Elliptische Kurven und Kryptographie

Wolfgang M. Ruppert

Sommersemester 1998

28. Juli 1998[1]

[1]Im Sommersemester 1998 am Mathematischen Institut der Universität Bayreuth abgehaltene Vorlesung

Inhaltsverzeichnis

Einführung 5

Kapitel 1. Affine und projektive Varietäten 7
1. Affine Varietäten 7
2. Projektive Varietäten 9
3. Rationale Abbildungen und Morphismen 12

Kapitel 2. Geometrische Addition auf ebenen Kubiken 15

Kapitel 3. Algebraische Kurven 21
1. Lokale Ringe nichtsingulärer Kurven 21
2. Divisoren 23
3. Differentialformen 24
4. Morphismen 25
5. Der Satz von Riemann-Roch 27

Kapitel 4. Elliptische Kurven 29
1. Einführung 29
2. Weierstraßgleichungen in Charakteristik $\neq 2, 3$ 32
3. Beliebige Charakteristik 35
4. Charakteristik 2 35

Kapitel 5. Isogenien 39

Kapitel 6. Endomorphismenringe elliptischer Kurven über $\mathbf{F}_q$ 45

Kapitel 7. Public-Key-Kryptographie 49
1. Einführung 49
2. RSA 50

Kapitel 8. ECM - Faktorisierung mit elliptischen Kurven 53
1. Primzahltests 53
2. Faktorisierung 55
3. Lenstras ECM-Verfahren 57

Kapitel 9. Diskrete Logarithmen 61
1. Public-Key-Kryptosysteme 61
2. Die naive Methode zur Berechnung diskreter Logarithmen 63
3. Die Baby-Step-Giant-Step-Methode nach Shanks 64
4. Pollards Monte-Carlo-Methode 64
5. Das Silver-Pohlig-Hellman-Verfahren 66
6. Die Index-Calculus-Methode 67

Kapitel 10. Kryptosysteme mit elliptischen Kurven - ECC 71

Kapitel 11. Die Weil-Paarung 77

Kapitel 12. Elliptische Kurven über $\mathbf{F}_p$ mit p Punkten 87

Kapitel 13. Wie bestimmt man $\#E(\mathbf{F}_p)$? 95
1. Punkte auf elliptischen Kurven 95
2. Elementare (naive) Bestimmung von $\#E(\mathbf{F}_p)$ 97
3. Bestimmung von $\#E(\mathbf{F}_p)$ durch Studium von $ord(P)$ 98
4. Elliptische Kurven, bei denen man Informationen über $\mathrm{End}(E)$ hat 100
5. Der Schoof-Algorithmus 105
6. Kombination des Schoof-Algorithmus mit anderen Algorithmen 114

Kapitel 14. Hyperelliptische Kryptosysteme 117

Literaturverzeichnis 123

Einführung

Elliptische Kurven sind algebraische Kurven, die sich durch eine Gleichung der Form $y^2 = x^3 + ax + b$ beschreiben lassen ($4a^3 + 27b^2 \neq 0$). 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. (Elliptische Kurven spielten auch eine entscheidende Rolle beim Beweis der Fermatschen Vermutung.)

Bei der **Kryptographie** geht es darum, eine Nachricht so zu verschlüsseln, daß ein Unbefugter nichts damit anfangen kann. Während dies früher hauptsächlich im militärischen und politischen Bereich eine Rolle spielte, ist heutzutage die Kryptographie auch im alltäglichen Leben wichtig, man denke z.B. an abhörsicheres Telefonieren mit Mobiltelefonen, an Sicherheitsmaßnahmen für Bankgeschäfte per Internet (Home Banking) und an Sicherheit beim Einsatz von Chipkarten (z.B. Telefonkarten, Krankenversichertenkarten).
Die Zahlentheorie, die Eigenschaften und Gesetzmäßigkeiten der natürlichen Zahlen studiert, war lange Zeit weit entfernt von jeder Anwendung. Dies hat sich drastisch verändert, als 1976 von Diffie und Hellman ein kryptographisches Verfahren vorgeschlagen wurde, dessen Sicherheit darauf beruht, daß man in einem endlichen Körper zwar leicht Potenzen berechnen kann, daß es aber im allgemeinen sehr schwer ist, Logarithmen zu berechnen. Kurz danach kam das RSA-Verfahren auf, dessen Sicherheit darauf beruht, daß es sehr schwer ist, bei einer großen natürlichen Zahl n die Primfaktorzerlegung zu finden. 1985 wurde von Koblitz und Miller der Vorschlag gemacht, auch elliptische Kurven für kryptographische Verfahren zu benutzen. Inzwischen werden tatsächlich elliptische Kurven in der Kryptographie verwendet.

Das vorliegende Skript gibt im wesentlichen den Inhalt der gehaltenen Vorlesung wieder, es ist parallel dazu entstanden. (Von daher gibt es sicher noch viele Fehler und Unvollständigkeiten.) Die vierstündige Vorlesung setzte Grundkenntnisse im Umfang einer Algebra-Vorlesung voraus, wollte einführen in die Theorie der elliptischen Kurven, in die Public-Key-Kryptographie und Anwendungen elliptischer Kurven in der Kryptographie behandeln.

Um ein gewisses Gefühl für die Sachen zu bekommen, wurden Beispiele gerechnet und auch einiges am Computer ausprobiert. Programmiert wurde dabei mit Maple V Release 3 oder Ubasic 8.8c, die beide Langzahlarithmetik haben. Die im Skript angegebenen Rechenzeiten beziehen sich auf ein Notebook mit einem 75 MHz-Pentium-Prozessor. Die Programme wurden explizit mit ins Skript aufgenommen, damit man einen Eindruck von ihrer Komplexität bzw. von ihrer Einfachheit erhält, sie sind in keiner Weise optimiert.

An dieser Stelle möchte ich mich auch bei den Leitern des Graduiertenkollegs Komplexe Mannigfaltigkeiten – Th. Peternell und F.-O. Schreyer – bedanken, die es mir ermöglicht haben, die Vorlesung im Rahmen des Graduiertenkollegs zu halten.

KAPITEL 1

Affine und projektive Varietäten

Wir legen im folgenden stets einen vollkommenen Körper K zugrunde, d.h. der algebraische Abschluß $\overline{K}$ ist galoissch über K. Die Galoisgruppe von $\overline{K}$ über K wird mit G_K bezeichnet.

Beispiele für vollkommene Körper:

- alle algebraisch abgeschlossenen Körper,
- alle Körper der Charakteristik 0,
- alle endlichen Körper.

Nicht vollkommen ist z.B. der Körper $\mathbf{F}_p(t)$.

1. Affine Varietäten

DEFINITION. $\mathbf{A}^n = \mathbf{A}^n(\overline{K}) = \{(x_1, \ldots, x_n) : x_i \in \overline{K}\}$ heißt n-dimensionaler affiner Raum. $\mathbf{A}^n(K) = \{((x_1, \ldots, x_n) \in \mathbf{A}^n : x_i \in K\}$ ist die Menge der K-rationalen Punkte von $\mathbf{A}^n$.

Die Galoisgruppe G_K operiert auf $\mathbf{A}^n$ durch $\sigma(x_1, \ldots, x_n) = (\sigma x_1, \ldots, \sigma x_n)$. Man erhält sofort:

$$\mathbf{A}^n(K) = \{P \in \mathbf{A}^n : \sigma P = P \text{ für alle } \sigma \in G_K\}.$$

DEFINITION. $V \subseteq \mathbf{A}^n$ heißt affine algebraische Menge, falls es Polynome $f_1, \ldots, f_r \in \overline{K}[x_1, \ldots, x_n]$ gibt mit

$$V = \{P \in \mathbf{A}^n : f_1(P) = \cdots = f_r(P) = 0\}.$$

Können $f_1, \ldots, f_r$ aus $K[x_1, \ldots, x_n]$ gewählt werden, so sagt man, daß V über K definiert ist. In diesem Fall ist $V(K) = V \cap \mathbf{A}^n(K)$ die Menge der K-rationalen Punkte von V.

Beispiel: In $\mathbf{A}^2$ benutzen wir die Koordinaten x, y. Algebraische Mengen sind

$$\{y = x^2\}, \quad \{y^2 = x^3\}, \quad \{x - 1 = y^2 - 2 = 0\} = \{(1, \sqrt{2}), (1, -\sqrt{2})\}.$$

Ein Grundproblem der Zahlentheorie ist folgendes: Sei $V \subseteq \mathbf{A}^n$ über $\mathbf{Q}$ definiert. Bestimme/beschreibe $V(\mathbf{Q})$, die Menge der $\mathbf{Q}$-rationalen Punkte von V.

Beispiel: Sei p eine Primzahl und $V \subseteq \mathbf{A}^2$ gegeben durch die Gleichung $x^p + y^p = 1$. Dann ist

$$V(\mathbf{Q}) = \{(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}) : t \in \mathbf{Q}\} \text{ für } p = 2$$

und

$$V(\mathbf{Q}) = \{(0, 1), (1, 0)\} \text{ für } p > 2$$

(gemäß der Fermatschen Vermutung).

Sei $V \subseteq \mathbf{A}^n$ über K definiert durch Gleichungen $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. Sei $P \in V$ und $\sigma \in G_K$. Dann gilt $f_i(P) = 0$ und damit $0 = \sigma(f_i(P)) = f_i(\sigma P)$ für alle i, d.h. es gilt auch $\sigma P \in V$. Die Galoisgruppe G_K operiert also auf V. Es ist dann klar, daß gilt:

$$V(K) = \{P \in V : \sigma P = P \text{ für alle } \sigma \in G_K\}.$$

Beispiel: Die algebraische Menge $V = \{x = 1, y^2 = 2\} = \{(1, \sqrt{2}), (1, -\sqrt{2})\} \subseteq \mathbf{A}^2$ ist über $\mathbf{Q}$ definiert, aber $V(\mathbf{Q}) = \emptyset$. Ist $\sigma \in G_{\mathbf{Q}}$ mit $\sigma\sqrt{2} = -\sqrt{2}$, so vertauscht σ die beiden Punkte von V.

