3) Man kann praktisch keine $a \neq a'$ finden mit $H(a) = H(a')$. (Man sagt, $H$ ist (stark) kollisionsresistent.)

(4) Eigenschaft 3 impliziert, dass $H$ auch schwach kollisionsresistent ist: Zu gegebenem $a \in \Sigma^*$ kann man kein $a' \in \Sigma^*$ finden mit mit $a \neq a'$ und $H(a) = H(a')$.)

**Anwendungsbeispiele:**

(1) Wir nehmen an, $A$ sendet eine Nachricht $a$ an $B$, $B$ empfängt $a'$. Wie kann $B$ sicher sein, dass $a' = a$ ist? $A$ sendet ebenfalls den Hashwert $H(a)$, $B$ berechnet $H(a')$. Ist jetzt $H(a) \neq H(a')$, so stimmt etwas nicht. Ist $H(a) = H(a')$, so kann $B$ wegen der Kollisionsresistenz von $H$ ziemlich sicher sein, dass $a = a'$ gilt. Mit kryptographischen Hash-Funktionen kann man also überprüfen, ob eine Nachricht verändert wurde oder nicht.
(2) Unter Unix werden die Passwörter der Benutzer verschlüsselt in der Datei /etc/passwd abgespeichert, auf die jeder Zugriff hat ('ypcat passwd'). Für die Verschlüsselungsfunktion $H$ ist dann (schwache) Kollisionsresistenz ganz wichtig.

Wir geben einige aktuelle Hash-Funktionen an:

(1) MD5 (message digest): 128-Bit-Hashwert (32-stellige Hexadezimalzahl, 39-stellige Dezimalzahl)
(2) SHA-1 (secure hash algorithm): 160-Bit-Hashwert (40-stellige Hexadezimalzahl, 49-stellige Dezimalzahl)
(3) RIPEMD-160 (Das Programm RACE - Research and Development in Advanced Communication Technologies - wurde von der EU ins Leben gerufen. RIPE steht dann für RACE Integrity Primitives Evaluation. RIPEMD für RIPE Message Digest.)
(4) HAVAL: 256-Bit-Hashwert (64-stellige Hexadezimalzahl, 78-stellige Dezimalzahl)

Die Werte werden dabei als Hexadezimalzahlen (Basis 16) mit den Ziffern 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f angegeben.

**Beispiel:** MD5 ist auf vielen Rechnern installiert.

(1) Durch Aufruf von 'md5 -sKryptographie' etc. erhält man folgende Ergebnisse:

```
MD5 ("Kryptographie") = 04ba1a046db60a74079137de9ff46b89
MD5 ("kryptographie") = 1f2f100a07480d4ed2874cccc25d1aef
MD5 ("cryptographie") = f1bd003f7df56250d3f277b81e97218c
MD5 ("Cryptographie") = 3071a3f52819e57de1740f5286297737
```

Dabei steht -s für eine Zeichenkette. Bei einer Datei erfolgt der Aufruf durch 'md5 datei'. Schreibt man in die Datei datei das Wort Kryptographie, so erhält man

```
MD5 (datei) = f9300c33c0082e60e8850073081d1d62
```

Der Unterschied zu obiger Zeichenkette besteht darin, dass die Datei datei noch ein 14. Zeichen mit der ascii-Nummer 10 enthält.
(2) Will man testen, ob beim Übertragen von Daten (im Internet oder per Diskette) (wahrscheinlich) keine Fehler passiert sind, kann man die MD5-Hashwerte vor und nach der Übertragung vergleichen, wenn dies möglich ist.

Natürlich ist eine Hash-Funktion $H : \Sigma^* \to \Sigma^n$ nie injektiv. Wählt man eine Zufallsfolge $a_1, a_2, \ldots, a_k \in \Sigma^*$, so ist die Wahrscheinlichkeit, dass es Indizes $i < j \leq k$ gibt mit $H(a_i) = H(a_j)$, größer als 99 %, falls $k \geq 3.1\sqrt{|\Sigma^n|} = 3.1|\Sigma|^{n/2}$. Speichert man die Werte $(H(a_i), a_i)$ in einer Datei und sortiert diese nach $H(a_i)$, so sollte man bei entsprechender Wahl von $k$ eine Kollision finden. Dies nennt man **Geburtstagsattacke**. Für die Praxis muss daher $n$ (mit $\Sigma = \{0, 1\}$) so groß sein, dass eine Geburtstagsattacke praktisch nicht durchzuführen ist.

**Beispiel:** Sei SHA-1a definiert durch

$$\text{SHA-1a}(a) = \text{die ersten 12 Bits von SHA-1}(a).$$

Wir bestimmen die Hashwerte der ersten 1000 natürlichen Zahlen in Dezimaldarstellung. In den folgenden Fällen trat der gleiche Hashwert auf.

| SHA-1a('$n$') | $n$ |
|---|---|
| 0159 | 161 |
| 0159 | 244 |
| 0558 | 293 |
| 0588 | 337 |
| 1368 | 150 |
| 1368 | 988 |
| 93ac | 418 |
| 93ac | 931 |
| acf1 | 188 |
| acf1 | 541 |
| b202 | 406 |
| b202 | 678 |
| edd6 | 499 |
| edd6 | 595 |

## 2. SHA-1

Das US-amerikanische National Institute of Standards and Technology (NIST) hat am 1. August 2002 im Dokument 'Federal Information Processing Standards Publication 180-2' (FIPS 180-2) kryptographische Hashfunktionen als Standard festgelegt - Secure Hash Standard. Um einen Eindruck vom Aufbau von Hash-Funktionen zu gewinnen, soll im Folgenden SHA-1 beschrieben werden.

Wir verwenden hier 32-Bit-Worte, also Bitfolgen $(a_1a_2\dots a_{31}a_{32})$ der Länge 32. Vermöge

$$(a_1a_2\dots a_{31}a_{32}) \quad \longleftrightarrow \quad a=\sum_{i=1}^{32} a_i 2^{32-i}$$

erhält man eine Bijektion mit den ganzen Zahlen $a$ mit $0 \le a \le 2^{32}-1$. Wir werden jetzt ein paar Operationen einführen: Seien $a$, $b$ und $c$ Zahlen mit $0 \le a,b,c \le 2^{32}-1$ und zugehörig die Bitfolgen $(a_1\dots a_{32})$, $(b_1\dots b_{32})$ und $(c_1\dots c_{32})$.

- ROTL sei der zirkuläre Linksshift, d.h.
$$\mathrm{ROTL}((a_1a_2\dots a_{32})) = (a_2a_3\dots a_{32}a_1).$$
- $c = a \oplus b$ wird durch die komponentenweise Addition modulo 2 definiert, d.h. $c_i \equiv a_i + b_i \bmod 2$.
- $c = a \wedge b$ wird durch das logische UND definiert, d.h. $c_i \equiv a_i b_i \bmod 2$.
- $c = \neg a$ wird durch das logische NICHT definiert, d.h. $c_i \equiv 1 - a_i \bmod 2$.
- $c = a + b$ ist die Addition modulo $2^{32}$: $c \equiv a + b \bmod 2^{32}$.

Damit kann man die SHA-1-Funktionen $f_0, f_1, \dots, f_{79}$ definieren. Sie operieren auf 32-Bit-Worten bzw. auf den Zahlen zwischen 0 und $2^{32}-1$.

$$f_t(x,y,z) = \begin{cases} (x \wedge y) \oplus ((\neg x) \wedge z) & 0 \le t \le 19, \\ x \oplus y \oplus z & 20 \le t \le 39, \\ (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) & 40 \le t \le 59, \\ x \oplus y \oplus z & 60 \le t \le 79. \end{cases}$$

Weitere werden folgende Konstanten benutzt

$$K_t = \begin{cases} 0x5a827999 = 1518500249 & 0 \le t \le 19, \\ 0x6ed9eba1 = 1859775393 & 20 \le t \le 39, \\ 0x8f1bbcdc = 2400959708 & 40 \le t \le 59, \\ 0xca62c1d6 = 3395469782 & 60 \le t \le 79. \end{cases}$$

$((K_{20}/K_0)^2 \approx 3/2$, $(K_{40}/K_0)^2 \approx 5/2$, $(K_{60}/K_0)^2 \approx 10/2$.)

Wir nehmen an, wir haben eine Nachricht $M$ in Form einer Bytefolge gegeben (1 Byte = 8 Bits), wobei wir uns Bytes durch Zahlen zwischen 0 und $2^8 - 1 = 255$ repräsentiert denken.

**Padding - Auffüllen:** An die Nachricht werden Bytes angehängt, sodass die Bytelänge der neuen Nachricht durch 64 teilbar ist.

- Sei $L$ die Bytelänge von $M$.
- Bestimme eine 8-Byte-Darstellung der Zahl $8L$, d.h.

$$8L = \ell_1 \cdot 256^7 + \ell_2 \cdot 256^6 + \cdots + \ell_7 \cdot 256 + \ell_8 \quad \text{mit} \quad 0 \le \ell_i \le 255.$$

- Hänge an $M$ ein Byte 128 an. Dies entspricht der Bitfolge (10000000).
- Bestimme $0 \le k \le 64$ mit $k \equiv -\ell - 9 \bmod 64$. Hänge an $M$ nun $k$ Bytes 0 an.
- Hänge an $M$ die Bytes $\ell_1, \ell_2, \ldots, \ell_8$ an.
- Die Bytezahl des modifizierten $M$ ist jetzt durch 64 teilbar.

Nun wird $M$ in 64-Byte-Blöcke $M_1, M_2, \ldots, M_N$ unterteilt.
Die folgenden Zahlen liefern die Startwerte für die Hashwerte.

$$\begin{aligned} H_0 &= 0x67452301 = 1732584193, \\ H_1 &= 0xefcdab89 = 4023233417, \\ H_2 &= 0x98badcfe = 2562383102, \\ H_3 &= 0x10325476 = 271733878, \\ H_4 &= 0xc3d2e1f0 = 3285377520. \end{aligned}$$

Für jeden 64-Byte-Block $M_i$, $i = 1, \ldots, N$ werden jetzt nacheinander folgende Schritte durchgeführt:

(1) $M_i$ hat 64 Bytes, dies wird in 16 Blöcke mit je 4 Bytes aufgeteilt, die mit $W_0, \ldots, W_{15}$ bezeichnet werden. $W_i$ hat also 4 Bytes, ist also ein 32-Bit-Wort, das einer Zahl zwischen 0 und $2^{32} - 1$ entspricht.

(2) $W_{16}, \ldots, W_{79}$ werden wie folgt definiert:

$$W_t = \mathrm{ROTL}(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) \quad \text{für} \quad 16 \le t \le 79.$$

(3) Man setzt

$$a := H_0, \quad b := H_1, \quad c := H_2, \quad d := H_3, \quad e := H_4.$$

(4) Für $0 \le t \le 79$ führt man folgende Berechnungen durch:

$$\begin{aligned} T &:= \mathrm{ROTL}^5(a) + f_t(b,c,d) + e + K_t + W_t, \\ e &:= d, \\ d &:= c, \\ c &:= \mathrm{ROTL}^{30}(b), \\ b &:= a, \\ a &:= T. \end{aligned}$$

(5) Nun werden die Hash-Werte aktualisiert:

$$H_0 := a + H_0, \quad H_1 := b + H_1, \quad H_2 := c + H_2, \quad H_3 := d + H_3, \quad H_4 := e + H_4.$$

Am Ende hat man $H_0, H_1, H_2, H_3, H_4$. Jedes $H_i$ ist ein 32-Bit-Wort, hängt man die $H_i$'s aneinander, erhält man einen 160-Bit-Hashwert:

$$\text{SHA-1}(M) = H_0 H_1 H_2 H_3 H_4.$$

**Bemerkung:** Wir haben eine Maple-Funktion 'SHA_1' nach obigen Anweisungen geschrieben, die allerdings nicht sehr schnell arbeitet.

**Beispiel:** Die folgenden Beispiele sind offiziel dokumentiert, dienen als auch zum Testen, ob richtig programmiert wurde:

SHA-1('abc') =
= A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D,
SHA-1( 'abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq') =
= 84983E44 1C3BD26E BAAE4AA1 F95129E5 E54670F1.

## 3. Eine Verschlüsselung mit elliptischen Kurven: PSEC-1

Wir stellen nun ein Verschlüsselungsverfahren mit elliptischen Kurven dar, bei dem die Nachricht nicht in eine Punktefolge der elliptischen Kurven übersetzt werden muss.

**Ein Verschlüsselungsverfahren mit elliptischen Kurven (PSEC-1):**

(1) **Schlüsselerzeugung:**
   (a) Man legt eine elliptische Kurve $E$ über $\mathbf{F}_p$ zugrunde, die durch eine Gleichung $y^2 = x^3 + ax + b$ gegeben wird, dazu einen Punkt $P \in E(\mathbf{F}_p)$.
   (b) $\operatorname{ord}(P)$ sollte eine Primzahl sein.
   (c) Man wählt ganze Zahlen $\ell_m \geq 1$, $\ell_r \geq 0$ mit $2^{\ell_m+\ell_r} < p$.
   (d) Man legt eine Hash-Funktion $h$ fest. Für die Bitlänge $n$ der Hashwerte sollte $n \leq \operatorname{ord}(P)$ gelten.
   (e) Jeder Teilnehmer $A$ wählt sich eine Zahl $k_A$ mit $0 < k_A < \operatorname{ord}(P)$ als geheimen Schlüssel, berechnet $K_A = k_A \cdot P \in C(\mathbf{F}_p)$ und macht $K_A$ als seinen öffentlichen Schlüssel öffentlich zugänglich.

(2) **Verschlüsselung:**
   (a) Will $B$ eine Nachricht $m$ verschlüsselt an $A$ schicken, wandelt $B$ die Nachricht in eine Bitfolge um und bildet Blöcke der Bitlänge $\ell_m$. Die Nachricht ist also jetzt eine Folge $m_1, m_2, \ldots$, wobei $m_i$ Bitlänge $\ell_m$ hat.
   (b) $B$ wählt eine Zufallszahl $r_i$ mit Bitlänge $\ell_r$. Nun bezeichne $m_i \| r_i$ die Bitfolge, die durch aneinanderfügen von $m_i$ und $r_i$ entsteht. $m_i \| r_i$ hat Länge $\ell_m + \ell_r$, kann also als Zahl zwischen 0 und $2^{\ell_m+\ell_r} - 1$ dargestellt werden, insbesondere ist die Zahl kleiner als $p$.
   (c) $B$ berechnet den Hashwert $s_i = h(m_i \| r_i)$ und damit

$$Q_i = s_i \cdot P, \quad R_i = s_i \cdot K_A, \quad t_i = (m_i \| r_i) \oplus x_{R_i},$$

   wobei $\oplus$ für die komponentenweise Addition der Bitfolgen modulo 2 steht, und schickt das Tripel

$$(x_{Q_i}, y_{Q_i}, t_i)$$

   an $A$.

(3) **Entschlüsselung:**
   (a) $A$ empfängt $(x_{Q_i}, y_{Q_i}, t_i)$, berechnet

$$k_A \cdot (x_{Q_i}, y_{Q_i}) = k_A \cdot Q_i = k_A s_i \cdot P = s_i \cdot K_A = R_i$$

   und damit

$$t_i \oplus x_{R_i} = (m_i \| r_i) \oplus x_{R_i} \oplus x_{R_i} = m_i \| r_i.$$

   Die ersten $\ell_m$ Bits davon liefern $m_i$.
   (b) Man kann auch noch einen Sicherheitstest machen: Man testet, ob

$$h(t_i \oplus x_{R_i}) \cdot P = Q_i$$

   gilt. Ist alles in Ordnung ist, so hat man nämlich

$$h(t_i \oplus x_{R_i}) \cdot P = h(m_i \| r_i) \cdot P = s_i \cdot P = Q_i.$$

   Im andern Fall liegt ein Fehler vor.

**Bemerkung:** Ein Außenstehender kommt an $Q_i = s_i P$ und $K_A = k_A P$ und möchte $R_i = s_i k_A P$ bestimmen zur Entschlüsselung. Dies ist wieder das Diffie-Hellman-Problem.

KAPITEL 8

# Digitale Signaturen

## 1. Einführung

Hier sind einige Eigenschaften, die eine eigenhändige Unterschrift hat bzw. haben sollte (entnommen: B. Schneier, Angewandte Kryptographie, S. 41):

- Eine Unterschrift ist authentisch. Sie überzeugt den Empfänger des Dokuments davon, dass der Unterzeichner das Dokument willentlich unterschrieben hat.
- Eine Unterschrift ist fälschungssicher. Sie beweist, dass der Unterzeichner und kein anderer das Dokument unterschrieben hat.
- Eine Unterschrift ist nicht wiederverwendbar. Sie ist Bestandteil des Dokuments und kann in kein anderes Dokument übertragen werden.
- Das unterzeichnete Dokument ist unveränderbar. Nachdem das Dokument unterschrieben ist, kann es nicht mehr geändert werden.
- Die Unterschrift kann nicht zurückgenommen werden. Unterschrift und Dokument liegen physisch vor. Der Unterzeichner kann später nicht behaupten, dass er das Dokument nicht unterschrieben hat.

Eine digitale Signatur soll für ein Dokument, das als Datei vorliegt, Ähnliches bewirken, was eine eigenhändige Unterschrift für ein gewöhnliches Dokument tut. Wie kann man das erreichen?

## 2. Allgemeine Verfahren

Wir geben im folgenden einige mögliche Verfahren an:

**Unterschreiben mit einem Public-Key-Datenverschlüsselungssystem:**

(1) Man legt ein Public-Key-Kryptosystem zugrunde, wo jeder Teilnehmer $A$ die öffentliche Verschlüsselungsfunktion $f_A$ bekannt gibt, die private Entschlüsselungsfunktion $f_A^{-1}$ geheim hält.
(2) $A$ will eine Nachricht/Datei $M$ an $B$ übermitteln und $B$ soll sicher sein, dass die Nachricht wirklich von $A$ stammt.
   (a) $A$ wendet $f_A^{-1}$ auf $M$ an und schickt $f_A^{-1}(M)$ an $B$.
   (b) $B$ wendet $f_A$ auf die erhaltene Nachricht an und erhält mit $f_A(f_A^{-1}(M)) = M$ eine sinnvolle Nachricht, die natürlich nur von $A$ stammen kann, da nur $A$ die Funktion $f_A^{-1}$ kennt.

Man überzeugt sich schnell, dass die gewünschten Forderungen an eine Unterschrift erfüllt sind.

**Bemerkungen:**

(1) Das beschriebene Verfahren ist natürlich nicht besonders effizient, wenn es sich um längere Nachrichten oder Dateien handelt.
(2) Verschlüsselung ist bisher noch nicht im Spiel: Jeder kann $f_A^{-1}(M)$ entschlüsseln durch Anwenden von $f_A$.

Das folgende Verfahren beschreibt eine effizientere Version:

**Unterschreiben mit einem Public-Key-Verfahren unter Verwendung einer Hash-Funktion:**

(1) Man legt ein Public-Key-Verfahren mit öffentlichen Schlüsseln $f_A$ zugrunde. Außerdem einigt man sich auf eine Hashfunktion $H$.
(2) $A$ will eine Nachricht $M$ mit Unterschrift an $B$ senden.

(a) $A$ berechnet den Hashwert $H(M)$, wendet $f_A^{-1}$ darauf an, erhält also $f_A^{-1}(H(M))$.
(b) $A$ schickt $M$ und $f_A^{-1}(H(M))$ an $B$.
(c) $B$ besorgt sich den öffentlichen Schlüssel $f_A$ von $A$, berechnet aus $M$ den Hashwert $H(M)$ und mit $f_A$ den Wert $f_A(f_A^{-1}(H(M)))$. Stimmen beide Werte überein, dann akzeptiert $B$ die Unterschrift, da $f_A^{-1}$ nur von $A$ stammen kann.

**Beispiel:** Bei dem Programmpaket PGP gibt es eine Variante, die getrennt zum Klartext eine Signatur erstellt, die z.B. wie folgt aussehen kann:

```
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.1 Int. for non-commercial use <http://www.pgpinternational.com>

iQCVAwUAPu7NLSCnOW/GZY2vAQFtiAP+Pa3RS33n2QOj9oIRZd85RgG5H9LCKxgS
PlytCQ/u8Pd9+6sWPOHc2x3pvrWA3YyYpieT/VKshPrpaVIECBkNpod30bywjI3p
rpimj4nzFnvbKIIfYnpBgILPsUGAaJSTGd+4UH2S6FUWCKyOnMnBb3WTsl0C0B0f
bCpWrQqkZ30=
=Lh3I
-----END PGP SIGNATURE-----
```

Es gibt aber auch eine Variante, bei der der Text komprimiert (aber unverschlüsselt) eingefügt wird. Das kann dann so aussehen:

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.1 Int. for non-commercial use <http://www.pgpinternational.com>

owEBzAAz/4kAlQMFAD7uzPwgpzlvxmWNrwEBHgED/iVvmUvZuyExHqj/gfdVo7CI
6Vyr93WNBqk0pnoIxVS7ko6Y9YAil07dd9/Oytp1hte5uOSCKKJ40+8Ya7XShqXi
9EjQnLP+et1cJsCNPG3Y201T9n38JUCVYTkMDOCMpDquCjSMIjZkfNRNyA73F4Aw
a899F/WFt/lL+hfymwrfrDJiBFRFU1RHAAAASGV1dGUgaXN0IERpZW5zdGFnLCBk
ZXIgMTcuIEp1bmkgMjAwMy4NCg==
=SDDY
-----END PGP MESSAGE-----
```

Die nächste Variante:

**Digitale Signatur mit Verschlüsselung:**

(1) Wieder legen wir ein Public-Key-Kryptosystem mit öffentlichen Verschlüsselungsfunktionen $f_A$ zugrunde.
(2) Will $A$ eine Nachricht $M$ unterschrieben und verschlüsselt an $B$ senden, bildet er $H(M)$, dann $f_A^{-1}(H(M))$ und hängt dies an das Ende von $M$, d.h. man hat $Mf_A^{-1}(H(M))$. Darauf wendet $A$ jetzt den öffentlichen Schlüssel von $B$ an und erhält $f_B(Mf_A^{-1}(H(M)))$. Dies wird an $B$ verschickt.
(3) $B$ wendet seine private Entschlüsselungsfunktion $f_B^{-1}$ auf $f_B(Mf_A^{-1}(H(M)))$ an und hat dann $Mf_A^{-1}(H(M))$. Auf den Schluss $f_A^{-1}(H(M))$ wendet er $f_A$ an, erhält $H(M)$, was mit dem Hashwert $H(M)$ des ersten Teils $M$ übereinstimmt.

**Beispiel:** Auch bei PGP gibt es die Möglichkeit, eine Datei zu verschlüsseln und zu unterschreiben. Das Ergebnis sieht dann z.B. so aus:

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.1 Int. for non-commercial use <http://www.pgpinternational.com>

qANQR1DBwE4Dxi7IkKjsDEwQBACv3iXdt9WGR6IjY4KUddFVfRfWXgfL1lcb7xza
t6TIyUVjkGhp4j1hQUj1M+Tt/UY6eJ/X7CpHOtU3ONu22wqJ/em6LM5I/xcY6dvF
j0gEQiuLKAp/n6UHxGJzwoFCiXMZOVMk4r37TPCnEINCXNU8s68FsxWuLVKRfsdA
SRcZVAP/fCa4b1+1sFMjGGydLl7Pbj7Ha+K9mXNXNTL5NH4fBRGcQ/m1tExTVdNf
3IHQne8M+LRduPrHa3r8pJbyhpSEhlNfBnuMFwHqPn4FpnZwS6Z9imTcuSLqvb/1
Ig7hUpwJSUnFYB5ehPGNLyw5zqw7uM3LiIbpRITyHSOAqllpr2XJwC1edOTrWSdM
```

```
2AUY48riUTBV3AZ5DcoVqE7Btej2lr52OZbBipRjGpluIRHOhqKHreQSNWG4cKlX
oQb8lPOUQBhg7To1L/B6wj7n7fvMc6A1Je15ggEfWC++4OVBLeD159PNBxPd2T7N
iG0agKUC4n908BOH/u0mN9TuLDAgda1v5Mz5kCzvaYMzO4ur1Gv6dcTQMVtUpjzK
6pPKcnIn7N4Z7i1U5nXdeIBc925v5Q5z5xo+rSiU1o8WPedWpZVuxcqBNscfN4sK
SOM4Q9tCZZYdqF1cM7eRYWrLTSXwSpq/I5YqUc3+gYglL7VYYuc=
=VAAf
-----END PGP MESSAGE-----
```

Wir geben jetzt explizite Algorithmen an, mit denen man signieren kann.

## 3. Das ElGamal-Signatur-Verfahren

**Unterschreiben mit nach ElGamal:**

(1) Jeder Teilnehmer $A$ wählt sich eine (große) Primzahl $p_A$, eine Zahl $g_A$ mit $2 \leq g_A \leq p_A - 2$, sodass $g_A$ Ordnung $p_A - 1$ in $(\mathbf{Z}/p_A\mathbf{Z})^*$ hat, und eine (zufällige) Zahl $e_A$ mit $2 \leq e_A \leq p_A - 2$. Dann berechnet $A$ die Zahl $f_A \equiv g_A^{e_A} \bmod p_A$. Der öffentliche Schlüssel von $A$ ist das Tripel $(p_A, g_A, f_A)$, der geheime Schlüssel ist $e_A$. Außerdem einigen sich alle Teilnehmer auf eine feste Hashfunktion $H$, z.B. SHA-1.

(2) Will $A$ eine Nachricht $M$ unterschreiben, so bestimmt er den Hashwert $h = H(M)$, wählt ein zufälliges $z$ mit $1 \leq z \leq p_A - 2$ und $\mathrm{ggT}(z, p_A - 1) = 1$ und berechnet nacheinander

$$b \equiv g_A^z \bmod p_A \quad \text{und} \quad c \equiv \frac{1}{z}(h - be_A) \bmod (p_A - 1),$$

wobei $0 \leq b, c \leq p - 1$ gewählt wird. ($\frac{1}{z} \bmod (p_A - 1)$ existiert wegen $\mathrm{ggT}(z, p_A - 1) = 1$.) Die Signatur ist das Paar $(b, c)$.

(3) Wie überprüft ein Empfänger $B$ der Nachricht $M$ mit der Signatur $(b, c)$, ob alles in Ordnung ist? Er berechnet $h = H(M)$ und testet dann, ob

$$1 \leq b \leq p_A - 1 \quad \text{und} \quad g_A^h \equiv f_A^b b^c \bmod p_A$$

gilt. Wenn ja, akzeptiert $B$ die Unterschrift, denn ist alles in Ordnung, so folgt die Testgleichung aus

$$g_A^h \equiv g_A^{cz+be_A} \equiv f_A^b b^c \bmod p.$$

**Beispiel:** Wir wählen $p = 10^{60} + 1059$, $g = 14$ (die kleinste Primitivwurzel modulo $p$) und zufällig

$$e = 821763456327843489347568374596809621874065621232000974902930.$$

Dann erhält man mit $f \equiv g^e \bmod p$

$$f = 373114969933957387267276925286835074651999005365255048110 69.$$

Wir wollen die Unix-Datei datei mit ElGamal signieren, die nur den Text 'Kryptographie' enthält (14 Bytes). Der SHA-1-Hashwert $h$ ist

$$\begin{aligned} h &= (83a67d1760ef5ef6adbdff1a00009dd8124d872c)_{16} = \\ &= 751590611671963742963395332599948545481746777900. \end{aligned}$$

Wir wählen als Zufallszahl

$$z = 165232161538517826534178653278412537846215378521378651782653181157235 41$$

und erhalten mit $b \equiv g^z \bmod p$ und $c = z^{-1}(h - be) \bmod p - 1$ die Signatur $(b, c)$ mit

$$\begin{aligned} b &= 31493949701428742454491632499399482522901836186219900908254 9, \\ c &= 26461363827908836487198423791869743190475874200324338027880 8. \end{aligned}$$

Man testet schnell, dass tatsächlich $g^h \equiv f^b b^c \bmod p$ gilt.

**Bemerkungen:** Wie sicher ist die ElGamal-Signatur?

(1) Wie kann ein Außenstehender $C$ die Unterschrift von $A$ fälschen? Natürlich kann $C$ sich ein zufälliges $z$ wählen, damit $b \equiv g_A^z \bmod p_A$ berechnen, dann aber braucht $C$ noch $c$, sodass gilt $g_A^h \equiv f_A^b b^c \bmod p_A$ (oder $g_A^h \equiv g_A^{be_A+cz} \bmod p_A$). Dies ist aber gleichwertig mit

$$h \equiv be_A + cz \bmod (p_A - 1).$$

Eine gültige Signatur ist also äquivalent mit der Kenntnis des privaten Schlüssels $e_A$ von $A$. Diesen kann man aber im allgemeinen nur durch Logarithmenberechnung aus $g_A^{e_A} \equiv f_A \bmod p_A$ erhalten.

(2) Wenn nicht verschlüsselt wird, sind eventuell $h$ und $(b, c)$ zugänglich. Dann weiß man, dass gilt

$$h \equiv b \cdot e_A + c \cdot z \bmod p_A - 1.$$

Dies ist eine Gleichung mit den beiden Unbekannten $e_A$ und $z$. Damit ist klar: $z$ muss auf jeden Fall geheim gehalten werden!

(3) Angenommen wir sehen, dass jemand 2 Nachrichten signiert mit Unterschriften $(b, c_1)$ und $(b, c_2)$ und Hashwerten $h_1$, $h_2$, also gleicher erster Komponente in den Signaturen. Damit liegt auch bei beiden Signaturen (modulo $p_A - 1$) die gleiche Zufallszahl $z$ vor. Nach Definition erhalten wir dann ein Gleichungssystem

$$\begin{aligned} c_1 z &\equiv h_1 - be_A \bmod (p_A - 1), \\ c_2 z &\equiv h_2 - be_A \bmod (p_A - 1), \end{aligned}$$

woraus wir (im Fall $c_1 \neq c_2$) schnell $z$ und $e_A$ berechnen können. (Etwas genauer: Aus den beiden Gleichungen erhält man zunächst

$$z \equiv \frac{h_1 - h_2}{c_1 - c_2} \bmod \frac{p_A - 1}{\mathrm{ggT}(p_A - 1, c_1 - c_2)}.$$

Dies liefert $\mathrm{ggT}(p_A - 1, c_1 - c_2)$ Möglichkeiten für $z$ modulo $p_A - 1$, die man durchprobiert, mit $z$ dann aus einer der Gleichungen $e$ bestimmt und testet, ob $g_A^e \equiv f_A \bmod p_A$ gilt.) Man muss also darauf achten, dass der Zufallszahlengenerator gut ist, insbesondere sollte er lauter verschiedene Zahlen liefern.

(4) Lässt man die Testbedingung $1 \leq b \leq p_A - 1$ weg, so lassen sich leicht Unterschriften fälschen, wenn man bereits eine Unterschrift $(b, c)$ von $A$ (eines Dokuments $M$ mit Hashwert $h = H(M)$) kennt. Zu einer Nachricht $M'$ berechnet man nacheinander

$$h' = H(M'), \quad u \equiv \frac{h'}{h} \bmod (p_A - 1), \quad b' \equiv \begin{cases} bu & \bmod (p_A - 1), \\ b & \bmod p_A, \end{cases} \quad c' \equiv cu \bmod (p_A - 1),$$

wobei $b'$ mit Hilfe des chinesischen Restsatzes berechnet wird. Dann gilt, wenn man bedenkt, dass die Exponenten modulo $p_A - 1$ abgeändert werden können:

$$g_A^{h'} \equiv g_A^{hu} \equiv (f_A^b b^c)^u \equiv f_A^{bu} b^{cu} \equiv f_A^{b'} b^{c'} \equiv f_A^{b'} b'^{c'} \bmod p_A,$$

was zeigt, dass $(b', c')$ die Signaturtestgleichung für $M'$ erfüllt. Allerdings gilt im Fall $h \neq h'$ die Ungleichung $b' > p_A$. Dies zeigt, dass die Testbedingung $1 \leq b \leq p_A - 1$ notwendig ist.

## 4. DSA - Digital Signature Algorithm

Das NIST - National Institute of Standards and Technology der US-Regierung hat am 27. Januar 2000 einen Standard für digitale Unterschriften - Digital Signature Standard (DSS) - festgelegt, der im Folgenden beschrieben wird (Federal Information Processing Standards Publication FIPS 186-2).

**DSA - Digital Signature Algorithm:**

(1) *Schlüsselerzeugung:* Jeder Teilnehmer $A$ hat folgendes zu tun:
- $A$ wählt sich eine 160 Bit lange Primzahl $q$ (mit Zufallszahlengenerator und Primzahltest).
- $A$ sucht sich eine weitere Primzahl $p$ mit $p \equiv 1 \bmod q$ und einer Bitzahl $\equiv 0 \bmod 64$ zwischen 512 und 1024.
- $A$ bestimmt einen Erzeuger $g$ der zyklischen Untergruppe der Ordnung $q$ von $\mathbf{F}_p^*$: Ist $g_0 \in \mathbf{Z}$ mit $g_0^{\frac{p-1}{q}} \not\equiv 0, 1 \bmod p$, so liefert $g \equiv g_0^{\frac{p-1}{q}} \bmod p$ einen solchen Erzeuger.

- $A$ wählt eine Zufallszahl $e_A$ mit $0 < e_A < q$ als geheimen Schlüssel. Der öffentliche Schlüssel wird $f_A \equiv g^{e_A} \bmod p$ zusammen mit $q$, $p$ und $g$.

($q$, $p$ und $g$ können allen Teilnehmern der Benutzergruppe gemeinsam sein.)

(2) *Signieren einer Nachricht:* Wie signiert $A$ eine Nachricht/Datei $M$?
- $A$ berechnet den 160-Bit-Hash-Wert $h = \text{SHA-1}(M)$ der Nachricht $M$.
- $A$ wählt eine Zufallszahl $z$ mit $0 < z < q$ und berechnet dann
$$r = (g^z \bmod p) \bmod q,$$
d.h. zuerst $\widetilde{r}$ mit $1 \le \widetilde{r} \le p-1$ und $\widetilde{r} \equiv g^z \bmod p$, sodann $r$ mit $0 \le r \le q-1$ und $r \equiv \widetilde{r} \bmod q$.
- $A$ berechnet sich $s$ mit
$$s \equiv \frac{1}{z}(h + e_A r) \bmod q.$$
- Ist $r = 0$ oder $s = 0$ wählt man eine andere Zufallszahl $z$. Dieser Fall ist allerdings sehr unwahrscheinlich.
- Die Signatur ist dann das 320-Bit-lange Zahlenpaar $(r, s)$ (mit $0 \le r, s \le q-1$). Kurz:
$$r \equiv (g^z \bmod p) \bmod q \quad \text{und} \quad s \equiv \frac{1}{z}(h + e_A r) \bmod q.$$

(3) *Signaturüberprüfung:* Wie kann ein Empfänger $B$ sehen, dass die Unterschrift $(r, s)$ der Nachricht $M$ tatsächlich von $A$ stammt?
- $B$ holt sich den öffentlichen Schlüssel $(q, p, g, f_A)$ von $A$ und berechnet sich den SHA-1-Hash-Wert $h$ der Nachricht $M$.
- Ist eine der Bedingungen $0 < r < q$, $0 < s < q$ verletzt, wird die Unterschrift nicht akzeptiert.
- Dann berechnet $B$
$$u_1 = s^{-1} h \bmod q \quad \text{und} \quad u_2 = s^{-1} r \bmod q$$
und damit
$$v = (g^{u_1} f_A^{u_2} \bmod p) \bmod q.$$
- Gilt nun $v = r$, so akzeptiert $B$ die Unterschrift.
- Warum gilt $v = r$, wenn alles richtig gelaufen ist? Man hat
$$u_1 + e_A u_2 \equiv s^{-1} h + s^{-1} e_A r = s^{-1}(h + e_A r) \equiv z \bmod q$$
und damit ($\text{ord}\,(g) = q$)
$$g^z \equiv g^{u_1 + e_A u_2} \equiv g^{u_1} g^{e_A u_2} \equiv g^{u_1} f_A^{u_2} \bmod p,$$
was dann sofort $r = v$ liefert.