DEFINITION. Eine Menge $V \subseteq \mathbf{A}^n$ heißt eine affine Varietät, falls es Polynome $f_1, \ldots, f_r \in \overline{K}[x_1, \ldots, x_n]$ gibt, so daß $V = \{f_1 = \cdots = f_r = 0\}$ gilt und $(f_1, \ldots, f_r) \subseteq \overline{K}[x_1, \ldots, x_n]$ ein Primideal ist. Ist V über K definiert, so heißt $K[V] = K[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ der affine Koordinatenring von V über K; dieser ist ein Integritätsring; sein Quotientenkörper heißt der Funktionenkörper $K(V)$ von V über K. Analog definiert man $\overline{K}[V]$ und $\overline{K}(V)$.

Beispiele:

1. Ein Polynom $f \in \overline{K}[x, y]$ ist genau dann irreduzibel, wenn $(f) \subseteq \overline{K}[x, y]$ ein Primideal ist. Ist also $f(x, y) \in \overline{K}[x, y]$ irreduzibel, so ist $\{f = 0\}$ eine affine Varietät.
2. $\mathbf{A}^n$ ist eine Varietät und $K[\mathbf{A}^n] = K[x_1, \ldots, x_n]$, $K(\mathbf{A}^n) = K(x_1, \ldots, x_n)$.

Bemerkung: $V \subseteq \mathbf{A}^n$ werde durch die Polynome $f_1, \ldots, f_r$ beschrieben, so daß für den affinen Koordinatenring $\overline{K}[V] = \overline{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ gilt. Ein $F \in \overline{K}[V]$ wird gegeben durch ein Polynom $f \in \overline{K}[x_1, \ldots, x_n]$. Ist g ein anderes Polynom, das F repräsentiert, so gibt es Polynome $h_1, \ldots, h_r$ mit $g - f = f_1 h_1 + \cdots + f_r h_r$. Für einen Punkt $P \in V$ folgt dann $f(P) = g(P)$. Also definiert F durch $V \to \overline{K}, P \mapsto f(P)$ eine Funktion auf V.

DEFINITION. Die Dimension einer Varietät V ist der Transzendenzgrad von $\overline{K}(V)$ über $\overline{K}$. Wir schreiben dafür auch $\dim V$. (D.h. es gibt einen Körperhomomorphismus $\varphi : \overline{K}(t_1, \ldots, t_d) \to \overline{K}(V)$, so daß $\overline{K}(V)$ über $\varphi(\overline{K}(t_1, \ldots, t_d))$ algebraisch ist und $d = \dim V$.) Eine Varietät der Dimension 1 heißt Kurve.

Beispiele:

1. Sei $f(x, y) \in \overline{K}[x, y]$ irreduzibel mit $\deg_y f \geq 1$. In $Quot(\overline{K}[x, y]/(f(x, y))$ ist y algebraisch über $\overline{K}(x)$, also ist $\dim\{f = 0\} = 1$.
2. Sei $V = \{y^2 = xz - x, z = x^2\} \subseteq \mathbf{A}^3$. Dann ist V eine Varietät (Übung!) der Dimension 1, denn y und z sind im Funktionenkörper $\overline{K}(V)$ von x algebraisch abhängig.

DEFINITION. Sei V eine durch $f_1, \ldots, f_r \in \overline{K}[x_1, \ldots, x_n]$ definierte Varietät in $\mathbf{A}^n$, so daß also $(f_1, \ldots, f_r)$ ein Primideal ist, und $P \in V$. Dann heißt V glatt oder nichtsingulär in P, falls für den Rang der Jacobi-Matrix gilt

$$Rang((\frac{\partial f_i}{\partial x_j}(P))_{i,j}) = n - \dim V.$$

Andernfalls heißt P singulärer Punkt von V. Sind alle Punkte von V glatt, so heißt V glatt oder nichtsingulär.

Beispiele:

1. Bei einer Kurve $\{f = 0\} \subseteq \mathbf{A}^2$ ist die Jacobi-Matrix $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$, also ist $P \in C$ genau dann singulär, wenn $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$ ist.
2. Die Neilsche Parabel $y^2 = x^3$ wird beschrieben durch $f = y^2 - x^3$. Nun ist $\frac{\partial f}{\partial x} = -3x^2$ und $\frac{\partial f}{\partial y} = 2y$. Ist also $char(K) \neq 2, 3$, so ist C genau in $P = (0, 0)$ singulär.
3. $V = \{y^2 = xz - z, z = x^2\} \subseteq \mathbf{A}^3$ ist eine glatte Kurve. (Übung!)

Singularitäten ebener Kurven: Sei $C = \{f(x, y) = 0\} \subseteq \mathbf{A}^2$ eine Kurve und $P = (0, 0)$. Ist $f = \sum_{i,j} a_{ij} x^i y^j$, so ist $f_\ell = \sum_{i+j=\ell} a_{ij} x^i y^j$ der homogene Anteil vom Grad ℓ. Dann kann man schreiben

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

m heißt die Multiplizität von C in P.

- $m = 0$: Dann ist $P \notin C$.
- $m = 1$: Dann ist P glatter Punkt von C. Der lineare Anteil $f_1 = ax + by$ liefert die Tangente $ax + by = 0$ von C in P. Es ist $a = \frac{\partial f}{\partial x}(P)$, $b = \frac{\partial f}{\partial y}(P)$.
- $m \geq 2$: Dann ist C singulär in P. Man kann faktorisieren

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

Die Geraden $\alpha_i x + \beta_i y = 0$ werden ebenfalls Tangenten von C in P genannt.

DEFINITION. Sei V eine Varietät und $P \in V$. Dann ist $M_P = \{f \in \overline{K}[V] : f(P) = 0\}$ ein maximales Ideal. Die Lokalisierung von $\overline{K}[V]$ in M_P heißt der lokale Ring von V in P:

$$\overline{K}[V]_P = \{\frac{f}{g} \in \overline{K}(V) : f, g \in \overline{K}[V], g(P) \neq 0\}.$$

Für $\varphi \in \overline{K}[V]_P$ ist $\varphi(P)$ wohldefiniert. Die Funktionen aus $\overline{K}[V]_P$ heißen regulär oder definiert in P.

Beispiel: Sei $V = \{y^2 = x^3\}$ und $\varphi = \frac{y}{x}, \psi = \frac{y^2}{x^2} \in \overline{K}(V)$. Dann ist ψ definiert in $P = (0,0)$, denn in $\overline{K}(V)$ kann man auch schreiben

$$\psi = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x.$$

Man zeige, daß φ nicht in P definiert ist.

2. Projektive Varietäten

Projektive Räume sollen affine Räume vervollständigen bzw. kompaktifizieren.

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

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

Die Äquivalenzklasse von $(a_0, \ldots, a_n)$ 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 $\mathbf{P}^n = \{(a_0 : \cdots : a_n) : (a_0, \ldots, a_n) \in \overline{K}^n \setminus \{0\}\}$. Wie im affinen Fall definiert man die Menge der K-rationalen Punkte von $\mathbf{P}^n$ durch

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

Beispiel: $\mathbf{P}^1 = \{(1 : a) : a \in \overline{K}\} \cup \{(0 : 1)\}$.

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.

Wie im affinen Fall operiert G_K auf $\mathbf{P}^n$ und $\mathbf{P}^n(K) = \{P \in \mathbf{P}^n : \sigma P = P \text{ für alle } \sigma \in G_K\}$.

DEFINITION. Ein Polynom $f \in \overline{K}[x_0, x_1, \ldots, x_n]$ heißt homogen vom Grad d, falls für alle $\lambda \in \overline{K}$ gilt $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$. Äquivalent dazu ist, daß f sich schreiben läßt als

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

Ein homogenes Polynom f vom Grad d erfüllt die Eulersche Relation

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

Bemerkung: Sei $P = (a_0 : \cdots : a_n) = (b_0 : \cdots : b_n) \in \mathbf{P}^n$ und f homogen vom Grad d. Dann gibt es ein $\lambda \in \overline{K}^*$ mit $a_i = \lambda b_i$ und daher

$$f(a_0, \ldots, a_n) = \lambda^d f(b_0, \ldots, b_n).$$

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

DEFINITION. Eine Teilmenge $V \subseteq \mathbf{P}^n$ heißt projektive algebraische Menge, falls es homogene Polynome $f_1, \ldots, f_r \in \overline{K}[x_0, \ldots, x_n]$ gibt mit

$$V = \{P \in \mathbf{P}^n : f_1(P) = \cdots = f_r(P) = 0\}.$$

V heißt über K definiert, falls $f_1, \ldots, f_r \in K[x_0, \ldots, x_n]$ gewählt werden können. Dann ist $V(K) = V \cap \mathbf{P}^n(K)$ die Menge der K-rationalen Punkte von V.
V heißt projektive Varietät, falls die $f_1, \ldots, f_r$ so gewählt werden können, daß $(f_1, \ldots, f_r)$ ein Primideal in $\overline{K}[x_0, \ldots, x_n]$ ist.

Beispiele:

1. Eine Gerade in $\mathbf{P}^2$ ist eine algebraische Menge, die durch eine lineare Gleichung $a_0x_0 + a_1x_1 + a_2x_2 = 0$ gegeben wird mit $(a_0, a_1, a_2) \neq 0$.
2. Eine Hyperebene im $\mathbf{P}^n$ wird durch eine lineare Gleichung $a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0$ mit $(a_0, a_1, \ldots, a_n) \neq 0$ gegeben.
3. Je zwei Geraden im $\mathbf{P}^2$ schneiden sich, denn für $P = (p_0 : p_1 : p_2) \in \mathbf{P}^2$ gilt

$$P \in \{a_0x_0 + a_1x_1 + a_2x_2 = 0\} \cap \{b_0x_0 + b_1x_1 + b_2x_2 = 0\} \iff \begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \end{pmatrix} = 0$$

und das lineare Gleichungssystem hat eine nichttriviale Lösung, da der Rang der Matrix ≤ 2 ist.