**Bemerkungen:**

(1) Da $g$ Ordnung $q$ in $(\mathbf{Z}/p\mathbf{Z})^*$, ist klar, dass gilt
$$x \equiv y \bmod q \quad \Longleftrightarrow \quad g^x \equiv g^y \bmod p.$$
Ein Ausdruck wie $(g^{u_1} f^{u_2} \bmod p) \bmod q$ ist allerdings nur dann sinnvoll, wenn man genau weiß, welchen Repräsentanten modulo $p$ man zunächst nehmen muss, z.B. zwischen 0 und $p-1$.

(2) Ein Vorteil dieses Signaturverfahrens ist, dass die Signatur $(r, s)$ recht kurz ist: 320 Bits, was einer 80-stelligen Hexadezimalzahl entspricht.

**Beispiel:** Wir wollen ein Beispiel für eine DSA-Unterschrift angeben. Wir starten mit der 160-Bit-Primzahl
$$q = 1461501637330902918203684832716283019655932542929 = 2^{160} - 47.$$
Dann wählen wir die 512-Bit-Primzahl $p$ mit

$$\begin{aligned} p &= 1 + 2^{512} - (2^{512} \bmod q) - 260 \cdot q = \\ &= 13407807929942597099574024998205846127479365820592393377723561443721764030073546\backslash\backslash \\ &\quad 9768018742981669034276896518677607800160950209247554403363608771901553499 49 \end{aligned}$$

Mit $g_0 = 2$ findet man, dass

$$\begin{aligned} g &= 2^{(p-1)/q} \bmod p = \\ &= 12280246724468801505418109787560177527401535079309733528636401789422926107758081\backslash\backslash \\ &\quad 30487843127337955673072003576151510425353429120714826317783193329238668368 0 \end{aligned}$$

Ordnung $q$ in der multiplikativen Gruppe von $\mathbf{Z}/p\mathbf{Z}$ hat. Als geheimen Schlüssel wählen wir $e$ mit $0 < e < q$

$$e = 706887085027907282087671971171458291728603445938$$

und berechnen dazu

$$\begin{aligned} f &= g^e \bmod p = \\ &= 11775894991298881369448454813182491618825719454351838742200532832248921266669224\backslash\backslash \\ &\quad 40113116630136571048493825351039594748400251483852739455389675027830542977 5. \end{aligned}$$

Der öffentliche Schlüssel ist jetzt $(q, p, g, f)$, der private $e$.
Wir wollen eine Unix-Datei signieren, die nur den Text 'Kryptographie' enthält (14 Bytes). Der SHA-1-Hashwert $h$ ist

$$\begin{aligned} h &= (83a67d1760ef5ef6adbdff1a00009dd8124d872c)_{16} = \\ &= 75159061167196374296339533259994854548174677790 0. \end{aligned}$$

Als Zufallszahl wählen wir

$$z = 450513945073814914190301259918863086680294471512$$

und berechnen nacheinander

$$\begin{aligned} r &= (g^z \bmod p) \bmod q = \\ &= 97090100625522794843667750705070966857375757612 2 = \\ &= (AA10B4F426D83FCA75131509EF605B2E4C7C13BA)_{16}, \\ s &= (h + er)/z \bmod q = \\ &= 40728014677942257093429943657626153453521100143 5 = \\ &= (475712CB5A6BDB53B94555D0BE5151FDF03FA65B)_{16}. \end{aligned}$$

Die Signatur $(r, s)$ ist also (in Hexadezimaldarstellung)

AA10B4F426D83FCA75131509EF605B2E4C7C13BA475712CB5A6BDB53B94555D0BE5151FDF03FA65B.

Zur Sicherheit haben wir $u_1 \equiv h/s \bmod q$, $u_2 \equiv r/s \bmod q$, $v \equiv (g^{u_1} f^{u_2} \bmod p) \bmod q$ berechnet und getestet, dass tatsächlich $r = v$ gilt.

**Bemerkungen:**

(1) Was passiert, wenn zwei Nachrichten zufällig mit der gleichen Zufallszahl $z$ signiert werden? Man hat dann $r_i \equiv (g^z \bmod p) \bmod q$, also $r_1 = r_2 = r$. Weiter gilt $s_i z \equiv h_i + e_A r_i \bmod q$, ausgeschrieben:

$$\begin{aligned} s_1 \cdot z - r \cdot e_A &\equiv h_1 \bmod q, \\ s_2 \cdot z - r \cdot e_A &\equiv h_2 \bmod q. \end{aligned}$$

Kennt jemand die Hashwerte $h_1$, $h_2$ und die Signaturen $(r, s_1)$, $(r, s_2)$, so ist dies ein lineares Gleichungssystem mit den 2 Unbekannten $z$ und $e$, woraus man im Fall $s_1 \neq s_2$ sofort $z$ und den privaten Schlüssel $e_A$ berechnen kann. Es ist also wichtig, dass der Zufallszahlengenerator gut ist.

(2) Was passiert, wenn zwei Nachrichten mit Hashwerten $h_1$ und $h_2$ Signaturen $(r, s_1)$ und $(r, s_2)$ mit gleicher erster Komponente haben? Natürlich kann man dann probieren, ob die gleiche Zufallszahl $z$ benutzt wurde, wie oben. Aber das muss nicht sein. Wir haben damit nur zwei Gleichungen mit drei Unbekannten $e_A, z_1, z_2$:

$$s_1 z_1 \equiv h_1 + e_A r, \quad s_2 z_2 \equiv h_2 + e_A r,$$

was noch keine Lösung liefert. (Dies ist ganz anders als bei der ElGamal-Signatur.) Es ist auch nicht klar, wie man zu gegebenem $r$ ein $z$ findet man $r = (g^z \bmod p) \bmod q$.

(3) Die Signatur kann man fälschen, wenn man $e_A$, also den Logarithmus von $f_A$ zur Basis $g$ in $\mathbf{F}_p^*$ berechnen kann. Nun scheint es so zu sein, dass die Rechenschwierigkeit und damit die Sicherheit in erster Linie von der Größe von $p$ und nicht hauptsächlich von der Größe von $q = \operatorname{ord}(g)$ abhängt.

**Beispiel:** Um einen Eindruck von der Unregelmäßigkeit der Funktion

$$r(z) \equiv (g^z \bmod p) \bmod q$$

zu geben, betrachten wir die Größen

$$q = 19, \quad p = 9767, \quad g_0 = 2, g = 2534$$

und listen sämtliche Urbilder auf:

$$\begin{aligned}
r^{-1}(0) &= \{2\},\\
r^{-1}(1) &= \{0, 16, 17\},\\
r^{-1}(2) &= \{5, 15\},\\
r^{-1}(3) &= \{3\},\\
r^{-1}(4) &= \emptyset,\\
r^{-1}(5) &= \{4, 13\},\\
r^{-1}(6) &= \{14\},\\
r^{-1}(7) &= \{1, 6, 8\},\\
r^{-1}(8) &= \emptyset,\\
r^{-1}(9) &= \emptyset,\\
r^{-1}(10) &= \emptyset,\\
r^{-1}(11) &= \emptyset,\\
r^{-1}(12) &= \emptyset,\\
r^{-1}(13) &= \emptyset,\\
r^{-1}(14) &= \{10, 12, 18\},\\
r^{-1}(15) &= \emptyset,\\
r^{-1}(16) &= \{7\},\\
r^{-1}(17) &= \emptyset,\\
r^{-1}(18) &= \{9, 11\}.
\end{aligned}$$

## 5. ECDSA - Elliptic Curve Digital Signature Algorithm

Wir beschreiben das Analogon von DSA für elliptische Kurven.

**ECDSA:** Als systemweite Parameter wählt man eine elliptische Kurve $E$ über $\mathbf{F}_p$ und einen Punkt $P \in E(\mathbf{F}_p)$ der Ordnung $q$, wo $q$ eine Primzahl ist. ($q$ sollte ungefähr die gleiche Größe wie $p$ haben.) Außerdem benutzt man noch eine festgewählte Hashfunktion $H$, z.B. SHA-1.

(1) *ECDSA-Schlüsselerzeugung:* Jeder Teilnehmer $A$ wählt sich eine (zufällige) Zahl $e_A$ mit $1 < e_A < q - 1$ und berechnet $Q_A = e_A P$. Der öffentliche Schlüssel von $A$ ist $Q_A$, der private $e_A$.

(2) *ECDSA-Signatur-Erzeugung:* $A$ unterschreibt eine Nachricht $M$ folgendermaßen:

(a) $A$ wählt eine Zufallszahl $z$ mit $1 < z < q - 1$.

(b) $A$ berechnet

$$zP = (x_1, y_1) \text{ mit } 0 \le x_1 \le p - 1 \text{ und } r \equiv x_1 \bmod q \text{ mit } 0 \le r \le q - 1.$$

Ist $r = 0$, wählt $A$ eine andere Zufallszahl $z$.

(c) $A$ berechnet den Hashwert der Nachricht $M$

$$h = H(M) \quad \text{und damit} \quad s \equiv \frac{1}{z}(h + e_A r) \bmod q.$$

Im Fall $s = 0$, wählt $A$ eine andere Zufallszahl.

(d) Die Signatur für die Nachricht $M$ ist das Paar $(r, s)$, die $A$ seiner Nachricht an $B$ dann hinzufügt.

(3) *ECDSA-Signatur-Verifikation:* $B$ erhält also eine Nachricht $M$ und eine Signatur $(r, s)$. Um zu sehen, ob die Signatur $(r, s)$ gültig ist, geht $B$ folgendermaßen vor:

(a) $B$ holt sich $A$'s öffentlichen Schlüssel $Q_A$, überprüft, ob $r$ und $s$ im Intervall $[1, q-1]$ liegen. Dann bestimmt $B$ den Hashwert $h = H(M)$ und berechnet nacheinander

$$u_1 \equiv s^{-1}h \bmod q, \quad u_2 \equiv s^{-1}r \bmod q, \quad (x_0, y_0) = u_1 P + u_2 Q_A, \quad v \equiv x_0 \bmod q.$$

(b) $B$ akzeptiert die Unterschrift nur dann, falls $v = r$ gilt.

(c) Warum gilt $v = r$, wenn alles richtig gelaufen ist? Es ist

$$(x_0, y_0) = u_1 P + u_2 Q_A = s^{-1}hP + s^{-1}re_A P = s^{-1}(h + e_A r)P = zP = (x_1, y_1),$$

also $x_0 = x_1$ und damit $r = v$.

**Bemerkung:** ECDSA ist ein Signierfahren, dessen Verwendung von NIST gebilligt wurde. In FIPS 186-2 werden einige elliptische Kurven zur Benutzung vorgeschlagen.

**Beispiel:** Wir legen die in FIPS 186-2 vorgeschlagene Kurve P-192 zugrunde. Die Kurve hat folgende Parameter:

$$\begin{aligned}
p &= \text{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFF} = \\
&= 6277101735386680763835789423207666416083908700390324961279, \\
a &= -3 = \\
&= \text{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFFFFFFFFFFFC} = \\
&= 6277101735386680763835789423207666416083908700390324961276, \\
b &= \text{64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1} = \\
&= 2455155546008943817740293915197451784769108058161191238065, \\
N &= \#E(\mathbf{F}_p) = q = \text{ (Primzahl)} \\
&= \text{FFFFFFFFFFFFFFFFFFFFFF99DEF836146BC9B1B4D22831} = \\
&= 6277101735386680763835789423176059013767194773182842284081, \\
P_x &= \text{188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF1012} = \\
&= 6020462823756886567582134805875261119166987663688468 4818, \\
P_y &= \text{7192B95FFC8DA78631011ED6B24CDD573F977A11E794811} = \\
&= 1740503322936220314048575522802194103640234889273866506 41.
\end{aligned}$$

Wir haben nachgeprüft, dass $p$ und $q$ (wahrscheinliche) Primzahlen sind, und dass $P \in E(\mathbf{F}_p)$ und $k \cdot P = O$ gilt.
Als privaten Schlüssel wählen wir ein zufälliges $e$ und berechnen damit den öffentlichen Schlüssel $Q = e \cdot P$:

$$\begin{aligned}
e &= 7988816221172147949467540136143450192000430724830324002 20, \\
Q_x &= 2469655474632002103680255327003088032581337503959444564894, \\
Q_y &= 4713630799105072385697259043111238489376273439315784616463.
\end{aligned}$$

Wir wollen eine Unix-Datei signieren, die nur den Text 'Kryptographie' enthält (14 Bytes). Der SHA-1-Hashwert $h$ ist

$$\begin{aligned}
h &= (\text{83a67d1760ef5ef6adbdff1a00009dd8124d872c})_{16} = \\
&= 7515906116719637429633953325999485454 81746777900.
\end{aligned}$$

Als Zufallszahl wählen wir

$$z = 44435801450156040444515434650633281125849996798520723370 16.$$

Damit erhalten wir

$$\begin{aligned}
(x_1, y_1) &= z \cdot P, \\
x_1 &= 489785007923979678227522847057604798173196131631703249 0986, \\
y_1 &= 146884515390843427859590837114863299965203427840423005 6799, \\
r &= x_1 \bmod q = \\
&= 489785007923979678227522847057604798173196131631703249 0986 = \\
&= \text{C7BFF0D8DC7D258FF02E48728E94A092DF0F5529FE2E27EA}, \\
s &= (h + er/z \bmod q = \\
&= 495237524624582693763459056817134500207592853847666724 0416 = \\
&= \text{C9F935CA0F907B80126F032FEC11D472D1FF8CD7E6947FE0}.
\end{aligned}$$

Die Signatur ist also

C7BFF0D8DC7D258FF02E48728E94A092DF0F5529FE2E27EA C9F935CA0F907B80126F032FEC11D472D1FF8CD7E6947FE0

mit 96 Zeichen in Hexadezimaldarstellung.
Zum Überprüfen der Signatur bilden wir nacheinander

$$\begin{aligned}
u_1 &= h/s \bmod q = 421868469842310579831926997959527918153546118150850430 6157, \\
u_2 &= r/s \bmod q = 237802567568274826283257813965363959270302375759542767 6524, \\
(x_0, y_0) &= u_1 P + u_2 Q = (489785007923979678227522847057604798173196131631703249 0986, \\
&\quad 146884515390843427859590837114863299965203427840423005 6799), \\
v &= x_0 \bmod q = 489785007923979678227522847057604798173196131631703249 0986.
\end{aligned}$$

Die Signatur ist gültig, da $r = v$ gilt.

KAPITEL 9

# Endomorphismen

## 1. Elliptische Kurven über C

Das Studium elliptischer Kurven über dem Körper $\mathbf{C}$ der komplexen Zahlen ist in mancher Hinsicht einfacher als der Allgemeinfall, da man hier Mittel der Funktionentheorie zur Verfügung hat. Im Folgenden soll ein kurzer Überblick (ohne Beweise) gegeben werden.

**Gitter:** Ein Gitter in $\mathbf{C}$ ist eine Untergruppe der additiven Gruppe von $\mathbf{C}$ der Gestalt

$$\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 = \{z_1\omega_1 + z_2\omega_2 \in \mathbf{C} : z_1, z_2 \in \mathbf{Z}\} \subseteq \mathbf{C},$$

wo $\omega_1, \omega_2$ eine $\mathbf{R}$-Basis von $\mathbf{C}$ ist. (Dies ist gleichwertig mit $\omega_1 \neq 0$, $\omega_2 \neq 0$ und $\frac{\omega_2}{\omega_1} \notin \mathbf{R}$.) $\omega_1, \omega_2$ nennt man dann eine Gitterbasis von $\Lambda$. Die folgende Äquivalenz zeigt, wie Gitterbasen eines Gitters auseinander hervorgehen:

$$\mathbf{Z}\omega_1' + \mathbf{Z}\omega_2' = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 \iff \text{es gibt } a,b,c,d \in \mathbf{Z} \text{ mit } ad - bc = \pm 1 \text{ und } \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Zwei Gitter $\Lambda, \Lambda'$ nennt man ähnlich ($\Lambda \sim \Lambda'$), wenn es ein $\mu \in \mathbf{C}^*$ gibt mit $\Lambda' = \mu\Lambda$. Jedes Gitter ist dann ähnlich einem Gitter der Gestalt

$$\Lambda = \mathbf{Z} + \mathbf{Z}\tau \quad \text{mit} \quad \operatorname{Im}(\tau) > 0.$$

Da ein Gitter $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 \subseteq \mathbf{C}$ eine Untergruppe der additiven Gruppe von $\mathbf{C}$ ist, kann man die Faktorgruppe $\mathbf{C}/\Lambda$ bilden:

$$\mathbf{C}/\Lambda = (\mathbf{R}\omega_1 + \mathbf{R}\omega_2)/(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) \simeq \mathbf{R}/\mathbf{Z} \oplus \mathbf{R}/\mathbf{Z}.$$

Topologisch ist $\mathbf{C}/\Lambda$ ein Torus.

**Doppeltperiodische Funktionen:** Eine meromorphe komplexe Funktion $f(z)$ heißt doppeltperiodisch bzgl. eines Gitters $\Lambda$, wenn

$$f(z+\omega) = f(z) \text{ für alle } \omega \in \Lambda$$

gilt. Gleichwertig damit ist die Bedingung $f(z+\omega_1) = f(z+\omega_2) = f(z)$, wenn $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ ist. Welche doppeltperiodischen Funktionen (bzgl. $\Lambda$) gibt es?

- Ist $f$ doppeltperiodisch und holomorph, so ist $f$ nach dem Satz von Liouville konstant.
- Die (historisch) wichtigste doppeltperiodische Funktion ist die Weierstraßsche $\wp$-Funktion, die durch
$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$
definiert wird. $\wp(z)$ hat in allen Punkten $\omega \in \Lambda$ einen Pol zweiter Ordnung und ist sonst holomorph.
- Die Ableitung der Weierstraßschen $\wp$-Funktion
$$\wp'(z) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^3}$$
ist ebenfalls doppeltperiodisch bzgl. $\Lambda$.

Version vom 19.7.2003 - 26.12.2006

- Man kann zeigen, dass jede doppeltperiodische Funktion die Gestalt
$$\frac{f(\wp(z),\wp'(z))}{g(\wp(z),\wp'(z))} \text{ mit Polynomen } f(x,y), g(x,y) \in \mathbf{C}[x,y]$$
hat. Die Menge aller bzgl. $\Lambda$ doppeltperiodischen Funktionen bildet einen Körper.

**Der Zusammenhang mit elliptischen Kurven:** Definiert man für ein Gitter $\Lambda$
$$s_m = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^m},$$
so erhält man für die Laurentreihenentwicklungen von $\wp$ und $\wp'$ in $z=0$:
$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3s_4z^2 + 5s_6z^4 + \cdots = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{2n+2}z^{2n},\\ \wp'(z) &= -\frac{2}{z^3} + 6s_4z + 20s_6z^3 + \ldots\end{aligned}$$
Da es keine nichtkonstanten holomorphen doppeltperiodischen Funktionen gibt, erhält man daraus schnell die Relation
$$\wp'^2 = 4\wp^3 - g_2\wp - g_3 \quad \text{mit} \quad g_2 = 60s_4 \quad \text{und} \quad g_3 = 140s_6,$$
wobei außerdem die Bedingung $g_2^3 - 27g_3^2 \neq 0$ erfüllt ist.
Definiert man nun eine (ebene projektive) Kurve $E$ über $\mathbf{C}$ durch die Gleichung
$$y^2 = x^3 - \frac{1}{4}g_2x - \frac{1}{4}g_3,$$
so ist
$$4(-\frac{1}{4}g_2)^3 + 27(-\frac{1}{4}g_3)^2 = -\frac{1}{16}(g_2^3 - 27g_3^2) \neq 0,$$
d.h. $E$ ist eine elliptische Kurve. Für $z \in \mathbf{C}\setminus\Lambda$ gilt dann
$$(\wp(z), \frac{1}{2}\wp'(z)) \in E(\mathbf{C}).$$
Man kann dann zeigen, dass durch die Zuordnung
$$z \mapsto (\wp(z), \frac{1}{2}\wp'(z)), \quad \omega \mapsto O \text{ für } \omega \in \Lambda$$
sogar ein Gruppenisomorphismus
$$\mathbf{C}/\Lambda \simeq E(\mathbf{C})$$
definiert wird.

Umgekehrt gilt, dass sich jede elliptische Kurve $E$ über $\mathbf{C}$ auf obige Weise darstellen lässt, d.h. ist $E$ gegeben durch $y^2 = x^3 + ax + b$, so gibt es ein Gitter $\Lambda$ mit $a = -\frac{1}{4}g_2(\Lambda)$, $b = -\frac{1}{4}g_3(\Lambda)$, $E(\mathbf{C}) \simeq \mathbf{C}/\Lambda$, etc. Wir geben daher eine elliptische Kurve über $\mathbf{C}$ oft in der Gestalt $\mathbf{C}/\Lambda$ an. Damit kann man Fragen nach Eigenschaften elliptischer Kurven über $\mathbf{C}$ auf Fragen über den Quotienten $\mathbf{C}/\Lambda$ zurückführen.

**Isomorphie:** Sind $\Lambda_1$ und $\Lambda_2$ Gitter in $\mathbf{C}$, sind $E_1$ und $E_2$ die zugehörigen elliptischen Kurven, so gilt
$$j(E_1) = j(E_2) \quad \Longleftrightarrow \quad E_1 \simeq E_2 \quad \Longleftrightarrow \quad \Lambda_1 \sim \Lambda_2.$$
Ist $E_\tau$ die zu $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ (mit $\mathrm{Im}\,(\tau) > 0$) gehörige elliptische Kurve, so gilt für die $j$-Invariante
$$j(E_\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots \quad \text{mit} \quad q = e^{2\pi i\tau}.$$

**Gruppenstruktur:** Gehört die elliptische Kurve $E$ zum Gitter $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, so haben wir jetzt die Gruppenisomorphien
$$E(\mathbf{C}) \simeq \mathbf{C}/\Lambda = (\mathbf{R}\omega_1 \oplus \mathbf{R}\omega_2)/(\mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2) \simeq \mathbf{R}/\mathbf{Z} \oplus \mathbf{R}/\mathbf{Z}.$$
Ist $A$ eine abelsche Gruppe und $m \in \mathbf{N}$, so definiert man die Untergruppe der $m$-Torsionspunkte durch
$$A[m] = \{a \in A : ma = 0\}.$$

Für eine elliptische Kurve über $\mathbf{C}$ ergibt sich dann

$$E(\mathbf{C})[m] \simeq (\mathbf{C}/\Lambda)[m] = \frac{1}{m}\Lambda/\Lambda \simeq Z_m \oplus Z_m.$$

**Isogenien:** Eine (analytische) Isogenie zwischen zwei elliptischen Kurven $C/\Lambda_1$ und $\mathbf{C}/\Lambda_2$ ist eine nichtkonstante holomorphe Abbildung

$$\phi : \mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2 \quad \text{mit} \quad \phi(0) = 0.$$

Man kann zeigen, dass es dann eine komplexe Zahl $\alpha \neq 0$ gibt mit

$$\phi(z) \equiv \alpha z \bmod \Lambda_2 \quad \text{und} \quad \alpha\Lambda_1 \subseteq \Lambda_2.$$

Offensichtlich ist $\phi$ dann auch ein Gruppenhomomorphismus. Wegen $\alpha\Lambda_1 \subseteq \Lambda_2$ gibt es eine $\mathbf{Z}$-Basis $\omega_1, \omega_2$ von $\Lambda_2$ und $d_1, d_2 \in \mathbf{N}$ mit

$$\alpha\Lambda_1 = \mathbf{Z} \cdot d_1\omega_1 + \mathbf{Z} \cdot d_2\omega_2, \quad \Lambda_2 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 \quad \text{und} \quad d_1 | d_2.$$

Für den Kern der Isogenie $\phi$ gilt

$$\mathrm{Kern}(\phi) = \frac{1}{\alpha}\Lambda_2/\Lambda_1 \simeq \Lambda_2/\alpha\Lambda_1 = (\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2)/(\mathbf{Z}d_1\omega_1 + \mathbf{Z}d_2\omega_2) \simeq Z_{d_1} \oplus Z_{d_2}.$$

Man definiert den Grad von $\phi$ durch

$$\deg \phi = d_1 d_2 = \#\mathrm{Kern}(\phi).$$

Wegen

$$\frac{d_1 d_2}{\alpha}\Lambda_2 = \frac{d_1 d_2}{\alpha}(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) = \mathbf{Z}\frac{d_1 d_2 \omega_1}{\alpha} + \mathbf{Z}\frac{d_1 d_2 \omega_2}{\alpha} \subseteq \mathbf{Z}\frac{d_1\omega_1}{\alpha} + \mathbf{Z}\frac{d_2\omega_2}{\alpha} = \Lambda_1$$

definiert auch

$$\widehat{\phi} : \mathbf{C}/\Lambda_2 \to \mathbf{C}/\Lambda_1, \quad \widehat{\phi}(z) \equiv \frac{d_1 d_2}{\alpha} z \bmod \Lambda_1$$

eine Isogenie. Man nennt $\widehat{\phi}$ die zu $\phi$ duale Isogenie. Es ist

$$\mathrm{Kern}(\widehat{\phi}) = \frac{\alpha}{d_1 d_2}\Lambda_1/\Lambda_2 = (\mathbf{Z}\frac{\omega_1}{d_2} + \mathbf{Z}\frac{\omega_2}{d_1})/(\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2) \simeq Z_{d_1} \oplus Z_{d_2},$$

insbesondere

$$\deg \widehat{\phi} = d_1 d_2 = \deg \phi.$$

Aus den Definitionen ersieht man sofort

$$\widehat{\phi}\phi = \deg \phi : \mathbf{C}/\Lambda_1 \to \mathbf{C}\Lambda_1 \quad \text{und} \quad \phi\widehat{\phi} = \deg \phi : \mathbf{C}/\Lambda_2 \to \mathbf{C}\Lambda_2,$$

wobei $\deg \phi$ hier die Multiplikation mit $\deg \phi$ meint.

**Endomorphismen:** Ein Endomorphismus einer elliptischen Kurve $\mathbf{C}/\Lambda$ ist eine Isogenie der elliptischen Kurve auf sich selbst oder die Nullabbildung. Die Menge der Endomorphismen $\mathrm{End}(\mathbf{C}/\Lambda)$ wird also nach den Bemerkungen zu den Isogenien beschrieben durch

$$\mathrm{End}(\Lambda) = \{\alpha \in \mathbf{C} : \alpha\Lambda \subseteq \Lambda\},$$

wobei zu $\alpha \in \mathrm{End}(\Lambda)$ der Endomorphismus $z \mapsto \alpha z$ gehört, d.h.

$$\mathrm{End}(\mathbf{C}/\Lambda) = \{(z \mapsto \alpha z) : \alpha \in \mathrm{End}(\Lambda)\}.$$

Wir werden uns daher einen Endomorphismus als komplexe Zahl vorstellen, wobei eigentlich die Multiplikation mit dieser komplexen Zahl gemeint ist, also $\mathrm{End}(\mathbf{C}/\Lambda) \simeq \mathrm{End}(\Lambda)$. Ist $m \in \mathbf{Z}$, so gilt $m\Lambda \subseteq \Lambda$, also liefert $z \mapsto mz$ einen Endomorphismus von $\mathbf{C}/\Lambda$. Wir haben

$$\mathbf{Z} \subseteq \mathrm{End}(\Lambda) \subseteq \mathbf{C}.$$

Die Endomorphismen bilden offensichtlich einen Ring, den Endomorphismenring $\mathrm{End}(\mathbf{C}/\Lambda) \simeq \mathrm{End}(\Lambda)$ von $\mathbf{C}/\Lambda$.

LEMMA. *Sei $\tau \in \mathbf{C}$ mit $\mathrm{Re}\,(\tau) > 0$ und $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$. Ist $\alpha \in \mathrm{End}(\Lambda)$, $\alpha \notin \mathbf{Z}$, so gilt:*

(1) $\mathbf{Q}(\tau)$ *ist ein imaginärquadratischer Zahlkörper, d.h. es gibt ein* $D \in \mathbf{Z}$ *quadratfrei mit* $D < 0$ *und*

$$\mathbf{Q}(\tau) = \mathbf{Q}(\sqrt{D}) = \{u + v\sqrt{D} : u, v \in \mathbf{Q}\}.$$

(2) $\alpha$ *genügt einer Gleichung*

$$\alpha^2 - S\alpha + N = 0 \quad \textit{mit} \quad S, N \in \mathbf{Z}$$

*und* $\mathbf{Q}(\alpha) = \mathbf{Q}(\tau)$.

*Beweis:* Wegen $\alpha\Lambda \subseteq \Lambda$ und $\Lambda = \mathbf{Z} \cdot + \mathbf{Z} \cdot \tau$ gibt es $a, b, c, d \in \mathbf{Z}$ mit

$$\alpha \cdot 1 = a \cdot 1 + b \cdot \tau, \quad \alpha \cdot \tau = c \cdot 1 + d \cdot \tau,$$

was man auch als

$$\alpha \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} \alpha - a & -b \\ -c & \alpha - d \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} = 0$$

schreiben kann. Die Determinante der Matrix muss 0 sein, was sofort

$$\alpha^2 - (a + d)\alpha + (ad - bc) = 0$$

impliziert. Schreibt man $S = a + d$, $N = ad - bc$, so hat man die behauptete quadratische Gleichung $\alpha^2 - S\alpha + N = 0$. Wegen $\alpha \notin \mathbf{Z}$ gilt $b \neq 0$, sodass aus $\alpha = a + b\tau$ sofort

$$\tau = -\frac{a}{b} + \frac{1}{b}\alpha$$

und damit $\mathbf{Q}(\alpha) = \mathbf{Q}(\tau)$ folgt. $\mathbf{Q}(\alpha) = \mathbf{Q}(\tau)$ ist dann ein quadratischer Zahlkörper, also gibt es ein $D \in \mathbf{Z}$ quadratfrei mit $\mathbf{Q}(\alpha) = \mathbf{Q}(\tau) = \mathbf{Q}(\sqrt{D})$. Wegen $\tau \notin \mathbf{R}$ muss schließlich $D < 0$ gelten. ■

Das Lemma liefert leicht folgenden Satz:

Satz. *Für ein Gitter* $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ *und zugehörige elliptische Kurve* $E_\tau$ *gibt es folgende Möglichkeiten:*

(1) $\mathrm{End}(\mathbf{C}/\Lambda) = \mathbf{Z}$.
(2) $\mathbf{Z} \subsetneq \mathrm{End}(\mathbf{C}/\Lambda) \subseteq \mathbf{Q}(\sqrt{D})$ *mit* $D \in \mathbf{Z}$, $D < 0$ *quadratfrei und* $\mathbf{Q}(\tau) = \mathbf{Q}(\sqrt{D})$. *Man sagt in diesem Fall, dass* $E_\tau$ *komplexe Multiplikation hat.*

**Komplexe Multiplikation:** Den letzten Satz kann man noch genauer formulieren: Hat $\mathbf{C}/\Lambda$ komplexe Multiplikation, d.h. ist $\mathrm{End}(\mathbf{C}/\Lambda) \neq \mathbf{Z}$, dann ist $\mathrm{End}(\mathbf{C}/\Lambda)$ eine Ordnung in einem imaginärquadratischen Körper, d.h. es gibt $D \in \mathbf{Z}$, $D < 0$, $D$ quadratfrei, $f \in \mathbf{N}$ mit

$$\mathrm{End}(E) \simeq \begin{cases} \mathbf{Z}[f\frac{1+\sqrt{D}}{2}] & D \equiv 1 \bmod 4, \\ \mathbf{Z}[f\sqrt{D}] & D \equiv 2, 3 \bmod 4. \end{cases}$$

**Elliptische Kurven über Q mit komplexer Multiplikation:** Ist $E$ eine über $\mathbf{Q}$ definierte elliptische Kurve mit komplexer Multiplikation, so gibt es genau 13 mögliche $j$-Invarianten und Endomorphismenringe. Diese sind in der folgenden Tabelle zusammengestellt. Eine Kurve $E$ ist durch $j(E)$ natürlich nur bis auf $\overline{\mathbf{Q}}$-Isomorphie bestimmt. (Ist $E : y^2 = x^2 + ax + b$ und $j \neq 0, 1728$, so erhält man die anderen Kurven durch $y^2 = x^3 + au^2x + bu^3$, wo $u$ ein Repräsentantensystem von $\overline{\mathbf{Q}}^* / \overline{\mathbf{Q}}^{*2}$ durchläuft.)

| End($E$) | $j(E)$ | Beispiel für $E$ |
|---|---|---|
| $\mathbf{Z}[\sqrt{-1}]$ | $2^6 \cdot 3^3$ | $y^2 = x^3 - x$ |
| $\mathbf{Z}[2\sqrt{-1}]$ | $2^3 \cdot 3^3 \cdot 11^3$ | $y^2 = x^3 - 11x - 14$ |
| $\mathbf{Z}[\sqrt{-2}]$ | $2^6 \cdot 5^3$ | $y^2 = x^3 - 30x - 56$ |
| $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ | $0$ | $y^2 = x^3 - 1$ |
| $\mathbf{Z}[\sqrt{-3}]$ | $2^4 \cdot 3^3 \cdot 5^3$ | $y^2 = x^3 - 15x - 22$ |
| $\mathbf{Z}[\frac{1+3\sqrt{-3}}{2}]$ | $-2^{15} \cdot 3 \cdot 5^3$ | $y^2 = x^3 - 120x - 506$ |
| $\mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$ | $-3^3 \cdot 5^3$ | $y^2 = x^3 - 35x - 98$ |
| $\mathbf{Z}[\sqrt{-7}]$ | $3^3 \cdot 5^3 \cdot 17^3$ | $y^2 = x^3 - 595x - 5586$ |
| $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}]$ | $-2^{15}$ | $y^2 = x^3 - 264x - 1694$ |
| $\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$ | $-2^{15} \cdot 3^3$ | $y^2 = x^3 - 152x - 722$ |
| $\mathbf{Z}[\frac{1+\sqrt{-43}}{2}]$ | $-2^{18} \cdot 3^3 \cdot 5^3$ | $y^2 = x^3 - 3440x - 77658$ |
| $\mathbf{Z}[\frac{1+\sqrt{-67}}{2}]$ | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | $y^2 = x^3 - 29480x - 1948226$ |
| $\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$ | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | $y^2 = x^3 - 8697680x - 9873093538$ |

## 2. Algebraische Formeln für die Multiplikation mit $m$ in $E(K)$

Wir erinnern an die Formeln für die Addition auf einer elliptischen Kurve $E$, die über einem Körper $K$ der Charakteristik $\neq 2, 3$ durch eine Gleichung $y^2 = x^3 + ax + b$ gegeben ist: Für $P_1, P_2 \in E(K)$ berechnet sich $P_3 = P_1 + P_2 \in E(K)$ wie folgt:

- Ist $P_1 = O$, so ist $P_3 = P_2$, ist $P_2 = O$, so ist $P_3 = P_1$.
- Für die anderen Fälle kann man schreiben $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$.
- Gilt $x_1 = x_2$ und $y_1 + y_2 = 0$, so ist $P_1 + P_2 = O$.
- Für die restlichen Fälle gilt nun $x_1 \neq x_2$ oder $x_1 = x_2$, $y_1 = y_2 \neq 0$. Setzt man

$$m = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{falls } x_1 \neq x_2, \\ \frac{3x_1^2 + a}{2y_1} & \text{falls } x_1 = x_2 \end{cases} \quad \text{und} \quad x_3 = m^2 - x_1 - x_2, \quad y_3 = -m(x_3 - x_1) - y_1,$$

so ist $P_3 = (x_3, y_3) = P_1 + P_2$.

Wir wollen mit der angegebenen Formel für einen Punkt $P \in E(K)$ den Punkt $P_2 = 2 \cdot P \in E(K)$ berechnen.

- Für $P = O$ ist $2P = O$.
- Für den Rest schreiben wir $P = (x, y)$.
- Ist $y = 0$, so gilt $2P = O$.

- Nun können wir $y \neq 0$ annehmen. Mit den obigen Bezeichnungen erhält man, wenn man $y^2$ durch $x^3+ax+b$ ersetzt:

$$\begin{aligned} m &= \frac{3x^2+a}{2y}, \\ m^2 &= \left(\frac{3x^2+a}{2y}\right)^2 = \frac{9x^4+6ax^2+a^2}{4y^2}, \\ x_2 &= m^2-2x = \frac{9x^4+6ax^2+a^2}{4y^2} - 2x = \frac{(9x^4+6ax^2+a^2)-8xy^2}{4y^2} = \\ &= \frac{(9x^4+6ax^2+a^2)-8x(x^3+ax+b)}{4y^2} = \frac{x^4-2ax^2-8bx+a^2}{4y^2}, \\ y_2 &= -m(x_2-x)-y = \frac{x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2}{(2y)^3} \end{aligned}$$

Wir fassen das Ergebnis in folgendem Lemma zusammen, wobei wir auch auf gleiche Weise noch die Formel für $3 \cdot P$ hergeleitet haben:

LEMMA. *Für einen Punkt $P=(x,y) \in E_{a,b}(K)$ gilt mit $2P=(x_2,y_2)$, $3P=(x_3,y_3)$*

$$\begin{aligned} x_2 &= \frac{1}{(2y)^2}(x^4-2ax^2-8bx+a^2), \\ y_2 &= \frac{1}{(2y)^3}(x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2), \\ x_3 &= \frac{1}{(3x^4+12bx+6ax^2-a^2)^2} \cdot (x^9-12ax^7-96bx^6+30a^2x^5-24abx^4+36a^3x^3+48b^2x^3 \\ &\qquad +48a^2bx^2+96ab^2x+9a^4x+64b^3+8ba^3), \\ y3 &= \frac{1}{(3x^4+12bx+6ax^2-a^2)^3} \cdot (y(x^{12}+22ax^{10}+220bx^9-165a^2x^8-528abx^7-1776b^2x^6 \\ &\qquad -92a^3x^6+264a^2bx^5-185a^4x^4-960ab^2x^4-320b^3x^3-80a^3bx^3 \\ &\qquad -624a^2b^2x^2-90a^5x^2-132a^4bx-896ab^3x-3a^6-512b^4-96b^2a^3)) \end{aligned}$$

*Dabei muss man die Formeln richtig lesen, wenn ein Nenner 0 wird: Ist $y=0$, so ist $2P=O$, ist $3x^4+12bx+6ax^2-a^2=0$, so ist $3P=O$.*

Der folgende Satz mit der Definition der $m$-Teilungspolynome (division polynomials) verallgemeinert das letzte Lemma. Ein Beweis findet sich beispielsweise bei S. Lang, Elliptic Curves - Diophantine Analysis, er benutzt Eigenschaften der Weierstraßschen $\wp$-Funktion.

SATZ. (1) *Die sogenannten $m$-Teilungspolynome $\psi_m \in \mathbf{Z}[a,b,x,y]$ werden rekursiv wie folgt definiert:*

$$\begin{aligned} \psi_1 &= 1, \\ \psi_2 &= 2y, \\ \psi_3 &= 3x^4+6ax^2+12bx-a^2, \\ \psi_4 &= 4y(x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \textit{für } m \geq 2, \\ \psi_{2m} &= \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \textit{für } m \geq 2. \end{aligned}$$

*(Man sieht leicht, dass auch $\psi_{2m}$ ein Polynom in $a,b,x,y$ ist.)*

(2) *Weiter wird definiert $\phi_1 = x$, $\omega_1 = y$ und (mit $\psi_0 = 0$)*

$$\begin{aligned} \phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \\ 4y\omega_m &= \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2. \end{aligned}$$

*Für ungerades $m$ sind $\psi_m, \phi_m, \frac{1}{y}\omega_m$ Polynome in $a, b, x, y^2$, für gerades $m$ sind $\frac{1}{2y}\psi_m, \phi_m, \omega_m$ Polynome in $a, b, x, y^2$. Ersetzt man $y^2$ durch $x^3+ax+b$, so kann man die angegebenen Ausdrücke als Polynome in $x$ auffassen, was ab hier passieren soll.*

(3) *Als Polynome in $x$ gilt*

$$\begin{aligned}\phi_m(x) &= x^{m^2} + \dots,\\ \psi_m(x)^2 &= m^2 x^{m^2-1} + \dots\end{aligned}$$

*und*

$$\psi_m = \begin{cases} mx^{(m^2-1)/2} + \dots & \text{für } m \equiv 1 \bmod 2,\\ y(mx^{(m^2-4)/2} + \dots) & \text{für } m \equiv 0 \bmod 2.\end{cases}$$

(4) *Ist $K$ ein Körper der Charakteristik $\neq 2, 3$, sind $a, b \in K$ mit $4a^3 + 27b^2 \neq 0$, so sind die Polynome $\phi_m(x)$ und $\psi_m(x)^2$ teilerfremd in $K[x]$.*

(5) *Ist $K$ ein Körper der Charakteristik $\neq 2, 3$, sind $a, b \in K$ mit $4a^3 + 27b^2 \neq 0$, so gilt für die durch $y^2 = x^3 + ax + b$ definierte elliptische Kurve $E$ und $P = (x, y) \in E(K)$*

$$m \cdot P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right) \text{ für } \psi_m(P) \neq 0 \quad \text{und} \quad m \cdot P = O \text{ für } \psi_m(P) = 0.$$

**Beispiel:** Mit den angegebenen Rekursionsformeln wurden die folgenden Teilungspolynome mit Hilfe von Maple berechnet, wobei bei $\psi_7$ einfach die Maple-Anordnung übernommen wurde.

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
\psi_5 &= 5x^{12} + 62x^{10}a + 380x^9b - 105x^8a^2 + 240x^7ab - 300x^6a^3 - 240x^6b^2 - 696x^5ba^2\\
&\quad -1920ax^4b^2 - 125x^4a^4 - 80a^3x^3b - 1600b^3x^3 - 50a^5x^2 - 240b^2x^2a^2 - 640ab^3x\\
&\quad -100bxa^4 - 32b^2a^3 - 256b^4 + a^6,\\
\psi_7 &= 7x^{24} - a^{12} - 112x^{19}ab - 571872x^{16}ab^2 - 2132480x^{13}ab^3 - 92568x^{17}a^2b - 31808x^{15}a^3b\\
&\quad -615360x^{14}a^2b^2 - 161840x^{13}a^4b - 297472x^{12}a^3b^2 - 608160x^{11}a^5b - 425712x^9ba^6\\
&\quad -2603776x^{11}b^3a^2 - 1192800x^{10}b^2a^4 - 3727360x^9a^3b^3 - 831936x^8a^5b^2 - 53824x^7a^7b\\
&\quad -190400x^6b^2a^6 - 3293696x^{10}b^4a - 7069440x^8b^4a^2 - 1314560x^7b^3a^4 + 57288x^5a^8b\\
&\quad -168448a^5x^5b^3 + 134400a^7x^4b^2 + 1680a^9x^3b - 2954x^{20}a^2 - 19852x^{18}a^3 - 35231x^{16}a^4\\
&\quad -82264x^{14}a^5 - 111916x^{12}a^6 + 308x^{22}a - 42168x^{10}a^7 - 42896x^{18}b^2 - 829696x^{15}b^3\\
&\quad -928256x^{12}b^4 + 3944x^{21}b + 15673x^8a^8 + 14756x^6a^9 - 1555456x^9b^5 + 1302x^4a^{10}\\
&\quad +196a^{11}x^2 - 2809856b^6x^6 - 802816b^7x^3 + 3328b^4a^6 + 160b^2a^9 + 152320b^3x^3a^6\\
&\quad -7127040b^5x^7a - 2293760b^4x^6a^3 - 3698688b^5x^5a^2 + 394240b^4x^4a^4 + 3696a^8b^2x^2\\
&\quad +392a^{10}bx + 96768b^4a^5x^2 - 3039232b^6ax^4 + 831488b^5a^3x^3 + 544768b^6x^2a^2\\
&\quad +64512b^5xa^4 + 7168b^3a^7x + 24576a^3b^6 + 65536b^8 + 229376b^7ax.
\end{aligned}$$

Die $m$-Torsionspunkte einer elliptischen Kurve nennt man auch $m$-Teilungspunkte. Man erhält dann mit den oben angegebenen Formeln für $\psi_m$

$$\begin{aligned}E(\overline{K})[m] &= \{P \in E(\overline{K}) : mP = O\} = \{O\} \cup \{(x, y) \in E(\overline{K}) : \psi_m(x, y) = 0\} =\\ &= \begin{cases}\{O\} \cup \{(x, y) \in \overline{K} \times \overline{K} : y^2 = x^3 + ax + b, mx^{(m^2-1)/2} + \dots = 0\} \text{ für } m \equiv 1 \bmod 2,\\ \{O\} \cup \{(x, y) \in \overline{K} \times \overline{K} : y^2 = x^3 + ax + b, y(mx^{(m^2-4)/2} + \dots = 0\} \text{ für } m \equiv 0 \bmod 2.\end{cases}\end{aligned}$$

Daraus erhält man sofort die Abschätzung

$$\begin{aligned}\#E(\overline{K})[m] &\leq m^2,\\ \#E(\overline{K})[m] &< m^2, \text{ wenn } K \text{ Charakteristik } p \text{ hat und } p|m \text{ gilt.}\end{aligned}$$

Man kann dann folgenden Satz beweisen.

SATZ. *Sei $E$ eine elliptische Kurve über $K$ und $m \in \mathbf{N}$. Ist $m$ teilerfremd zur Charakteristik von $K$ oder hat $K$ Charakteristik 0, so gilt*

$$E(\overline{K})[m] \simeq Z_m \oplus Z_m \quad \text{und} \quad \#E(\overline{K})[m] = m^2.$$

*Hat $K$ Charakteristik $p$, so gilt*

$$E(\overline{K})[p^n] \simeq Z_{p^n} \text{ für alle } n \geq 1 \quad \text{oder} \quad E(\overline{K})[p^n] = 0 \text{ für alle } n \geq 1.$$

**Beispiel:** Das 7-te Teilungspolynom ist

$$\begin{aligned}\psi_7 \;=\;& 7x^{24} + 308ax^{22} + 3944bx^{21} - 2954a^2x^{20} - 112abx^{19} + (-19852a^3 - 42896b^2)x^{18} \\ & -92568a^2bx^{17} + (-35231a^4 - 571872ab^2)x^{16} + (-829696b^3 - 31808a^3b)x^{15} \\ & +(-82264a^5 - 615360a^2b^2)x^{14} + (-2132480ab^3 - 161840a^4b)x^{13} \\ & +(-111916a^6 - 928256b^4 - 297472a^3b^2)x^{12} + (-608160a^5b - 2603776b^3a^2)x^{11} \\ & +(-42168a^7 - 3293696b^4a - 1192800b^2a^4)x^{10} + (-1555456b^5 - 425712ba^6 - 3727360a^3b^3)x^9 \\ & +(15673a^8 - 7069440b^4a^2 - 831936a^5b^2)x^8 + (-53824a^7b - 1314560b^3a^4 - 7127040b^5a)x^7 \\ & +(14756a^9 - 2809856b^6 - 190400b^2a^6 - 2293760b^4a^3)x^6 \\ & +(57288a^8b - 168448a^5b^3 - 3698688b^5a^2)x^5 \\ & +(1302a^{10} + 134400a^7b^2 + 394240b^4a^4 - 3039232b^6a)x^4 \\ & +(-802816b^7 + 1680a^9b + 152320b^3a^6 + 831488b^5a^3)x^3 \\ & +(196a^{11} + 3696a^8b^2 + 96768b^4a^5 + 544768b^6a^2)x^2 \\ & +(392a^{10}b + 64512b^5a^4 + 7168b^3a^7 + 229376b^7a)x \\ & +(3328b^4a^6 + 160b^2a^9 + 24576a^3b^6 - a^{12} + 65536b^8).\end{aligned}$$

Wir nehmen jetzt an, wir rechnen in einem Körper der Charakteristik 7. Dann ist

$$\psi_7 \pmod 7 = 3bx^{21} + 3a^2b^2x^{14} + (6a^7b + 5a^4b^3 + 3ab^5)x^7 + (6a^{12} + 6a^9b^2 + 3a^6b^4 + 6a^3b^6 + 2b^8).$$

Setzen wir

$$f_7(z) = 3bz^3 + 3a^2b^2z^2 + (6a^7b + 5a^4b^3 + 3ab^5)z + (6a^{12} + 6a^9b^2 + 3a^6b^4 + 6a^3b^6 + 2b^8),$$

so ist

$$\psi_7(x) \equiv f_7(x^7) \bmod 7.$$

Die Diskriminante von $f_7$ in Charakteristik 7 ist

$$b^2(4a^3 + 27b^2)^8.$$

Für $b = 0$ wird $f_7(z) = 6a^{12}$.
Sei jetzt $E$ eine durch $y^2 = x^3 + ax + b$ über einem Körper $K$ der Charakteristik 7 definierte elliptische Kurve. Dann gilt

$$E(\overline{K})[7] = \{O\} \cup \{(x, y) \in \overline{K} \times \overline{K} : y^2 = x^3 + ax + b, f_7(x^7) = 0\}.$$

Ist $b \neq 0$, so hat $f_7$ genau drei verschiedenen Nullstellen in $\overline{K}$, also folgt $\#E(\overline{K})[7] = 7$. Ist $b = 0$, so ist $f_7$ konstant und $\neq 0$, also folgt $\#E(\overline{K})[7] = 1$.

## 3. Endomorphismen

Sei $K$ ein Körper der Charakteristik $\neq 2, 3$ und $E$ eine durch $y^2 = x^3 + ax + b$ definierte elliptische Kurve über $K$. Ein Endomorphismus $\phi$ von $E$ ist eine Abbildung

$$\phi : E(\overline{K}) \to E(\overline{K}) \quad \text{mit} \quad \phi(O) = O,$$

wenn es endlich viele homogene Polynome

$$f_0^{(i)}(x_0, x_1, x_2), f_1^{(i)}(x_0, x_1, x_2), f_2^{(i)}(x_0, x_1, x_2) \in \overline{K}[x_0, x_1, x_2], i = 1, \ldots, l$$

gibt, sodass für jeden Punkt $P = (x_0 : x_1 : x_2) \in E(\overline{K})$ (mindestens) ein $i$ existiert mit

$$\phi((x_0 : x_1 : x_2)) = (f_0^{(i)}(x_0, x_1, x_2) : f_1^{(i)}(x_0, x_1, x_2) : f_2^{(i)}(x_0, x_1, x_2)).$$

Die Menge der Endomorphismen von $E$ bezeichnen wir mit $\mathrm{End}(E)$. Können die obigen Polynome $f_i$ in $K[x_0, x_1, x_2]$ gewählt werden, so sagt man, $\phi$ ist über $K$ definiert. Die Menge der über $K$ definierten Endomorphismen von $E$ bezeichnen wir mit $\mathrm{End}_K(E)$. Natürlich gilt dann

$$\mathrm{End}_K(E) \subseteq \mathrm{End}_{\overline{K}}(E).$$

Für $m \in \mathbf{N}$ wird die Multiplikation mit $m$ in $E(\overline{K})$ beschrieben durch

$$(x, y) \mapsto \left(\frac{\phi_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega_m(x, y)}{\psi_m(x, y)^3}\right), \quad O \mapsto O.$$

Man überlegt sich damit, dass für jedes $m \in \mathbf{Z}$ die Abbildung

$$E(\overline{K}) \to E(\overline{K}), \quad P \mapsto mP$$

ein über $K$ definierter Endomorphismus ist.

Wir stellen einige Eigenschaften von Endomorphismen zusammen:

Satz. *Sei $E$ eine über einem Körper $K$ definierte elliptische Kurve.*

(1) *Jeder Endomorphismus $\phi \in \mathrm{End}(E)$ ist ein Gruppenhomomorphismus, d.h. $\phi(P+Q) = \phi(P) + \phi(Q)$.*
(2) *Durch*
$$(\phi_1, \phi_2)(P) = \phi_1(P) + \phi_2(P) \quad \text{und} \quad (\phi_1\phi_2)(P) = \phi_1(\phi_2(P))$$
*wird auf $\mathrm{End}(E)$ eine Addition und Multiplikation definiert, die $\mathrm{End}(E)$ zu einem Ring macht, dem Endomorphismenring. Dabei ist $P \mapsto O$ die $0$, $P \mapsto P$ die $1$ in $\mathrm{End}(E)$.*
(3) *$\mathrm{End}_K(E)$ ist ein Unterring von $\mathrm{End}(E)$.*
(4) *$\mathrm{End}(E)$ ist nullteilerfrei, d.h. $\phi_1\phi_2 = 0$ impliziert $\phi_1 = 0$ oder $\phi_2 = 0$.*
(5) *Durch*
$$\mathbf{Z} \to \mathrm{End}_K(E), \quad m \mapsto (P \mapsto mP)$$
*wird ein injektiver Ringhomomorphismus definert. Man kann dann $\mathbf{Z}$ als Unterring von $\mathrm{End}_K(E)$ auffassen, also $\mathbf{Z} \subseteq \mathrm{End}_K()$. Dann meint $m \in \mathbf{Z} \cap \mathrm{End}_K(E)$ die Multiplikation mit $m$ in $E(\overline{K})$.*

**Beispiel:** Sei $K$ ein Körper der Charakteristik $\neq 2, 3$ und $i \in \overline{K}$ mit $i^2 = -1$. Sei $a \in K^*$ und $E$ die durch die Gleichung $y^2 = x^3 + ax$ über $K$ definierte elliptische Kurve. Wir haben die Implikationen

$$(x, y) \in E(\overline{K}) \implies y^2 = x^3 + ax \implies (iy)^2 = (-x)^3 + a(-x) \implies (-x, iy) \in E(\overline{K}),$$

Damit sieht man, dass durch

$$\phi : E(\overline{K}) \to E(\overline{K}), \quad \phi(x, y) = (-x, iy), \quad \phi(O) = O$$

ein Endomorphismus $\phi \in \mathrm{End}(E)$ definiert wird. Weiter gilt für $(x, y) \in E(\overline{K})$

$$\phi^2(x, y) = \phi(\phi(x, y)) = \phi(-x, iy) = (x, i^2y) = (x, -y) = -(x, y) = (-1)(x, y),$$

d.h. in $\mathrm{End}(E)$ gilt

$$\phi^2 = -1.$$

Gilt $i \in K$, so ist $\phi$ über $K$ definiert, d.h. $\phi \in \mathrm{End}_K(E)$.

**Der duale Endomorphismus:** Man kann (mit deutlich mehr Theorie) jedem $\phi \in \mathrm{End}(E)$ ein $\widehat{\phi} \in \mathrm{End}(E)$ zuordnen, sodass folgende Eigenschaften erfüllt sind:

(1) $\widehat{\phi_1 + \phi_2} = \widehat{\phi_1} + \widehat{\phi_2}$.
(2) $\widehat{\phi_1\phi_2} = \widehat{\phi_2}\widehat{\phi_1}$.
(3) $\widehat{\widehat{\phi}} = \phi$.
(4) $\phi\widehat{\phi} = \widehat{\phi}\phi \in \mathbf{N}_0$. Man setzt dann $\mathrm{N}\phi = \phi\widehat{\phi}$ oder auch $\deg \phi = \phi\widehat{\phi}$.
(5) $\mathrm{N}\phi = 0 \iff \phi = 0$.

(6) Es ist $\phi + \widehat{\phi} \in \mathbf{Z}$. Man setzt $\mathrm{Sp}\phi = \phi + \widehat{\phi}$.
(7) Für $m \in \mathbf{Z}$ ist $\widehat{m} = m$ und $\mathrm{N}m = m\widehat{m} = m^2$.

Damit können wir folgenden Satz beweisen:

SATZ. *Jeder Endomorphismus $\phi \in \mathrm{End}(E)$ genügt einer quadratischen Gleichung über $\mathbf{Z}$, nämlich*

$$\phi^2 - \mathrm{Sp}(\phi)\phi + \mathrm{N}(\phi) = 0.$$

*Außerdem gilt*

$$|\mathrm{Sp}(\phi)| \leq 2\sqrt{\mathrm{N}(\phi)}.$$

*Beweis:* In $\mathrm{End}(E)$ gilt

$$0 = (\phi - \phi)(\phi - \widehat{\phi}) = \phi\phi - \phi\widehat{\phi} - \phi\phi + \phi\widehat{\phi} = \phi^2 - \phi(\widehat{\phi} + \phi) + \phi\widehat{\phi} = \phi^2 - \mathrm{Sp}(\phi)\phi + \mathrm{N}(\phi),$$

wie behauptet. Wir wählen nun $u, v \in \mathbf{Z}$ und berechnen

$$0 \leq \mathrm{N}(u + v\phi) = (u + v\phi)(u + v\widehat{\phi}) = u^2 + \mathrm{Sp}(\phi)uv + \mathrm{N}(\phi)v^2.$$

Also folgt für jede rationale Zahl $t \in \mathbf{Q}$

$$t^2 + \mathrm{Sp}(\phi)t + \mathrm{N}(\phi) \geq 0,$$

d.h. $t^2 + \mathrm{Sp}(\phi)t + \mathrm{N}(\phi)$ hat höchstens eine Nullstelle. Dies impliziert

$$(\mathrm{Sp}(\phi))^2 - 4\mathrm{N}(\phi) \leq 0$$

und somit

$$|\mathrm{Sp}(\phi)| \leq 2\sqrt{\mathrm{N}(\phi)}.$$

Dies beweist die Behauptung. ■

Man kann nun zeigen, dass es nur drei Typen von Endomorphismenringen elliptischer Kurven geben kann:

(1) $\mathrm{End}(E) = \mathbf{Z}$. Man sagt dann auch, $E$ ist gewöhnlich.
(2) $\mathbf{Z} \subsetneq \mathrm{End}(E) \subseteq \mathbf{Q}(\sqrt{d})$ mit einer quadratfreien ganzen Zahl $d < 0$. Man sagt in diesem Fall, $E$ hat komplexe Multiplikation. $\mathrm{End}(E)$ ist dann eine sogenannte Ordnung in dem imaginärquadratischen Zahlkörper $\mathbf{Q}(\sqrt{d})$, d.h. es gibt ein $D \in \mathbf{Z}$, $D < 0$, $D \equiv 0, 1 \bmod 4$ mit

$$\mathrm{End}(E) = \mathbf{Z}[\frac{(D \bmod 2) + \sqrt{D}}{2}] = \mathbf{Z} + \mathbf{Z}\frac{(D \bmod 2) + \sqrt{D}}{2}.$$

(3) $\mathrm{End}(E)$ ist Ordnung in einem definiten Quaternionenschiefkörper $Q_{a,b}$ mit $a, b \in \mathbf{Z}$. Dabei ist $Q_{a,b}$ definiert durch

$$Q_{a,b} = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k \quad \text{mit} \quad i^2 = a, \quad j^2 = b, \quad k = ij, \quad ji = -ij$$

und es gilt $a, b < 0$. Dass $\mathrm{End}(E)$ Ordnung in $Q_{a,b}$ ist, bedeutet, dass es über $\mathbf{Q}$ linear unabhängige $\omega_1, \omega_2, \omega_3, \omega_4 \in Q_{a,b}$ gibt mit $\mathrm{End}(E) = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\omega_3 + \mathbf{Z}\omega_4$. Man nennt $E$ in diesem Fall supersingulär.

**Beispiel:** Wird die elliptische Kurve $E$ durch eine Gleichung $y^2 = x^3 + ax$ über $K$ definiert, ist $i \in \overline{K}$ mit $i^2 = -1$, so hat man den Endomorphismus $\phi$ mit $\phi(x, y) = (-x, iy)$. Wir haben gesehen, dass $\phi^2 = -1$ ist. Also ist $E$ supersingulär oder $\mathrm{End}(E)$ liegt in $\mathbf{Q}(\sqrt{-1})$.

## 4. Der Frobenius-Endomorphismus

**Bemerkung:** Sei $K$ ein Körper der Charakteristik $p$.

(1) Für $u, v \in K$ gilt
$$(uv)^p = u^p v^p \quad \text{und} \quad (u+v)^p = u^p + v^p.$$
Daher ist $u \mapsto u^p$ ein Körperisomorphismus.

(2) Die multiplikative Gruppe von $\mathbf{F}_{p^n}$ hat $p^n - 1$ Elemente, also gilt für $\alpha \in \mathbf{F}_{p^n}^*$ die Gleichung $\alpha^{p^n-1} = 1$ und damit $\alpha^{p^n} = \alpha$. Da $\alpha = 0$ die letzte Gleichung trivialerweise erfüllt, folgt
$$\alpha^{p^n} = \alpha \quad \text{für alle } \alpha \in \mathbf{F}_{p^n}.$$

(3) Da das Polynom $x^{p^n} - x \in \overline{\mathbf{F}_p}[x]$ höchstens $p^n$ Nullstellen in $\overline{\mathbf{F}_p}$ hat, folgt
$$\{\alpha \in \overline{\mathbf{F}_p} : \alpha^{p^n} = \alpha\} = \mathbf{F}_{p^n}.$$
Anders interpretiert: Für $\alpha \in \overline{\mathbf{F}_p}$ gilt
$$\alpha \in \mathbf{F}_{p^n} \quad \Longleftrightarrow \quad \alpha^{p^n} = \alpha.$$
Dies liefert ein einfaches Kriterium für $\alpha \in \mathbf{F}_{p^n}$.

LEMMA. *Sei $E$ eine durch $y^2 = x^3 + ax + b$ definierte elliptische Kurve über $\mathbf{F}_p$ (mit $p \geq 5$). Dann wird durch*
$$\pi : E(\overline{\mathbf{F}_p}) \to E(\overline{\mathbf{F}_p}), \quad (x, y) \mapsto (x^p, y^p) \quad \text{und} \quad O \mapsto O$$
*ein Endomorphismus der elliptischen Kurve definiert. $\pi$ wird als Frobenius-Endomorphismus von $E$ bezeichnet. Natürlich ist $\pi$ über $\mathbf{F}_p$ definiert.*

*Beweis:* Wegen $a, b \in \mathbf{F}_p$ gilt $a^p = a$ und $b^p = b$. Ist nun $(x, y) \in E(\overline{\mathbf{F}_p})$, so gilt $y^2 = x^3 + ax + b$. Wir potenzieren nun mit $p$ und erhalten
$$(y^p)^2 = (y^2)^p = (x^3 + ax + b) = x^{3p} + a^p x^p + b^p = (x^p)^3 + ax^p + b,$$
also gilt wieder $(x^p, y^p) \in E(\mathbf{F}_p)$. Indem man sich die Additionsformeln ansieht, sieht man, dass auch
$$\pi(P_1 + P_2) = \pi(P_1) + \pi(P_2) \quad \text{für} \quad P_1, P_2 \in E(\overline{\mathbf{F}_p})$$
gilt. Wir bemerken schließlich noch, dass man projektiv $\pi$ durch eine einzige Formel, nämlich
$$\pi((x_0 : x_1 : x_2)) = (x_0^p : x_1^p : x_2^p)$$
definieren kann. ■

Mit Hilfe des Frobenius-Endomorphismus kann man leicht charakterisieren, wann ein Endomorphismus über $\mathbf{F}_p$ definiert ist:

SATZ. *Ist $E$ über $\mathbf{F}_p$ definiert und $\pi$ der zugehörige Frobenius-Endomorphismus, so gilt:*
$$\mathrm{End}_{\mathbf{F}_p}(E) = \{\phi \in \mathrm{End}(E) : \pi\phi = \phi\pi\}.$$

Den folgenden Satz werden wir nicht beweisen:

LEMMA. *Für den Frobenius-Endomorphismus einer über $\mathbf{F}_p$ definierten elliptischen Kurve $E$ gilt*
$$\mathrm{N}\pi = p.$$

**Bemerkung:** Ist $E$ über $\mathbf{F}_p$ definiert mit Frobenius $\pi$, so ist $E$ natürlich erst recht über $\mathbf{F}_{p^n}$ definiert. Der zugehörige Frobenius-Endomorphismus ist dann $\pi^n$ mit $\mathrm{N}\pi^n = p^n$.

**Überlegung:** Sei $E$ eine über $\mathbf{F}_p$ definierte elliptische Kurve mit $p \geq 5$. Für $P \in E(\overline{\mathbf{F}_p})$ gilt:

$$P \in E(\mathbf{F}_p) \quad \Longleftrightarrow \quad \pi(P) = P \quad \Longleftrightarrow \quad (\pi - 1)(P) = O \quad \Longleftrightarrow \quad P \in \mathrm{Kern}(\pi - 1).$$

Also erhalten wir die Formeln

$$E(\mathbf{F}_p) = \mathrm{Kern}(\pi - 1) \quad \text{und} \quad \#E(\mathbf{F}_p) = \#\mathrm{Kern}(\pi - 1).$$

Man kann nun zeigen, dass

$$\#\mathrm{Kern}(\pi - 1) = \mathrm{N}(\pi - 1)$$

gilt. (Da $\pi - 1$ ein sogenannter separabler Morphismus ist.) Damit folgt

$$\#E(\mathbf{F}_p) = \mathrm{N}(\pi - 1) = (\pi - 1)(\widehat{\pi} - 1) = \pi\widehat{\pi} - \pi - \widehat{\pi} + 1 = \mathrm{N}\pi - \mathrm{Sp}\pi + 1 = p + 1 - \mathrm{Sp}\pi.$$

Nun haben wir früher eine Abschätzung zwischen Spur und Norm hergeleitet. Diese liefert jetzt:

$$|\mathrm{Sp}\pi| \leq 2\sqrt{\mathrm{N}\pi} = 2\sqrt{p}.$$

Da $2\sqrt{p}$ keine ganze Zahl ist, folgt $|\mathrm{Sp}\pi| < 2\sqrt{p}$. Wir formulieren das wichtige Ergebnis nochmals als Satz:

Satz. *Für eine über $\mathbf{F}_p$ definierte elliptische Kurve $E$ gilt*

$$N = \#E(\mathbf{F}_p) = p + 1 - s \quad \textit{und} \quad |s| < 2\sqrt{p},$$

*wobei $s = \mathrm{Sp}(\pi)$ die Spur des Frobenius bezeichnet.*

**Bemerkung:** Kennen wir für eine elliptische Kurve $E$ über $\mathbf{F}_p$ die Anzahl der Punkte $N = \#E(\mathbf{F}_p)$, so können wir mit $s = (p + 1) - N$ die Spur des Frobenius $\pi$ ausrechnen. $\pi$ genügt dann der Gleichung

$$\pi^2 - s\pi + p = 0 \quad \text{und} \quad \pi = \frac{s + \sqrt{s^2 - 4p}}{2}.$$

**Beispiele:** In den folgenden Beispielen haben wir für eine elliptische Kurve $E_{a,b}$ über $\mathbf{F}_p$ zunächst $N = \#E(\mathbf{F}_p)$ bestimmt, damit die Spur des Frobenius $\mathrm{Sp}(\pi)$ berechnet und $\pi$ bestimmt.

| $p$ | $a$ | $b$ | $j$ | $N$ | $\mathrm{Sp}(\pi)$ | $\frac{\mathrm{Sp}(\pi)}{\sqrt{p}}$ | $\pi$ |
|---|---|---|---|---|---|---|---|
| 5 | 0 | 1 | 0 | 6 | 0 | 0.00 | $\sqrt{-5}$ |
| 5 | 0 | 2 | 0 | 6 | 0 | 0.00 | $\sqrt{-5}$ |
| 5 | 1 | 0 | 3 | 4 | 2 | .89 | $1 + 2\sqrt{-1}$ |
| 5 | 1 | 1 | 2 | 9 | -3 | -1.34 | $\frac{-3+\sqrt{-11}}{2}$ |
| 5 | 1 | 2 | 1 | 4 | 2 | .89 | $1 + 2\sqrt{-1}$ |
| 5 | 2 | 0 | 3 | 2 | 4 | 1.79 | $2 + \sqrt{-1}$ |
| 5 | 2 | 1 | 4 | 7 | -1 | -.45 | $\frac{-1+\sqrt{-19}}{2}$ |
| 5 | 3 | 0 | 3 | 10 | -4 | -1.79 | $-2 + \sqrt{-1}$ |
| 5 | 3 | 2 | 4 | 5 | 1 | .45 | $\frac{1+\sqrt{-19}}{2}$ |
| 5 | 4 | 0 | 3 | 8 | -2 | -.89 | $-1 + 2\sqrt{-1}$ |
| 5 | 4 | 1 | 1 | 8 | -2 | -.89 | $-1 + 2\sqrt{-1}$ |
| 5 | 4 | 2 | 2 | 3 | 3 | 1.34 | $\frac{3+\sqrt{-11}}{2}$ |

| $p$ | $a$ | $b$ | $j$ | $N$ | $\mathrm{Sp}(\pi)$ | $\frac{\mathrm{Sp}(\pi)}{\sqrt{p}}$ | $\pi$ |
|---|---|---|---|---|---|---|---|
| 11 | 0 | 1 | 0 | 12 | 0 | 0.00 | $\sqrt{-11}$ |
| 11 | 1 | 1 | 9 | 14 | -2 | -.60 | $-1+\sqrt{-10}$ |
| 11 | 2 | 1 | 8 | 16 | -4 | -1.21 | $-2+\sqrt{-7}$ |
| 11 | 3 | 1 | 3 | 18 | -6 | -1.81 | $-3+\sqrt{-2}$ |
| 11 | 4 | 1 | 10 | 9 | 3 | .90 | $\frac{3+\sqrt{-35}}{2}$ |
| 11 | 5 | 1 | 6 | 11 | 1 | .30 | $\frac{1+\sqrt{-43}}{2}$ |
| 11 | 7 | 1 | 4 | 15 | -3 | -.90 | $\frac{-3+\sqrt{-35}}{2}$ |
| 11 | 8 | 1 | 5 | 17 | -5 | -1.51 | $\frac{-5+\sqrt{-19}}{2}$ |
| 11 | 9 | 1 | 2 | 8 | 4 | 1.21 | $2+\sqrt{-7}$ |
| 11 | 10 | 1 | 7 | 10 | 2 | .60 | $1+\sqrt{-10}$ |

| $p$ | $a$ | $b$ | $j$ | $N$ | $\mathrm{Sp}(\pi)$ | $\frac{\mathrm{Sp}(\pi)}{\sqrt{p}}$ | $\pi$ |
|---|---|---|---|---|---|---|---|
| 1021 | 101 | 1009 | 9 | 1080 | -58 | -1.82 | $-29+6\sqrt{-5}$ |
| 2039 | 101 | 1009 | 96 | 2088 | -48 | -1.06 | $-24+\sqrt{-1463}$ |
| 4093 | 101 | 1009 | 1297 | 4100 | -6 | -.09 | $-3+2\sqrt{-1021}$ |
| 8191 | 101 | 1009 | 117 | 8208 | -16 | -.18 | $-8+3\sqrt{-903}$ |
| 16381 | 101 | 1009 | 6234 | 16366 | 16 | .13 | $8+21\sqrt{-37}$ |
| 32749 | 101 | 1009 | 7928 | 32995 | -245 | -1.35 | $\frac{-245+\sqrt{-70971}}{2}$ |
| 65521 | 101 | 1009 | 29884 | 65891 | -369 | -1.44 | $\frac{-369+\sqrt{-125923}}{2}$ |
| 131071 | 101 | 1009 | 88083 | 131469 | -397 | -1.10 | $\frac{-397+5\sqrt{-14667}}{2}$ |
| 262139 | 101 | 1009 | 217154 | 262599 | -459 | -.90 | $\frac{-459+5\sqrt{-33515}}{2}$ |
| 524287 | 101 | 1009 | 423696 | 525392 | -1104 | -1.52 | $-552+\sqrt{-219583}$ |

| $p$ | $a$ | $b$ | $j$ | $N$ | $\mathrm{Sp}(\pi)$ | $\frac{\mathrm{Sp}(\pi)}{\sqrt{p}}$ | $\pi$ |
|---|---|---|---|---|---|---|---|
| 1048573 | 101 | 1009 | 937878 | 1046776 | 1798 | 1.76 | $899+6\sqrt{-6677}$ |
| 2097143 | 101 | 1009 | 342133 | 2099765 | -2621 | -1.81 | $\frac{-2621+\sqrt{-1518931}}{2}$ |
| 4194301 | 101 | 1009 | 1867125 | 4194200 | 102 | .05 | $51+10\sqrt{-41917}$ |
| 8388593 | 101 | 1009 | 4245114 | 8393292 | -4698 | -1.62 | $-2349+2\sqrt{-717698}$ |
| 16777213 | 101 | 1009 | 4502893 | 16781626 | -4412 | -1.08 | $-2206+\sqrt{-11910777}$ |
| 33554393 | 101 | 1009 | 5424899 | 33553640 | 754 | .13 | $377+2\sqrt{-8353066}$ |
| 67108859 | 101 | 1009 | 38285860 | 67097456 | 11404 | 1.39 | $5702+\sqrt{-34596055}$ |
| 134217689 | 101 | 1009 | 80252345 | 134211534 | 6156 | .53 | $3078+\sqrt{-124743605}$ |
| 268435399 | 101 | 1009 | 166242490 | 268452000 | -16600 | -1.01 | $-8300+3\sqrt{-22171711}$ |
| 536870909 | 101 | 1009 | 74485459 | 536843196 | 27714 | 1.20 | $13857+2\sqrt{-86213615}$ |