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

$$\phi_i : \mathbf{A}^n \to \mathbf{P}^n, \quad (a_1, \ldots, a_n) \mapsto (a_0 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_n).$$

ϕ_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

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

Also $U_i \simeq A^n$ und $H_i \simeq \mathbf{P}^{n-1}$. Der projektive Raum $\mathbf{P}^n$ wird überdeckt von den affinen Mengen $U_0, \ldots, U_n$.
Sei $V = \{P \in \mathbf{P}^n : f_1(P) = \cdots = f_r(P) = 0\}$ eine algebraische Menge. Dann ist

$$V \cap U_0 \simeq \{(x_1, \ldots, x_n) \in \mathbf{A}^n : f_1(1, x_1, \ldots, x_n) = \cdots = f_r(1, x_1, \ldots, x_n) = 0\}$$

eine affine Teilmenge von U_0 (unter Benutzung der Bijektion $\phi_i : \mathbf{A}^n \simeq U_i$).

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

$$\tilde{f}(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$$

ein homogenes Polynom vom Grad d.

DEFINITION. Sei $V = \{f_1 = \cdots = f_r = 0\} \subseteq \mathbf{A}^n$ eine affine algebraische Menge. Dann heißt

$$\overline{V} = \{P \in \mathbf{P}^n : \tilde{f}_1(P) = \cdots = \tilde{f}_r(P) = 0\}$$

der projektive Abschluß von V.

Beispiel: Wir betrachten die Parabel $f = y - x^2 = 0$ in $\mathbf{A}^2$. Betrachten wir $\mathbf{A}^2$ als U_0, so können wir die Gleichung $f = x_2 - x_1^2 = 0$ schreiben. Der projektive Abschluß wird dann gegeben durch $\tilde{f} = x_0^2(\frac{x_2}{x_0} - \frac{x_1^2}{x_0^2}) = x_0x_2 - x_1^2$. Im affinen Teil U_1 (mit $x_1 = 1$) wird daraus die Hyperbel $x_0x_2 = 1$, im affinen Teil U_2 (mit $x_2 = 1$) wieder eine Parabel $x_0 - x_1^2 = 0$. Wieviele Punkte sind durch den projektiven Abschluß hinzugekommen?

$$H_0 \cap \overline{V} = \{(0 : x_1 : x_2) \in \mathbf{P}^2 : x_1^2 = 0\} = \{(0 : 0 : 1)\}.$$

Wir denken uns im folgenden oft $\mathbf{A}^n \subseteq \mathbf{P}^n$, wo wir $\mathbf{A}^n$ mit U_0 identifizieren.

SATZ. 1. *Ist $V \subseteq \mathbf{A}^n$ eine affine Varietät, so ist $\overline{V} \subseteq \mathbf{P}^n$ eine projektive Varietät und $V = \overline{V} \cap \mathbf{A}^n$.*
2. *Ist $V \subseteq \mathbf{P}^n$ eine projektive Varietät, so ist entweder $V \cap \mathbf{A}^n = \emptyset$ oder $V \cap \mathbf{A}^n$ eine affine Varietät und $V = \overline{V \cap \mathbf{A}^n}$.*
3. *Ist V affin und über K definiert, so ist auch $\overline{V}$ über K definiert.*

Bemerkung: Wir werden oft eine affine Schreibweise benutzen, uns aber den projektiven Abschluß vorstellen. Die Punkte von V in H_0 heißen dann die unendlich fernen Punkte von V.

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

$$\phi(x_0 : \cdots : x_n) = (y_0 : \cdots : y_n) \iff A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix}.$$

ϕ ist offensichtlich bijektiv, ϕ^{-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 ϕ 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. Sei V eine projektive Varietät und $\mathbf{A}^n \subseteq \mathbf{P}^n$ mit $V \cap \mathbf{A}^n \neq \emptyset$. Dann definieren wir

$$\dim V = \dim V \cap \mathbf{A}^n \quad \text{und} \quad K(V) = K(V \cap \mathbf{A}^n).$$

Ist $P \in V$ und $\mathbf{A}^n$ geeignet mit $P \in \mathbf{A}^n \subseteq \mathbf{P}^n$, so heißt P nichtsingulär, falls $P \in V \cap \mathbf{A}^n$ nichtsingulär ist. Der lokale Ring von V in P wird durch

$$\overline{K}[V]_P = \overline{K}[V \cap \mathbf{A}^n]_P$$

definiert.

Natürlich muß man sich überlegen, daß diese Begriffe dann auch unabhängig von der Auswahl $\mathbf{A}^n \subseteq \mathbf{P}^n$ sind.

Beispiel: Sei $f(x_0, x_1, x_2) \in \overline{K}[x_0, x_1, x_2]$ irreduzibel und homogen vom Grad d. Dann ist $C = \{P \in \mathbf{P}^2 : f(P) = 0\}$ eine ebene Kurve vom Grad d. Ein Punkt $P \in C$ ist 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 $P \in C$ nichtsingulär, so ist

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

die Tangente in P an C. Ist $P = (p_0 : p_1 : p_2) \in C$ mit $p_0 \neq 0$, so identifizieren wir oft auch P mit dem Punkt $(\frac{p_1}{p_0}, \frac{p_2}{p_0}) \in \mathbf{A}^2$, d.h. wir schreiben $(p_0 : p_1 : p_2) \simeq (\frac{p_1}{p_0}, \frac{p_2}{p_0})$.

Wir wollen jetzt noch Schnitte von Kurven mit Geraden in $\mathbf{P}^2$ betrachten.

DEFINITION. Sei L eine Gerade, C eine Kurve in $\mathbf{P}^2$ und $P \in \mathbf{P}^2$ ein Punkt mit $P \in L$. Nach Koordinatenwechsel können wir o.E. $P = (0,0)$, $L = \{y = \alpha x\}$, $C = \{f(x,y) = 0\}$ schreiben. Dann ist

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

Schreibt man

$$f(x, \alpha x) = x^m g(x) \text{ mit } g(x) \in \overline{K}[x] \text{ und } g(0) \neq 0,$$

so heißt m die Schnittmultiplizität von L mit C in P. Wir schreiben dafür auch $(L \cdot C)_P$.

Beispiel: Wir betrachten den Schnitt von $y = x^n$ mit $y = 0$ in $(0,0)$. Die Kurve wird beschrieben durch $f(x,y) = y - x^n = 0$, einsetzen von $y = 0$ in $f(x,y)$ ergibt $f(x,0) = -x^n$, also ist die Schnittmultiplizität n.

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

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

d.h. L schneidet C in genau d Punkten, wenn man mit Multiplizitäten zählt.

LEMMA. *Jedes homogene Polynom $f(x_0, x_1) \in \overline{K}[x_0, x_1]$ zerfällt in Linearfaktoren.*

Beweis: Sei $f = \sum_i a_i x_0^{d-i} x_1^i$ und o.E. $a_d \neq 0$ (sonst kann man x_1 sofort abspalten). Dann zerfällt $f(1,x)$ über $\overline{K}$ in Linearfaktoren:

$$f(1,x) = a_d(x-\alpha_1)\dots(x-\alpha_d),$$

woraus sofort folgt

$$f(x_0,x_1) = x_0^d f(1,\frac{x_1}{x_0}) = x_0^d a_d(\frac{x_1}{x_0}-\alpha_1)\dots(\frac{x_1}{x_0}-\alpha_d) = a_d(x_1-\alpha_1 x_0)\dots(x_1-\alpha_d x_0).\blacksquare$$

Beweis des Satzes: Sei o.E. $L = \{x_2 = \alpha x_0 + \beta x_1\}$ und $C = \{f(x_0,x_1,x_2) = 0\}$. Dann faktorisiert nach dem Lemma

$$f(x_0,x_1,\alpha x_0+\beta x_1) = c x_0^{n_0} \prod_i (x_1-\alpha_i x_0)^{n_i}.$$

Es ist $\sum_i n_i = d$, n_0 ist die Schnittmultiplizität von L mit C in $(0:1:\beta)$, n_i die Schnittmultiplizität in $(1:\alpha_i:\alpha+\beta\alpha_i)$. $\blacksquare$

Der Satz ist ein Spezialfall des Satzes von Bezout.

SATZ. *Ist $P \in C$ nichtsingulär, L die Tangente in P an C, so ist die Schnittmultiplizität $(L\cdot C)_P \geq 2$.*

Beweis: O.E. $P = (0,0)$, $f = ax + by +$ Terme höheren Grades. Die Tangente ist dann $ax+by = 0$. O.E. $b \neq 0$. Dann ist die Tangente $y = -\frac{a}{b}x$. Mit

$$f(x,-\frac{a}{b}x) = ax + b(-\frac{a}{b}x) + \text{ Terme höheren Grades } = x^2(\dots)$$

folgt die Behauptung. $\blacksquare$

DEFINITION. Sei $C \subseteq \mathbf{P}^2$ eine ebene Kurve und $P \in C$ ein glatter Punkt. P heißt Wendepunkt von C, falls für die Tangente L in P an C gilt $(L\cdot C)_P \geq 3$. In diesem Fall heißt L auch Wendetangente.

DEFINITION. Sei $C = \{f(x_0,x_1,x_2) = 0\}$ eine ebene Kurve. Definiert man

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

Dann heißt

$$H_C = \{H(f) = 0\}$$

die Hessesche von C.

SATZ. *Sei C eine Kurve und $P \in C$ ein glatter Punkt. Genau dann ist P ein Wendepunkt, wenn auch $P \in H_C$ gilt.*

3. Rationale Abbildungen und Morphismen

DEFINITION. Seien $V \subseteq \mathbf{P}^m$ und $W \subseteq \mathbf{P}^n$ Varietäten. Eine rationale Abbildung $\phi : V \to W$ wird gegeben durch $f_0,\dots,f_n \in \overline{K}(V)$, nicht alle 0, so daß $\phi(P) = (f_0(P):\dots:f_n(P)) \in W$, falls alle f_i in P definiert sind. Wir schreiben auch $\phi = (f_0:\dots:f_n)$.

Beispiel: Wir betrachten $C_1 = \{y^2 = x^3+x+2\} \subseteq \mathbf{P}^2$ und $C_2 = \{y^2 = x^3-59x-138\} \subseteq \mathbf{P}^2$. Dann liefert

$$(x,y) \mapsto (\frac{x^4-x^3+11x^2+9x+12}{(x-1)^2(x+1)}, \frac{y(x+3)(x^4-4x^3-2x^2-20x-7)}{(x-1)^3(x+1)^2})$$

eine rationale Abbildung $\phi : C_1 \to C_2$.