**Überlegung:** Sei $E$ über $\mathbf{F}_p$ definiert. Wir haben bereits bemerkt, dass für $\alpha \in \overline{\mathbf{F}_p}$ gilt

$$\alpha \in \mathbf{F}_{p^n} \quad \Longleftrightarrow \quad \alpha^{p^n} = \alpha.$$

Damit gilt auch für $P = (x, y) \in E(\overline{\mathbf{F}_p})$

$$P \in E(\mathbf{F}_{p^n}) \quad \Longleftrightarrow \quad x^{p^n} = x, y^{p^n} = y \quad \Longleftrightarrow \quad \pi^n(x, y) = (x^{p^n}, y^{p^n}) = (x, y) \quad \Longleftrightarrow \quad \pi^n(P) = P$$

und damit

$$E(\mathbf{F}_{p^n}) = \mathrm{Kern}(\pi^n - 1) \quad \text{und} \quad \#E(\mathbf{F}_{p^n}) = \#\mathrm{Kern}(\pi^n - 1).$$

Wie früher gilt $\#\mathrm{Kern}(\pi^n - 1) = \mathrm{N}(\pi^n - 1)$ und damit

$$\#E(\mathbf{F}_{p^n}) = \mathrm{N}(\pi^n - 1) = (\pi^n - 1)(\widehat{\pi}^n - 1) = p^n + 1 - (\pi^n + \widehat{\pi}^n) = p^n + 1 - \mathrm{Sp}(\pi^n).$$

Wir formulieren dies nochmals als Satz:

SATZ. *Für eine über $\mathbf{F}_p$ definierte elliptische Kurve $E$ gilt*

$$\#E(\mathbf{F}_{p^n}) = p^n + 1 - \mathrm{Sp}(\pi^n) = p^n + 1 - (\pi^n + \widehat{\pi}^n).$$

**Beispiel:** Durch $y^2 = x^3 + 11x + 101$ wird eine elliptische Kurve über $\mathbf{F}_p$ mit $p = 1009$ definiert. Man findet $N = \#E(\mathbf{F}_p) = 1002$ und damit für die Spur des Frobenius $s = (p+1) - N = (1009+1) - 1002 = 8$. Der Frobenius-Endomorphismus $\pi$ genügt also der Gleichung

$$\pi^2 - 8\pi + 1009 = 0.$$

Wir können dann schreiben

$$\pi = 4 + \sqrt{-993}$$

und erhalten damit folgende Tabelle:

| $n$ | $\pi^n$ | $\mathrm{Sp}(\pi^n)$ | $\#E(\mathbf{F}_{p^n})$ |
|---|---|---|---|
| 1 | $4 + \sqrt{-993}$ | 8 | 1002 |
| 2 | $-977 + 8\sqrt{-993}$ | -1954 | 1020036 |
| 3 | $-11852 - 945\sqrt{-993}$ | -23704 | 1027267434 |
| 4 | $890977 - 15632\sqrt{-993}$ | 1781954 | 1036487140608 |
| 5 | $19086484 + 828449\sqrt{-993}$ | 38172968 | 1045817284691082 |
| 6 | $-746303921 + 22400280\sqrt{-993}$ | -1492607842 | 1055229680262433284 |
| 7 | $-25228693724 - 656702801\sqrt{-993}$ | -50457387448 | 106472674592921125741 8 |
| 8 | $551191106497 - 27855504928\sqrt{-993}$ | 1102382212994 | 107430928659056027258572 8 |
| 9 | $29865280819492 + 439769086785\sqrt{-993}$ | 59730561638984 | 108397807017092788813027050 6 |
| 10 | $-317229579899537 + 31624357166632\sqrt{-993}$ | -634459159799074 | 109373387280252714171929647 3476 |

LEMMA. *Sei $E$ eine über $\mathbf{F}_p$ definierte elliptische Kurve mit Frobenius $\pi$ und $s_n = \mathrm{Sp}(\pi^n)$. Dann gilt für alle $n \geq 2$ (mit $s_0 = 2$)*

$$s_n = s_1 s_{n-1} - p s_{n-2}.$$

*Beweis:* Wir haben die Gleichungen

$$\begin{aligned} \pi s_{n-1} &= \pi(\pi^{n-1} + \widehat{\pi}^{n-1}) = \pi^n + \pi\widehat{\pi}\widehat{\pi}^{n-2} = \pi^n + p\widehat{\pi}^{n-2}, \\ \widehat{\pi} s_{n-1} &= \widehat{\pi}(\pi^{n-1} + \widehat{\pi}^{n-1}) = \widehat{\pi}^n + \pi\widehat{\pi}\pi^{n-2} = \widehat{\pi}^n + p\pi^{n-2}, \end{aligned}$$

was durch Addition zu

$$s_1 s_{n-1} = (\pi + \widehat{\pi}) s_{n-1} = (\pi^n + \widehat{\pi}^n) + p(\pi^{n-2} + \widehat{\pi}^{n-2}) = s_n + p s_{n-2}$$

führt. Dies beweist die Behauptung. ■

SATZ. *Für eine elliptische Kurve $E$ über $\mathbf{F}_p$ ($p \geq 5$) mit Frobenius $\pi$ sind folgende Aussagen äquivalent:*

(1) $E(\overline{\mathbf{F}_p})[p] = 0$.
(2) $\mathrm{Sp}(\pi) \equiv 0 \bmod p$.
(3) $\mathrm{Sp}(\pi) = 0$.
(4) $\#E(\mathbf{F}_p) = p + 1$.
(5) $\pi^2 = -p$. *($\pi = \pm\sqrt{-p}$.)*

*Beweis:*

$1 \Longrightarrow 2$**:** Aus $\mathrm{Sp}(\pi^n) = \mathrm{Sp}(\pi)\mathrm{Sp}(\pi^{n-1}) - p\mathrm{Sp}(\pi^{n-2})$ folgt durch Induktion $\mathrm{Sp}(\pi^n) \equiv \mathrm{Sp}(\pi)^n \bmod p$. Wäre $\mathrm{Sp}(\pi) \not\equiv 0 \bmod p$, so würde $\mathrm{Sp}(\pi^{p-1}) \equiv \mathrm{Sp}(\pi)^{p-1} \equiv 1 \bmod p$ und damit

$$\#E(\mathbf{F}_{p^{p-1}}) = p^{p-1} + 1 - \mathrm{Sp}(\pi^{p-1}) \equiv 1 - \mathrm{Sp}(\pi)^{p-1} \equiv 0 \bmod p$$

folgen, in $E(\mathbf{F}_{p^{p-1}})$ gäbe es also Elemente der Ordnung $p$, was der Voraussetzung $E(\overline{\mathbf{F}_p})[p] = 0$ widerspräche. Daher muss $\mathrm{Sp}(\pi) \equiv 0 \bmod p$ gelten.

$2 \Longrightarrow 3$**:** Aus $\mathrm{Sp}(\pi) \equiv 0 \bmod p$ folgt $\mathrm{Sp}(\pi) = tp$ für ein $t \in \mathbf{Z}$. Wegen $|\mathrm{Sp}(\pi)| < 2\sqrt{p}$ gilt dann $|t|p < 2\sqrt{p}$, also $t^2 p < 2$, was nur die Möglichkeit $t = 0$ und damit $\mathrm{Sp}(\pi) = 0$ übriglässt.

$3 \iff 4$**:** Dies folgt aus der Formel $\#E(\mathbf{F}_p) = p + 1 - \mathrm{Sp}(\pi)$.

$3 \iff 5$**:** Dies ist klar wegen $\pi^2 - \mathrm{Sp}(\pi)\pi + p = 0$.

$3 \Longrightarrow 1$**:** Ist $\mathrm{Sp}(\pi) \equiv 0 \bmod p$, so folgt wie zuvor $\mathrm{Sp}(\pi^n) \equiv 0 \bmod p$ und damit

$$\#E(\mathbf{F}_{p^n}) = p^n + 1 - \mathrm{Sp}(\pi^n) \equiv 1 \bmod p,$$

also

$$p \nmid \#E(\mathbf{F}_{p^n}),$$

d.h. $E(\mathbf{F}_{p^n})$ enthält für kein $n$ ein Element der Ordnung $p$. Wegen

$$E(\overline{\mathbf{F}_p}) = \cup_{n \geq 1} E(\mathbf{F}_{p^n})$$

folgt daraus $E(\overline{\mathbf{F}_p})[p] = 0$. ■

Ist $\pi$ der Frobenius-Endomorphismus einer über $\mathbf{F}_p$ definierten elliptischen Kurve $E$, so gilt $\pi^2 = -p$, was sofort

$$\mathrm{End}_K(E) \neq \mathbf{Z}$$

zeigt. Der folgende Satz, den wir nicht beweisen werden, charakterisiert die beiden verbleibenden Möglichkeiten:

SATZ. *Für eine über $\mathbf{F}_p$ definierte elliptische Kurve $E$ gilt:*

$$E \text{ ist supersingulär, d.h. } \mathrm{End}(E) \text{ ist nicht kommutativ} \iff E(\overline{\mathbf{F}_p})[p] = 0 \iff \#E(\mathbf{F}_p) = p + 1.$$

Wir erwähnen noch eine weitere Eigenschaft supersingulärer Kurven:

SATZ. *Für eine über $\mathbf{F}_p$ definierte supersinguläre elliptische Kurve $E$ gilt:*

$$E(\mathbf{F}_p) \subseteq E(\overline{\mathbf{F}_p})[p+1] = E(\mathbf{F}_{p^2}).$$

*Beweis:* Da $E$ supersingulär ist, gilt $\#E(\mathbf{F}_p) = p + 1$ und damit $(p+1) \cdot E(\mathbf{F}_p) = \{O\}$, was die erste Inklusion beweist. Der Frobenius-Endomorphismus $\pi$ genügt der Gleichung $\pi^2 + p = 0$, womit man für $P \in E(\overline{\mathbf{F}_p})$ erhält

$$P \in E(\mathbf{F}_{p^2}) \iff \pi^2 P = P \iff -pP = P \iff (p+1)P = O \iff P \in E(\overline{\mathbf{F}_p})[p+1].$$

Dies liefert $E(\mathbf{F}_{p^2}) = E(\overline{\mathbf{F}_p})[p+1]$. ■

## 5. Bestimmung von $\#E(\mathbf{F}_p)$ für elliptische Kurven mit $j(E) = 1728$

Eine elliptische Kurve $E$ über $\mathbf{F}_p$, $p \geq 5$, mit $j(E) = 1728$ wird durch eine Gleichung $y^2 = x^3 + ax$ mit $a \in \mathbf{F}_p^*$ beschrieben. Sei $i \in \mathbf{F}_{p^2}$ mit $i^2 = -1$. Wir haben zwei (nichttriviale) Endomorphismen $\pi$ und $\phi$:

$$\pi(x, y) = (x^p, y^p) \quad \text{und} \quad \phi(x, y) = (-x, iy),$$

wobei die Gleichungen

$$\pi^2 - s\pi + p = 0 \quad \text{und} \quad \phi^2 = -1$$

erfüllt sind. Wir unterscheiden zwei Fälle:

**Der Fall $p \equiv 3 \bmod 4$:** Dann gilt (wegen $i^4 = 1$) mit $i^p = i^3 = -i$:

$$\pi\phi(x, y) = \pi(-x, iy) = (-x^p, i^p y^p) = (-x^p, -iy^p) = -(-x^p, iy^p) = -\phi(x^p, y^p) = -\phi\pi(x, y),$$

also $\pi\phi = -\phi\pi$, d.h. $\mathrm{End}(E)$ ist nicht kommutativ, damit $E$ supersingulär und nach einem oben zitierten Satz

$$\#E(\mathbf{F}_p) = p + 1.$$

**Der Fall $p \equiv 1 \bmod 4$:** Wegen $i^p = i$ sieht man in diesem Fall mit analoger Rechnung wie oben

$$\pi\phi = \phi\pi.$$

Man kann sich dann überlegen, dass es $m, n \in \mathbf{Z}$ gibt mit $\pi = m + n\phi$. Es folgt:

$$\begin{aligned} 0 &= \pi^2 - s\pi + p = (m + n\phi)^2 - s(m + n\phi) + p = \\ &= (m^2 + 2mn\phi + n^2\phi^2) - (sm + sn\phi) + p = \\ &= (m^2 + 2mn\phi - n^2) - (sm + sn\phi) + p = \\ &= (m^2 - n^2 - sm + p) + n(2m - s)\phi. \end{aligned}$$

Wegen $\phi, \pi \notin \mathbf{Z}$ erhält man durch Koeffizientenvergleich $s = 2m$ und dann $p = m^2 + n^2$. Somit ist

$$\#E(\mathbf{F}_p) = p + 1 - 2m.$$

Da $m \neq 0$ gilt, ist $E$ nicht supersingulär. Nun weiß man, dass zu jeder Primzahl $p \equiv 1 \bmod 4$ ganze Zahlen $m, n$ existieren mit $p = m^2 + n^2$. Die Darstellung ist eindeutig bis auf Vertauschung von $m$ und $n$ und Vorzeichen. Damit erhalten wir folgenden Satz:

Satz. *Sei $E : y^2 = x^3 + ax$ eine elliptische Kurve über $\mathbf{F}_p$.*

(1) *Ist $p \equiv 3 \bmod 4$, so gilt $\#E(\mathbf{F}_p) = p + 1$.*
(2) *Ist $p \equiv 1 \bmod 4$, so gibt es $m, n \in \mathbf{N}$ mit $p = m^2 + n^2$. Dann ist*

$$\#E(\mathbf{F}_p) \in \{p + 1 - 2m, p + 1 + 2m, p + 1 - 2n, p + 1 + 2n\}.$$

Will man den Satz praktisch anwenden im Fall $p \equiv 1 \bmod 4$, muss man die Gleichung $p = m^2 + n^2$ lösen. Dies ist schnell möglich mit Hilfe des sogenannten Cornacchia-Algorithmus (H. Cohen, A Course in Computational Algebraic Number Theory, Algorithm 1.5.2).

**Cornacchia-Algorithmus:** Sei $d \in \mathbf{N}$ und $p$ eine Primzahl mit $p > d$. Bestimmt werden $x, y \in \mathbf{Z}$ mit $p = x^2 + dy^2$, oder gesagt, dass die Gleichung nicht lösbar ist.

(1) Berechne das Legendre-Symbol $\left(\frac{-d}{p}\right)$. Ist $\left(\frac{-d}{p}\right) = -1$, so hat die Gleichung keine Lösung und man ist fertig.
(2) Bestimme mit dem Quadratwurzelalgorithmus ein $x_0 \in \mathbf{Z}$ mit $x_0^2 \equiv -d \bmod p$ und $0 < x_0 < p$. Ist $x_0 < \frac{1}{2}p$, setze $x_0 := p - x_0$. Setze $a := p$, $b := x_0$, $l = \lfloor \sqrt{p} \rfloor$.
(3) Ist $b > l$, setze $r := a \bmod b$, $a := b$, $b := r$ und gehe zu 3.
(4) Ist $(p - b^2) \bmod d \neq 0$ oder ist $c = \frac{p - b^2}{d}$ kein Quadrat, so hat die Gleichung $x^2 + dy^2 = p$ keine Lösung in ganzen Zahlen. Im andern Fall ist $(x, y) = (b, \sqrt{c})$ eine Lösung.

Es ist klar, dass der Algorithmus sehr schnell ist, da nur schnelle Algorithmen verwendet werden: im 1. Schritt eine Legendre-Symbol-Berechnung, im 2. Schritt eine Quadratwurzelberechnung modulo $p$, im 3. Schritt Divisionen mit Rest.

Damit erhalten wir folgendes Verfahren:

**Verfahren zur Bestimmung von $\#E(\mathbf{F}_p)$ für $y^2 = x^3 + ax$:**

(1) Ist $p \equiv 3 \bmod 4$, so gilt $\#E(\mathbf{F}_p) = p + 1$ und man ist fertig.
(2) Ist $p \equiv 1 \bmod 4$, bestimmt man mit dem Cornacchia-Algorithmus ($d = 1$) Zahlen $m, n \in \mathbf{N}$ mit $p = m^2 + n^2$. Setze

$$M = \{p + 1 - 2m, p + 1 + 2m, p + 1 - 2n, p + 1 + 2n\}.$$

Dann ist $\#E(\mathbf{F}_p) \in M$.
(a) Wähle $P \in E(\mathbf{F}_p)$.
(b) Berechne für alle $\widetilde{N} \in M$ den Punkt $\widetilde{N} \cdot P$. Gilt $\widetilde{N} \cdot P \neq O$, streiche $\widetilde{N}$ aus $M$ heraus, da in diesem Fall sicher $\widetilde{N} \neq \#E(\mathbf{F}_p)$ gilt
(c) Enthält $M$ mehr als ein Element, gehe zurück zu a.
(d) Enthält $M$ genau ein Element, so ist dies $N = \#E(\mathbf{F}_p)$.

**Beispiele:** Wir haben jeweils eine Primzahl $p \equiv 1 \bmod 4$ gewählt, dazu $a = 1, \ldots, 10$ und dafür $\#E(\mathbf{F}_p)$ mit obigem Verfahren bestimmt. 'Testpunkte' meint der Anzahl der Punkte, die gebraucht wurden, bis $N$ eindeutig bestimmt war.

$p = 2^{128} - 159$ (Gesamtzeit: 5.35 sec)

| $a$ | Testpunkte | Sp($\pi$) |
|---|---|---|
| 1 | 2 | -13861985124986332638 |
| 2 | 1 | -13861985124986332638 |
| 3 | 1 | 13861985124986332638 |
| 4 | 2 | -13861985124986332638 |
| 5 | 1 | -34190273998293893488 |
| 6 | 1 | 13861985124986332638 |
| 7 | 1 | -34190273998293893488 |
| 8 | 1 | -13861985124986332638 |
| 9 | 2 | -13861985124986332638 |
| 10 | 1 | -34190273998293893488 |

$p = 2^{128} - 275$ (Gesamtzeit: 5.82 sec)

| $a$ | Testpunkte | Sp($\pi$) |
|---|---|---|
| 1 | 1 | 28948405524762753818 |
| 2 | 1 | 22871801093434664740 |
| 3 | 1 | -22871801093434664740 |
| 4 | 1 | -28948405524762753818 |
| 5 | 1 | 28948405524762753818 |
| 6 | 1 | 28948405524762753818 |
| 7 | 1 | 28948405524762753818 |
| 8 | 1 | -22871801093434664740 |
| 9 | 1 | -28948405524762753818 |
| 10 | 1 | 22871801093434664740 |

$p = 2^{512} - 875$ (Gesamtzeit: 156.05 sec)

| $a$ | Testpunkte | Sp($\pi$) |
|---|---|---|
| 1 | 1 | -20503249850504491326845755299584943659985123494892501014291042230587313120727 8 |
| 2 | 1 | -10767035932209543714918732437188541049102101423884336528519746096338795520694 0 |
| 3 | 1 | -10767035932209543714918732437188541049102101423884336528519746096338795520694 0 |
| 4 | 1 | 20503249850504491326845755299584943659985123494892501014291042230587313120727 8 |
| 5 | 1 | -20503249850504491326845755299584943659985123494892501014291042230587313120727 8 |
| 6 | 1 | 20503249850504491326845755299584943659985123494892501014291042230587313120727 8 |
| 7 | 1 | -20503249850504491326845755299584943659985123494892501014291042230587313120727 8 |
| 8 | 1 | 10767035932209543714918732437188541049102101423884336528519746096338795520694 0 |
| 9 | 1 | 20503249850504491326845755299584943659985123494892501014291042230587313120727 8 |
| 10 | 1 | -10767035932209543714918732437188541049102101423884336528519746096338795520694 0 |

$p = 2^{1024} - 179$ (Gesamtzeit: 812.18 sec)

| $a$ | Testpunkte | Sp($\pi$) (unvollständig aufgeschrieben) |
|---|---|---|
| 1 | 1 | -20761263342439561330856243289262138264514755179995216668291 19 ... |
| 2 | 1 | -16971953286843611184833550683580005691935602457029760074040 73 ... |
| 3 | 1 | 16971953286843611184833550683580005691935602457029760074040 736 ... |
| 4 | 2 | 20761263342439561330856243289262138264514755179995216668291 195 ... |
| 5 | 1 | -16971953286843611184833550683580005691935602457029760074040 73 ... |
| 6 | 1 | -20761263342439561330856243289262138264514755179995216668291 19 ... |
| 7 | 1 | -16971953286843611184833550683580005691935602457029760074040 73 ... |
| 8 | 1 | 16971953286843611184833550683580005691935602457029760074040 736 ... |
| 9 | 1 | 20761263342439561330856243289262138264514755179995216668291 195 ... |
| 10 | 1 | 20761263342439561330856243289262138264514755179995216668291 19 ... |

Wir wollen jetzt noch zeigen, dass für $p = m^2 + n^2$ tatsächlich alle vier Zahlen

$$p + 1 - 2m, \quad p + 1 + 2m, \quad p + 1 - 2n, \quad p + 1 + 2n$$

als Punktezahl $\#E(\mathbf{F}_p)$ einer elliptischen Kurve $y^2 = x^3 + ax$ auftritt. Wir beginnen mit folgendem Satz:

SATZ. *Sei $p \equiv 1 \bmod 4$, $i \in \mathbf{F}_p^*$ mit $i^2 = -1$ und $\zeta \in \mathbf{F}_p^*$ mit $\left(\frac{\zeta}{p}\right) = -1$.*

(1) *Die Zahlen $1, \zeta, \zeta^2, \zeta^3$ bilden ein Repräsentantensystem der Faktorgruppe $\mathbf{F}_p^*/\mathbf{F}_p^{*4}$. Daher liefern die vier Kurven $E_j$, $j = 0, 1, 2, 3$ mit der Gleichung $y^2 = x^3 + \zeta^j x$ ein Repräsentantensystem aller elliptischen Kurven über $\mathbf{F}_p$ mit der $j$-Invariante 1728 (bis auf Isomorphie).*

(2) *Für die Spur des Frobenius $\mathrm{Sp}\pi_j$ von $E_j$ gilt:*

$$\mathrm{Sp}\pi_0 \equiv 2 \bmod 8, \quad \mathrm{Sp}\pi_1 \equiv 0 \bmod 4, \quad \mathrm{Sp}\pi_2 \equiv 6 \bmod 8, \quad \mathrm{Sp}\pi_3 \equiv 0 \bmod 4$$

*und*

$$\mathrm{Sp}\pi_2 = -\mathrm{Sp}\pi_0, \quad \mathrm{Sp}\pi_3 = -\mathrm{Sp}\pi_1.$$

(3) *Für die Anzahl der $\mathbf{F}_p$-rationalen Punkte von $E_j$ gilt:*

$$\#E_0(\mathbf{F}_p) \equiv \begin{cases} 0 \bmod 8 & \text{für } p \equiv 1 \bmod 8, \\ 4 \bmod 8 & \text{für } p \equiv 5 \bmod 8 \end{cases}, \qquad \#E_2(\mathbf{F}_p) \equiv \begin{cases} 4 \bmod 8 & \text{für } p \equiv 1 \bmod 8, \\ 0 \bmod 8 & \text{für } p \equiv 5 \bmod 8 \end{cases}$$

$$\#E_1(\mathbf{F}_p) \equiv \#E_3(\mathbf{F}_p) \equiv 2 \bmod 4.$$

*Beweis:*

(1) Sei $p - 1 = 2^e u$ mit ungeradem $u$ und $e \geq 2$. Dann ist

$$\mathbf{F}_p^* \simeq \mathbf{Z}/2^e\mathbf{Z} \oplus \mathbf{Z}/u\mathbf{Z} \quad \text{und} \quad \mathbf{F}_p^{*4} \simeq 4\mathbf{Z}/2^e\mathbf{Z} \oplus \mathbf{Z}/u\mathbf{Z},$$

was sofort $\mathbf{F}_p^*/\mathbf{F}_p^{*4} \simeq \mathbf{Z}/4\mathbf{Z}$ impliziert. Sei $\gamma$ ein Erzeuger der Gruppe $\mathbf{F}_p^*$. Dann gibt es ein $z$ mit $0 \leq z \leq p - 2$ mit $\zeta = \gamma^z$. Wegen $\left(\frac{\zeta}{p}\right) = -1$ gilt $z \equiv 1 \bmod 2$. Für $x, y \in \mathbf{Z}$ folgt

$$\begin{aligned} \zeta^x \equiv \zeta^y \bmod \mathbf{F}_p^{*4} &\iff \zeta^{x-y} = \gamma^{4u} \text{ für ein } u \in \mathbf{Z} \\ &\iff \gamma^{(x-y)z} = \gamma^{4u} \text{ für ein } u \in \mathbf{Z} \\ &\iff (x - y)z \equiv 4u \bmod p - 1 \text{ für ein } u \in \mathbf{Z} \\ &\iff (x - y)z \equiv 0 \bmod 4, \text{ (nun ist } z \equiv 1 \bmod 2) \\ &\iff x \equiv y \bmod 4. \end{aligned}$$

Also repräsentieren die Zahlen $1, \zeta, \zeta^2, \zeta^3$ die Faktorgruppe $\mathbf{F}_p^*/\mathbf{F}_p^{*4}$. Der Rest folgt dann mit der Klassifikation elliptischer Kurven des Typs $y^2 = x^3 + ax$.

(2) Wir erinnern an die Formeln für die Multiplikation mit 2 auf einer elliptischen Kurve mit der Gleichung $y^2 = x^3 + ax + b$:

$$2 \cdot (x, y) = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{(2y)^2}, \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{(2y)^3}\right).$$

Für $a = \zeta^j$ und $b = 0$ ergibt dies

$$2 \cdot (x, y) = \left(\frac{(x^2 - \zeta^j)^2}{(2y)^2}, \frac{(x^2 - \zeta^j)(x^4 + 6\zeta^j x^2 + \zeta^{2j})}{(2y)^3}\right).$$

(3) Wir betrachten $E_1$ und $E_3$, also die Kurven $y^2 = x^3 + \zeta^j x$ mit $j \equiv 1 \bmod 2$. Wegen

$$x^3 + \zeta^j x = x(x^2 + \zeta^j) = x(x^2 - \zeta^j i^2)$$

und $\left(\frac{\zeta^j}{p}\right) = 1$ gilt

$$E_j(\mathbf{F}_p)[2] = \{O, (0, 0)\},$$

was insbesondere $\#E_j(\mathbf{F}_p) \equiv 0 \bmod 2$ impliziert. Wir nehmen jetzt an, es wäre $\#E_j(\mathbf{F}_p) \equiv 0 \bmod 4$. Dann gäbe es einen Punkt $P = (x, y) \in E_j(\mathbf{F}_p)$ mit $\operatorname{ord}(P) = 4$. Dies implizierte $2 \cdot P = (0, 0)$ und mit den vorangegangenen Formeln

$$(0,0) = 2 \cdot (x,y) = (\frac{(x^2-\zeta^j)^2}{(2y)^2}, \frac{(x^2-\zeta^j)(x^4+6\zeta^j x^2+\zeta^{2j})}{(2y)^3}),$$

also $x^2 = \zeta^j$, was $\left(\frac{\zeta^j}{p}\right) = -1$ widerspricht. Daher muss $\#E_j(\mathbf{F}_p) \equiv 2 \bmod 4$ gelten. Für die Spur des Frobenius impliziert dies

$$\operatorname{Sp}\pi_j = p + 1 - \#E_j(\mathbf{F}_p) \equiv 1 + 1 - 2 \equiv 0 \bmod 4.$$

(4) Wir betrachten jetzt die Kurve $E_2$. Wegen

$$x^3 + \zeta^2 x = x^3 - \zeta^2 i^2 x = x(x - \zeta i)(x + \zeta i) = x(x - \zeta i)(x - \zeta i^3)$$

gilt

$$E_2(\mathbf{F}_p)[2] = \{O, (0,0), (\zeta i, 0), (\zeta i^3, 0)\}.$$

Wir nehmen an, es gibt einen Punkt $P = (x, y) \in E_2(\mathbf{F}_p)$ mit $\operatorname{ord} P = 4$. Dann hat $2P$ Ordnung 2, d.h. $2P \in \{(0,0), (\zeta i, 0), (\zeta i^3, 0)\}$. Da aber die $x$-Koordinate von $2P$ nach obiger Formel ein Quadrat in $\mathbf{F}_p$ ist, bleibt nur der Fall $2P = (0, 0)$. Die Verdoppelungsformel liefert

$$(0,0) = (\frac{(x^2-\zeta^2)^2}{(2y)^2}, \frac{(x^2-\zeta^2)(x^4+6\zeta^2 x^2+\zeta^4)}{(2y)^3}),$$

was nur durch $x = \pm\zeta$ erfüllt wird. Wegen $P = (x, y) \in E_2(\mathbf{F}_p)$ muss gelten

$$y^2 = x^3 + \zeta^2 x = x(x^2 + \zeta^2) = x \cdot 2\zeta^2 = \pm 2 \cdot \zeta^3.$$

Wir unterscheiden jetzt zwei Fälle:

(a) Ist $p \equiv 1 \bmod 8$, so ist 2 ein Quadrat in $\mathbf{F}_p$, also $\pm 2\zeta^3$ kein Quadrat in $\mathbf{F}_p$, d.h. es gibt keinen Punkt $P$ mit obigen Eigenschaften, was sofort

$$E_2(\mathbf{F}_p)[4] = E_2(\mathbf{F}_p)[2]$$

und damit

$$\#E_2(\mathbf{F}_p) \equiv 4 \bmod 8$$

liefert. Für die Spur des Frobenius ergibt dies

$$\operatorname{Sp}(\pi_2) = p + 1 - \#E_2(\mathbf{F}_p) \equiv 1 + 1 - 4 \equiv 6 \bmod 8.$$

(b) Ist $p \equiv 5 \bmod 8$, so ist 2 kein Quadrat in $\mathbf{F}_p$, also $\left(\frac{2\zeta}{p}\right) = 1$. Daher ist die Gleichung $y^2 = \pm 2 \cdot \zeta^3$ in $\mathbf{F}_p$ lösbar, es gibt also einen Punkt $P = (x, y) \in E_2(\mathbf{F}_p)[4]$ mit $\operatorname{ord} P = 4$. Dies zeigt $E_2(\mathbf{F}_p)[4] \neq E_2(\mathbf{F}_p)[2]$, was sofort

$$\#E_2(\mathbf{F}_p) \equiv 0 \bmod 8 \quad \text{und} \quad \operatorname{Sp}\pi_2 = p + 1 - \#E_2(\mathbf{F}_p) \equiv 6 - 0 \equiv 6 \bmod 8$$

impliziert.

(5) Wir betrachten die Kurve $E_0$. Aus

$$x^3 + x = x(x^2 + 1) = x(x - i)(x - i^3)$$

folgt

$$E_0(\mathbf{F}_p)[2] = \{O, (0,0), (i,0), (i^3, 0)\}.$$

Wir nennen die Multiplikation mit 2 kurz $\alpha$, also

$$\alpha((x,y)) = 2(x,y) = ((\frac{x^2-1}{2y})^2, \frac{(x^2-1)(x^4+6x^2+1)}{(2y)^3}),$$

und haben dann

$$\alpha^{-1}((0,0)) = \{(1, \pm\sqrt{2}), (-1, \pm i\sqrt{2})\}.$$

Wir unterscheiden zwei Fälle:

(a) Ist $p \equiv 5 \bmod 8$, so ist $i$ kein Quadrat in $\mathbf{F}_p$, also $(\pm i, 0) \neq 2P$ für alle $P \in E_0(\mathbf{F}_p)$. Wegen $p \equiv 5 \bmod 8$ ist $\sqrt{2} \notin \mathbf{F}_p$, also $(0,0) \neq 2P$ für alle $P \in E_0(\mathbf{F}_p)$. Damit folgt $E_0(\mathbf{F}_p)[4] = E_0(\mathbf{F}_p)[2]$, also

$$\#E_0(\mathbf{F}_p) \equiv 4 \bmod 8 \quad \text{und} \quad \mathrm{Sp}\pi_0 \equiv 2 \bmod 8.$$

(b) Ist $p \equiv 1 \bmod 8$, so sind $(1, \pm\sqrt{2}), (-1, \pm i\sqrt{2}) \in E_0(\mathbf{F}_p)$, also folgt

$$\#E_0(\mathbf{F}_p) \equiv 0 \bmod 8 \quad \text{und} \quad \mathrm{Sp}_0\pi \equiv 2 \bmod 8.$$

(6) Wir haben

$$\begin{aligned}
\mathrm{Sp}(\pi_j) &= -\sum_x \left(\frac{x^3 + \zeta^j x}{p}\right) = -\sum_x \left(\frac{(\zeta x)^3 + \zeta^j(\zeta x)}{p}\right) = \\
&= -\sum_x \left(\frac{\zeta^3 x^3 + \zeta^{j+1} x}{p}\right) = -\sum_x \left(\frac{\zeta^3(x^3 + \zeta^{j-2} x)}{p}\right) = \\
&= -\sum_x \left(\frac{\zeta}{p}\right)^3 \left(\frac{x^3 + \zeta^{j-2} x}{p}\right) = \sum_x \left(\frac{x^3 + \zeta^{j-2} x}{p}\right) = -\mathrm{Sp}(\pi_{j-2}),
\end{aligned}$$

was $\mathrm{Sp}(\pi_2) = -\mathrm{Sp}(\pi_0)$ und $\mathrm{Sp}(\pi_3) = -\mathrm{Sp}(\pi_1)$ beweist. ■

**Bemerkung:** Ist $p \equiv 1 \bmod 4$, sind $m, n \in \mathbf{Z}$ mit $p = m^2 + n^2$, so kann man nach eventueller Vertauschung von $m$ und $n$ o.E. $m \equiv 1 \bmod 2$, $n \equiv 0 \bmod 2$ annehmen. Vertauscht man eventuell $m$ mit $-m$, so kann man weiter $m \equiv 1 \bmod 4$ annehmen. Wir übernehmen die Bezeichnungen des letzten Satzes. Früher haben wir bereits gesehen, dass gilt

$$\#E_j(\mathbf{F}_p) \in \{p+1-2m, p+1+2m, p+1-2n, p+1+2n\}, \quad \text{also} \quad \mathrm{Sp}(\pi_j) \in \{2m, -2m, 2n, -2n\}.$$

Die Kongruenzen des letzten Satzes implizieren dann wegen $2m \equiv 2 \bmod 8$, $-2m \equiv 6 \bmod 8$, $2n \equiv 0 \bmod 4$

$$\mathrm{Sp}\pi_0 = 2m, \quad \mathrm{Sp}\pi_2 = -2m, \quad \mathrm{Sp}\pi_1 = \pm n, \quad \mathrm{Sp}\pi_3 = -\mathrm{Sp}\pi_1.$$

Dies zeigt insbesondere, dass tatsächlich alle Zahlen aus

$$\{p+1-2m, p+1+2m, p+1-2n, p+1+2n\}$$

als $\#E(\mathbf{F}_p)$ einer elliptischen Kurve mit der Gleichung $y^2 = x^3 + ax$ auftreten. Wir formulieren dies nochmals als Satz:

Satz. *Sei $p \equiv 1 \bmod 4$ eine Primzahl, $p \geq 5$, und seien $m, n$ ganze Zahlen mit $p = m^2 + n^2$. Dann gibt es $a_1, a_2, a_3, a_4 \in \mathbf{F}_p^*$ mit*

$$\#E_{a_1,0}(\mathbf{F}_p) = p+1-2m, \quad \#E_{a_2,0}(\mathbf{F}_p) = p+1+2m, \quad \#E_{a_3,0}(\mathbf{F}_p) = p+1-2n, \quad \#E_{a_4,0}(\mathbf{F}_p) = p+1+2n.$$

*Dabei sind $a_1, a_2, a_3, a_4$ Repräsentanten von $\mathbf{F}_p^*/\mathbf{F}_p^{*4}$.*

## 6. Bestimmung von $\#E(\mathbf{F}_p)$ für elliptische Kurven mit $j(E) = 0$

Eine elliptische Kurve $E$, die über $\mathbf{F}_p$ mit $p \geq 5$ definiert ist, und $j$-Invariante 0 besitzt, wird durch eine Gleichung $y^2 = x^3 + b$ mit $b \in \mathbf{F}_p^*$ beschrieben. Sei $\rho \in \mathbf{F}_p^*$ mit $\rho^2 + \rho + 1 = 0$. Dann ist $\rho$ eine primitive 3-te Einheitswurzel, d.h. es gilt $\rho^3 = 1$, $\rho \neq 1$. Nun hat man:

$$(x,y) \in E(\overline{\mathbf{F}_p}) \quad \Longrightarrow \quad y^2 = x^3 + b \quad \Longrightarrow \quad y^2 = (\rho x)^3 + b \quad \Longrightarrow \quad (\rho x, y \in E(\overline{\mathbf{F}_p}).$$

Daher definiert

$$\varphi : E(\overline{\mathbf{F}_p}) \to E(\overline{\mathbf{F}_p}), \quad (x,y) \mapsto (\rho x, y)$$

einen Endomorphismus von $E$. Man sieht leicht, dass $\phi^3 = 1$ gilt. Da $\phi \neq 1$ ist, folgt aus der Nullteilerfreiheit von $\mathrm{End}(E)$, dass $\phi^2 + \phi + 1 = 0$ ist. Bezeichnet $\pi$ den Frobenius-Endomorphismus $(x,y) \mapsto (x^p, y^p)$, so gilt

$$\begin{aligned}
\phi\pi(x,y) &= \phi(x^p, y^p) = (\rho x^p, y^p), \\
\pi\phi(x,y) &= \pi(\rho x, y) = (\rho^p x^p, y^p).
\end{aligned}$$

Wir unterscheiden jetzt zwei Fälle:

**Der Fall** $p \equiv 2 \bmod 3$**:** Hier ist $\rho^p = \rho^2 \neq \rho$, also $\pi\phi \neq \phi\pi$, der Endomorphismenring $\mathrm{End}(E)$ ist nichtkommutativ, $E$ also supersingulär und damit $\#E(\mathbf{F}_p) = p+1$.