DEFINITION. Eine rationale Abbildung $\phi : V \to W$ heißt in $P \in V$ definiert, falls es ein $g \in \overline{K}(V)$ gibt, so daß $((gf_0)(P):\dots:(gf_n)(P))$ sinnvoll definiert ist.
Eine rationale Abbildung $\phi : V \to W$ heißt Morphismus, falls sie in allen Punkten $P \in V$ definiert ist.
Ein Isomorphismus $\phi : V \to W$ ist ein Morphismus, so daß es einen Morphismus $\psi : W \to V$ gibt mit $\phi\circ\psi = id_W$ und $\psi\circ\phi = id_V$.
Sind V und W über K definiert, so heißt eine rationale Abbildung $\phi = (f_0:\dots:f_n) : V \to W$ über K definiert, falls es $g \in \overline{K}(V)$ gibt mit $gf_0,\dots,gf_n \in K(V)$. Analoge Definition für Morphismen und Isomorphismen.

Beispiel: $C = \{y^2 = x^3 - x\} \subseteq \mathbf{P}^2$ ist über $\mathbf{Q}$ definiert, $(x, y) \mapsto (-x, iy)$ liefert eine rationale Abbildung $C \to C$, die nicht über $\mathbf{Q}$ definiert ist.

Beispiel: Wir betrachten die durch $y^2 = x^3 - x$ definierte ebene Kurve $C \subseteq \mathbf{P}^2$. Wir definieren eine rationale Abbildung $\phi : C \to \mathbf{P}^1$ durch $\phi = (1 : \frac{x}{y})$. Da wir auch $\phi = (y : x)$ schreiben können, ist offensichtlich ϕ in allen endlichen Punkten von C definiert. Im Unendlichen gibt es auf C nur einen Punkt, nämlich $(0 : 0 : 1)$. Wir verwenden affine Koordinaten u, v mit $(u : v : 1) = (x_0 : x_1 : x_2)$. Projektiv lautet die Kurve $x_0 x_2^2 = x_1^3 - x_0^2 x_1$, in u, v-Koordinaten also $u = v^3 - u^2 v$. Wegen $(1 : x : y) = (x_0 : x_1 : x_2) = (u : v : 1) = (1 : \frac{v}{u} : \frac{1}{u})$ gilt im Funktionenkörper $x = \frac{v}{u}$ und $y = \frac{1}{u}$. Damit erhält man

$$\phi = (x : y) = (\frac{v}{u} : \frac{1}{u}) = (v : 1),$$

so daß ϕ im unendlich fernen Punkt (mit den Koordinaten $(u, v) = (0, 0)$) definiert ist und den Wert $(0 : 1)$ hat. Also ist ϕ in allen Punkten von C definiert und damit ein Morphismus.

Bemerkung: Jedes $f \in \overline{K}(V)$ definiert eine rationale Abbildung $V \to \mathbf{P}^1$ durch $(1 : f)$, die wir ebenfalls mit f bezeichnen.

Bemerkung: Sind V und W über K isomorph, so gibt es eine Bijektion $V(K)$ mit $W(K)$.

Beispiel: $C = \{x^2 + y^2 = 1\} \subseteq \mathbf{P}^2$. Dann liefert die Funktion $\frac{y-1}{x}$ einen Isomorphismus $C \to \mathbf{P}^1$, der über $\mathbf{Q}$ definiert ist. Die Umkehrabbildung ist $t \mapsto (-\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2})$. Insbesondere ist $C(\mathbf{Q}) \simeq \mathbf{P}^1(\mathbf{Q})$, genauer:

$$C(\mathbf{Q}) = \{(t_0^2 + t_1^2 : -2t_0 t_1 : t_0^2 - t_1^2) : (t_0 : t_1) \in \mathbf{P}^1(\mathbf{Q})\}.$$

Beispiel: $C = \{x^2 + y^2 = 3\} \subseteq \mathbf{P}^2$. Dann ist $C(\mathbf{Q}) = \emptyset$, denn angenommen, es wäre $(a : b : c) \in C(\mathbf{Q})$, so o.E. $a, b, c \in \mathbf{Z}$ mit ggT 1 und $3a^2 = b^2 + c^2$. Betrachtung modulo 3 liefert $b \equiv c \equiv a \equiv 0 \bmod 3$, einen Widerspruch. Insbesondere ist C nicht zu $\mathbf{P}^1$ über $\mathbf{Q}$ isomorph.

Literatur: [**13**], [**2a**].

KAPITEL 2

Geometrische Addition auf ebenen Kubiken

Sei $C \subseteq \mathbf{P}^2$ eine über K definierte ebene Kubik. C wird gegeben durch eine Gleichung $f = 0$ mit

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + \cdots + a_9x_2^3$$

oder in affiner Form

$$\tilde{f} = a_0 + a_1x + a_2y + a_3x^3 + \cdots + a_9y^3$$

mit $a_0, \ldots, a_9 \in K$. (Dabei ist $\tilde{f}(x,y) = f(1,x,y)$ und $f(x_0,x_1,x_2) = x_0^3\tilde{f}(\frac{x_1}{x_0}, \frac{x_2}{x_0})$.)

Eine Gerade $L \subseteq \mathbf{P}^2$ wird gegeben durch eine Gleichung $b_0x_0 + b_1x_1 + b_2x_2 = 0$ (oder affin durch $b_0 + b_1x + b_2y = 0$) und ist entweder in C enthalten (und damit C reduzibel) oder schneidet C richtig gezählt in genau drei Punkten $P_1, P_2, P_3 \in \mathbf{P}^2$, wofür wir dann auch schreiben

$$L \cdot C = P_1 + P_2 + P_3,$$

(d.h. $\mathcal{L} \cdot C$ ist der Geradenschnitt (L) auf C). Explizit: Ist $b_2 \neq 0$, so o.E. $b_2 = -1$, d.h. L ist gegeben durch $x_2 = b_0x_0 + b_1x_1$. Der Schnitt mit C berechnet sich dann durch Einsetzen aus

$$f(x_0, x_1, b_0x_0 + b_1x_1) = 0.$$

Nun ist $f(x_0, x_1, b_0x_0 + b_1x_1) \in \overline{K}[x_0, x_1]$ homogen und kubisch, zerfällt also über $\overline{K}$ in Linearfaktoren:

$$f(x_0, x_1, b_0x_0 + b_1x_1) = (\alpha_0x_0 + \alpha_1x_1)(\beta_0x_0 + \beta_1x_1)(\gamma_0x_0 + \gamma_1x_1),$$

so daß wir

$$P_1 = (\alpha_1 : -\alpha_0 : b_0\alpha_1 - b_1\alpha_0), P_2 = (\beta_1 : -\beta_0 : b_0\beta_1 - b_1\beta_0), P_3 = (\gamma_1 : -\gamma_0 : b_0\gamma_1 - b_1\gamma_0)$$

erhalten.

Sei nun C eine nichtsinguläre über K definierte Kubik. Wir definieren eine Abbildung

$$\varphi : C \times C \to C$$

wie folgt: Sind $A, B \in C$ mit $A \neq B$, so schneidet die durch A und B gehende Gerade L die Kurve C in einem dritten Punkt P: $L \cdot C = A + B + P$. Wir setzen $\varphi(A,B) = P$. Ist $A = B$, so nehmen wir für L die Tangente in A an C, die durch die Gleichung

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

gegeben wird.
Sind $A, B \in C(K)$, so gilt auch $\varphi(A,B) \in C(K)$, wie aus obiger expliziter Berechnung ersichtlich ist.

Bemerkung: Durch $C \times C \to C$, $(A,B) \mapsto \varphi(A,B)$ wird keine Gruppenstruktur auf C definiert. (Würde durch die Verknüpfung φ eine Gruppenstruktur definiert werden, so hätte die Gleichung $\varphi(P,P) = P$ genau eine Lösung, nämlich das Nullelement der Gruppe. Die Gleichung $\varphi(P,P) = P$ beschreibt aber genau die Wendepunkte, von denen es 9 gibt.)

Wir wählen jetzt $O \in C$ und definieren eine Verknüpfung auf C durch

$$A \oplus B = \varphi(\varphi(A,B), O).$$

SATZ. *$(C, \oplus)$ ist eine abelsche Gruppe mit neutralem Element O.*

Beweisskizze:

1. $A \oplus B = B \oplus A$ ist klar.

2. Sei L die Gerade durch A und O, so daß $L \cdot C = A + O + A'$. Dann ist
$$A \oplus O = \varphi(\varphi(A, O), O) = \varphi(A', O) = A.$$
3. Sei L_0 die Tangente in O und $L_0 \cdot C = O + O + P_0$. Sei L die Gerade durch A und P_0 und $\tilde{A} \in C$, so daß $L \cdot C = A + P_0 + \tilde{A}$. Dann gilt
$$A \oplus \tilde{A} = \varphi(\varphi(A, \tilde{A}), O) = \varphi(P_0, O) = O,$$
d.h. $\tilde{A}$ ist invers zu A.
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, so daß 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 [**2**]. ■

Sind $A, B, O \in C(K)$, so auch $A \oplus B = \varphi(\varphi(A, B), O) \in C(K)$, also ist $C(K)$ eine Untergruppe von C. Damit erhalten wir:

SATZ. *Ist C eine über K definierte nichtsinguläre ebene Kubik und $O \in C(K)$, so ist $(C(K), \oplus, O)$ eine abelsche Gruppe.*

Beispiel: Die Kurve $C = \{x_0^3 = x_1^3 + x_2^3\}$, 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 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 liefern*

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

isomorphe Gruppenstrukturen auf $C(K)$.