**Der Fall** $p \equiv 1 \bmod 3$**:** Hier ist $\rho^p = \rho$ und somit $\phi\pi = \pi\phi$. Mit der Identifikation $\mathbf{Z}[\phi] \simeq \mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$ kann man jetzt sehen, dass $\pi \in \mathbf{Z}[\phi] \simeq \mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$ gilt, d.h. es gibt $m, n \in \mathbf{Z}$ mit

$$\pi = \frac{m + n\sqrt{-3}}{2}.$$

Dann ist

$$p = \pi\widehat{\pi} = \frac{m^2 + 3n^2}{4} \quad \text{und} \quad \mathrm{Sp}(\pi) = m, \quad \text{also} \quad N = \#E(\mathbf{F}_p) = (p+1) - \mathrm{Sp}(\pi) = p + 1 - m.$$

Umgekehrt kann man zu $p \equiv 1 \bmod 3$ ganze Zahlen $m, n$ finden mit $p = \frac{m^2+3n^2}{4}$. Allerdings ist $\pi$ dann nur bis auf Einheiten und Konjugation bestimmt, d.h. mit $\zeta = \frac{-1+\sqrt{-3}}{2}$

$$\pi \text{ oder } \widehat{\pi} = \begin{cases} \frac{m+n\sqrt{-3}}{2}, \\ -\frac{m+n\sqrt{-3}}{2}, \\ \zeta\frac{m+n\sqrt{-3}}{2} = \frac{(-m-3n)/2+(m-n)/2\sqrt{-3}}{2}, \\ -\zeta\frac{m+n\sqrt{-3}}{2} = \frac{(m+3n)/2+(-m+n)/2\sqrt{-3}}{2}, \\ \zeta^2\frac{m+n\sqrt{-3}}{2} = \frac{(-m+3n)/2+(-m-n)/2\sqrt{-3}}{2}, \\ -\zeta^2\frac{m+n\sqrt{-3}}{2} = \frac{(m-3n)/2+(m+n)/2\sqrt{-3}}{2} \end{cases}$$

und damit

$$\mathrm{Sp}(\pi) \in \{m, -m, \frac{-m-3n}{2}, \frac{m+3n}{2}, \frac{-m+3n}{2}, \frac{m-3n}{2}\}.$$

Damit erhalten wir folgenden Satz:

Satz. *Es definiere $y^2 = x^3 + b$ eine elliptische Kurve $E$ über $\mathbf{F}_p$.*

(1) *Ist $p \equiv 2 \bmod 3$, so ist $E$ supersingulär und $\#E(\mathbf{F}_p) = p+1$.*
(2) *Ist $p \equiv 1 \bmod 3$, so gibt es $m, n \in \mathbf{Z}$ mit $p = \frac{m^2+3n^2}{4}$. Dann ist*

$$\begin{aligned} \#E(\mathbf{F}_p) \quad \in \{ \quad & p+1-m, p+1+m, \\ & p+1-\frac{-m-3n}{2}, p+1-\frac{m+3n}{2}, p+1-\frac{-m+3n}{2}, p+1-\frac{m-3n}{2}\}. \end{aligned}$$

Um den letzten Satz anwenden zu können, ist folgende Variante des Cornacchia-Algorithmus nützlich:

**2. Cornacchia-Algorithmus:** Gegeben ist eine Primzahl $p$ und eine ganze Zahl $D$ mit $D < 0$, $D \equiv 0$ oder $1 \bmod 4$ und $\mathrm{ggT}(p, D) = 1$. Bestimmt werden $x, y \in \mathbf{Z}$ mit

$$p = \frac{x + y\sqrt{D}}{2} \cdot \frac{x - y\sqrt{D}}{2} = \frac{x^2 - Dy^2}{4},$$

oder gesagt, dass die Gleichung nicht lösbar ist.

(1) Berechne das Legendre-Symbol $\left(\frac{D}{p}\right)$. Ist $\left(\frac{D}{p}\right) = -1$, so hat die Gleichung keine Lösung und man ist fertig.
(2) Bestimme mit dem Quadratwurzelalgorithmus ein $x \in \mathbf{Z}$ mit $x^2 \equiv D \bmod p$ und $0 < x < p$. Ist $x \not\equiv D \bmod 2$, setze $x := x + p$. Setze $l = \lfloor\sqrt{4p}\rfloor$, $x_0 := 2p$, $x_1 = x$.
(3) Ist $x_1 > l$, setze $x_2 := x_0 \bmod x_1$, $x_0 := x_1$, $x_1 := x_2$ und gehe zu 3.
(4) Ist $x_1^2 \not\equiv 4p \bmod D$ oder ist $q = \frac{x_1^2-4p}{D}$ kein Quadrat, so hat die Gleichung $x^2 - Dy^2 = 4p$ keine Lösung in ganzen Zahlen. Im andern Fall ist $(x, y) = (x_1, \sqrt{q})$ eine Lösung.

Damit kann man folgendes Verfahren durchführen:

**Verfahren zur Bestimmung von $\#E(\mathbf{F}_p)$ für elliptische Kurven der Gestalt $y^2 = x^3 + b$:**

(1) Ist $p \equiv 2 \bmod 3$, so gilt $\#E(\mathbf{F}_p) = p+1$ und man ist fertig.

(2) Ist $p \equiv 1 \bmod 3$, bestimmt man mit dem 2. Cornacchia-Algorithmus ($D = -3$) Zahlen $m, n \in \mathbf{N}$ mit $4p = m^2 + 3n^2$ und setzt

$$M = \{ \quad p+1-m, p+1+m, \\ p+1-\frac{-m-3n}{2}, p+1-\frac{m+3n}{2}, p+1-\frac{-m+3n}{2}, p+1-\frac{m-3n}{2}\}.$$

Dann ist $\#E(\mathbf{F}_p) \in M$.

(a) Wähle $P \in E(\mathbf{F}_p)$.
(b) Berechne für alle $\widetilde{N} \in M$ den Punkt $\widetilde{N} \cdot P$. Gilt $\widetilde{N} \cdot P \neq O$, streiche $\widetilde{N}$ aus $M$ heraus, da in diesem Fall sicher $\widetilde{N} \neq \#E(\mathbf{F}_p)$ gilt
(c) Enthält $M$ mehr als ein Element, gehe zurück zu a.
(d) Enthält $M$ genau ein Element, so ist dies $N = \#E(\mathbf{F}_p)$.

**Beispiel:** Wir betrachten Kurven $E_{0,b}$, die über $\mathbf{F}_p$ durch die Gleichung $y^2 = x^3 + b$ definiert sind mit mit $p = 10^{10} + 33$. Mit dem 2. Cornacchia-Algorithmus findet man wie oben beschrieben

$$\#E(\mathbf{F}_p) \in \{9999803617, 9999869187, 9999934464, 10000065604, 10000130881, 10000196451\}.$$

In der folgenden Tabelle haben wir für $1 \leq b \leq 100$ jeweils $\#E(\mathbf{F}_p)$ berechnet.

| $\#E_{0,b}(\mathbf{F}_p)$ | $b$ |
|---|---|
| 9999803617 | 20, 30, 45, 53, 55, 58, 70, 71, 73, 79, 82, 87, 97 |
| 9999869187 | 4, 6, 9, 11, 14, 21, 32, 38, 46, 48, 49, 50, 52, 57, 62, 68, 69, 72, 75, 78, 88, 93 |
| 9999934464 | 1, 8, 12, 13, 17, 18, 22, 27, 28, 33, 42, 43, 47, 63, 64, 67, 76, 77, 92, 96, 98, 100 |
| 10000065604 | 10, 15, 29, 35, 41, 59, 74, 80, 95 |
| 10000130881 | 5, 37, 40, 60, 65, 85, 89, 90 |
| 10000196451 | 2, 3, 7, 16, 19, 23, 24, 25, 26, 31, 34, 36, 39, 44, 51, 54, 56, 61, 66, 81, 83, 84, 86, 91, 94, 99 |

## 7. Bestimmung von $\#E(\mathbf{F}_p)$ für elliptische Kurven mit spezieller $j$-Invariante

Mit der Theorie der 'Komplexen Multiplikation' kann man zeigen, dass für eine über $\mathbf{Q}$ definierte elliptische Kurve $E$ gilt: Gibt es ein $D$ in folgender Tabelle mit $j(E) = j_D$, so gilt $\mathrm{End}(E) = \mathbf{Z}[\frac{(D \bmod 2)+\sqrt{D}}{2}]$.

| $D$ | $j_D$ |
|---|---|
| -3 | $0$ |
| -4 | $2^6 \cdot 3^3 = 1728$ |
| -7 | $-3^3 \cdot 5^3$ |
| -8 | $2^6 \cdot 5^3$ |
| -11 | $-2^{15}$ |
| -12 | $2^4 \cdot 3^3 \cdot 5^3$ |
| -16 | $2^3 \cdot 3^3 \cdot 11^3$ |
| -19 | $-2^{15} \cdot 3^3$ |
| -27 | $-2^{15} \cdot 3 \cdot 5^3$ |
| -28 | $3^3 \cdot 5^3 \cdot 17^3$ |
| -43 | $-2^{18} \cdot 3^3 \cdot 5^3$ |
| -67 | $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ |
| -163 | $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ |

Ist jetzt $E$ eine über $\mathbf{F}_p$, $p \geq 5$, definierte elliptische Kurve und gibt es ein $D$ in obiger Tabelle mit $j(E) \equiv j_D \bmod p$, so gibt es zwei Möglichkeiten:

(1) Die Gleichung $4p = x^2 - Dy^2$ hat keine Lösung in ganzen Zahlen. Dann ist $E$ supersingulär und damit $\#E(\mathbf{F}_p) = p + 1$.
(2) Die Gleichung $4p = x^2 - Dy^2$ ist in ganzen Zahlen lösbar. Dann gibt es $s, t \in \mathbf{Z}$ mit

$$\pi = \frac{s + t\sqrt{-D}}{2}, \quad \mathrm{Sp}(\pi) = s \quad \text{und} \quad N = \#E(\mathbf{F}_p) = p + 1 - s.$$

Bestimmt man mit dem 2. Cornacchia-Algorithmus $m, n \in \mathbf{Z}$ mit $4p = m^2 - Dn^2$, so ist

$$\pi = \begin{cases} \frac{\pm m \pm n\sqrt{D}}{2} \text{ oder } \frac{\frac{\pm m \pm 3n}{2} + \frac{\pm m \pm n}{2}\sqrt{D}}{2} & \text{für } D = -3, \\ \frac{\pm m \pm n\sqrt{D}}{2} \text{ oder } \frac{\pm n \pm m\sqrt{D}}{2} & \text{für } D = -4, \\ \frac{\pm m \pm n\sqrt{D}}{2} & \text{für } D < -4 \end{cases}$$

und

$$s = \mathrm{Sp}(\pi) = \begin{cases} \pm m \text{ oder } \frac{\pm m \pm 3n}{2} & \text{für } D = -3, \\ \pm m \text{ oder } \pm n & \text{für } D = -4, . \\ \pm m & \text{für } D < -4 \end{cases}$$

$$\#E(\mathbf{F}_p) = \begin{cases} p + 1 \pm m \text{ oder } p + 1 + \frac{\pm m \pm 3n}{2} & \text{für } D = -3, \\ p + 1 \pm m \text{ oder } p + 1 \pm n & \text{für } D = -4, . \\ p + 1 \pm m & \text{für } D < -4 \end{cases}$$

Wie zuvor kann man dann schnell die Gruppenordnung $\#E(\mathbf{F}_p)$ explizit bestimmen, indem man für einige Testpunkte $P \in E(\mathbf{F}_p)$ bestimmt, von welchen der 2 bzw. 4 bzw. 6 möglichen Zahlen für $\#E(\mathbf{F}_p)$ sie annulliert werden.

**Bemerkung:** Ist $p$ (hinreichend groß) gegeben, so kann man sich elliptische Kurven $E_i$ über $\mathbf{F}_p$ verschaffen, die sämtliche elliptische Kurven über $\mathbf{F}_p$ mit einer der obigen $j$-Invarianten $j_D$ repräsentieren. (Dies sind 26, 28, 30 oder 32 Kurven je nach der Restklasse von $p$ mod 12.) Mit der dargestellten Methode kann man dann schnell $N_i = \#E_i(\mathbf{F}_p)$ bestimmen. Auf diese Weise kann man sich Beispielmaterial besorgen.

**Beispiel:**

| $p$ | $a$ | $b$ | $j(E)$ | $D$ | $N = \#E(\mathbf{F}_p)$ | $\pi$ |
|---|---|---|---|---|---|---|
| 65521 | 0 | 1 | 0 | -3 | 65856 | $\frac{-334+224\sqrt{-3}}{2}$ |
| 65521 | 0 | 17 | 0 | -3 | 65353 | $\frac{169+279\sqrt{-3}}{2}$ |
| 65521 | 0 | 289 | 0 | -3 | 65019 | $\frac{503+55\sqrt{-3}}{2}$ |
| 65521 | 0 | 4913 | 0 | -3 | 65188 | $\frac{334+224\sqrt{-3}}{2}$ |
| 65521 | 0 | 18000 | 0 | -3 | 65691 | $\frac{-169+279\sqrt{-3}}{2}$ |
| 65521 | 0 | 43916 | 0 | -3 | 66025 | $\frac{-503+55\sqrt{-3}}{2}$ |
| 65521 | 1 | 0 | 1728 | -4 | 65344 | $\frac{178+240\sqrt{-4}}{2}$ |
| 65521 | 17 | 0 | 1728 | -4 | 66002 | $\frac{-480+89\sqrt{-4}}{2}$ |
| 65521 | 289 | 0 | 1728 | -4 | 65700 | $\frac{-178+240\sqrt{-4}}{2}$ |
| 65521 | 4913 | 0 | 1728 | -4 | 65042 | $\frac{480+89\sqrt{-4}}{2}$ |
| 65521 | 64479 | 22535 | 62146 | -7 | 65268 | $\frac{254+168\sqrt{-7}}{2}$ |
| 65521 | 26467 | 49486 | 62146 | -7 | 65776 | $\frac{-254+168\sqrt{-7}}{2}$ |
| 65521 | 35431 | 20060 | 8000 | -8 | 65088 | $\frac{434+96\sqrt{-8}}{2}$ |
| 65521 | 18283 | 11196 | 8000 | -8 | 65956 | $\frac{-434+96\sqrt{-8}}{2}$ |
| 65521 | 53119 | 8268 | 32753 | -11 | 65844 | $\frac{-322+120\sqrt{-11}}{2}$ |
| 65521 | 19477 | 63185 | 32753 | -11 | 65200 | $\frac{322+120\sqrt{-11}}{2}$ |
| 65521 | 52522 | 8666 | 54000 | -12 | 65856 | $\frac{-334+112\sqrt{-12}}{2}$ |
| 65521 | 43507 | 52929 | 54000 | -12 | 65188 | $\frac{334+112\sqrt{-12}}{2}$ |
| 65521 | 29266 | 24170 | 25412 | -16 | 65344 | $\frac{178+120\sqrt{-16}}{2}$ |
| 65521 | 5665 | 23158 | 25412 | -16 | 65700 | $\frac{-178+120\sqrt{-16}}{2}$ |
| 65521 | 44444 | 57732 | 32558 | -19 | 65072 | $\frac{450+56\sqrt{-19}}{2}$ |
| 65521 | 2200 | 62428 | 32558 | -19 | 65972 | $\frac{-450+56\sqrt{-19}}{2}$ |
| 65521 | 1167 | 64743 | 29948 | -27 | 65353 | $\frac{169+93\sqrt{-27}}{2}$ |
| 65521 | 9658 | 43425 | 29948 | -27 | 65691 | $\frac{-169+93\sqrt{-27}}{2}$ |
| 65521 | 20063 | 8465 | 4562 | -28 | 65776 | $\frac{-254+84\sqrt{-28}}{2}$ |
| 65521 | 32359 | 48231 | 4562 | -28 | 65268 | $\frac{254+84\sqrt{-28}}{2}$ |
| 65521 | 22103 | 7105 | 59584 | -43 | 65522 | $\sqrt{-65521}$ |
| 65521 | 32230 | 49693 | 59584 | -43 | 65522 | $\sqrt{-65521}$ |
| 65521 | 65254 | 178 | 19617 | -67 | 65025 | $\frac{497+15\sqrt{-67}}{2}$ |
| 65521 | 53879 | 22741 | 19617 | -67 | 66019 | $\frac{-497+15\sqrt{-67}}{2}$ |
| 65521 | 24476 | 5523 | 24372 | -163 | 65403 | $\frac{119+39\sqrt{-163}}{2}$ |
| 65521 | 62817 | 8805 | 24372 | -163 | 65641 | $\frac{-119+39\sqrt{-163}}{2}$ |

**Beispiel:** Wir haben mit der oben skizzierten Methode elliptische Kurven konstruiert und solche ausgewählt, für die $\#E(\mathbf{F}_p)$ eine Primzahl ist.

Wir beginnen mit 64-Bit-Primzahlen:

| $p$ | $a$ | $b$ | $N = \#E(\mathbf{F}_p)$ |
|---|---|---|---|
| 9223372036854775931 | 706127013620351338 | 2603706003204691085 | 9223372032648612541 |
| 9223372036854776077 | 0 | 2 | 9223372032735870907 |
| 9223372036854776077 | 954628876316813125 | 5512495440358641968 | 9223372032735870907 |
| 9223372036854776393 | 8809455572592569958 | 827832928524412870 | 9223372042581799811 |
| 9223372036854776687 | 5555598361380362491 | 6076997560344862862 | 9223372042921567151 |
| 9223372036854777509 | 8306428617986173894 | 6760210303815587416 | 9223372038729380641 |
| 9223372036854777509 | 4895547348523890822 | 5959673804505516961 | 9223372030783846597 |
| 9223372036854777517 | 3268309909360506276 | 7044498763947773333 | 9223372032825838777 |
| 9223372036854777803 | 2647300762451623865 | 4384047516268769292 | 9223372042014077369 |
| 9223372036854777853 | 8629049279901497239 | 792430342604374152 | 9223372042908901511 |

Es folgen 128-Bit-Primzahlen:

$$
\begin{aligned}
p_1 &= 170141183460469231731687303715884105979\\
a_1 &= 137943779540306223129401394663898616533\\
b_1 &= 214649359467753390681906060346569929 64\\
N_1 &= 170141183460469231711174102350554548609\\
p_2 &= 170141183460469231731687303715884106231\\
a_2 &= 0\\
b_2 &= 7\\
N_2 &= 170141183460469231757681811340322366803\\
p_3 &= 170141183460469231731687303715884107477\\
a_3 &= 133346895172991286934197953076651856129\\
b_3 &= 105772778870127003640548235424271037623\\
N_3 &= 170141183460469231705631596464693983033
\end{aligned}
$$

256-Bit-Primzahlen:

$$
\begin{aligned}
p_1 &= 57896044618658097711785492504343953926634992332820282019728792003956564829357\\
a_1 &= 36046373489321731200796849223424695402702523322183455626748314402256715232673\\
b_1 &= 33865128959110276911254259688727490324833310118031311601896582402452088007575\\
N_1 &= 57896044618658097711785492504343953927115147393064579442095186354627759634327\\
p_2 &= 57896044618658097711785492504343953926634992332820282019728792003956564830611\\
a_2 &= 0\\
b_2 &= 2\\
N_2 &= 57896044618658097711785492504343953926554352043299187794996766992582654853713\\
p_3 &= 57896044618658097711785492504343953926634992332820282019728792003956564830611\\
a_3 &= 23280886944642796747389379486780125140490525826906548124573097179925292102281\\
b_3 &= 37780902431241680723355778435945678818846468930023952568608658813686602086 83\\
N_3 &= 57896044618658097711785492504343953926554352043299187794996766992582654853713
\end{aligned}
$$

1024-Bit-Primzahl (gehört zu $D = -67$):

$$
\begin{aligned}
p &= 898846567431157953864652595394512366808988489471153286367150405788663379027504 81\\
&\quad 566354238661203768010560056939935696678829394884407208311246423715319737062188 88\\
&\quad 394671243274263815110980062304705972654147604250288441907534117123144073695655 52\\
&\quad 704136185816752553422931491199736229692398581524176781648121120754 57\\
a &= 123894988092884117142097409103370713536521744116108126498580743551202790532829 73\\
&\quad 578519040264280014125698552928082090414947045477733594942297791137440356674688 50\\
&\quad 396298107957655582036542816075698637494647997806356424971593988302142697952480 20\\
&\quad 531811566580872306003173566971309296944218505365407876277998625069 47\\
b &= 651056591245389719580457777187770939735945001238937033369988918686257797961845 34\\
&\quad 409316158132643739759162951083771515848935303928940018426650841440439023712811 87\\
&\quad 602075027358952651037894430153308697664851608637575591964346140518858677790695 11\\
&\quad 640513052655007941416584357257117635803961570793361029092123870615 63\\
N &= 898846567431157953864652595394512366808988489471153286367150405788663379027504 81\\
&\quad 566354238661203768010560056939935696678829394884407208311246423715319737056440 10\\
&\quad 048093147419113202540361351430645730382503894337725302336382387312195408286127 89\\
&\quad 520622968096482942885826021765745228258339900571914286695783737075 57
\end{aligned}
$$

KAPITEL 10

# Wie bestimmt man $\#E(\mathbf{F}_p)$?

Sei $p \geq 5$ eine Primzahl und seien $a, b \in \mathbf{F}_p$ mit $4a^3 + 27b^2 \neq 0$. Dann definiert $y^2 = x^3 + ax + b$ eine elliptische Kurve $E$ über $\mathbf{F}_p$. Wir wollen die Gruppenordnung

$$N = \#E(\mathbf{F}_p)$$

bestimmen.

## 1. Berechnung mit der Formel

Wir haben die folgende Formel für $\#E(\mathbf{F}_p)$ kennengelernt:

$$N = \#E(\mathbf{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left( \frac{x^3 + ax + b}{p} \right).$$

Da bei der Auswertung $x$ von 0 bis $p-1$ läuft, wächst die Laufzeit wie $O(p^{1+\varepsilon})$.

**Beispiel:** Die folgenden Beispiele wurden mit obiger Formel berechnet.

| Bitzahl | $p$ | $a$ | $b$ | $N$ | Zeit |
|---|---|---|---|---|---|
| 10 | 1021 | 101 | 1009 | 1080 | 1 s |
| 12 | 4093 | 101 | 1009 | 4100 | 3 s |
| 14 | 16381 | 101 | 1009 | 16366 | 11 s |
| 16 | 65521 | 101 | 1009 | 65891 | 50 s |
| 18 | 262139 | 101 | 1009 | 262599 | 3 m 37 s |
| 20 | 1048573 | 101 | 1009 | 1046776 | 15 m 16 s |
| 22 | 4194301 | 101 | 1009 | 4194200 | 1 h 4 m 50 s |
| 24 | 16777213 | 101 | 1009 | 16781626 | 4 h 35 m 15 s |

Für größere Primzahlen funktioniert das Verfahren praktisch nicht mehr.

## 2. Bestimmung von $\#E(\mathbf{F}_p)$ durch Studium von $\operatorname{ord}(P)$

LEMMA. *Sei $E$ eine elliptische Kurve über $\mathbf{F}_p$ mit $p \geq 5$. Für $P \in E(\mathbf{F}_p)$ werde definiert*

$$M_P = \{m \in \mathbf{N} : p + 1 - \lfloor 2\sqrt{p} \rfloor \leq m \leq p + 1 + \lfloor 2\sqrt{p} \rfloor \text{ und } m \cdot P = O\},$$

$$n_{\min} = \lceil \frac{p + 1 - \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} \rceil \quad \text{und} \quad n_{\max} = \lfloor \frac{p + 1 + \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} \rfloor.$$

*Dann gilt:*

(1) $\#E(\mathbf{F}_p) \in M_P$.
(2) $M_P = \{n \cdot \operatorname{ord}(P) : n_{\min} \leq n \leq n_{\max}\}$.
(3) $n_{\min} \leq n_{\max}$ *und man hat die Implikation*

$$n_{\min} = n_{\max} \quad \Longrightarrow \quad N = n_{\min} \cdot \operatorname{ord}(P).$$

(4)
$$\begin{aligned} \operatorname{ord}(P) \le \lfloor 2\sqrt{p} \rfloor \quad &\Longrightarrow \quad n_{\min} < n_{\max} \quad \Longrightarrow \quad \#M_P \ge 2. \\ \operatorname{ord}(P) \ge 2\lfloor 2\sqrt{p} \rfloor + 1 \quad &\Longrightarrow \quad n_{\min} = n_{\max} \quad \textit{und} \quad M_P = \{N\}. \end{aligned}$$

*Beweis:*

(1) Der Satz von Hasse liefert für $N = \#E(\mathbf{F}_p)$ die Abschätzung
$$p + 1 - 2\sqrt{p} \le N \le p + 1 + 2\sqrt{p},$$
was äquivalent zu
$$p + 1 - \lfloor 2\sqrt{p} \rfloor \le N \le p + 1 + \lfloor 2\sqrt{p} \rfloor$$
ist. Wegen $N \cdot P = O$ folgt $N \in M_P$.

(2) $M_P$ enthält alle Vielfachen von $\operatorname{ord}(P)$, die im angegebenen Intervall liegen, d.h.
$$M_P = \{n \cdot \operatorname{ord}(P) : p + 1 - \lfloor 2\sqrt{p} \rfloor \le n \cdot \operatorname{ord}(P) \le p + 1 + \lfloor 2\sqrt{p} \rfloor\}.$$
Durch einfache Umformungen erhält man die Behauptung.

(3) Die Aussage folgt sofort aus
$$N \in M_P = \{n \cdot \operatorname{ord}(P) : n_{\min} \le n \le n_{\max}\}.$$

(4) Im Fall $\operatorname{ord}(P) \le \lfloor 2\sqrt{p} \rfloor$ gilt
$$\begin{aligned} n_{\max} - n_{\min} &= \lfloor \frac{p + 1 + \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} \rfloor - \lceil \frac{p + 1 - \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} \rceil > \\ &> \left( \frac{p + 1 + \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} - 1 \right) - \left( \frac{p + 1 - \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} + 1 \right) = \\ &= \frac{2\lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} - 2 = \frac{2}{\operatorname{ord}(P)} (\lfloor 2\sqrt{p} \rfloor - \operatorname{ord}(P)) \ge 0, \end{aligned}$$
was die Behauptung beweist.
Im Fall $\operatorname{ord}(P) \ge 2\lfloor 2\sqrt{p} \rfloor + 1$ gilt
$$\begin{aligned} n_{\max} - n_{\min} &= \lfloor \frac{p + 1 + \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} \rfloor - \lceil \frac{p + 1 - \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} \rceil \le \\ &\le \frac{p + 1 + \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} - \frac{p + 1 - \lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} = \\ &= \frac{2\lfloor 2\sqrt{p} \rfloor}{\operatorname{ord}(P)} < 1, \end{aligned}$$
was $n_{\min} = n_{\max}$ und damit die Behauptung liefert. ■

**Bestimmung von $\#E(\mathbf{F}_p)$ durch Bestimmung von $M_P$:** Wir berechnen
$$N_{\min} = p + 1 - \lfloor 2\sqrt{p} \rfloor \quad \text{und} \quad N_{\max} = p + 1 + \lfloor 2\sqrt{p} \rfloor,$$
wählen einen Punkt $P \in E(\mathbf{F}_p)$ und bestimmen dann
$$M_P = \{m \in \mathbf{N} : N_{\min} \le m \le N_{\max} \text{ und } m \cdot P = O\},$$
indem wir alle $2\lfloor 2\sqrt{p} \rfloor + 1$ Möglichkeiten durchprobieren. Enthält $M_P$ nur ein Element, dann ist dies $N = \#E(\mathbf{F}_p)$. Andernfalls sagen wir, dass das Verfahren nicht funktioniert hat.

**Bemerkungen:**

(1) In den folgenden Beispielen hat das Verfahren stets funktioniert, wobei $P = (x_0, y_0)$ mit minimalem $x_0 \ge 0$ gewählt wurde. (Maple-Funktion 'Ep_anzahl_mp')

(2) Es ist klar, dass es Beispiele gibt, in denen das Verfahren nicht funktioniert. Man könnte dann mit einem neuen Punkt $P$ starten.

(3) Die Laufzeit des Verfahrens ist $O(p^{\frac{1}{2}+\varepsilon})$.

| Bitzahl | $p$ | $a$ | $b$ | $N$ | Zeit |
|---|---|---|---|---|---|
| 10 | 1021 | 101 | 1009 | 1080 | |
| 12 | 4093 | 101 | 1009 | 4100 | |
| 14 | 16381 | 101 | 1009 | 16366 | |
| 16 | 65521 | 101 | 1009 | 65891 | |
| 18 | 262139 | 101 | 1009 | 262599 | |
| 20 | 1048573 | 101 | 1009 | 1046776 | 1 s |
| 22 | 4194301 | 101 | 1009 | 4194200 | 2 s |
| 24 | 16777213 | 101 | 1009 | 16781626 | 4 s |
| 26 | 67108859 | 101 | 1009 | 67097456 | 9 s |
| 28 | 268435399 | 101 | 1009 | 268452000 | 17 s |
| 30 | 1073741789 | 101 | 1009 | 1073716497 | 36 s |
| 32 | 4294967291 | 101 | 1009 | 4294872714 | 1 m 22 s |
| 34 | 17179869143 | 101 | 1009 | 17179986303 | 2 m 50 s |
| 36 | 68719476731 | 101 | 1009 | 68719711992 | 5 m 57 s |
| 38 | 274877906899 | 101 | 1009 | 274878404165 | 11 m 40 s |
| 40 | 1099511627689 | 101 | 1009 | 1099512539944 | 24 m 38 s |
| 42 | 4398046511093 | 101 | 1009 | 4398043942557 | 48 m 9 s |
| 44 | 17592186044399 | 101 | 1009 | 17592179161868 | 1 h 40 m 51 s |

Die Erfahrung zeigt, dass in den meisten Fällen $M_P$ nur ein Element enthält, das dann natürlich die Gruppenordnung ist. Im folgenden Verfahren suchen wir nur ein Element von $M_P$, bestimmen damit $\operatorname{ord}(P)$ und damit wiederum $M_P$.

**Verfahren zur Bestimmung von $\#E(\mathbf{F}_p)$ durch Bestimmung von $\operatorname{ord}(P)$:** Wir starten wie beim letzten Verfahren, stoppen aber, sobald wir ein Element $m \in M_P$ gefunden haben.

(1) Nach Faktorisierung von $m$ kann man wegen $\operatorname{ord}(P) | m$ schnell $\operatorname{ord}(P)$ bestimmen.
(2) Man berechnet

$$n_{\min} = \lceil \frac{N_{\min}}{\operatorname{ord}(P)} \rceil \quad \text{und} \quad n_{\max} = \lfloor \frac{N_{\max}}{\operatorname{ord}(P)} \rfloor.$$

(3) Gilt jetzt $n_{\min} = n_{\max}$, so ist

$$\#E(\mathbf{F}_p) = n_{\min} \cdot \operatorname{ord}(P).$$

Gilt $n_{\min} < n_{\max}$, so hat das Verfahren nicht funktioniert. ($\operatorname{ord}(P)$ ist zu klein zur Bestimmung von $\#E(\mathbf{F}_p)$.)