Beweis: Wir werden später einen durchsichtigen Beweis sehen. Elementar kann man dies wie folgt beweisen: Sei $A \in C$, L die Gerade durch A und O' mit $L \cdot C = A + O' + B$, sei M die Gerade durch B und O mit $M \cdot C = B + O + A'$. Wir definieren $\lambda : C \to C$ durch $\lambda(A) = A'$. Als Übung rechne man nach, daß λ ein Gruppenisomorphismus ist. ■

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. *$P \oplus \varphi(P, O) = O$, der dritte Punkt auf der Geraden durch P und O ist der zu P inverse Punkt.*
2. *$P \oplus Q \oplus R = O$ genau dann, wenn P, Q, R von einer Geraden ausgeschnitten werden, d.h. es gibt eine Gerade L mit $L \cdot C = P + Q + R$.*
3. *P ist ein Wendepunkt genau 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. Nach 1. gilt:
$$O = \varphi(P, Q) \oplus \varphi(\varphi(P, Q), O) = \varphi(P, Q) \oplus (P \oplus Q)$$
und damit: P, Q, R schneiden Gerade aus genau dann, wenn $R = \varphi(P, Q)$, was wiederum zu $R \oplus (P \oplus Q) = O$ äquivalent ist.
3. Folgt sofort aus 2. ■

Was passiert, wenn C eine singuläre über K definierte Kubik ist?
Ist C reduzibel, so enthält C immer eine Gerade als Komponente, so daß in diesem Fall φ nicht sinnvoll definiert werden kann.
Sei C nun eine irreduzible singuläre ebene Kubik. C hat genau einen singulären Punkt P_0. Ist $A \in C$ mit $A \neq P_0$ und L die Gerade durch A und P_0, so gilt $L \cdot C = A + P_0 + P_0$. D.h. wenn man mit P_0 startet, kommt man immer wieder zu P_0, was keine sinnvolle Gruppenstruktur ergeben kann. Sei $C_{ns} = C \setminus \{P_0\}$ die Menge der nichtsingulären Punkte von C. Sind $A, B \in C_{ns}$, so schneidet auch die Verbindungsgerade C wieder in einem dritten nichtsingulären Punkt, d.h. $\varphi : C_{ns} \times C_{ns} \to C_{ns}$ ist sinnvoll definiert. Damit erhält man:

SATZ. *Sei C eine singuläre irreduzible ebene Kubik und $O \in C_{ns}$. Dann bildet $(C_{ns}, O, \oplus)$ mit der Verknüpfung $A \oplus B = \varphi(\varphi(A, B), O)$ eine abelsche Gruppe. Ist C über K definiert und $O \in C_{ns}(K)$, so ist $C_{ns}(K)$ eine Untergruppe.*

Frage: Was kann man über die Gruppenstruktur von C_{ns} sagen?

Wie schauen über K definierte singuläre irreduzible ebene Kubiken aus? Sei $C = \{f = 0\}$ singulär in P_0. Da P_0 die einzige Singularität ist, gilt $P_0 \in C(K)$, nach Koordinatenwechsel über K können wir also $P_0 = (1 : 0 : 0) \simeq (0, 0)$ annehmen und damit

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

Man unterscheidet geometrisch zwei Fälle:

1. Zerfällt $b_0 x^2 + b_1 xy + b_2 y^2$ über $\overline{K}$ in zwei verschiedene Linearfaktoren, so hat C in P_0 einen gewöhnlichen Doppelpunkt.
2. Ist $b_0 x^2 + b_1 xy + b_2 y^2$ ein Quadrat in $\overline{K}[x, y]$, so hat C in P_0 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 $y^2 = x^3 + x^2 y$.*

Beweis: Wir nehmen die Bezeichnungen wie oben. Schon in $K[x, y]$ kann man schreiben $b_0 x^2 + b_1 xy + b_2 y^2 = \beta(\gamma x + \delta y)^2$, nach Koordinatenwechsel kann man also

$$f = by^2 + (c_0 x^3 + c_1 x^2 y + c_2 xy^2 + c_3 y^3)$$

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

$$f = (x^3 + c_1 x^2 y + c_2 xy^2 + c_3 y^3) - y^2.$$

Sei jetzt $char(K) \neq 3$. Durch $x = x' - \frac{1}{3}c_1 y$ 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

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

Speziell gilt über dem algebraischen Abschluß : $C_{ns} \simeq \overline{K}^+$.

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*

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

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, die von 3 annulliert werden, daß $\overline{K}^+$ aber nur ein Element, das von 3 annulliert wird, besitzt.

Literatur: [**2**], [**13**].

KAPITEL 3

Algebraische Kurven

In diesem Abschnitt stellen wir einige grundlegende Aussagen über algebraische Kurven zusammen.

1. Lokale Ringe nichtsingulärer Kurven

SATZ. *Sei C eine irreduzible algebraische Kurve und $P \in C$ ein nichtsingulärer Punkt. Dann ist der lokale Ring $\overline{K}[C]_P$ ein diskreter Bewertungsring, d.h. es gibt ein $t \in M_P$, so daß sich jedes $f \in \overline{K}[C]_P$, $f \neq 0$ eindeutig schreiben läßt als $f = u \cdot t^m$ mit $u \in \overline{K}[C]_P^*$, d.h. $u(P) \neq 0$ und $m \geq 0$. Jedes $f \in \overline{K}(C)_P$, $f \neq 0$ schreibt sich dann eindeutig als $f = u \cdot t^m$ mit $u \in \overline{K}[C]_P^*$, d.h. $u(P) \neq 0$ und $m \in \mathbf{Z}$. Der Exponent $v_P(f) := m$ liefert eine diskrete Bewertung und wird als Null- bzw. Polstellenordnung bezeichnet, je nachdem ob $v_P(f) > 0$ oder $v_P(f) < 0$ gilt. Definiert man noch $v_P(0) = \infty$, so gelten die Eigenschaften:*

1. *$v_P(fg) = v_P(f) + v_P(g)$,*
2. *$v_P(f+g) \geq v_P(f) + v_P(g)$ und $v_P(f+g) = v_P(f) + v_P(g)$, falls $v_P(f) \neq v_P(g)$.*

t heißt uniformisierendes Element oder Ortsuniformisierende. Statt t kann man auch jedes $t' = ut$ mit $u \in \overline{K}[C]_P^*$ wählen. Ist $C \in \mathbf{P}^2$ und $P \in C \cap \mathbf{A}^2 \subsetneq C$, $\ell(x,y) = 0$ eine von der Tangente verschiedene affine Gerade durch P, so kann man $t = \ell(x,y)$ wählen.

Beweisskizze: Wir wollen zunächst zeigen, daß das maximale Ideal M_P des lokalen Rings $\overline{K}[C]_P$ ein Hauptideal ist, d.h. von einem Element erzeugt wird. Wir betrachten nur den ebenen Fall, ziehen uns aufs Affine zurück und können $P = (0,0)$ und $C = \{f(x,y) = 0\}$ annehmen. Das maximale Ideal M_P wird von x und y erzeugt, d.h. $M_P = (x,y)$. Nach Koordinatenwechsel können wir annehmen, daß $y = 0$ die Tangente und $\ell = x$ ist. Dann ist

$$f = y + \text{Terme höheren Grades} = y(1 + g(x,y)) - x^2 h(x,y)$$

mit $g(0,0) = h(0,0) = 0$. Im lokalen Ring $\overline{K}[C]_P$ gilt dann $y(1+g(x,y)) = x^2 h(x,y)$, $(1+g(x,y))(P) = 1$, also

$$y = \frac{x^2 h(x,y)}{1 + g(x,y)} \in (x)$$

und damit $M_P = (x,y) = (x) = (t)$, was wir zeigen wollten.
Existenz: Sei $a \in \overline{K}[C]_P$. Ist $a(P) \neq 0$, so ist a Einheit in P und wir sind fertig. Ist $a(P) = 0$, so ist $a \in M_P = (t)$, d.h. $a = ta_1$ mit $a_1 \in \overline{K}[C]_P$. Wir können jetzt die gleiche Betrachtung mit a_1 statt a anstellen. Man erhält eine Folge

$$a = ta_1 = t^2 a_2 = t^3 a_3 = \ldots$$

Wegen $a_n = ta_{n+1}$ gilt $(a_n) \subset (a_{n+1})$, also

$$(a) \subset (a_1) \subset (a_2) \subset \ldots$$

Nun benutzen wir (ohne Beweis) die Tatsache, daß der lokale Ring noethersch ist, also wird die Idealfolge stationär, d.h. es gibt einen Index m mit $a_m(P) \neq 0$ und damit $a = a_m t^m$, was wir zeigen wollten.
Eindeutigkeit: Sei $ut^m = vt^n$. Ist $m = n$, sind wir fertig. Wir können also o.E. $m < n$ annehmen. Dann ist aber $u = vt^{n-m}$, was sofort den Widerspruch $0 \neq u(P) = v(P)t(P)^{n-m} = 0$ liefern würde.
Die übrigen Aussagen überlegt man sich schnell selbst. ■

Beispiel: Wir betrachten die Kurve $C \subseteq \mathbf{P}^2$, die durch $y^2 = x^3 - 1$ gegeben wird. Dann ist $C = \{x_0 x_2^2 = x_1^3 - x_0^3\}$. Der einzige Punkt im Unendlichen ist $P = (0:0:1)$. Um die Kurve dort zu untersuchen, verwenden wir affine Koordinaten u, v mit

$$(x_0 : x_1 : x_2) = (u : v : 1).$$

Die Kurvengleichung wird zu $u = v^3 - u^3$. Die Tangente in P ist also $u = 0$, damit können wir v als Ortsuniformisierende in P nehmen. Aus $u(1+u^2) = v^3$ und $(1+u^2)(P) = 1$ ersieht man dann, daß gilt

$$v_P(u) = 3 \quad \text{und} \quad v_P(v) = 1.$$

Was ist $v_P(x)$ und $v_P(y)$? Es gilt:

$$(1 : x : y) = (x_0 : x_1 : x_2) = (u : v : 1) = (1 : \frac{v}{u} : \frac{1}{u}),$$

also im Funktionenkörper $\overline{K}(C)$:

$$x = \frac{v}{u} \quad \text{und} \quad y = \frac{1}{u}$$

und damit

$$v_P(x) = v_P(v) - v_P(u) = -2 \quad \text{und} \quad v_P(y) = -v_P(u) = -3.$$

Beispiel: Für $\mathbf{P}^1 = \{(1 : x), x \in \overline{K}\} \cup \{(0 : 1)\}$ ist $x - a$ uniformisierend im Punkt $a \in \overline{K} \subseteq \mathbf{P}^1$ und $\frac{1}{x}$ uniformisierend im unendlich fernen Punkt $\infty = (0 : 1)$.

FOLGERUNG. *Sei C ein irreduzible Kurve und $P \in C$ nichtsingulär. Ist $\phi : C \to \mathbf{P}^n$ eine rationale Abbildung, so ist ϕ in P definiert. Ist C nichtsingulär, so ist ϕ ein Morphismus.*

Beweis: Eine rationale Abbildung $\phi : C \to \mathbf{P}^n$ wird gegeben durch Funktionen $f_0, \ldots, f_n \in \overline{K}(C)$, die nicht alle 0 sind:

$$\phi = (f_0 : \cdots : f_n).$$

O.E. sind alle f_i von 0 verschieden. Sei t uniformisierend in P und $f_i = u_i t^{e_i}$ mit $u_i(P) \neq 0$. Sei $e = \min(e_0, \ldots, e_n)$. Dann ist

$$\phi = (u_0 t^{e_0 - e} : \cdots : u_n t^{e_n - e})$$

und ϕ mit dieser Darstellung in P definiert. ■

LEMMA. *Sei $P \in C$ nichtsingulärer Punkt und t uniformisierend in P. Sei $n \geq 1$ fest. Dann hat jedes $f \in \overline{K}(C)$ eine eindeutige Darstellung*

$$f = \frac{a_{-N}}{t^N} + \frac{a_{-N+1}}{t^{N-1}} + \cdots + \frac{a_{-1}}{t} + a_0 + a_1 t + a_2 t^2 + \cdots + a_{n-1} t^{n-1} + g t^n$$

mit $a_i \in \overline{K}$ und $g \in \overline{K}[C]_P$.

Beweis: Wir zeigen die Behauptung zunächst für den Fall, daß f in P definiert ist. Wir machen Induktion nach n.
$n = 1$: Wähle $a_0 = f(P)$. Dann ist $(f - a_0)(P) = 0$, also $f - a_0 \in M_P$, also gibt es ein g mit $f - a_0 = gt$, wo g in P definiert ist.
Sei die Behauptung bereits bis n gezeigt. Dann haben wir

$$f = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + g t^n.$$

Wir wenden den Fall $n = 1$ auf g an und erhalten $g = a_n + ht$ und damit

$$f = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + a_n t^n + h t^{n+1}.$$

Dies zeigt die Existenzbehauptung durch Induktion. Die Eindeutigkeit ist klar. Ist nun $f \in \overline{K}(C)$ mit $v_P(f) = -N$ und $N \geq 1$, so ist ft^N definiert in P, also gibt es nach dem ersten Teil eine Darstellung

$$f t^N = b_0 + b_1 t + \cdots + b_{n+N-1} t^{n*N-1} + g t^{n+N}$$

und damit

$$f = \frac{b_0}{t^N} + \cdots + b_N + b_{N+1} t + \cdots + g t^n,$$

was wir zeigen wollten. ■

Durch Limesbildung erhält man daraus schnell den folgenden Satz:

SATZ. *Sei P ein nichtsingulärer Punkt einer Kurve C und t eine Ortsuniformisierende in P. Dann gibt es eine Inklusion*

$$\overline{K}(C) \subseteq \overline{K}((t)),$$

so daß die Bewertung v_P mit der natürlichen Bewertung auf $\overline{K}((t))$ übereinstimmt.

2. Divisoren

Sei jetzt C eine nichtsinguläre irreduzible projektive Kurve, die über einem Körper K definiert ist.

Die Divisorengruppe $\mathrm{Div}(C)$ von C ist die freie abelsche Gruppe, die von den Punkten von C erzeugt wird. Ein Divisor $D \in \mathrm{Div}(C)$ ist also eine formale Linearkombination

$$D = \sum_{P \in C} n_P P \quad \text{mit} \quad n_P \in \mathbf{Z}, n_P = 0 \text{ für fast alle } P.$$

Der Grad von D ist $\deg(D) = \sum n_P$, daher $\deg : \mathrm{Div}(C) \to \mathbf{Z}$ ein Gruppenhomomorphismus. Die Divisoren vom Grad 0 bilden eine Untergruppe

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg(C) = 0\}.$$

Die Galoisgruppe G_K operiert auf $\mathrm{Div}(C)$ und $\mathrm{Div}^0(C)$ durch $\sigma(\sum n_P P) = \sum n_P \sigma P$. Ein Divisor $D \in \mathrm{Div}(C)$ ist über K definiert, falls $\sigma D = D$ gilt für alle $\sigma \in G_K$. Sei $\mathrm{Div}_K(C)$ die Gruppe der Divisoren, die über K definiert sind und analog $\mathrm{Div}^0_K(C)$.
Ist $f \in \overline{K}(C)^*$, so heißt

$$(f) = \mathrm{div}(f) = \sum v_P(f) P$$

der zu f gehörige Hauptdivisor.

Beispiel: Wir betrachten wieder C mit der affinen Gleichung $y^2 = x^3 - 1$. Wir wollen den Hauptdivisor der Funktion x bestimmen. Im unendlich fernen Punkt $P = (0:0:1)$ wissen wir bereits $v_P(x) = -2$. Im Endlichen hat x keine Polstellen. Nullstellen sind in $P_1 = (0, i)$ und $P_2 = (0, -i)$. Da $x = 0$ weder Tangente in P_1 noch in P_2 ist, kann man x als uniformisierendes Element in P_1 und P_2 wählen, d.h. $v_{P_1}(x) = v_{P_2}(x) = 1$. Damit erhält man

$$(x) = P_1 + P_2 - 2P.$$

SATZ. *Seien $f, g \in \overline{K}(C)^*$.*

1. $(fg) = (f) + (g)$, *d.h. die Hauptdivisoren bilden eine Untergruppe von* $\mathrm{Div}(C)$.
2. *Es gilt $(f) = 0$ genau dann, wenn $f \in \overline{K}^*$ gilt.*
3. $\deg((f)) = 0$, *d.h.* $\sum_{P \in C} v_P(f) = 0$, *eine Funktion hat also richtig gezählt genau so viele Pol- wie Nullstellen. Damit*

$$\{\textit{Hauptdivisoren}\} \subseteq \mathrm{Div}^0(C) \subseteq \mathrm{Div}(C).$$

DEFINITION. Zwei Divisoren $D_1, D_2 \in \mathrm{Div}(C)$ heißen linear äquivalent, $D_1 \sim D_2$, wenn sie sich um einen Hauptdivisor unterscheiden: $D_1 = D_2 + (f)$ mit einer Funktion f. Die Picardgruppe (oder Divisorenklassengruppe) $\mathrm{Pic}(C)$ ist der Quotient von $\mathrm{Div}(C)$ modulo den Hauptdivisoren und analog $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\{\text{Hauptdivisoren}\}$. Weiter definieren wir

$$\mathrm{Pic}_K(C) = \{c \in \mathrm{Pic}(C) : \sigma c = c \text{ für alle } \sigma \in G_K\}$$

und ebenso $\mathrm{Pic}^0_K(C)$.

Wir haben die exakte Sequenz

$$0 \to \mathrm{Pic}^0(C) \to \mathrm{Pic}(C) \xrightarrow{\deg} \mathbf{Z} \to 0.$$

SATZ. $\mathrm{Pic}^0 \mathbf{P}^1 = \mathbf{Z}$, *d.h. jeder Divisor vom Grad 0 auf $\mathbf{P}^1$ ist Hauptdivisor.*

Beweis: Für $a \in \overline{K}$ gilt: $\mathrm{div}(x - a) = (a) - (\infty)$. Ist nun $D \in \mathrm{Div}^0(\mathbf{P}^1)$, d.h. $D = \sum_{i=1}^m n_i(a_i) - (\sum n_i)(\infty)$, so hat man

$$\mathrm{div}(\prod_{i=1}^m (x - a_i)^{n_i}) = \sum n_i((a_i) - (\infty)) = D,$$

D ist also Hauptdivisor. ■

Geradenschnitte: Sei C eine nichtsinguläre ebene Kurve vom Grad $d \geq 2$ und $L = \{a_0 x_0 + a_1 x_1 + a_2 x_2 = 0\}$ eine Gerade. Den durch

$$(L) = \sum_{P \in C} (L \cdot C)_P P$$

definierten Divisor nennt man einen Geradenschnitt. (L) hat Grad d. Ist $L' = \{b_0x_0 + b_1x_1 + b_2x_2 = 0\}$ eine andere Gerade, so unterscheiden sich (L) und (L') um den Hauptdivisor $(\frac{a_0x_0+a_1x_1+a_2x_2}{b_0x_0+b_1x_1+b_2x_2})$, d.h. je zwei Geradenschnitte sind linear äquivalent.

3. Differentialformen

Sei wieder C eine glatte projektive irreduzible Kurve.

Der Raum Ω_C der meromorphen Differentialformen auf C ist der $\overline{K}(C)$-Vektorraum, der von Symbolen df, $f \in \overline{K}(C)$, erzeugt wird, zusammen mit den Relationen

$$d(f+g) = df + dg, \quad d(fg) = fdg + gdf, \quad da = 0 \text{ für } a \in \overline{K}.$$

Jedes $\omega \in \Omega_C$ hat also eine Darstellung

$$\omega = \sum_{i=1}^{n} f_i dg_i \text{ mit } f_i, g_i \in \overline{K}(C).$$

Beispiel: $C = \mathbf{P}^1$ mit $\overline{K}(C) = \overline{K}(x)$.

1. $d(x^2) = xdx + xdx = 2xdx$ und durch Induktion $d(x^n) = nx^{n-1}dx$ für alle $n \geq 1$. Damit sieht man, daß für Polynome $f \in \overline{K}[x]$ gilt
$$df(x) = d(\sum a_i x^i) = \sum a_i i x^{i-1} dx = f'(x)dx.$$
2. Aus
$$0 = d(1) = d(f \cdot \frac{1}{f}) = \frac{1}{f}df + fd(\frac{1}{f})$$
erhält man $d(\frac{1}{f}) = -\frac{df}{f^2}$ und damit die übliche Regel
$$d(\frac{f(x)}{g(x)}) = \frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2}dx.$$
3. Also hat jedes $\omega \in \Omega_{\mathbf{P}^1}$ die Form $\omega = \frac{f(x)}{g(x)}dx$ und somit $\Omega = \overline{K}(C) \cdot dx$.