**Bemerkung:** Eine zugehörige Maple-Funktion ist 'Ep_anzahl_ord'.

**Beispiele:** Die folgenden Beispiele wurden mit 'Ep_anzahl_ord' gerechnet:

| Bitzahl | $p$ | $a$ | $b$ | $N$ | Zeit |
|---|---|---|---|---|---|
| 10 | 1021 | 101 | 1009 | 1080 | |
| 12 | 4093 | 101 | 1009 | 4100 | |
| 14 | 16381 | 101 | 1009 | 16366 | |
| 16 | 65521 | 101 | 1009 | 65891 | |
| 18 | 262139 | 101 | 1009 | 262599 | |
| 20 | 1048573 | 101 | 1009 | 1046776 | |
| 22 | 4194301 | 101 | 1009 | 4194200 | 1 s |
| 24 | 16777213 | 101 | 1009 | 16781626 | 3 s |
| 26 | 67108859 | 101 | 1009 | 67097456 | 1 s |
| 28 | 268435399 | 101 | 1009 | 268452000 | 13 s |
| 30 | 1073741789 | 101 | 1009 | 1073716497 | 11 s |
| 32 | 4294967291 | 101 | 1009 | 4294872714 | 12 s |
| 34 | 17179869143 | 101 | 1009 | 17179986303 | 2 m 4 s |
| 36 | 68719476731 | 101 | 1009 | 68719711992 | 4 m 21 s |
| 38 | 274877906899 | 101 | 1009 | 274878404165 | 8 m 41 s |
| 40 | 1099511627689 | 101 | 1009 | 1099512539944 | 17 m 48 s |
| 42 | 4398046511093 | 101 | 1009 | 4398043942557 | 9 m 29 s |
| 44 | 17592186044399 | 101 | 1009 | 17592179161868 | 9 m 11 s |

**Bestimmung von $\#E(\mathbf{F}_p)$ durch Bestimmung von $\operatorname{ord}(P)$ mit Benutzung der baby-step-giant-step-Methode:** Das Verfahren läuft wie das letzte Verfahren mit folgendem Unterschied:

(1) Man bestimmt $m$ mit $m^2 \geq 1 + 2\lfloor 2\sqrt{p} \rfloor$. Jede Zahl zwischen $N_{\min}$ und $N_{\max}$ lässt sich dann in der Form

$$N_{\min} + mj - i \quad \text{mit} \quad 1 \leq i, j \leq m$$

schreiben.

(2) Wie früher berechnet man zwei Listen

$$B[i] = iP, 1 \leq i \leq m \quad G[j] = (N_{\min} + mj)P, 1 \leq j \leq m,$$

bestimmt ein gemeinsames Element $B[i] = G[j]$ und hat damit

$$(N_{\min} + mj - i) \cdot P = O.$$

(3) Mit Hilfe von $N_{\min} + mj - i$ bestimmt man $\operatorname{ord}(P)$. Der Rest ist wie beim letzten Verfahren.

**Bemerkungen:**

(1) Die Laufzeit wird jetzt $O(p^{\frac{1}{4}+\varepsilon})$. Dabei ist natürlich der Speicherbedarf nicht berücksichtig.
(2) Maple-Funktion 'Ep_anzahl_ord_bsgs'.

**Beispiele:** Berechnet mit Ep_anzahl_ord_bsgs.

| Bitzahl | $p$ | $a$ | $b$ | $N$ | Zeit |
|---|---|---|---|---|---|
| 10 | 1021 | 101 | 1009 | 1080 | |
| 12 | 4093 | 101 | 1009 | 4100 | |
| 14 | 16381 | 101 | 1009 | 16366 | |
| 16 | 65521 | 101 | 1009 | 65891 | |
| 18 | 262139 | 101 | 1009 | 262599 | |
| 20 | 1048573 | 101 | 1009 | 1046776 | |
| 22 | 4194301 | 101 | 1009 | 4194200 | |
| 24 | 16777213 | 101 | 1009 | 16781626 | |
| 26 | 67108859 | 101 | 1009 | 67097456 | |
| 28 | 268435399 | 101 | 1009 | 268452000 | |
| 30 | 1073741789 | 101 | 1009 | 1073716497 | 1 s |
| 32 | 4294967291 | 101 | 1009 | 4294872714 | 1 s |
| 34 | 17179869143 | 101 | 1009 | 17179986303 | 1 s |
| 36 | 68719476731 | 101 | 1009 | 68719711992 | 2 s |
| 38 | 274877906899 | 101 | 1009 | 274878404165 | 3 s |
| 40 | 1099511627689 | 101 | 1009 | 1099512539944 | 4 s |
| 42 | 4398046511093 | 101 | 1009 | 4398043942557 | 6 s |
| 44 | 17592186044399 | 101 | 1009 | 17592179161868 | 9 s |
| 46 | 70368744177643 | 101 | 1009 | 70368744225405 | 14 s |
| 48 | 281474976710597 | 101 | 1009 | 281474946817398 | 21 s |
| 50 | 1125899906842597 | 101 | 1009 | 1125899935492590 | 33 s |
| 52 | 4503599627370449 | 101 | 1009 | 4503599664198343 | 51 s |
| 54 | 18014398509481951 | 101 | 1009 | 18014398435681546 | 1 m 23 s |
| 56 | 72057594037927931 | 101 | 1009 | 72057593514890274 | 2 m 18 s |
| 58 | 288230376151711717 | 101 | 1009 | 288230376865390808 | 4 m 1 s |
| 60 | 1152921504606846883 | 101 | 1009 | 1152921502669114992 | 7 m 6 s |
| 62 | 4611686018427387847 | 101 | 1009 | 4611686020501489568 | 12 m 38 s |
| 64 | 18446744073709551557 | 101 | 1009 | 18446744069501970108 | 23 m 31 s |
| 66 | 73786976294838206459 | 101 | 1009 | 73786976294583568102 | 45 m 13 s |
| 68 | 295147905179352825833 | 101 | 1009 | 295147905196091501672 | 1 h 26 m 57 s |
| 70 | 118059162071741130338 9 | 101 | 1009 | 118059162076294040017 4 | 2 h 56 m 6 s |

Danach gab es Speicherplatzprobleme und das Programm wurde abgebrochen.

### 3. Bestimmung von $N = \#E(\mathbf{F}_p)$ unter Benutzung von Kongruenzbedingungen für $N$

Wird für $p \geq 5$ die elliptische Kurve $E$ über $\mathbf{F}_p$ durch die Gleichung $y^2 = x^3 + ax + b$ definiert, so sind die 2-Teilungspunkte

$$E(\overline{\mathbf{F}_p})[2] = \{O\} \cup \{(c_1, 0), (c_2, 0), (c_3, 0)\},$$

wenn $c_1, c_2, c_3$ die drei Nullstellen des Polynomen $x^3 + ax + b$ in $\overline{\mathbf{F}_p}$ sind. Jetzt gilt

$$\#E(\mathbf{F}_p) \equiv \begin{cases} 0 \bmod 2, \text{ falls ein } c_i \text{ in } \mathbf{F}_p \text{ ist,} \\ 1 \bmod 2, \text{ falls } x^3 + ax + b \text{ irreduzibel über } \mathbf{F}_p \text{ ist.} \end{cases}$$

Dadurch kann man die Anzahl der Möglichkeiten für $N = \#E(\mathbf{F}_p)$ einschränken. Wir skizzieren dies gleich etwas allgemeiner:

**Verfahren zur Bestimmung von $\#E(\mathbf{F}_p)$, wenn Kongruenzbedingungen bekannt sind:** Wir nehmen an, wir kennen ganze Zahlen $N_L$ und $L$ mit $L \geq 1$, $0 \leq N_L \leq L - 1$, sodass für die Anzahl der Punkte $N = \#E(\mathbf{F}_p)$ gilt:

$$N \equiv N_L \bmod L.$$

Wir starten mit

$$N_{\min} = p + 1 - \lfloor \sqrt{4p} \rfloor, \quad N_{\max} = p + 1 + \lfloor \sqrt{4p} \rfloor$$

und korrigieren dies jetzt zu

$$N_{\min} := N_{\min} + ((N_L - N_{\min}) \bmod L), \quad N_{\max} := N_{\max} - ((N_{\max}) - N_L) \bmod L),$$

sodass $N_{\min} \equiv N_{\max} \equiv N_L \bmod L$ gilt. Wir setzen

$$m = \lceil \sqrt{1 + \frac{N_{\max} - N_{\min}}{L}} \rceil,$$

sodass dann

$$N_{\min} + (m^2 - 1)L \geq N_{\max}$$

gilt. Also können wir $N = \#E(\mathbf{F}_p)$ wegen $N \equiv N_L \bmod L$ und $N_{\min} \leq N \leq N_{\max}$ als

$$N = N_{\min} + (mj - i)L \quad \text{mit} \quad 1 \leq i, j \leq m$$

schreiben. Mit der baby-step-giant-step-Methode finden wir ein Paar $(i, j)$, indem wir nach einem gemeinsamen Element der beiden Listen

$$B[i] = iL \cdot P, i = 1, \ldots, m \quad \text{und} \quad G[j] = (N_{\min} + jmL) \cdot P, j = 1, \ldots, m$$

suchen. Der Rest funktioniert wie früher.

**Bemerkung:** Es gilt

$$m \approx \sqrt{\frac{4\sqrt{p}}{L}} = \frac{2p^{\frac{1}{4}}}{L^{\frac{1}{2}}}.$$

Kann man also $N$ mod $L$ für ein hinreichend großes $L$ bestimmen, so kann man $N$ schnell berechnen.

**Beispiele:** Wir haben das letzte Verfahren angewandt, wobei zuerst $N \bmod 2$ bestimmt wurde durch Faktorisierungsversuch von $x^3 + ax + b$.

| Bitzahl | $p$ | $a$ | $b$ | $N$ | Zeit |
|---|---|---|---|---|---|
| 10 | 1021 | 101 | 1009 | 1080 | |
| 12 | 4093 | 101 | 1009 | 4100 | |
| 14 | 16381 | 101 | 1009 | 16366 | |
| 16 | 65521 | 101 | 1009 | 65891 | |
| 18 | 262139 | 101 | 1009 | 262599 | |
| 20 | 1048573 | 101 | 1009 | 1046776 | |
| 22 | 4194301 | 101 | 1009 | 4194200 | |
| 24 | 16777213 | 101 | 1009 | 16781626 | |
| 26 | 67108859 | 101 | 1009 | 67097456 | |
| 28 | 268435399 | 101 | 1009 | 268452000 | |
| 30 | 1073741789 | 101 | 1009 | 1073716497 | |
| 32 | 4294967291 | 101 | 1009 | 4294872714 | 1 s |
| 34 | 17179869143 | 101 | 1009 | 17179986303 | 1 s |
| 36 | 68719476731 | 101 | 1009 | 68719711992 | 1 s |
| 38 | 274877906899 | 101 | 1009 | 274878404165 | 2 s |
| 40 | 1099511627689 | 101 | 1009 | 1099512539944 | 2 s |
| 42 | 4398046511093 | 101 | 1009 | 4398043942557 | 4 s |
| 44 | 17592186044399 | 101 | 1009 | 17592179161868 | 6 s |
| 46 | 70368744177643 | 101 | 1009 | 70368744225405 | 9 s |
| 48 | 281474976710597 | 101 | 1009 | 281474946817398 | 14 s |
| 50 | 1125899906842597 | 101 | 1009 | 1125899935492590 | 21 s |
| 52 | 4503599627370449 | 101 | 1009 | 4503599664198343 | 33 s |
| 54 | 18014398509481951 | 101 | 1009 | 18014398435681546 | 52 s |
| 56 | 72057594037927931 | 101 | 1009 | 72057593514890274 | 1 m 25 s |
| 58 | 288230376151711717 | 101 | 1009 | 288230376865390808 | 1 m 24 s |
| 60 | 1152921504606846883 | 101 | 1009 | 1152921502669114992 | 3 m 57 s |
| 62 | 4611686018427387847 | 101 | 1009 | 4611686020501489568 | 6 m 54 s |
| 64 | 18446744073709551557 | 101 | 1009 | 18446744069501970108 | 12 m 50 s |
| 66 | 73786976294838206459 | 101 | 1009 | 73786976294583568102 | 23 m 40 s |
| 68 | 295147905179352825833 | 101 | 1009 | 295147905196091501672 | 23 m 41 s |
| 70 | 118059162071741130338 9 | 101 | 1009 | 118059162076294040017 4 | 1 h 29 m 53 s |

Wie kommt man jetzt weiter?

## 4. Die Idee von Schoof

**Der Schoof-Algorithmus zur Bestimmung von $\#E(\mathbf{F}_p)$:** Sei $E$ eine durch $y^2 = x^3 + ax + b$ über $\mathbf{F}_p$, $p \geq 5$, definierte elliptische Kurve.

(1) Der Frobenius-Endomorphismus $\pi$ einer elliptischen Kurve $E$ über $\mathbf{F}_p$ erfüllt die Gleichung

$$\pi^2 - s\pi + p = 0 \quad \text{mit} \quad s = \mathrm{Sp}(\pi) \quad \text{und} \quad N = p + 1 - s.$$

Für $P = (x, y) \in E(\overline{\mathbf{F}_p})$ gilt also

$$\pi^2(P) - s\pi(P) + pP = O, \quad \text{d.h.} \quad (x^{p^2}, y^{p^2}) - s(x^p, y^p) + p(x, y) = O.$$

(2) Sei jetzt $\ell$ eine (kleine) Primzahl. $E(\overline{\mathbf{F}_p})[\ell]$ ist ein 2-dimensionaler $\mathbf{F}_\ell$-Vektorraum. Wählt man

$$P_\ell \in E(\overline{\mathbf{F}_p})[\ell],$$

dann ist auch $\pi(P_\ell), \pi^2(P_\ell) \in E(\overline{\mathbf{F}_p})[\ell]$, d.h. es gilt

$$\ell \cdot P_\ell = \ell \cdot \pi(P_\ell) = \ell \cdot \pi^2(P_\ell) = O.$$

Die obige Gleichung wird damit zu

$$\pi^2(P_\ell) + (p \bmod \ell)P_\ell = (s \bmod \ell)\pi(P_\ell).$$

(3) Man berechnet jetzt

$$\pi^2(P_\ell) + (p \bmod \ell)P_\ell \quad \text{und} \quad \pi(P_\ell)$$

und bestimmt durch Probieren ein $s_\ell \in \{0, 1, \ldots, \ell - 1\}$ mit

$$\pi^2(P_\ell) + (p \bmod \ell)P_\ell = s_\ell \pi(P_\ell).$$

Dann folgt

$$s \equiv s_\ell \mod \ell \quad \text{und} \quad N \equiv p + 1 - s_\ell \mod \ell.$$

(4) Für $x, y \in \overline{\mathbf{F}_p}$ gilt:

$$(x, y) \in E(\overline{\mathbf{F}_p}) \quad \Longleftrightarrow \quad y^2 = x^3 + ax + b, \quad \psi_\ell(x, y) = 0,$$

wobei $\psi_\ell$ das $\ell$-te Teilungspolynom bezeichnet. Schoof schlug vor, zur Beschreibung des oben verwendeten Punktes $P_\ell = (x, y)$ nur die Relationen

$$y^2 = x^3 + ax + b \quad \text{und} \quad \psi_\ell(x, y) = 0$$

zu verwenden. Dann rechnet man mit Polynomen und und reduziert diese modulo der angegebenen Polynome.

(5) Bestimmt man für alle kleinen Primzahlen $\ell$ einen Wert $s_\ell \equiv s \bmod \ell$, bis

$$L = \prod_\ell \ell > 2\lfloor 2\sqrt{p} \rfloor$$

erfüllt ist, so erhält man mit dem chinesischen Restsatz ein $s_L$ mit

$$s_L \equiv s_\ell \equiv s \bmod \ell \quad \text{und damit} \quad s \equiv s_L \bmod L.$$

Wegen $|s| \leq \lfloor 2\sqrt{p} \rfloor$, ist dann $s$ durch $s_L$ eindeutig bestimmt, woraus man sofort $N = p + 1 - s$ erhält.

**Beispiel:** Wir wählen $p = 2097143$ und $a = 101$, $b = 1009$. Die elliptische Kurve über $\mathbf{F}_p$ habe die Gleichung $y^2 = x^3 + ax + b$. Das 3-Teilungspolynom

$$\psi_3 = 3x^4 + 606x^2 + 12108x + 2086942$$

ist irreduzibel über $\mathbf{F}_p$. Wir wählen $P = (x, y)$ und rechnen mit den Relationen $y^2 = x^3 + ax + b$ und $\psi_3(x) = 0$. Da $P$ dann ein 3-Teilungspunkt ist, gilt

$$pP = (p \bmod 3)P = -P = (x, 2097142y).$$

Mit der square-and-multiply-Methode erhält man

$$\begin{aligned}\pi(P) = (x^p, y^p) &= (60699x^3 + 44409x^2 + 1103791x + 1575455,\\ &\quad 859177y + 1649020yx + 1348501yx^2 + 1461989yx^3),\\ \pi^2(P) = (x^{p^2}, y^{p^2}) &= (1167020x^3 + 728686x^2 + 534997x + 1178009,\\ &\quad 902707y + 30579yx + 215302yx^2 + 1343675yx^3)\\ \pi^2(P) + pP &= (60699x^3 + 44409x^2 + 1103791x + 1575455,\\ &\quad 859177y + 1649020yx + 1348501yx^2 + 1461989yx^3)\end{aligned}$$

Man sieht sofort: $\pi^2 P + pP = \pi P$, also $s \equiv 1 \bmod 3$ und damit

$$N = (p+1) - s \equiv 2 + 1 - 1 = 2 \bmod 3.$$

**Bemerkungen:**

(1) Der Schoof-Algorithmus ist deterministisch. Die Laufzeit lässt sich im Prinzip durch $O(\ln^8 p)$ abschätzen. Der Algorithmus hat damit eine polynomiale Laufzeit.
(2) Die vorangegangenen Algorithmen zur Bestimmung von $\#E(\mathbf{F}_p)$ benutzen nur die Gruppenstruktur. Beim Schoof-Algorithmus werden Eigenschaften des Frobenius-Endomorphismus benutzt. 'Mehr Theorie führt zu schnelleren Algorithmen'.
(3) In der angegebenen Form ist der Schoof-Algorithmus nur beschränkt praktikabel. Für eine 160-Bit-Primzahl müsste man alle Primzahlen $\ell \leq 67$ betrachten. $\psi_{67}$ ist ein Polynom vom Grad 2244.

**Beispiel:** Wir betrachten die elliptische Kurve $E$ über $\mathbf{F}_p$, die durch $y^2 = x^3 + ax + b$ definiert wird mit der 100-Bit-Primzahl

$$p = 1267650600228229401496703205361 = 2^{100} - 15$$

und zufällig gewählten

$$a = 232480488953850415089295547599, \quad b = 183801659806149243712100544227.$$

Mit dem Schoof-Verfahren wurden Kongruenzen $N \bmod \ell$ für die Primzahlen $\ell \leq 19$ bestimmt:

| $\ell$ | Zeit für $\pi P$ | Zeit für $\pi^2 P$ | Gesamtzeit | | |
|---|---|---|---|---|---|
| 3 | 0.44 sec | 0.31 sec | 0.80 sec | $N \equiv 1 \bmod 3$ | $N \equiv 4 \bmod 6$ |
| 5 | 2.60 sec | 2.68 sec | 5.61 sec | $N \equiv 3 \bmod 5$ | $N \equiv 28 \bmod 30$ |
| 7 | 10.49 sec | 10.48 sec | 20.97 sec | $N \equiv 2 \bmod 7$ | $N \equiv 58 \bmod 210$ |
| 11 | 75.10 sec | 75.94 sec | 226.48 sec | $N \equiv 4 \bmod 11$ | $N \equiv 268 \bmod 2310$ |
| 13 | 124.30 sec | 123.41 sec | 343.81 sec | $N \equiv 9 \bmod 13$ | $N \equiv 7198 \bmod 30030$ |
| 17 | 296.96 sec | 296.18 sec | 844.06 sec | $N \equiv 7 \bmod 17$ | $N \equiv 7198 \bmod 510510$ |
| 19 | 524.29 sec | 511.75 sec | 1664.28 sec | $N \equiv 11 \bmod 19$ | $N \equiv 2559748 \bmod 9699690$ |

Für den Rest (mit der baby-step-giant-step-Methode) wurden 102 sec benötigt. Als Ergebnis erhält man (nach 52.35 min)

$$N = 1267650600228230327875372604188.$$

**Beispiel:** Wir starten mit der 128-Bit-Primzahl

$$p = 340282366920938463463374607431768211297 = 2^{128} - 159$$

und

$$a = 54888570589234400456411094666766336965, \quad b = 45970690709668886750906437588199065735.$$

Dazu betrachten wir die elliptische Kurve über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$.

| $\ell$ | Zeit für $\pi P$ | Zeit für $\pi^2 P$ | Gesamtzeit | | |
|---|---|---|---|---|---|
| 3 | .58 sec | .61 sec | 1.19 sec | $N \equiv 2 \bmod 3$ | $N \equiv 5 \bmod 6$ |
| 5 | 3.05 sec | 3.09 sec | 7.46 sec | $N \equiv 1 \bmod 5$ | $N \equiv 11 \bmod 30$ |
| 7 | 13.91 sec | 14.94 sec | 34.41 sec | $N \equiv 6 \bmod 7$ | $N \equiv 41 \bmod 210$ |
| 11 | 87.88 sec | 82.44 sec | 235.05 sec | $N \equiv 1 \bmod 11$ | $N \equiv 881 \bmod 2310$ |
| 13 | 143.36 sec | 122.49 sec | 391.20 sec | $N \equiv 11 \bmod 13$ | $N \equiv 7811 \bmod 30030$ |
| 17 | 212.02 sec | 193.48 sec | 998.61 sec | $N \equiv 6 \bmod 17$ | $N \equiv 127931 \bmod 510510$ |
| 19 | 347.40 sec | 335.29 sec | 1859.97 sec | $N \equiv 7 \bmod 19$ | $N \equiv 8296091 \bmod 9699690$ |
| 23 | 9304.25 sec | 9806.54 sec | 354.72 min | $N \equiv 11 \bmod 23$ | $N \equiv 95593301 \bmod 223092870$ |

Dann wurde mit der baby-step-giant-step-Methode ($m = 575105$) in 18 Stunden, 24 Minuten

$$N = 340282366920938463459267529435889931581$$

berechnet.

**Bemerkung:** Will man $\pi P$ berechnen, muss man $x^p$ mod $\psi_\ell$ berechnen (mit der square-and-multiply-Methode). Aufwendig wird dies dadurch, dass $\psi_\ell$ Grad $\frac{\ell^2-1}{2}$ hat. Hat $\psi_\ell$ einen Teiler $g_\ell$ kleineren Grades, kann man auch diesen statt $\psi_\ell$ nehmen. Elkies und Atkin haben (neben anderen) Ideen entwickelt, wie man hier weitermachen kann. Dies führte zum sogenannten SEA-Algorithmus (Schoof-Elkies-Atkin), auf den hier aber nicht mehr eingegangen wird.

KAPITEL 11

# Elliptische Kurven mit $\#E(\mathbf{F}_p) = p$ oder $\#E(\mathbf{F}_p) = p+1$

## 1. Logarithmenberechnung für Kurven mit $\#E(\mathbf{F}_p) = p+1$

**1.1. Die Weil-Paarung.** Sei $E$ eine elliptische Kurve über $\mathbf{F}_p$, $p \geq 5$, und $m$ eine natürliche Zahl mit $\mathrm{ggT}(m,p) = 1$. Dann gibt es eine Abbildung

$$e_m : E(\overline{\mathbf{F}_p})[m] \times E(\overline{\mathbf{F}_p})[m] \to \overline{\mathbf{F}_p}^*,$$

die als Weil-Paarung bezeichnet wird. Sie hat folgende Eigenschaften:

(1) $e_m$ ist bilinear, d.h. für $P, P_1, P_2, Q, Q_1, Q_2 \in E(\overline{\mathbf{F}_p})[m]$ gilt:

$$e_m(P_1+P_2, Q) = e_m(P_1,Q)e_m(P_2,Q) \quad \text{und} \quad e_m(P, Q_1+Q_2) = e_m(P,Q_1)e_m(P,Q_2).$$

(2) Aus der Bilinearität folgt sofort $(e_m(P,Q))^m = 1$ für $P, Q \in E(\overline{\mathbf{F}_p})[m]$, d.h. $e_m(P,Q)$ ist eine $m$-te Einheitswurzel. Wählt man $h \in \mathbf{N}$ minimal mit $m | p^h - 1$, so enthält $\mathbf{F}_{p^h}^*$ alle $m$-ten Einheitswurzeln von $\overline{\mathbf{F}_p}$, also gilt

$$\mathrm{Bild}(e_m) \subseteq \mathbf{F}_{p^h}^*.$$

(3) $e_m$ ist alternierend, d.h. $e_m(P,P) = 1$, woraus sofort

$$e_m(Q,P) = e_m(P,Q)^{-1}$$

für $P, Q \in E(\overline{\mathbf{F}_p})[m]$ folgt.

(4) $e_m$ ist nicht ausgeartet, d.h. für $P \in E(\overline{\mathbf{F}_p})[m]$ hat man die Implikation

$$e_m(P,Q) = 1 \text{ für alle } Q \in E(\overline{\mathbf{F}_p})[m] \quad \Longrightarrow \quad P = O.$$

(5) $e_m$ ist mit dem Frobenius-Endomorphismus $\pi$ verträglich:

$$\pi e_m(P,Q) = e_m(\pi P, \pi Q).$$

(6) Ist $m'$ eine natürliche Zahl mit $\mathrm{ggT}(m',p) = 1$, so ist $e_{mm'}$ in folgender Weise mit $e_m$ verträglich: Für $P \in E(\overline{\mathbf{F}_p})[mm']$ und $Q \in E(\overline{\mathbf{F}_p})[m]$ gilt

$$e_{mm'}(P,Q) = e_m(m'P, Q).$$

(7) Hat $P \in E(\overline{\mathbf{F}_p})[m]$ die Ordnung $m$, so gibt es einen Punkt $P' \in E(\overline{\mathbf{F}_p})[m]$, sodass auch $e_m(P,P')$ Ordnung $m$ hat, d.h. $e_m(P,P')$ ist eine primitive $m$-te Einheitswurzel.

(8) Gilt $E(\overline{\mathbf{F}_p})[m] \subseteq E(\mathbf{F}_{p^d})$, so folgt $m | p^d - 1$.

Für die Anwendung ist wichtig, dass sich die Weil-Paarung $e_m(P,Q)$ explizit berechnen lässt, worauf aber hier nicht eingegangen werden soll.

**1.2. Anwendung auf supersinguläre elliptische Kurven.** Sei $E$ eine supersinguläre elliptische Kurve über $\mathbf{F}_p$ mit $p \geq 5$. Dies ist äquivalent mit $\#E(\mathbf{F}_p) = p+1$. Wir haben dann bereits gesehen, dass

$$\#E(\mathbf{F}_p) = p+1 \quad \text{und} \quad E(\mathbf{F}_p) \subseteq E(\overline{\mathbf{F}_p})[p+1] = E(\mathbf{F}_{p^2})$$

gilt. Für $m = p+1$ gilt $m | p^2 - 1$, also wird die Weil-Paarung zu einer Abbildung

$$e_{p+1} : E(\mathbf{F}_{p^2}) \times E(\mathbf{F}_{p^2}) \to \mathbf{F}_{p^2}^*.$$

Seien $P, Q \in E(\mathbf{F}_p)$ mit $Q = xP$. Man sucht sich einen Punkt $R \in E(\mathbf{F}_{p^2})$ mit $\mathrm{ord}\,(P) = \mathrm{ord}\,(e_{p+1}(P,R))$. Dann gilt

$$e_{p+1}(Q,R) = e_{p+1}(xP,R) = e_{p+1}(P,R)^x.$$

Kann man jetzt das Logarithmenproblem

$$e_{p+1}(P,R)^y = e_{p+1}(Q,R)$$

in $\mathbf{F}_{p^2}^*$ lösen, d.h. findet man ein $y$, das der angegebenen Gleichung genügt, so folgt (wegen der Bedingung an die Ordnungen) $x = y$. Also hat man das Logarithmenproblem in $E(\mathbf{F}_p)$ gelöst.
Diese Beobachtung haben Menezes, Okamoto und Vanstone 1993 gemacht.

SATZ (Menezes-Okamoto-Vanstone-Reduktion). *Ist $E$ eine supersinguläre elliptische Kurve über $\mathbf{F}_p$, $p \geq 5$, und kann man diskrete Logarithmen in der multiplikativen Gruppe $\mathbf{F}_{p^2}^*$ berechnen, so kann man auch in $E(\mathbf{F}_p)$ diskrete Logarithmen berechnen.*

Die Folge davon ist, dass supersinguläre elliptische Kurven für kryptographische Anwendungen nicht nützlich sind, da die Sicherheit die gleiche ist wie die in der Untergruppe der Ordnung $p+1$ von $\mathbf{F}_{p^2}^*$.

## 2. Logarithmenberechnung für elliptische Kurven mit $\#E(\mathbf{F}_p) = p$

**2.1. Funktionentheorie.** Ist $K$ ein Körper und $f(x) \in K(x) \setminus \{0\}$ eine rationale Funktion, d.h. $f(x) = \frac{g(x)}{h(x)}$ mit Polynomen $g(x)$ und $h(x)$, so lässt sich für jedes $a \in \overline{K}$ die Funktion zerlegen in der Form

$$f(x) = (x-a)^v f_a(x) \quad \text{mit} \quad f_a \in \overline{K}(x) \quad \text{und} \quad f_a(a) \neq 0.$$

Man schreibt $v_a(f) = v$ und nennt $v$ die Bewertung von $f$ in $a$: Ist $v > 0$, so hat $f$ in $a$ eine $v$-fache Nullstelle, ist $v < 0$, so hat $f$ in $a$ eine $|v|$-fache Polstelle.

Ist $E$ eine durch $y^2 = x^3 + ax + b$ über $\mathbf{F}_p$, $p \geq 5$, definierte elliptische Kurve, so betrachtet man rationale Funktionen in $x, y$ als Funktionen auf $E(\overline{\mathbf{F}_P})$. Algebraisch sind die Funktionen Elemente des Funktionenkörpers

$$\overline{\mathbf{F}_p}(E) = \text{Quotientenkörper}\left(\overline{\mathbf{F}_p}[x,y]/(x^3+ax+b-y^2)\right).$$

Ähnlich wie oben kann man für jede Funktion $f$ und jeden Punkt $P \in E(\overline{\mathbf{F}_p})$ eine Bewertung $v_P(f)$ definieren, die dann für $v_P(f) > 0$ bzw. $v_P(f) < 0$ besagt, dass $f$ in $P$ eine $|v_P(f)|$-fache Nullstelle bzw. Polstelle hat. Im Fall $v_P(f) = 0$ gilt $f(P) \neq 0$.

Wir definieren jetzt für $P_1, P_2 \in E(\overline{\mathbf{F}_p})$ eine Funktion $\ell(P_1,P_2) = A + Bx + Cy$: $\ell(P_1,P_2) = 0$ soll die Verbindungsgerade von $P_1$ und $P_2$ beschreiben. Etwas genauer:

(1) Ist $P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2)$, $P_1 \neq P_2$, so soll gelten
$$A + Bx_1 + Cy_1 = 0 \quad \text{und} \quad A + Bx_2 + Cy_2 = 0.$$
(2) Ist $P_1 = P_2$, so soll $\ell(P_1,P_2) = A + Bx + Cy = 0$ die Tangente an $E$ in $P$ sein.
(3) Für $P_0 = (x_0,y_0)$ sei $\ell(P_0,O) = x - x_0$.
(4) $\ell(O,O) = 1$.

Man kann dann genau sagen, welche Pole und Nullstellen die Funktion $\ell(P,Q)$ hat. Als Beispiel: Sind $P, Q, -(P+Q), O$ vier schiedene Kurvenpunkte, so gilt für $R \in E(\overline{\mathbf{F}_p})$

$$v_R(\ell(P,Q)) = \begin{cases} 1 & \text{für } R \in \{P, Q, -(P+Q)\}, \\ -3 & \text{für } R = O, \\ 0 & \text{sonst.} \end{cases}$$

Mit Hilfe der Funktionen $\ell(P,Q)$ lassen sich ganz explizit Funktionen mit verlangten Null- und Polstellen konstruieren. Dabei gibt es allerdings eine Einschränkung: Sind $P_1, \ldots, P_r \in E(\overline{\mathbf{F}_p})$ paarweise verschiedene Punkte und $n_1, \ldots, n_r \in \mathbf{Z}$, dann gilt:

$$\text{Es gibt eine Funktion } f \text{ mit } v_P(f) = \begin{cases} n_i & \text{für } P = P_i, \\ 0 & \text{sonst,} \end{cases} \quad \Longleftrightarrow \quad \begin{cases} n_1 + \cdots + n_r = 0 \text{ und} \\ n_1P_1 + \cdots + n_rP_r = O. \end{cases}$$

Ist $N = \#E(\mathbf{F}_p)$, so folgt aus diesem Kriterium sofort, dass es für jeden Punkt $P \in E(\mathbf{F}_p) \setminus \{O\}$ eine Funktion $f_P$ mit folgender Eigenschaft gibt:

$$v_Q(f_P) = \begin{cases} N & \text{für } Q = P, \\ -N & \text{für } Q = O, \\ 0 & \text{sonst.} \end{cases}$$

Man kann $f_P$ mit Hilfe obiger Funktionen $\ell(P_i, P_j)$ effektiv in $O(\ln N)$ Schritten (mit der square-and-multiply-Methode) konstruieren. Man kann für $P, Q \in E(\mathbf{F}_p)$ auch zeigen, dass es ein $c_{P,Q} \in \mathbf{F}_p^*$ gibt mit

$$f_{P+Q} = c_{P,Q} \cdot f_P \cdot f_Q \cdot \frac{\ell(P+Q,O)^N}{\ell(P,Q)^N}.$$

**Beispiel:** Ist $P \in E(\mathbf{F}_p)$ mit $7P = O$, so ist

$$g = \frac{\ell(P,P)^3 \ell(2P,2P)\ell(2P,4P)\ell(P,6P)}{\ell(2P,O)^3 \ell(4P,O)\ell(6P,O)\ell(7P,O)}$$

eine Funktion mit $v_P(g) = 7$, $v_O(g) = -7$.

**2.2. Differentialrechnung.** Eine Differentialform auf $E$ ist ein formaler Ausdruck

$$\omega = \sum_i f_i dg_i \quad \text{mit} \quad f_i, g_i \in \overline{\mathbf{F}_p}(E),$$

wobei folgende Relationen gelten sollen:

$$d(fg) = f dg + g df, \quad d(f+g) = df + dg, \quad dc = 0 \text{ für } c \in \overline{\mathbf{F}_p}.$$

Die Differentiale bilden einen $\overline{\mathbf{F}_p}(E)$-Vektorraum $\Omega_E$.

Aus $y^2 = x^3 + ax + b$ folgt mit den üblichen Rechenregeln

$$2ydy = d(y^2) = d(x^3 + ax + b) = 3x^2 dx + a dx = (3x^2 + a)dx,$$

also

$$dy = \frac{3x^2 + a}{2y} dx \quad \text{und} \quad dx = \frac{2y}{3x^2 + a} dy.$$

Man sieht damit, dass $\Omega_E$ ein 1-dimensionaler $\overline{\mathbf{F}_p}(E)$-Vektorraum ist. Dann hat jede Differentialform $\omega$ eine eindeutige Darstellung als

$$\omega = f dx \quad \text{mit} \quad f \in \overline{\mathbf{F}_p}(E).$$

Wegen dieser Eindeutigkeit schreibt man auch

$$\frac{\omega}{dx} = f.$$

Wir nehmen jetzt die obige Relation

$$f_{P+Q} = c_{P,Q} \cdot f_P \cdot f_Q \cdot \frac{\ell(P+Q,O)^N}{\ell(P,Q)^N}$$

und bilden die logarithmische Abbildung

$$\frac{df_{P+Q}}{f_{P+Q}} = \frac{df_P}{f_P} + \frac{df_Q}{f_Q} + N\frac{d\ell(P+Q,O)}{\ell(P+Q,O)} - N\frac{d\ell(P,Q)}{\ell(P,Q)}.$$

Division durch $dx$ ergibt eine Beziehung zwischen Funktionen

$$\frac{1}{f_{P+Q}}\frac{df_{P+Q}}{dx} = \frac{1}{f_P}\frac{df_P}{dx} + \frac{1}{f_Q}\frac{df_Q}{dx} + N\frac{1}{\ell(P+Q,O)}\frac{d\ell(P+Q,O)}{dx} - N\frac{1}{\ell(P,Q)}\frac{d\ell(P,Q)}{dx}.$$

**2.3. Anwendung auf elliptische Kurven mit $\#E(\mathbf{F}_p) = p$.** Da in diesem Fall in $\mathbf{F}_p$ die Beziehung $N = p = 0$ gilt, folgt aus der letzten Gleichung

$$\frac{1}{f_{P+Q}}\frac{df_{P+Q}}{dx} = \frac{1}{f_P}\frac{df_P}{dx} + \frac{1}{f_Q}\frac{df_Q}{dx}.$$

Wir wählen jetzt einen Punkt $R \in E(\mathbf{F}_p)$, setzen dies ein und erhalten

$$\frac{1}{f_{P+Q}(R)}\frac{df_{P+Q}}{dx}(R) = \frac{1}{f_P(R)}\frac{df_P}{dx}(R) + \frac{1}{f_Q(R)}\frac{df_Q}{dx}(R).$$

Also liefert

$$\lambda_R : E(\mathbf{F}_p) \to \mathbf{F}_p, \quad P \mapsto \frac{1}{f_P(R)}\frac{df_P}{dx}(R)$$

eine additive Abbildung. $\lambda_R$ ist sogar ein Isomorphismus. Man kann $\lambda_R(P)$ schnell berechnen. Semaev hat 1998 damit folgenden Satz aufgestellt:

Satz (Semaev). *Sei $E$ eine elliptische Kurve über $\mathbf{F}_p$ mit $\#E(\mathbf{F}_p) = p$, seien $P, Q, R \in E(\mathbf{F}_p) \setminus \{O\}$. Dann gilt*

$$(\frac{\lambda_R(Q)}{\lambda_R(P)} \bmod p) \cdot P = Q.$$

Man kann also diskrete Logarithmen in $E(\mathbf{F}_p)$ lösen durch eine Division in $\mathbf{F}_p$. Dies geht sehr schnell. Wir haben dazu eine Maple-Funktion 'Ep_semaev' geschrieben und damit das folgende Beispiel gerechnet.