SATZ. *Ω_C ist ein 1-dimensionaler $\overline{K}(C)$-Vektorraum. Genauer gilt: Ist t uniformisierend in einem Punkt P, so ist $\Omega_C = \overline{K}(C)dt$.*

Beweis: Wir beweisen nur den ersten Teil des Satzes. Wir schreiben den Funktionenkörper in der Form

$$\overline{K}(C) = Quot(\overline{K}[x,y]/(f))$$

mit einem irreduziblen Polynom $f(x,y)$. Wie oben sieht man, daß dann gilt

$$\Omega_C = \overline{K}(C)dx + \overline{K}(C)dy.$$

Nun folgt aus $f(x,y) = 0$ sofort

$$\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy = 0.$$

Wäre $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0$, so wäre f eine p-Potenz (in Charakteristik p), also reduzibel. Wir können also o.E. $\frac{\partial f}{\partial y} \neq 0$ annehmen, woraus sofort

$$dy = -\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}}dx$$

und damit $\Omega_C = \overline{K}(C)dx$ folgt. ■

Sei $\omega \in \Omega_C$, $\omega \neq 0$ und $P \in C$. Ist t uniformisierend in P, so gibt es eine Funktion g mit $\omega = gdt$. Wir definieren die Ordnung von ω in P durch

$$v_P(\omega) = v_P(g).$$

Man kann zeigen, daß $v_P(\omega)$ unabhängig von der Wahl von t definiert ist. ω heißt regulär oder holomorph in P, falls $v_P(\omega) \geq 0$ gilt. Ist ω in allen Punkten von C holomorph, so nennen wir ω holomorph oder ganz. Außerdem gilt noch: Ist g definiert in P, so ist dg holomorph in P. Der Divisor

$$(\omega) = \operatorname{div}(\omega) := \sum_P v_P(\omega)P$$

heißt der zu ω assoziierte Divisor. Man nennt Divisoren von Differentialformen auch kanonische Divisoren.

Beispiel: $C = \mathbf{P}^1$ mit $\overline{K}(C) = \overline{K}(x)$. Wir wollen den Divisor von $\omega = dx$ berechnen.
Im Punkt $a \in \overline{K}$ ist $x - a$ uniformisierend, aus $\omega = dx = d(x-a)$ folgt dann $v_P(\omega) = 0$. Im Punkt $\infty = (0:1)$ ist $t = \frac{1}{x}$ uniformisierend. Mit

$$\omega = dx = d(\frac{1}{t}) = -\frac{1}{t^2}dt$$

ergibt sich $v_\infty(\omega) = -2$ und damit

$$(\omega) = -2\infty.$$

Sind $\omega_1, \omega_2 \in \Omega_C \setminus \{0\}$, so gibt es ein $f \in \overline{K}(C)^*$ mit $\omega_2 = f\omega_1$. Durch lokale Betrachtung sieht man sofort

$$(\omega_2) = (f) + (\omega_1),$$

d.h. je zwei kanonische Divisoren sind linear äquivalent. Aus der Darstellung sieht man auch: Ist ein Divisor linear äquivalent zu einem kanonischen Divisor, so ist er selbst ein kanonischer Divisor. Das Bild der kanonischen Divisoren in $\operatorname{Pic}(C)$ heißt die kanonische Klasse von C. Sie wird mit K_C bezeichnet. Oft bezeichnen wir mit K_C auch einfach einen kanonischen Divisor.

Beispiel: Wir betrachten $C \subseteq \mathbf{P}^2$ mit der affinen Gleichung $y^2 = x^3 - 1$. Im unendlich fernen Punkt $P = (0:0:1)$ hatten wir die affinen Koordinaten u, v mit der Gleichung $u = v^3 - u^3$, v war uniformisierend, $x = \frac{v}{u}$, also $x = g\frac{1}{v^2}$ mit einer Einheit g in P. Dann ist

$$dx = d(\frac{g}{v^2}) = \frac{1}{v^2}dg - \frac{2g}{v^3}dv,$$

schreiben wir $dg = hdv$, wo h in P definiert ist, erhalten wir

$$dx = \frac{hv - 2g}{v^3}dv.$$

Da g Einheit in P ist, folgt $v_P(dx) = -3$. Wir betrachten jetzt $Q = (a,b) \in C$. Ist $x = a$ keine Tangente in Q, so ist $x - a$ in Q uniformisierend und wegen $dx = d(x-a)$ gilt $v_Q(dx) = 0$. Ist $a = \zeta$ mit $\zeta^3 = 1$, so ist $x - \zeta$ Tangente in $Q = (\zeta, 0)$, y ist uniformisierend. Aus $y^2 = x^3 - 1$ folgt $2ydy = 3x^2dx$ und damit $dx = \frac{2y}{3x^2}dy$. In Q ist x Einheit und somit $v_Q(dx) = 1$. Sind $\zeta_1, \zeta_2, \zeta_3$ die drei dritten Einheitswurzeln, so gilt also

$$(dx) = (\zeta_1, 0) + (\zeta_2, 0) + (\zeta_3, 0) - 3(0:0:1).$$

Man sieht ebenso schnell $(dx) = (y)$ und daher $(\frac{dx}{y}) = 0$, d.h. $\frac{dx}{y}$ ist ein ganzes Differential. Insbesondere $K_C = 0$.

4. Morphismen

Für diesen Abschnitt seien alle Kurven nichtsingulär, irreduzibel, projektiv und über K definiert.
Wir sahen bereits, daß jede rationale Abbildung $\phi : C_1 \to C_2$ schon ein Morphismus ist. Außerdem kann man zeigen, daß ϕ konstant oder surjektiv ist.
Sei $\phi : C_1 \to C_2$ nichtkonstanter, über K definierter Morphismus. Dann liefert

$$\phi^* : K(C_2) \to K(C_1), \quad f \mapsto f \circ \phi$$

eine Inklusion von Körpern, wobei K fest bleibt. Weiter ist $\phi^*K(C_2) \subseteq K(C_1)$ eine endliche Körpererweiterung.

$$\deg \phi = [K(C_1) : \phi^*K(C_2)]$$

heißt der Grad von ϕ. ϕ heißt separabel, falls die Körpererweiterung separabel ist. Im allgemeinen findet man einen Körper L mit

$$\phi^*K(C_2) \subseteq L \subseteq K(C_1),$$

so daß L über $\phi^*K(C_2)$ separabel, $K(C_1)$ über L rein inseparabel ist. Der Grad teilt sich dann auf:

$$\deg_s = [L : \phi^*K(C_2)], \quad \deg_i \phi = [K(C_1) : L].$$

Umgekehrt: Ist $\psi : K(C_2) \to K(C_1)$ ein Körperhomomorphismus, der K festläßt, so gibt es einen Morphismus $\phi : C_1 \to C_2$ mit $\phi^* = \psi$. ϕ ist über K definiert.

Sei $\phi : C_1 \to C_2$ nichtkonstanter Morphismus und $P \in C_1$. Ist $t_{\phi(P)}$ uniformisierend in $\phi(P)$, so heißt

$$e_\phi(P) = v_P(\phi^* t_{\phi(P)})$$

der Verzweigungsindex von ϕ in P. Immer gilt $e_\phi(P) \geq 1$. Ist $e_\phi(P) = 1$, so heißt ϕ unverzweigt in P. Ist $e_\phi(P) = 1$ für alle $P \in C_1$, so heißt ϕ unverzweigt.

SATZ. *Sei $\phi : C_1 \to C_2$ nichtkonstanter Morphismus von Kurven. Dann gilt:*

1. $\deg \phi = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$ *für alle* $Q \in C_2$.
2. *Für fast alle* $Q \in C_2$ *gilt:* $\#\phi^{-1}(Q) = \deg_s \phi$.

FOLGERUNG. *$\phi : C_1 \to C_2$ ist genau dann unverzweigt, wenn für alle $Q \in C_2$ gilt $\#\phi^{-1}Q = \deg \phi$.*

Beispiel: Wir betrachten $C \subseteq \mathbf{P}^2$ mit der affinen Gleichung $y^2 = x^3 - 1$. Die Funktion $x \in \overline{K}(C)$ liefert dann einen Morphismus $\phi : C \to \mathbf{P}^1$. Ist $\overline{K}(\mathbf{P}^1) = \overline{K}(t)$, so ist $\phi^* : \overline{K}(\mathbf{P}^1) \to \overline{K}(C)$ gegeben durch $t \mapsto x$ und daher $\phi^*\overline{K}(\mathbf{P}^1) = \overline{K}(x) \subseteq \overline{K}(C)$. Daher ist $\deg \phi = 2$. Wir haben $\phi((x_0, y_0)) = x_0$ und $\phi((0:0:1)) = (0:1) = \infty$. t ist uniformisierend in ∞ und daher

$$e_\phi((0:0:1)) = v_{(0:0:1)}(\phi^* \frac{1}{t}) = v_{(0:0:1)}(\frac{1}{x}) = 2.$$

Sei nun $Q = (a, b) \in C$. Ist $x = a$ keine Tangente in Q, so ist $x - a$ uniformisierend in Q und man sieht sofort, daß $e_\phi(Q) = 1$ gilt. Für $Q_i = (\zeta_i, 0)$ mit $\zeta_i^3 = 1$ ist $x = \zeta_i$ Tangente. y ist dort uniformisierend. Wegen

$$e_\phi(Q_1) = v_{Q_1}(x - \zeta_1) = v_{Q_1}(\frac{y^2}{(x - \zeta_2)(x - \zeta_3)}) = 2$$

ist also ϕ genau in $(0:0:1), Q_1, Q_2, Q_3$ verzweigt mit Verzweigungsindex 2.