**Beispiel:** Die elliptische Kurve $E$ über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$, wobei $p, a, b$ unten angegeben sind, erfüllt die Bedingung $\#E(\mathbf{F}_p) = p$. Die Primzahl $p$ hat 1024 Bits.

$$\begin{aligned}
p &= 898846567431157953864652595394512366808988489471153286367150405788663\backslash\backslash\\
&\quad 790275048156635423866120376801056005693993569667882939488440720831124\backslash\backslash\\
&\quad 423715319770476381212409510665313642395172282831258170394006880666525\backslash\backslash\\
&\quad 041681996623003243807835731780552189274925136481370193615649543891953\backslash\backslash\\
&\quad 190011846643653345911095245 3,\\
a &= 707070398127664141815607978566369654038981668897530600036496794163994\backslash\backslash\\
&\quad 400884267937687235100621595108808434905850229200709399523374518798509\backslash\backslash\\
&\quad 227560845236886800805309151246925759509374856995275443872094466424131\backslash\backslash\\
&\quad 652454854486369898654030334461881499540942964504825532640139900946546\backslash\backslash\\
&\quad 3\backslash\backslash\\
&\quad 110510246710406342609099042 4,\\
b &= 727081824489767843942464808148436719719330206696517315131869344942221\backslash\backslash\\
&\quad 2\backslash\backslash\\
&\quad 119777218917055741754412772328869050988091273423370986302337948575826\backslash\backslash\\
&\quad 2\backslash\backslash\\
&\quad 413246529536043974413006580055801016853979805778160597943946196605946\backslash\backslash\\
&\quad 0\backslash\backslash\\
&\quad 953939425839757725974427419399481919339271538971943236394106124558241\backslash\backslash\\
&\quad 0\backslash\backslash\\
&\quad 179675631051266899475394298 8
\end{aligned}$$

Wir wählen Punkte $P = (P_x, P_y)$, $Q = (Q_x, Q_y)$ und $R = (R_x, R_y)$ mit

$$\begin{aligned}
P_x &= 1,\\
P_y &= 448182253486667951262455678408394088984060356004568992837356429401544\backslash\backslash\\
&\quad 650305123787035011722649199865886651836278608513335275958462781291509\backslash\backslash\\
&\quad 991537927661174010225072099249612850295452468716174854798700441528163\backslash\backslash\\
&\quad 152694212815803826814529481277373537250872296808496099717179755906564\backslash\backslash\\
&\quad 9,\\
Q_x &= 275613941840048286899449092578743255624949018829849155905444161392233\backslash\backslash\\
&\quad 609625715643148257341405772337392312527812911545938019588882683573324850\backslash\backslash\\
&\quad 519842331439722761787910994961000132269706526076055328468476164629716\backslash\backslash\\
&\quad 660587388642868754579695815918919887147427419489379526507860645555614\backslash\backslash\\
&\quad 1,\\
Q_y &= 122802861075554731052944135646083368616974255889735628065788050071044\backslash\backslash\\
&\quad 585479744923644232420855314384371368102804784897022395701752459348574\backslash\backslash\\
&\quad 644456722171560898043271040916983779357678734620736334545636049791874\backslash\backslash\\
&\quad 597960002545324954552205801542202679161441191927889553890320722675976\backslash\backslash\\
&\quad 6,\\
R_x &= 101,\\
R_y &= 307370875624354696168636760854810105197572575209673463510968979749073\backslash\backslash\\
&\quad 660205654466543374491787149658086078409090730013627782569728856454286\backslash\backslash\\
&\quad 680712163276298789914888596231821588264453679753385097289701665713999\backslash\backslash\\
&\quad 449805418012576522642870620067776532830305165801931961023814728717748\backslash\backslash\\
&\quad 2.
\end{aligned}$$

Dabei wurde $Q$ zufällig gewählt. Wir berechnen $\lambda_R(P)$, $\lambda_R(Q)$ und den Quotienten $\frac{\lambda_R(Q)}{\lambda_R(P)}$:

$$\begin{aligned}
\lambda_R(P) &= 886193897166298515944713781607384900859325206813153272464499393785981\backslash\backslash\\
&\quad 0548963390915152992302550623699111226390096038235327457310001270612490\backslash\backslash\\
&\quad 1962010895492847550221890172531501881547994077495540512510062952867036\backslash\backslash\\
&\quad 4090918184882371878777853767077120170789978431252666991252225643681267\backslash\backslash\\
&\quad 3136562976314893033939750040,\\
\lambda_R(Q) &= 5443042864264571114886480092958978357912911952789402032305334291714945\backslash\backslash\\
&\quad 1659516925931077465857293759208904118684993717395240350637734651228033\backslash\backslash\\
&\quad 6807482693766451504273223021328403169071008825915245074324850737280661\backslash\backslash\\
&\quad 7572088293109312445696157800075716111415219249777339550261395063462385\backslash\backslash\\
&\quad 6460526623459819656489218509,\\
\frac{\lambda_R(Q)}{\lambda_R(P)} &= 167279917928626182295832315149656121740749481908400801276751553979484\backslash\backslash\\
&\quad 6\backslash\backslash\\
&\quad 7490903099425548961449657848469794962607539924189316199395820256558482\backslash\backslash\\
&\quad 4843490583161803739631957580492424807433717588698514134933220759469356\backslash\backslash\\
&\quad 3954335338534487360233563524146433936126009700894000242549259658605927\backslash\backslash\\
&\quad 1111058991270347665755801973.
\end{aligned}$$

Die Berechnung von $\lambda_R(P)$ benötigte 100.10 sec, die von $\lambda_R(P)$ dann 100.59 sec. In 19.02 sec haben wir nachgeprüft, dass tatsächlich

$$\frac{\lambda_R(P)}{\lambda_R(Q)} \cdot P = Q$$

gilt, d.h. wir haben $\log_P Q$ in $E(\mathbf{F}_p)$ berechnet.

## 3. Schlußbemerkungen

J. Buchmann (Einführung in die Kryptographie, Springer 1999) schreibt zu den Vorteilen von EC-Kryptographie:

- Man geht davon aus, dass eine Kurve $E(p, a, b)$ mit $p \approx 2^{163}$, sodass $\#E(\mathbf{F}_p)$ einen Primteiler $q \geq 2^{160}$ hat, die gleiche Sicherheit wie ein RSA-System mit 1024 Bit bietet.
- Durch die geringere Schlüssellänge bei EC-Verfahren ist es möglich EC-Kryptographie auf Smart-Cards ohne Koprozessor zu implementieren. Solche Smart-Cards sind wesentlich billiger als Chipkarten mit Koprozessor.

Allerdings kann man auch gewisse Bedenken anmelden:

- Elliptische Kurven haben eine reichhaltige Struktur, die man benutzen kann um Probleme zu lösen.
- Je mehr Theorie in die Bestimmung von $\#E(\mathbf{F}_p)$ einging, desto besser wurden die Laufzeitabschätzungen: von exponentieller Laufzeit $O(p^{1+\varepsilon})$ mit dem naiven Zählverfahren bis zu polynomialer Laufzeit $O(\ln^8 p)$ mit dem Schoof-Algorithmus.
- Die Weil-Paarung erlaubt es für (supersinguläre) Kurven mit $\#E(\mathbf{F}_p) = p + 1$, die Logarithmenberechnung in $E(\mathbf{F}_p)$ auf die Logarithmenberechnung in $\mathbf{F}_{p^2}^*$ zurückzuführen.
- Für Kurven mit $\#E(\mathbf{F}_p) = p$ konnten wir die Logarithmenberechnung auf eine Division in $\mathbf{F}_p$ zurückführen, was die Logarithmenberechnung trivial macht.
- Gibt es auch andere Typen elliptischer Kurven, für die die Logarithmenberechnung stark vereinfacht werden kann?

ANHANG A

# Übungen

**Aufgabe 1:** Entschlüsseln Sie folgenden Text. Nach welchem Verfahren wurde verschlüsselt?

```
AWSENIERELREENESHAMSSADLFNAMDREUOHEIGNEHTSEAREBEETIETAHTEDETTBARNNAKFOET
SNEFTHCIHCILSEIDAWHCEHCEREDNSNEMNEHCNEBEUGOSEIWTSEIDETTIPMANSPEACILTHNEH
DEFOEUEIGIRBISNEUMHCSESSEGASCUANNEDHDNIMNEREEURBNREDMREDAHCIOVLESECNDANE
HCRUNSUATHCISSIMLEIFOVNERUKRWMEZNERAWHCSENIECSEGCALHTETHDROWNUNEHOSDTTEA
ESEENEGICILTIRFHEHCSTULBSRUWCANTNOMHACETNISSRAREBEGTOSNENELLLKRETREAREDE
CEUKMNEHTSIEODREANHCEDHCHCSMKCERHCILNENEEDEDMRASEVNETNANHSUIMEBAELNAREDI
GSADEZNATULBSGEWEUHCNETTSEUMUNESIBDNREHSHCONNIEKIEZEFEGTEDNUDNANSEREEWHC
ZENIHCSUHCALINETHAWNIEHRALGTIEBUIWHCSREDDNATNISEENEJGATNOWNELALHINELNEGR
LEWDGEHCHCSEFPEOSEDERREHTUZNETEODNINESSEBAGNEGSETARBTENEBUEANEHCCRUDARTH
TKNEDTIMEWMEEDNIGEGRUDNEEGDNCIPSNETKESAHEURNNEKCUZADTNASALCARBARCTEOUNEH
ERDNIMSINAMTNLEDMEIWHINAVMANBARODDNEAFRENETSEGATSEUZPNESGELFREFTRRENTSEO
TORBBTIMERROHCSTUFEGTLLEILOEUNEVREBEKCABNENESEAKHCSELFFACSIETIMHAHCSREFR
RPAPSAKIESSOSIEWOBESNENHCSNAEILHNESSEOKDILTSSEHCSSEUIEPSSNESTKNANREBDRAH
HCUKASNENTKNLOKIPSUATEALEHCZNASNULATAAICLGUEUNIEEWDNUENIRKDNTUEAILRREREOK
EIDEBLESEDTSSEGNNERTBNEGANREUGDRHNIIETIETSERUMMIEVGNTESRNETZRTIZLENOLNEL
EOKISUNRKILSSREOSSEUNIEWEGEGEIDNHCIGDNUTIZNEEWNAIENIHAWNSSERELHCREMMALEG
AHEGETTEMNAMENIEEOKNNENNREAWINNEJTHCREDELHCSUKCUEJDNHREDEPPANOVNMORFLREM
NUSEGEBGTIELEGTEESEWZZZN
```

**Aufgabe 2:** Entschlüsseln Sie folgenden Text. Nach welchem Verfahren wurde verschlüsselt?

```
EHBANNUHACEPIHHIPLOOSIJEURREITSDUNNMIEZDIDUNRLEEDIHACUETIHGEOOLSDUUARHCT
SRTEUIDTMIMHEESISNBHEEMUADHSETHICNNUHICRAERMRTODUNNBIOSGKULSALEWIRZOUVEH
SESIRMEATGSIEHSESIRDOOTKRGADUNEZHIENSOCHNAEDINZEEHRJHAFHUEARBHAERDUNRQEU
DUNMKMRUEMNEIRSECLHEUNARDEENSAMHUERDUNESHESDSARWISNTIHCNWEISSNKEONENSDAL
WLIRMIRSECIHSDAZHRENVEENRNBERRZAWNBIHICRGEETSICEHSALEALLEDINLEAFFNDEORKO
TRMEATGSIRSECBHIREDUNNPEFFAFHMCINPELGAEKNEILSEKPRUHNCOLZEWFEIEFTUHECRHMC
IRWEEDRVOEHLOLEHNCOLTEEFURDEAUFTISRMIHACUEALLDFURENEENSTSRIEBDILRMITNHIC
NEISWASRTEHCUZNWEISSEBDILRMITNHICNEIHICEKTONENSWANLEERHEDINMEEHNCSUZNBRE
ESSDUNUZNBEERKHEHACUBHAHICRWEEDTGUHNCODGLEHNCOREHDUNTHIEERKRHLCIRDETWLES
EEMTOHECNKIEDHNUOSRLEAGENNLEEBMDURBHAHICHMCIRDEEMIAGNEERBGEBORMIHDCURSGE
ETISTKFRADUNDMNUTNHICHMCANSGIENHMEIEWDUREDKNUSDSAHICTNHICRMHERMIMSEARUSS
SCIHEWUZNSEAGEBHRCAUSWAHICTNHICSWSEISDSAHICEENRNKESWAEDITWLEMINIENTNSERT
ZLUESAAHMNMEUSACHEALLTWFIARRKKESNDUNNSEAMDUNUTTNHICRMHENINWEOTRNKERMA
```

**Aufgabe 3:** Entschlüsseln Sie folgenden Text:

```
RFJNERVAXYNEREFCNRGUREOFGYVPUREZBETRATRTRARAQRABIRZOREVAQREANPUGUNGGRRFR
VAJRAVTTRFPUARVGHAQFBORQRPXGRRVASEVFPUREJRVFFREFPUYRVREXNHZZRUENYFMJRVSV
ATREUBPUQRAOBQRAABPUORVQHAXRYURVGTYRVPUANPUYNHQRFUNGGRAJVEGNYNOJNREGFVAR
```

Version vom 13.5.2003 - 25.12.2006

VARZQBESQVRZRFFRTRUBREGQNAAJNERAJVENHSTROEBPURAHZORVZREFGRAGNTRFYVPUGVAQ
VRORETRMHTRURANYFJVEQRAFGRVYRACSNQREXYBZZRAQREFVPUQVRUNRATRUVANHSJNAQFNU
VPUMHZREFGRAZNYQVRNOGRVAVPUGVUERZNHREAHROREENFPUGRAZVPUFVRTYVPURANAQRERA
QVRVPUNYYREBEGRAVAQREPUEVFGYVPURAJRYGTRFRURAFBAQREAQVRZNFFVTXRVGQRFFRAJN
FFVPUFCNRGRENYFQNFNRQVSVPVHZURENHFFGRYYRAFBYYGRRFJNERVANPUGRPXVTREONHQRE
NHFQRESREARMHANRPUFGJVRRVAIVRERPXNHFFNUQVRUBRPUFGIBYYRAQRGRSBEZNHFQEHPXQ
REORFGNRAQVTXRVGHAQHARVAARUZONEXRVGQREFGNQGTBGGRFFRVARFHRQSYNAXRENTGRUBP
UHRROREQNFCYNGRNHQRENOGRVJNRUERAQQVRABEQZNHREAHAZVGGRYONENHFQRZORETUNATMH
JNPUFRAFPUVRARATYRVPUFPUENRTVZSRYFIREJHEMRYGRAONRHZRAIBAHAGRATRFRURAFPUV
RARFTRENQRMHNYFIREYNRATREGRFVPUQRESRYFRAMHZUVZZRYHZVARVARETRJVFFRAUBRURB
UARFVPUGONERAJNAQRYVASNREOHATHAQFGBSSMHZZNRPUGVTRAGHEZMHJREQRARVAJREXIBA
EVRFRAUNAQTRFPUNSSRAVATEBRFFGREIREGENHGURVGZVGUVZZRYHAQREQR

(Hinweis: Es wurde eine Verschlüsselungsfunktion $f_t(x) \equiv x + t \bmod 26$ verwendet.)

**Aufgabe 4:** Was steht in folgender Nachricht?

JBJZCMQLFYEZUDZGFBAANECNJBFBJMJBEUSPFBZAJBAEALDFBCUDRFWUXIPNFYZBRRXSKIZR
XIHNZGUMQDHXNEZGZVQLCNFDXFLHCDWYFDZGSFNELIDSMRSRRVHQFDZBOZYNDRGDZGHPCLGA
GZQRKSJMZMZGPIWXFACMMTDLYNZLZTVGSHISQRYEXJFYJMJJFQPSTDFYIVYEJMPIQKERFBMC
VOJMZRWYZEQDQSKVLIFAPLRRIJFDEZWYITHAFOCFFDVMIVWUCNFYFBDRZVFYSDBNWUJMQDUK
BKVOERPTFYSDBNWUJMFOSWYNTBFDRRVGVDOZNKXISDXIDEDRKSQDQSOJQJRRFDIWSDPWHQTS
DESDBHBCHPQDQSYLZTNZVMLCYNHPFODNAZZTZVGSJMIHDFLIFAPLTNTKCNNZLSGFCNLGERLG
YNCLDWALYCZGEUALQSCFJVPGEROYYPSOTHABPJDRIOYNTBFDWUIVQYJMDTFYRFOZNKXISDXI
DEDRRRCNZBWUTHABJVYNDTFYRFOZNKXISDXIDEDRRRVGDNLAJBVGOFTKZGZGTBGUQDQSJJBH
BCCLVGHOJZFYONWUDRCJKSABJVCNNZLDBXFYGXJMOFFTJMFQCNCLMOAZWUJMZVSHIVAEJMCL
TKJMJBDWALVVRUXSWVGNVGUBBJPIQLSQCNPLGAVICNGDJMFONTYNSFFYVGJBTNFOCCMNFDEN
JMXSTHEJQSGXODIVWUPIFSZGXHIIMTZTVGLIUJVXYVOZYNEUCNUBYCNKCLVGSHEUCNUBPHZG
JBGAXEERCLHLNWXJGNXINMUQCNSOZLBCXJSDIWSDCFFDUQXSZGUBLPJMDTFYNNHPQDOWJGUD
ZTPSJMYLLGIJQLFYZOTHKSBNIIZGJTFYFONTFYPNGFCNIKDESDDRQFRFNEZGJBIWCFFYYLXI
MNOYRQZGPIFDLNSUYBZVNEHPQDVVCIDQTJGAIVVGSHFQVGCLWUERCLVGSADSHPZGQLHNSOEU
CNUBVVIWHXBCCMGFAZIIJMZVBJZRVOJMZLVJBCSAQDVVOZTJQDVVRVZAZVGFCNGDJMURKSXI
VUTJEIJZKSJM

(Hinweis: Die Verschlüsselungsfunktion hat die Gestalt

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \bmod 26).$$

**Aufgabe 5:** $A$ und $B$ einigen sich für einen Diffie-Hellman-Schlüsselaustausch auf $p = 10^6 + 3$ und $g = 2$. $A$ gibt $g^a \equiv 491373 \bmod p$ öffentlich bekannt, $B$ veröffentlicht $g^b \equiv 911253 \bmod p$. Was ist der zugehörige Diffie-Hellman-Schlüssel?

**Aufgabe 6:** Warum ist die Wahl der 157-stelligen Primzahl

$$\begin{aligned} p \;=\; & 6864797660130609714981900799081393217269435300143305409394463459185543183397656\backslash\backslash \\ & 0521225596406614545549772963113914808580371219879997166438125740282911150571 51 \end{aligned}$$

und $g = 2$ für einen Diffie-Hellman-Schlüsselaustausch schlecht?

**Aufgabe 7:** Mit dem folgenden 1024-Bit-RSA-Schlüssel

```
N=9520505646841354354477414912194378044449465273303174016545576810962850470773324628587971892487661657384394726201407859089427302739586684148035131263556738904520504343870436386630230150271748060615897977801224541217058759467496437913641171875704793588738469332476178878440432377638638698380267811487826409407
e=2596501540047642096675658612416648557577126892719047459057884584808050128392724898705810516132998633832107652600383961569843809838069095676736853980970019033076153368720132173463419706938596412565327586488344121788094177296872571927273318926849212025941484068162684965662311358324405384070814369354151270289
```

wurde der Anfang eines Gedichts von Hermann Hesse wie folgt verschlüsselt:

```
IZGAIBDLQSYHRFIFJBTQEONEBVIDWUPTDGCFMUAGUIMAHYSSOMLSBXIXUJWMGUVXUJFKQY
BMPSFYTHRAHZDOVEVGOSIYPKEMZZUXFQBUJDNSUIAKJJXYIWFYRBCDYFNVXGHZEHEODTPC
CBNBEGWNHPEJCWEIQBZIZTKBMYXLMXDBPKVBMKFSCCKCOKUMDROWXUJXPQSGEOIIENGXEX
HIHYVJVH
```

Um welches Gedicht handelt es sich?

**Aufgabe 8:** Durch $y^2 = x^3 + x$ wird eine ebene affine Kurve $C$ über $\mathbf{F}_p$ definiert. Bestimme $\#C(\mathbf{F}_p)$ für alle Primzahlen $p \leq 50$. Was kann man vermuten?

**Aufgabe 9:** Zeige, dass durch $f = 1 - 6xy + 2x^3 + 4y^3$ eine Kurve über $\mathbf{Q}$ definiert wird, die irreduzibel, aber nicht absolut irreduzibel ist.

**Aufgabe 10:** Die Gleichung $y^2 = x^3$ definiere die Kurve $C$ über $\mathbf{Q}$. Zeige, dass gilt

$$C(\mathbf{Q}) = \{(t^3, t^2) : t \in \mathbf{Q}\}.$$

**Aufgabe 11:** Konstruiere ein Polynom $f(x, y) \in \mathbf{R}[x, y]$, sodass für die zugehörige ebene affine Kurve $C$ über $\mathbf{R}$ gilt

$$C(\mathbf{R}) = \{(0, 0)\} \cup \{(x, y) \in \mathbf{R}^2 : x^2 + y^2 = 1\}.$$

**Aufgabe 12:** Durch die folgenden Gleichungen werden ebene Kurven über $\mathbf{R}$ definiert. Skizziere sie und bestimme die Singularitäten.

(1) $x^2 = x^4 + y^4$,
(2) $xy = x^6 + y^6$,
(3) $x^3 = y^2 + x^4 + y^4$,
(4) $x^2y + xy^2 = x^4 + y^4$.

**Aufgabe 13:** Seien $p$ und $q$ verschiedene ungerade Primzahlen, $N = pq$, sowie $m$ eine natürliche Zahl mit

$$a^m \equiv 1 \bmod N \quad \text{für alle ganzen Zahlen } a \text{ mit } \mathrm{ggT}(a, N) = 1.$$

Man zerlege $m = 2^\ell u$ mit $u \equiv 1 \bmod 2$. (Es ist $\ell \geq 1$ wegen $(-1)^m \equiv 1 \bmod N$.) Man definiere weiter

$$\begin{aligned} A_i &= \{x \in (\mathbf{Z}/\mathbf{Z}N)^* : x^{2^i u} \equiv 1 \bmod p, x^{2^i u} \equiv 1 \bmod q\}, \\ B_i &= \{x \in (\mathbf{Z}/\mathbf{Z}N)^* : x^{2^i u} \equiv -1 \bmod p, x^{2^i u} \equiv -1 \bmod q\}, \\ C_i &= \{x \in (\mathbf{Z}/\mathbf{Z}N)^* : x^{2^i u} \equiv 1 \bmod p, x^{2^i u} \equiv -1 \bmod q\}, \\ D_i &= \{x \in (\mathbf{Z}/\mathbf{Z}N)^* : x^{2^i u} \equiv -1 \bmod p, x^{2^i u} \equiv 1 \bmod q\}. \end{aligned}$$

Man zeige:

(1) $A_{i+1} = A_i \cup B_i \cup C_i \cup D_i$ (disjunkte Vereinigung).
(2) Ist $B_i \neq \emptyset$, z.B. $b \in B_i$, wählt man mit dem chinesischen Restsatz ein $c$ mit $c \equiv b \bmod p$, $c \equiv 1 \bmod q$, so liefert $B_i \to C_i$, $x \mapsto cx \bmod N$ eine Bijektion.
(3) Im Fall $B_i \neq \emptyset$ gilt
$$\#A_i = \#B_i = \#C_i = \#D_i.$$
(4) Ist $B_i = \emptyset$ und $C_i \neq \emptyset$, so gilt
$$\#A_i = \#C_i \quad \text{und} \quad D_i = \emptyset.$$
(5) Ist $x \in C_i \cup D_i$, so gilt
$$1 < \mathrm{ggT}(x^{2^i u} - 1, N) < N,$$
man erhält also einen nichttrivialen Teiler von $N$.
(6) Wegen $N - 1 \in B_0$ und $A_\ell = (\mathbf{Z}/\mathbf{Z}N)^*$ gibt es ein $i$ mit $A_i \neq (\mathbf{Z}/\mathbf{Z}N)^*$, $A_{i+1} = (\mathbf{Z}/\mathbf{Z}N)^*$. Hierfür gilt
$$\#C_i \cup D_i = \frac{1}{2}\#(\mathbf{Z}/\mathbf{Z}N)^* = \frac{1}{2}\varphi(N).$$

**Aufgabe 14:** Sei $(N, e)$ ein öffentlicher RSA-Schlüssel und $(N, d)$ der zugehörige private RSA-Schlüssel. Skizziere ein (probabilistisches) Verfahren, wie man aus $(N, e)$ und $(N, d)$ die Faktorisierung von $N$ erhalten kann. (Hinweis: Die Voraussetzung in Aufgabe 13 ist mit $m = ed - 1$ erfüllt.)

**Aufgabe 15:** Die folgenden Zahlen $N$, $e$, $d$

```
N=116535848387059565955927804242072808192669086601378284820512028561467587370493879878052805259268672252790056898142817189091942855155441736725351092917963017602118551579268342662623510523636781709394581897824916849630157554383402443366976782105155603216757879846573268139930554590305217784348448516080032923183
e=5
d=699215090322357395735566825452436849156014519608269708923072171368805524222963279268316831555612033516740341388856903134551657130932650420352106557507070324735404214722780972191406987003607125034785407108071013153788680874672173652311832192178504101750246008947591703748186655689206486183093196063314702666 45
```

bilden ein RSA-Schlüsselpaar $(N, e)$, $(N, d)$. Bestimme die Primfaktorzerlegung von $N$.

**Aufgabe 16:** Eine leichte Verallgemeinerung der Caesar-Verschlüsselung für Dateien erhält man, wenn man sich als Schlüssel eine Bytefolge $s_0 s_1 \ldots s_{k-1}$, also ein Wort der Länge $k$, wählt und aus der Plaintextbytefolge $a_0 a_1 a_2 \ldots$ mittels

$$b_i \equiv a_i + s_{i \bmod k} \bmod 256$$

die Ciphertextbytefolge $b_0b_1b_2\ldots$ konstruiert. ($k = 1$ ergibt die übliche Caesar-Verschlüsselung.) Nachstehend findet sich die Bytefolge einer Datei, von der vermutet wird, dass es sich um eine mit obigem Verfahren verschlüsselte E-Mail handelt.

```
142,211,225,223,153,194,228,228,228,202,228,188,161,223,219,167,197,221,221,161,
202,228,180,194,224,217,222,190,157,216,217,133,198,189,198,146,179,233,194,143,
166,173,133,162,124,155,162,169,153,157,180,199,148,151,162,120,148,124,196,222,
179,212,221,234,202,214,130,129,216,228,232,189,143,223,213,216,229,169,207,214,
228,218,126,220,221,162,218,224,177,142,215,228,229,177,221,219,217,211,160,172,
198,146,154,228,177,226,231,213,211,214,186,194,160,223,226,126,228,226,221,146,
215,186,205,211,224,224,181,221,162,216,202,146,163,146,165,163,167,129,167,172,
162,150,162,123,143,164,171,214,121,121,125,214,222,146,181,202,160,231,231,185,
156,217,230,209,211,182,200,215,224,167,180,212,148,156,157,160,129,143,165,226,
171,127,167,162,165,147,165,117,167,179,199,162,112,230,221,232,205,146,155,174,
198,194,153,185,211,148,185,166,179,121,153,164,162,176, 90,120,218,227,215,146,
132,211,231,226,233,181,225,232,180,210,219,118,214,224,219,166,181,225,224,213,
211,217,173,207,160,214,222,142,170,148,200,218,215,116,129,164,171,153,145,223,
230,148,151,162,120,148,146,162,173,138,159,171,174,152,167,104,140,162,164,169,
128,143,156,193,170,197,156,138,124,182,218,196,212,174,148,185,231,173,141,146,
164,178,112,176,228,230,133,164,120,145,165,146,169,132,169,164,171,159,165,125,
129,157,162,171,128,159,148,156,178,183,155,181,155,124,191,194,222,225,174,133,
148,159,208,222,216,224,177,221,219,148,178,160,104,179,231,226,233,181,225,232,
150,133,174,186,214,226,226,222,194,227,180,225,206,160,189,207,219,159,222,194,
219,213,226,204,215,182,143,214,215,183, 90,195,227,174,133,201,183,205,216,217,
218,190,214,148,198,218,226,184,198,228,230,153,140,225,233,228,213,215,186,213,
178,223,226,126,228,226,221,146,215,186,205,211,224,224,181,221,162,216,202,176,
 82,180,231,212,227,181,210,232,174,133,194,169,212,229,233,232,194,227,126,193,
202,229,187,194,217,215,166,153,179,174,148,161,194,177,207,215,160,192,163,190,
162,167,147,171,126,143,163,162,172,128,163,166,173,149,166,120,151,164,170,167,
135,161,167,181,146,163,120,145,162,162,169,144,218,213,231,216,211,182,197,228,
211,167,189,216,162,233,211,219,117,198,228,222,218,190,214,217,226,147,214,173,
159,124,191,194,157,180,161,202,202,228,187,202,225,224,179,112,160,162,164,111,
181,183,207,230,215,231,196,156,200,237,213,215,130,129,198,183,209,164,158,196,
192,166,187,150,156,146,213,225,177,225,231,217,217,175,157,180,159,179,204,147,
184,189,126,168,225,182,213,215,224,237,125,187,217,226,204,230,176,155,146,166,
171, 90,194,232,213,217,231,187,155,146,196,200, 90,199,161,199,217,211,188,214,
229,172,153, 90,121,184,213,216,146,176,198,231,230,226,183,212,148,196,198,229,
187,216,225,228,237,112,219,213,233,217,215,188,129,210,211,175,200,161,224,237,
199,162,111,143,124,124,131, 90
```

Was steht in der Nachricht?

**Aufgabe 17:** Durch nachfolgende Polynome $f, g \in \mathbf{Q}[x, y]$ werden ebene affine Kurven $C_f$ und $C_g$ definiert. Bestimme den Durchschnitt $C_f(\overline{Q}) \cap C_g(\overline{\mathbf{Q}})$.

(1) $f = 20 + 79x + 47y + 13x^2 + 9xy$, $g = -67 - 252x - 150y - 21x^2 + 10y^2$.
(2) $f = 5 - 2x + x^2 - 6y + y^2$, $g = 13 + 2x - x^2 - 12y + 2y^2$.

**Aufgabe 18:** Das Polynom

$$f = a_0x_0^2 + a_1x_0x_1 + a_2x_0x_2 + a_3x_1^2 + a_4x_1x_2 + a_5x_2^2 \in K[x_0, x_1, x_2] \setminus \{0\}$$

definiert eine ebene projektive Quadrik $Q$ über dem Körper $K$. Dazu bildet man:

$$D(f) = 4a_0a_3a_5 - a_0a_4^2 - a_1^2a_5 - a_2^2a_3 + a_1a_2a_4 \quad \text{mit} \quad 2D(f) = \det \begin{pmatrix} 2a_0 & a_1 & a_2 \\ a_1 & 2a_3 & a_4 \\ a_2 & a_4 & 2a_5 \end{pmatrix}.$$

Man zeige die Äquivalenzen:

$$Q \text{ singulär} \quad \Longleftrightarrow \quad Q \text{ reduzibel über } \overline{K} \quad \Longleftrightarrow \quad D(f) = 0.$$

(Eventuell verlangt Charakteristik 2 eine besondere Behandlung.)

**Aufgabe 19:** Zeige, dass $f = x_0^4 + x_1^4 + x_2^4$ in Charakteristik 3 eine nichtsinguläre ebene Kurve definiert, bei der aber jeder Punkt ein Wendepunkt ist.

**Aufgabe 20:** Sei $K$ ein algebraisch abgeschlossener Körper der Charakteristik 2 und $C$ die durch $f = x_0^2 + x_1x_2$ über $K$ definierte ebene projektive Quadrik. Zeige, dass $C$ nichtsingulär ist und dass jede Tangente an $C$ durch den Punkt $(1:0:0)$ geht.

**Aufgabe 21:** Sei $C$ eine über einem algebraisch abgeschlossenen Körper $K$ durch ein Polynom $f \in K[x_0, x_1, x_2]$ definierte nichtsinguläre ebene projektive Kurve vom Grad $d \geq 2$ und $P \in \mathbf{P}^2$ ein Punkt, sodass jede Tangente an $C$ durch $P$ geht. Zeige dass dann $C$ eine Quadrik in Charakteristik 2 ist.
Zum Beweis kann man in folgenden Schritten vorgehen:

(1) Nimmt man o.E. $P = (1:0:0)$ an, so folgt $\frac{\partial f}{\partial x_0} = 0$.

(2) Die Eulersche Relation $d \cdot f = \frac{\partial f}{\partial x_0}x_0 + \frac{\partial f}{\partial x_1}x_1 + \frac{\partial f}{\partial x_2}x_2$ impliziert für $Q \in \mathbf{P}^2$

$$\frac{\partial f}{\partial x_1}(Q) = \frac{\partial f}{\partial x_2}(Q) = 0 \quad \Longrightarrow \quad d \cdot f(P) = \frac{\partial f}{\partial x_0}(Q) = \frac{\partial f}{\partial x_1}(Q) = \frac{\partial f}{\partial x_2}(Q) = 0.$$

Zeige, dass dann $d = 0$ in $K$ und die Polynomgleichung $\frac{\partial f}{\partial x_1}x_1 + \frac{\partial f}{\partial x_2}x_2 = 0$ gilt.

(3) Zeige, dass ein homogenes Polynom $g \in K[x_0, x_1, x_2]$ vom Grad $d-2$ existiert mit

$$\frac{\partial f}{\partial x_1} = x_2 g(x_0, x_1, x_2) \quad \text{und} \quad \frac{\partial f}{\partial x_2} = -x_1 g(x_0, x_1, x_2).$$

(4) Zeige, dass $C$ im Fall $d \geq 3$ Singularitäten hätte, und folgere damit die Behauptung.

**Aufgabe 22:** Sei $C$ eine über einem Körper $K$ durch ein Polynom $f \in K[x_0, x_1, x_2]$ definierte nichtsinguläre ebene projektive Kubik und $G \subseteq C(K)$ eine Teilmenge, sodass die geometrisch definierte Verknüpfung $\varphi$ auf $G$ eine Gruppenstruktur definiert. Sei $O \in G$ das neutrale Element der Gruppe. Zeige:

(1) $O$ ist ein Wendepunkt. Nach Koordinatenwechsel kann man annehmen, dass $O = (0:0:1)$ mit Wendetangente $x_0 = 0$ gilt. Dann hat das Polynom $f$ die Gestalt

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + a_3x_0x_1^2 + a_4x_0x_1x_2 + a_5x_0x_2^2 + a_6x_1^3.$$

(2) Für $P \in G$ gilt $\varphi(P, P) = O$ und $\frac{\partial f}{\partial x_2}(P) = 0$.

(3) Für $P \in G$, $P \neq O$ gilt die Gleichung

$$(a_2x_0 + a_4x_1 + 2a_5x_2)(P) = 0.$$

(4) In Charakteristik 2 ist $G \simeq \mathbf{Z}/2\mathbf{Z}$ oder $G = \{O\}$. (Ein Beispiel liefert $f = x_0^2x_1 + x_0x_1x_2 + x_0x_2^2 + x_1^3$.)

(5) In Charakteristik $\neq 2$ ist $G \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ oder $G \simeq \mathbf{Z}/2\mathbf{Z}$ oder $G = \{O\}$. (Ein Beispiel liefert $y^2 = x^3 - x$.)

**Aufgabe 23:** Das Polynom

$$f = tx_0^3 + t^2x_0^2x_1 + x_0x_1^2 + x_1x_2^2$$

definiert eine projektive ebene kubische Kurve $C$ über dem Körper $K = \mathbf{F}_2(t)$. Zeige:

(1) $C$ ist absolut irreduzibel.
(2) $C$ besitzt genau eine Singularität $S \in C(\overline{K})$.
(3) $S$ ist nicht über $K$ definiert, d.h. $S \notin C(K)$.

**Aufgabe 24:** Mit $p = 2340302707$ (32 Bits) wird durch

$$f = x_0^2x_1 + 2x_1^2x_2 - 3x_2^2x_0$$

eine nichtsinguläre Kubik $C$ über $\mathbf{F}_p$ definiert, die die Punkte

$$O = (1 : 0 : 0) \quad \text{und} \quad P = (1 : 1 : 1)$$

enthält. $C(\mathbf{F}_p)$ wird durch Wahl von $O$ als neutrales Element zu einer Gruppe. Damit wird ein Diffie-Hellman-Schlüsselaustausch durchgeführt: Die öffentlichen Schlüssel von $A$ und $B$ sind

$$P_A = a \cdot P = (1 : 219462279 : 1711373330) \quad \text{und} \quad P_B = b \cdot P = (1 : 625360275 : 1785020600)$$

(mit geheimgehaltenen Zahlen $a$ und $b$.) $A$ und $B$ benutzen als gemeinsamen Schlüssel die natürliche Zahl $K$ (in Dezimaldarstellung) mit

$$aP_B = bP_A = abP = (1 : K : \dots).$$

$A$ schickt an $B$ folgende Bytefolge:

```
[166, 0, 0, 0, 42, 215, 30, 231, 69, 129, 66, 190, 254, 38, 197, 60, 3,
73, 185, 224, 181, 188, 40, 193, 6, 137, 2, 168, 229, 99, 135, 45, 97,
75, 25, 217, 39, 234, 65, 12, 213, 15, 91, 57, 250, 119, 233]
```

Sie gehört zu einer Datei, die konventionell mit PGP mit dem Schlüssel $K$ verschlüsselt wurde ('pgp -c'). Welcher Begriff wurde hier verschlüsselt?

**Aufgabe 25:** Mit der 128-Bit-Primzahl

$$p = 340282366920938463463374607431768211297$$

und

$$f = +563x_0^3 - 231x_0^2x_1 - 262x_0^2x_2 + 45x_0x_1^2 + 52x_0x_1x_2 + 35x_0x_2^2 - 7x_1^3 + 2x_1^2x_2 - 5x_1x_2^2$$

wird eine ebene projektive Kubik $C$ über $\mathbf{F}_p$ definiert, die die Punkte

$$O = (0 : 0 : 1) \quad \text{und} \quad P = (4 : 28 : 25)$$

enthält. $C(\mathbf{F}_p)$ wird durch Wahl von $O$ als neutrales Element zu einer Gruppe. Damit wird ein Diffie-Hellman-Schlüsselaustausch durchgeführt: $A$ und $B$ wählen sich jeweils geheim Zahlen $a$ und $b$ und berechen $P_A = a \cdot P$ bzw. $P_B = b \cdot P$ mit dem Ergebnis

$$P_A = (1 : 590359590450754320546758962017031567 04 : 373308031684030294341566543597918006 67),$$
$$P_B = (1 : 881252073177881972499376066665886296 90 : 125913602333673121418256511252390873876).$$

$P_A$ und $P_B$ sind die öffentlichen Schlüssel von $A$ und $B$. Als gemeinsamen Schlüssel verwenden $A$ und $B$ die Zahl $K$ (in Dezimaldarstellung), für die gilt

$$aP_B = bP_A = abP = (1 : K : \dots), \quad 0 \leq K \leq p - 1.$$

Was ist $K$? (Hinweis: $C$ ist singulär.)

**Aufgabe 26:** Für eine Verschlüsselung mit ebenen Kubiken wird die durch

$$p = 2340302707, \quad f = x_0^2x_1 + 2x_1^2x_2 - 3x_2^2x_0$$

über $\mathbf{F}_p$ definierte Kurve $C$ zugrunde gelegt, wobei für die geometrische Addition der Punkt $O = (1 : 0 : 0) \in C(\mathbf{F}_p)$ als neutrales Element gewählt wird, außerdem hat man noch den Punkt $P = (1 : 1 : 1) \in C(\mathbf{F}_p)$. Der öffentliche Schlüssel von $A$ ist

$$K_A = k_A \cdot P = (1 : 219462279 : 1711373330),$$

wobei $k_A$ der private Schlüssel von $A$ ist. Eine als Zahl $m$ mit $0 \leq m \leq p-1$ dargestellte Nachricht wird mittels

$$\begin{aligned} Q &= m \cdot P = (1 : x_Q : y_Q) = (1 : 1415946736 : 668042169), \\ R &= m \cdot K_A = (1 : x_R : y_R), \\ s &= m \oplus x_R = 639270997 \end{aligned}$$

zu

$$(x_Q, y_Q, s) = (1415946736, 668042169, 639270997)$$

verschlüsselt. Was ist $m$?

**Aufgabe 27:** Für $d \in \mathbf{N}$ definiert $f = x_0^3 + x_1^3 + dx_2^3$ eine nichtsinguläre ebene Kubik $C$ über $\mathbf{Q}$. Bestimme eine Weierstraßsche Normalform $y^2 = x^3 + ax + b$ für $C$.

**Aufgabe 28:** Sei $p$ eine Primzahl mit $p \equiv 3 \bmod 4$ und $C$ die durch $y^2 = x^3 + x$ (bzw. homogen geschrieben $f = x_0x_2^2 - x_1^3 - x_0^2x_1 = 0$) definierte ebene projektive Kubik. Zeige, dass

$$\#C(\mathbf{F}_p) = p + 1$$

gilt. (Hinweis: Zeige, dass mit der Bezeichnung $X = \{x \in \mathbf{F}_p^* : \text{ es gibt ein } y \text{ mit } (x, y) \in C(\mathbf{F}_p)\}$ für $x \in \mathbf{F}_p^*$ gilt: $x \in X \iff -x \notin X$.)

**Aufgabe 29:** Für $p \geq 3$ definiert

$$y^2 = x^3 + x$$

(bzw. homogen geschrieben $f = x_0x_2^2 - x_1^3 - x_0^2x_1 = 0$) eine nichtsinguläre projektive kubische Kurve $C$ über $\mathbf{F}_p$. Zeige, dass

$$\#C(\mathbf{F}_p) \equiv 0 \bmod 4$$

gilt.

**Aufgabe 30:** Es folgt die Verschlüsselung $c_1c_2c_3c_4\ldots$ der ersten Zeilen einer Erzählung eines 1875 geborenen deutschen Schriftstellers. Dabei stimmen die Zeichen $c_1, c_3, c_5, \ldots$ mit dem Original überein. Der besseren Lesbarkeit halber wurde nach 70 Zeichen jeweils ein Zeilenumbruch eingefügt. Entschlüssle den Text. Wie wurde verschlüsselt?

```
Gvsuaw Bsdhfncadh!oees woo Bsdhfncadh- xif tejt!sfioen gufngzjgttfn!Gf
bvrusuah bmuljci tejn!Nbmf mavtftf,!hbtue!ao fioen Grveiljnhsoadhniutb
g!dfs!Jbhset 29/.- eat vntesen Lootjnfnu nooauemaog!ejnf to!gffbhsdsoi
eodf Nifnf {ejgue- woo tejnfr!Wphouog!io ees Qrjn{-Seheotfnttsatsf {u!
```

```
Mveocieo but blmejn!ejnfn!wfiueseo Tpbzjesgbnh vnuesnpmneo.!Ufbfrsejzu
 woo ees tciwjesiheo vne hegafhsljcieo,!eceo keuzu fioe!hpedhttf Ceiuu
sbmlejt- Vmtidhu,!Ejnerjnhljcikfiu vne Heoavihkfiu eet Ximlfnt frgosdf
rodfn!Asbfiu ees Wosmjtuahsttvneeo,!hbtue!dfr!Sdhsigtttflmes een Gostt
ciwjnheo eet qrpdvzjeseodfn!Tsifbxeskfs!io tejnfm!Ionfro,!jfnfm!‘nouut
 bnjmj dootjnvut’- xosio oadh!Cjcfrp eat Xeteo ees Ceseesbmlejt!bfsuei
t- budh!nbci ees Niutbgtmbhmzfiu oidhu Fiohblu {u!tvn!vfrnodhu vne eeo
 fnulbsueodfn!Sdhmunmfr!njcit!gffvneeo,!dfr!iim- cej {uoeimfnees Bbouu
zcaskfiu tejnfr!Ksaffue- fiombl!uotfruahs!sp ooftjg!wbr/ To!hbtue!es c
amd!nbci een Uef eat Grfif hetudhu,!io ees Iogfouog- eats!Lvfu vne Cex
ehuog!iin!wjeeeshfrttflmeo vne jhn {u!ejnfm!essqrjetsmidhfn!Aceod!vfri
emffn!wvesdfn/
```

**Aufgabe 31:** Bestimme Repräsentanten aller $\mathbf{F}_7$-Isomorphieklassen elliptischer Kurven $E$ über $\mathbf{F}_7$, dazu jeweils $j(E)$ und $\#E(\mathbf{F}_7)$.

**Aufgabe 32:** Über $K = \mathbf{F}_{29}$ ist $E_{a,b} : y^2 = x^3 + ax + b$ mit

$$(a, b) \in \{(4, 7), (8, 14), (14, 20), (18, 5)\}$$

eine elliptische Kurve mit

$$\#E_{a,b}(\mathbf{F}_{29}) = 32.$$

Bestimme jeweils die Struktur von $E(\mathbf{F}_{29})$ als abelsche Gruppe.

**Aufgabe 33:** Sei $p$ eine ungerade Primzahl und $\xi$ und $\omega$ Elemente im algebraischen Abschluss von $\mathbf{F}_p$, die den Gleichungen $\xi^4 = -1$ und $\omega = \xi - \xi^3$ genügen. Zeige, dass gilt

$$\omega^2 = 2, \quad 2^{\frac{p-1}{2}} = \frac{\omega^p}{\omega} \quad \text{und} \quad \omega^p = \begin{cases} \omega & \text{für } p \equiv 1, 7 \bmod 8, \\ -\omega & \text{für } p \equiv 3, 5 \bmod 8, \end{cases}$$

und folgere

$$2^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \bmod p \text{ für } p \equiv 1, 7 \bmod 8, \\ -1 & \bmod p \text{ für } p \equiv 3, 5 \bmod 8. \end{cases}$$

**Aufgabe 34:** Sei $p$ eine Primzahl $\equiv 1 \bmod 4$. Dann ist $\left(\frac{-1}{p}\right) = 1$, also gibt es ein $c \in \mathbf{F}_p^*$ mit $c^2 = -1$. Sei

$$f : \mathbf{F}_p^* \to \mathbf{F}_p^*, \quad x \mapsto x^{\frac{p-1}{4}}.$$

(1) Zeige, dass gilt

$$f(\mathbf{F}_p^*) = \{1, -1, c, -c\}.$$

(2) Beschreibe ein (probabilistisches) Verfahren, wie man $\pm c$ schnell finden kann, und teste es an Beispielen.

**Aufgabe 35:** Sei $n$ eine ungerade natürliche Zahl und $a \in \mathbf{Z}$. Das Jacobi-Symbol $\left(\frac{a}{n}\right)$ kann man (mit Hilfe des quadratischen Reziprozitätsgesetzes) effizient berechnen ohne Benutzung des Legendre-Symbols.

(1) Gilt $\mathrm{ggT}(a,n)=1$ und
$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n,$$
so ist $n$ zusammengesetzt. (Dies liefert einen Primzahltest.)

(2) Gilt für eine zusammengesetzte Zahl $n$ und $a \geq 2$ mit $\mathrm{ggT}(a,n)=1$ die Beziehung
$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n,$$
so heißt $n$ eine Eulersche Pseudoprimzahl zur Basis $a$. Bestimme alle Eulerschen Pseudoprimzahlen $\leq 10000$ zu den Basen 2 und 3.

**Aufgabe 36:** Der nachfolgende Text ist ElGamal-verschlüsselt mit den Parametern
$$p = 18446744073709551557, \quad g = 2, \quad f_A = 9131675346818833568,$$
wobei das Alphabet A,...,Z zugrundeliegt mit Plaintextblocklänge 13 und Ciphertextblocklänge 14.

```
ECHJXRQISHHGDBBFNGUXPAKLUWAUBLQQLHFUXRQWRVDQOLFGNWLNHQLCDVAMXSWUSPMHAP
BGWBTVLNBIWLTMFFYLELIPXMMBDZDRZLZRHZDNJSRBAUKQKRYDBDJYANBALANGBWSHVJNI
DATPKOTUAEVWSJETZAXYQUVDTNDMHHMWPAMAIKBLSDDATTZRUGUEUDVODKHWSZEFBRNWND
FKIFICPOEOZHWZGUUINIQWVQGBJWGBAAIJYISUFSOYGSNTOVIJQKLFRHDCTHBXXSJACDKD
```

Entschlüssle den Text. (Hinweis: Die benötigten Zufallszahlen wurden mit dem Maple-Zufallszahlengenerator 'rand(0..$p$)' erzeugt.)

**Aufgabe 37:** Entschlüssle!

```
AOTWNCC AOjjO: TO]jO@]OH

j_CCO @OcdA?O W]T ]Cj AOTn A]CO]C,
U]CH ROTUOA W]T j_TfOC cCH aOjdAUOTHOC!
?]ODOTO U_CCO UO]jj ]dA C]dA? NcD OTHOC,
N@j ]W UO]?OC cC?OTUOfj nc jO]C.

CNdA HOT OaCO COAW ]dA WO]COC @NcD,
j_CCO j_@@ W]dA jOCfOC, WOOT W]dA [cOA@OC;
cCjTOT OTHO @OaOC W]?ncDcOA@OC
?c ]dA N@@O j]CCO DOj?@]dA NcD.

cCH j_ j_@@ W]T VOHOT COcO ?Nf
COcO DTOcCHO, COcO aTcOHOT UO]jOC,
a]j ]dA @O]H@_j N@@O [TNOD?O gTO]jOC,
N@@OT j?OTCO fNj? cCH DTOcCH jO]C WNf.
```

**Aufgabe 38:** Die elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbf{F}_p$ mit
$$p = 2203081241, \quad a = 4107646, \quad b = 1676918659,$$
den Punkten
$$P = (590797101, 723642358), \quad Q_A = (54389314, 1147919690)$$
wurde zur ElGamal-Verschlüsselung eines Textes über dem Alphabet A,B,C,...,Z mit Blocklänge 5 und $k = 10$ (wie in der Vorlesung beschrieben) verwendet. Wer ist der Autor des nachfolgenden verschlüsselten Texts?

```
((1909189474,696100745),(2115369162,688731575))
((934604272,822337988),(1698857097,124188007))
((804639504,910110089),(485705139,748044864))
((1388034258,2150924025),(1173144954,2062502010))
((190651855,1471431170),(332536782,1434440588))
((1407203763,954659938),(184571163,928282898))
((1724152764,1552316821),(1695039911,1481854989))
((439911561,1838445703),(1085003459,904791905))
((1927188021,2099908029),(575917066,1381897631))
((1265096566,179382230),(970996439,1556172846))
((224863170,1375806897),(1350259004,289373326))
((825079301,624103485),(1986519137,427256414))
((1206580857,1290011495),(1583607528,346328542))
((2158670469,1541501734),(585210860,1894203734))
((991738532,1151480129),(945227993,1815454814))
((228686097,642970035),(358602598,493267132))
((2186816951,1430962365),(335903699,2126607766))
((1135287363,1795514752),(553732346,553963849))
((1348791939,151680338),(103820575,1852342000))
((34782822,1696323548),(1781554417,2078379987))
((170476170,767623232),(1646661927,1542718550))
((1934038904,1342482810),(942014770,2139865217))
((1452435923,2083329113),(1966442682,1829139491))
((2014988733,256653592),(1980742101,1792366406))
```

**Aufgabe 39:** Zeige: Ist $m$ eine natürliche Zahl, so läßt sich jede Zahl $x \in \mathbf{Z}$ mit $0 \leq x \leq m^2 - 1$ in der Form

$$x = mj - i \quad \text{mit} \quad 1 \leq i, j \leq m$$

schreiben.

**Aufgabe 40:** Das Massey-Omura-Kryptosystem zur Nachrichtenübertragung funktioniert nach folgendem Schema:
*Schlüsselerzeugung:*

- Man einigt sich auf eine (große) Primzahl $p$ und darauf, wie man eine Nachricht in eine Folge von Elementen $r_i \in \mathbf{F}_p^*$ umwandelt.
- Jeder Teilnehmer $A$ wählt sich eine (zufällige) Zahl $e_A$ mit $1 \leq e_A \leq p-2$ und $\mathrm{ggT}(e_A, p-1) = 1$ und berechnet sich (mit dem erweiterten euklidischen Algorithmus) eine Zahl $d_A$ mit

$$d_A e_A \equiv 1 \bmod p - 1.$$

  Das Paar $(e_A, d_A)$ ist der geheime Schlüssel von $A$. Es gibt keinen öffentlichen Schlüssel!

*Nachrichtenübertragung:*

- Will $A$ eine Nachricht $r_i \in \mathbf{F}_p^*$ an $B$ senden, berechnet er $s_i = r_i^{e_A}$ und schickt $s_i$ an $B$.
- $B$ empfängt $s_i$, berechnet $t_i = s_i^{e_B}$ und schickt $t_i$ an $A$ zurück.
- $A$ empfängt $t_i$, berechnet $u_i = t_i^{d_A}$ und schickt $u_i$ an $B$.
- $B$ empfängt $u_i$ und berechnet $v_i = u_i^{d_B}$. Dann ist $v_i$ identisch mit der Ausgangsnachricht $r_i$.

Im Folgenden liegt die Primzahl $p = 4398046511093$ zugrunde. $A$ schickt an $B$ eine Nachricht, wobei $C$ auf dem Übertragungsweg (unter Verwendung obiger Bezeichnungen)

$$s = 1201549027024, \quad t = 1560562300195, \quad u = 429298008146$$

auffängt. Was ist die Ausgangsnachricht?

**Aufgabe 41:** Für $g(x) = 1 + x^2 + x^{15} + x^{16} \in \mathbf{F}_2[x]$ beweise man folgende Eigenschaften:

1. Für $f(x) \in g(x)\mathbf{F}_2[x] = \{g(x)h(x) : h(x) \in \mathbf{F}_2[x]\}$ gilt $f(1) = 0$, d.h. $f(x)$ enthält eine gerade Anzahl von Monomen $\neq 0$.
2. Für ganze Zahlen $0 \leq m < n$ gilt

$$x^m + x^n \in g(x)\mathbf{F}_2[x] \quad \Longleftrightarrow \quad n \equiv m \bmod 32767.$$

Weiter sei $F = \{r(x) \in \mathbf{F}_2[x] : \deg r(x) \leq 15\}$ und

$$\gamma : \mathbf{F}_2[x] \to F, \quad m(x) \mapsto \text{Rest der Polynomdivision von } x^{16}m(x) \text{ durch } g(x),$$

d.h. man kann schreiben $x^{16}m(x) = q(x)g(x) + \gamma(m(x))$ mit einem Polynom $q(x)$.
Jeder Bitfolge $M = (m_1m_2m_3 \dots m_t)$ kann man ein Polynom $M(x) \in \mathbf{F}_2[x]$ zuordnen durch

$$M = (m_1m_2m_3 \dots m_{t-1}m_t) \mapsto M(x) = m_1x^{t-1} + m_2x^{t-2} + m_3x^{t-3} + \dots + m_{t-1}x + m_t.$$

Unter Benutzung dieser Abbildung bildet $\gamma$ Bitfolgen beliebiger (endlicher) Länge auf Polynome vom Grad $\leq 15$, also auf Bitfolgen der Länge 16 ab. Man zeige nun weiter:

3. Unterscheiden sich die Bitfolgen $M$ und $N$ in einer ungeraden Anzahl von Bits, so ist $\gamma(M) \neq \gamma(N)$.
4. Unterscheiden sich zwei Bitfolgen $M$ und $N$ mit Längen $\leq 32767$ in genau zwei Bits, so ist $\gamma(M) \neq \gamma(N)$.

(Auf diesem Prinzip beruht CRC-16 - cyclic redundancy code.)

**Aufgabe 42:** Für $p = 10^{20} + 39$ und $g = 3$ wurden folgende diskrete Logarithmen berechnet:

| $a$ | $\log_3(a)$ |
|---|---|
| 2 | 86792332251783168850 |
| 3 | 1 |
| 5 | 41025259664069146848 |
| 7 | 10465869232100529600 |
| 11 | 97981806285588131496 |
| 13 | 6351838317046312990 |
| 17 | 22945125767903614204 |
| 19 | 27629884555029366917 |
| 23 | 92869052686674421326 |
| 29 | 58629941811305283781 |

Man berechne $\log_3(q)$ für alle Primzahlen $q$ mit $31 \leq q \leq 100$.

**Aufgabe 43:** $A$ unterschreibt seine Dateien mit dem ElGamal-Signatur-Verfahren. Seine öffentlichen Schlüssel sind:

$$\begin{aligned} p_A &= 789746956799439217432898878450480984754072988193502405966258189471033246 9 \\ g_A &= 2 \\ f_A &= 122844596392163120195275926657056914762623780732911854408230765925041423 6 \end{aligned}$$

Wir finden zwei Dokumente von $A$ mit Hashwerten $h_i$ und Signaturen $(b_i, c_i)$:

$$\begin{aligned} h_1 &= (\text{cdbeadf03b29ac3eb9dc57f6e0cd9c9e})_{16} = 27348180342895980129931502809467516 4318 \\ b_1 &= 11032932343202944641896179738172228283956962785555810542438566686462319 69 \\ c_1 &= 16768222095847938473222744595864146483777032878931964829806340873311145 87 \\ h_2 &= (\text{f9300c33c0082e60e8850073081d1d62})_{16} = 33122724868863626843549933826247682390 6 \\ b_2 &= 11032932343202944641896179738172228283956962785555810542438566686462319 69 \\ c_2 &= 31197477677246333837391014181743421492328109693208008168062146638401734 71 \end{aligned}$$

Was ist der private Schlüssel $e_A$ von $A$?

**Aufgabe 44:** $A$ verwendet zum Unterschreiben seiner Dokumente das DSA-Verfahren mit öffentlichen Schlüsselparametern

$$\begin{aligned} q_A &= 524309 \\ p_A &= 9223372036869000547 \\ g_A &= 8308467587808723131 \\ f_A &= 8566038811843553785 \end{aligned}$$

Wir kommen an zwei signierte Dokumente von $A$ mit Hashwerten $h_i$ und Signaturen $(r_i, s_i)$, wobei

$$\begin{aligned} h_1 &= (\text{f9300c33c0082e60e8850073081d1d62})_{16} = 33122724868863626843549933826247682390 6 \\ r_1 &= 115641 \\ s_1 &= 355317 \\ h_2 &= (\text{cdbeadf03b29ac3eb9dc57f6e0cd9c9e})_{16} = 27348180342895980129931502809467516 4318 \\ r_2 &= 115641 \\ s_2 &= 116525 \end{aligned}$$

Was ist der private Schlüssel $e_A$ von $A$?

**Aufgabe 45:** Ein Gedicht wurde mit dem öffentlichen Schlüssel

$$p = 12345678912345678912345678 91, \quad g = 2, \quad f = 96854915447664651331527 3448$$

ElGamal-verschlüsselt. (11 Bytes Plaintextblocklänge, 12 Bytes Ciphertextblocklänge bzw. 24 Zeichen in Hexadezimalschreibweise.) Das Ergebnis (in Hexadezimalschreibweise) ist

```
00bc82b8428f11e489cc4d3d01622d58b530f361bc936f490000000008000000000000
00022e0c26cb4c2acf8fa1edf101022cd6e046e4b512079da90236e07608ca6006c3ec
4a13000000000000000000000200002517894393 6b585b65ba93c02b58dd3f4c606bdf5
ff6df000f8e94b444f86da9845118a00b8a9e9d6c529357379de4d00ba5a522eb705a4
62981f0400000000000020000000000017a1fcca041e1a49eb397bb022386badbfcb5
bc2dc7fdec033a770780a955c7325da2fc01dab0882ce7c7ade78ffbfc03a879e808d6
86e158feefa403d30b242cfbeeca90c4556600687dd24ffa11d798119680001cd4c967
7c6dc0876eb08802497fe9138fb465e24946000196f31ab93a9a14d066a32d002fd76f
6e24dbf205f9b4080000000000000000400000000039f5770ecfe0fcc73601063004e06
402cd7085ed553f8800184018c64828e05bc8ba12000f084dc03f103e96043677600c3
e1c4de070348500301520357c958a8a4225a5c86fd4f01ad5f7d20174a7d75ea9b8c01
fc996c45dba60e2191e9f8023236eec4a54d71e2b4c695000000000000000000000100
008db246056f066abe6af8f8023334bda1db5a6aa0d30a8d01a922bee2da5013a1de63
6f000000000000000000000800000329a9ee65bbde74979e643301181b19252d22bcaa1c
669501a58243003b90c596a6e9e403a8a0ac379a01919db821ac03009bf301a3b48596
1125b80247419bc60c0642b547389d02a8c875f2a2be00108104a900369e99f62a5c08
```

```
02bf4a9000c464e9fd5cbc19876b1e920105cf6bd3b9b2129df09f2f03848921cb27bf
c8c70ecb1d03adb157b1891ee4be900e92003e405f6dd4038e9edc3b49001169e36953
ab0fccececdc03580f881c7c3e7fdd2e6f7903ac7ccf7b13fd8df40a5b210086640453
105b19a9cc7ef6009e568e2b83f6b627997e930218c69d00c44a8b8e330a3e00000000
000002000000000003c988becd860b1f106cc6200f408a11567165c2eb99aea020a8f
2f6a88f349cb6a489002c230e7da1807c3e8310c80033517b57556ba80fef35d420238
e60c4bf153b8a1aa9969031940360e0729cd5347424a0274b4eb82e722235305cbda00
628fcf9cb00be1bfb369880000000800000000000000043a70d5a95749a87013d4f
000000000000008000000000027e15ebca5ec05435647cae00aa0134e2a80199f5a134
4400e25f1328d8d0fa759d8b6c034a839b6c674b39e17ddc410262814eae5b6650bfac
4af20228f4e2ab4cccd6d2bdd9290130852908e2a2404d5cab1d013811f2225fd89d60
275bb0031440020729c2de16c3e29e00c274ea8093932eaad3297a0339df989d6446f0
ee2bb92e02ebe2b70e353cb19b0587a80302c101b6ca14d6d78ddc8f017e29a0834a4f
642b10d11f02fb4698299d7176bd180cd90264b9b5bdda4f2865ab1c670110d16339f9
bfd5dd531b2801650a418d87e293ea249680033d2cfd56147f4795dddd2902d6297d98
b057e47667f3ae007e98ec7adf72dccd0b0a660000000000000000008000000157707d
3a7413962206f18703c4db46680891b1b9510c170289b12fe285bda753707dc602e2ae
1860ee46699cbc3e9e01ef57904ed4466f7ed72c190000000000000000000000200300
aeea0e341cf5daa00a1a01e3a839067bb83ca781436203a054639f2c11600d29364700
64e1ac87df0d0a5a96cfbe018acb0d62bfa7fdd69e39020032182a41e627dac328911f
00e97e3af5894569263579c703342e4becd416834d62b20403b1707dadddea172925ef
7b020b48b4fd134d7f82c9179e00a040c35ca9e8a9c5c4c039037d5ddeebdeb129bc73
fa4a02b24277f00ef7a17df8b51b000010000000000000000000098d22cbea686f62a
3d15c602638f96c47f24881d13505d032322450740d86e78e549cd00ec20e70d401378
e6cfbfa402e98a8bf923516538a0a556039ca28ae588a040f0d23c77033d3eacccb940
fc8534fde500000000020000000000000003136d79ef6b69ed08f214af0000221a9ab3
50b38aabbb9302be67109aa69557c5d9a313010bb20f860762441a4b1cfa03b545695c
f60c5b89b1e91f013db9b78468b3a9533b44f102bc19be301294626a9fcef200000002
000000000000000001a4414640a82db46c3b553c
```

Wer ist der Verfasser des Gedichts? (Hinweis: Entschlüssle die Teile, bei denen im Ciphertext viele Nullen auftreten.)

**Aufgabe 46:** Sei $d \in \mathbf{Z}$, $d < 0$, $d$ quadratfrei, $f \in \mathbf{N}$ und

$$\Lambda = \begin{cases} \mathbf{Z} + \mathbf{Z} f \frac{1+\sqrt{d}}{2} & d \equiv 1 \bmod 4, \\ \mathbf{Z} + \mathbf{Z} f \sqrt{d} & d \equiv 2, 3 \bmod 4. \end{cases}$$

Bestimme den Endomorphismenring $\mathrm{End}(\mathbf{C}/\Lambda)$.

**Aufgabe 47:** Sei $d$ eine quadratfreie ganze Zahl $\neq 0, 1$, d.h.

$$d \in \{-1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \dots\}.$$

Ein Unterring $R$ von $\mathbf{Q}(\sqrt{d})$ heißt Ordnung, wenn es endlich viele Elemente $\omega_1, \dots, \omega_r \in \mathbf{Q}(\sqrt{d})$ gibt mit

$$R = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_r$$

und $R \neq \mathbf{Z}$ gilt. Zeige, dass jede Ordnung in $\mathbf{Q}(\sqrt{d})$ die Form $R = \mathbf{Z} + \mathbf{Z} f \omega$ mit einer natürlichen Zahl $f$ und

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{für } d \equiv 1 \bmod 4 \\ \sqrt{d} & \text{für } d \equiv 2 \bmod 4 \text{ oder } d \equiv 3 \bmod 4 \end{cases}$$

hat.

**Aufgabe 48:** Das 5-te Teilungspolynom ist

$$\begin{aligned}\psi_5 \;=\;& 5x^{12}+62ax^{10}+380bx^9-105a^2x^8+240abx^7+(-300a^3-240b^2)x^6-696a^2bx^5\\ &+(-125a^4-1920ab^2)x^4+(-80a^3b-1600b^3)x^3+(-50a^5-240a^2b^2)x^2\\ &+(-100a^4b-640ab^3)x+(a^6-32a^3b^2-256b^4).\end{aligned}$$

(1) Zeige, dass die Diskriminante von $\psi_5$ bzgl. der Variablen $x$

$$2^{88}\cdot 5^{11}\cdot(4a^3+27b^2)^{22}$$

ist.

(2) Leite eine Bedingung her, wann für eine über einem Körper $K$ der Charakteristik 5 durch $y^2=x^3+ax+b$ definierte elliptische Kurve $E$ gilt $E(\overline{K})[5]=\{O\}$.

**Aufgabe 49:** In Charakteristik 11 ist eine durch $y^2=x^3+ax+b$ definierte elliptische Kurve $E$ genau dann supersingulär, wenn $a=0$ oder $b=0$ gilt. (Hinweis: Untersuche $\psi_{11}$ mod 11.)

**Aufgabe 50:** In Charakteristik 13 ist eine elliptische Kurve $E$ genau dann supersingulär, wenn $j(E)=5$ gilt. (Hinweis: Untersuche $\psi_{13}$ mod 13.)

**Aufgabe 51:** Sei $E$ eine über $\mathbf{F}_p$, $p\geq 5$, definierte elliptische Kurve. Dann gilt für alle $n\geq 1$

$$|\#E(\mathbf{F}_{p^n})-(p^n+1)|\leq 2\sqrt{p^n}.$$

**Aufgabe 52:** Sei $E$ eine über $\mathbf{F}_p$, $p\geq 5$, definierte elliptische Kurve. Zeige:

(1) Für die Anzahl der $\mathbf{F}_{p^2}$-rationalen Punkte gilt die Abschätzung

$$p^2+1-2p<\#E(\mathbf{F}_{p^2})\leq p^2+1+2p.$$

(2) Es gilt die Äquivalenz:

$$\#E(\mathbf{F}_{p^2})=p^2+1+2p \quad\Longleftrightarrow\quad E \text{ ist supersingulär.}$$

**Aufgabe 53:**

(1) Ist $p\geq 5$ eine Primzahl der Gestalt

$$p=\frac{1+11n^2}{4} \quad \text{mit} \quad n\in\mathbf{N},$$

ist $E$ eine über $\mathbf{F}_p$ durch die Gleichung $y^2=x^3+ax+b$ definierte elliptische Kurve mit $j$-Invariante

$$j(E)=-32768,$$

ist $u\in\mathbf{F}_p^*$ mit $\left(\frac{u}{p}\right)=-1$, und wird $E'$ definiert durch die Gleichung $y^2=x^3+au^2x+bu^3$, so gilt

$$\#E(\mathbf{F}_p)=p \quad \text{oder} \quad \#E'(\mathbf{F}_p)=p.$$

(2) Konstruiere Beispiele für die Situation in 1. Gibt es unendlich viele solcher Beispiele?

**Aufgabe 54:** Ist $E$ eine durch die Gleichung $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$ über $\mathbf{Q}$ definierte elliptische Kurve, so heißt

$$E(\mathbf{Q})_{\text{Torsion}} = \cup_{n \geq 1} E(\mathbf{Q})[n]$$

die Torsionsuntergruppe von $E(\mathbf{Q})$. Der Satz von Lutz-Nagell besagt:

$$(x, y) \in E(\mathbf{Q})_{\text{Torsion}} \quad \Longrightarrow \quad x, y \in \mathbf{Z} \quad \text{und} \quad y = 0 \text{ oder } y^2 | 4a^3 + 27b^2.$$

Bestimme mit Hilfe dieses Satzes die Torsionsuntergruppe $E(\mathbf{Q})_{\text{Torsion}}$ folgender elliptischer Kurven $E$:

(1) $y^2 = x^3 - 2$
(2) $y^2 = x^3 + 8$
(3) $y^2 = x^3 + 4$
(4) $y^2 = x^3 + 4x$
(5) $y^2 = x^3 - 432x + 15120$
(6) $y^2 = x^3 + 1$
(7) $y^2 = x^3 - 16x + 8784$
(8) $y^2 = x^3 - 44091x - 9401238$
(9) $y^2 = x^3 - 219x + 1658$
(10) $y^2 = x^3 - 58347x + 3954042$
(11) $y^2 = x^3 - 33339627x - 37244470086$
(12) $y^2 = x^3 - 4x$
(13) $y^2 = x^3 - 12987x + 477306$
(14) $y^2 = x^3 - 24003x + 1059426$
(15) $y^2 = x^3 - 1386747x + 355930794$