Sei $\phi : C_1 \to C_2$ nichtkonstanter Morphismus von Kurven. Durch lineare Fortsetzung erhalten wir Abbildungen

$$\phi^* : \mathrm{Div}C_2 \to \mathrm{Div}C_1, \quad Q \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P$$

und

$$\phi_* : \mathrm{Div}C_1 \to \mathrm{Div}C_2, \quad P \mapsto \phi(P).$$

Beispiel: Für den durch $f \in \overline{K}(C)$ definierten Morphismus $\phi : C \to \mathbf{P}^1$ gilt

$$(f) = \phi^*((0) - (\infty)).$$

SATZ. *Sei $\phi : C_1 \to C_2$ nichtkonstanter Morphismus von Kurven.*

1. $\deg \phi^* D = \deg \phi \cdot \deg D$
2. $\phi^* \mathrm{div} f = \mathrm{div} \phi^* f$
3. $\deg \phi_* D = \deg D$,
4. $\phi_* \circ \phi^*$ *ist die Multiplikation mit* $\deg \phi$ *auf* $\mathrm{Div}C_2$.
5. $\phi_*(Hauptdivisor) = Hauptdivisor$.

Beweis: Wir zeigen nur die letzte Aussage, und zwar nur für den Fall, daß $\overline{K}(C_1)$ über $\phi^*\overline{K}(C_2)$ galoissch ist mit Galoisgruppe G. Sei $f \in \overline{K}(C_1)^*$ und

$$\mathrm{div}(f) = \sum_i n_i P_i.$$

Sei $Q_i = \phi(P_i)$. Dann gilt $\phi_*(\mathrm{div}(f)) = \sum_i Q_i$. Nun ist $\phi^* Q_i = \sum_{\sigma \in G} \sigma P_i$. Andererseits operiert die Galoisgruppe so, daß gilt $\mathrm{div}(\sigma f) = \sum_i n_i (\sigma P_i)$. Damit erhalten wir

$$\phi^*(\phi_*(\mathrm{div}(f))) = \sum_i n_i \phi^* Q_i = \sum_i n_i \sum_\sigma \sigma P_i = \sum_\sigma (\sum_i n_i (\sigma P_i)) = \sum_\sigma \mathrm{div}(\sigma f) = \mathrm{div}(\prod_\sigma \sigma f).$$

Nun ist aber $\prod_\sigma \sigma f$ eigentlich die Norm, d.h. es gibt ein $g \in \overline{K}(C_2)$ mit $\phi^* g = \prod_\sigma \sigma f$ und damit

$$\phi^*(\phi_*(\mathrm{div}(f))) = \mathrm{div}(\phi^* g) = \phi^*(\mathrm{div}(g)).$$

Die Injektivität von $\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ liefert dann

$$\phi_*(\mathrm{div}(f)) = \mathrm{div}(g),$$

wie behauptet. ■

Beispiel: Sei C eine Kurve in Charakteristik p und $q = p^r$. Nimmt man die Koeffizienten der definierenden Gleichung zur q-ten Potenz, so erhält man eine Kurve $C^{(q)}$. Die Abbildung

$$(x_0 : x_1 : \cdots : x_n) \mapsto (x_0^q : x_1^q : \cdots : x_n^q)$$

liefert dann einen Morphismus $\phi_q : C \to C^{(q)}$, den sogenannten Frobenius-Morphismus. ϕ_q ist rein inseparabel und entspricht der Körpererweiterung $K(C)^q \subseteq K(C)$. $\deg_i \phi_q = q$ und $\deg_s \phi_q = 1$.

Sei $\phi : C_1 \to C_2$ nichtkonstanter Morphismus von Kurven. Durch

$$\phi^*(\sum f_i dg_i) = \sum (\phi^* f_i) d(\phi^{a\,s\,t} g_i)$$

erhält man dann eine Abbildung $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$, die genau dann injektiv ist, wenn ϕ separabel ist. Dies ist äquivalent damit, daß $\phi^* \neq 0$ ist.

LEMMA. *Sei $f \in \overline{K}(C)$ nichtkonstant. Schreibt man*

$$(f) = m_1 P_1 + \cdots + m_r P_r - n_1 Q_1 - \cdots - n_s Q_s, \quad P_i \neq Q_j,$$

so heißt $n_1 Q_1 + \cdots + n_s Q_s$ der Poldivisor $(f)_\infty$ von f. Es gilt

$$[\overline{K}(C) : \overline{K}(f)] = \deg(f)_\infty.$$

Beweis: f induziert einen Morphismus $\phi : C \to \mathbf{P}^1$ durch $\phi = (1 : f)$. Sei $\overline{K}(\mathbf{P}^1) = \overline{K}(t)$. Dann ist $\phi^* t = f$. Wir haben

$$\deg \phi = [\overline{K}(C) : \phi^* \overline{K}(t)] = [\overline{K}(C) : \overline{K}(f)].$$

Nach unserer Formel gilt weiter

$$\deg \phi = \sum_{i=1}^{s} e_\phi(Q_i) = \sum v_{Q_i}(\phi^* \frac{1}{t}) = \sum v_{Q_i}(\frac{1}{f}) = \sum n_i = \deg(f)_\infty,$$

woraus die Behauptung folgt. ■

5. Der Satz von Riemann-Roch

Ein Divisor $D = \sum n_P P \in \mathrm{Div}(C)$ heißt positiv oder effektiv, falls $n_P \geq 0$ für alle P gilt. Wir schreiben $D \geq 0$. Dies liefert eine partielle Ordnung auf $\mathrm{Div}(C)$ durch $D_1 \geq D_2 \iff D_1 - D_2 \geq 0$.

Beispiel: Sei $P_0 \in C$ und $f \in \overline{K}(C)^*$. Wir wollen ausdrücken, daß f höchstens in P_0 eine Polstelle hat, und zwar höchstens von Ordnung n, d.h. wir fordern $v_{P_0}(f) \geq -n$ und $v_P(f) \geq 0$ für $P \neq P_0$. Dies ist gleichwertig mit

$$(f) = \sum_{P \neq P_0} v_P(f) P + v_{P_0}(f) P_0 \geq -n P_0,$$

was wiederum zu $(f) + n P_0 \geq 0$ äquivalent ist.

Für $D \in \mathrm{Div}(C)$ definiert man

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* : (f) + D \geq 0\} \cup \{0\}$$

und man sieht schnell, daß $\mathcal{L}(D)$ ein $\overline{K}$-Vektorraum ist. Weiter definiert man

$$\ell(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

Die Bestimmung von $\mathcal{L}(D)$ bzw. $\ell(D)$ erweist sich als wichtige Aufgabe.

Beispiel: Wir wollen für $C = \mathbf{P}^1$ und $\infty = (0 : 1)$ den Vektorraum $\mathcal{L}(n\infty)$ bestimmen, d.h. wir suchen nach rationalen Funktionen, die im Endlichen überall definiert sind, im Unendlichen höchstens einen Pol

n-ter Ordnung haben. $f \in \overline{K}(\mathbf{P}^1) = \overline{K}(x)$ hat eine Darstellung $f = \frac{g(x)}{h(x)}$ mit teilerfremden Polynomen $g, h \in \overline{K}[x]$. Jede Nullstelle von h liefert eine Polstelle von f, daher kommen in $\mathcal{L}(n\infty)$ nur Polynome vor. Da $t = \frac{1}{x}$ uniformisierend in ∞ ist, gilt für

$$f = a_0 + a_1 x + \cdots + a_m x^m = a_0 + a_1 \frac{1}{t} + \cdots + a_m \frac{1}{t^m}$$

$v_\infty(f) \geq -m$, woraus sofort folgt

$$\mathcal{L}(n\infty) = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in \overline{K}\}$$

und $\ell(n\infty) = n + 1 = \deg(n\infty) + 1$.

Der folgende Satz ist elementar zu beweisen:

SATZ. *Für $D \in \mathrm{Div}(C)$ gilt:*

1. *Gilt $D' = D + (f)$, so ist $\mathcal{L}(D') = \frac{1}{f}\mathcal{L}(D)$. Damit folgt aus $D' \sim D$ sofort $\ell(D') = \ell(D)$. Insbesondere ist ℓ eine Funktion auf* $\mathrm{Pic}(C)$.
2. *Ist* $\deg(D) < 0$, *so ist $\mathcal{L}(D) = 0$, $\ell(D) = 0$. Ist* $\deg(D) \geq 0$, *so ist $\ell(D) \leq \deg(D) + 1$.*

Von fundamentaler Bedeutung ist der folgende Satz:

SATZ (Riemann-Roch). *Es gibt eine Konstante $g = g(C)$, das Geschlecht von C, so daß für alle $D \in \mathrm{Div}(C)$ gilt:*

$$\ell(D) = \deg D + 1 - g + \ell(K_C - D).$$

Durch Einsetzen von $D = 0$ und $D = K_C$ erhalt man sofort:

KOROLLAR. 1. *$\ell(K_C) = g$, insbesondere ist g eine ganze Zahl ≥ 0.*
2. $\deg K_C = 2g - 2$.
3. *Ist* $\deg D > 2g - 2$, *so ist $\ell(D) = \deg D + 1 - g$.*

Beispiel: Für $C = \mathbf{P}^1$ hatten wir ausgerechnet $K_C = (dx) = -2\infty$, also $\deg K_C = -2$ und damit $g = 0$. Riemann-Roch liefert dann $\ell(D) = \deg D + 1$ für $\deg D \geq 0$.

Beispiel: Für die durch $y^2 = x^3 - 1$ gegebene Kurve C war $K_C = (\frac{dx}{y}) = 0$ und somit $g = 1$.

SATZ (Adjunktionsformel). *Ist $C \subseteq \mathbf{P}^2$ eine nichtsinguläre Kurve vom Grad d, so gilt*

$$g = \frac{(d-1)(d-2)}{2}.$$

(Ist $L \not\subseteq C$ eine Gerade, so ist $(d-3)(L)$ ein kanonischer Divisor auf C.)

Bemerkung: Sei ω eine Differentialform. Dann gilt:

$$f \in \mathcal{L}((\omega)) \iff (f) + (\omega) \geq 0 \iff (f\omega) \geq 0,$$

woraus folgt:

$$\mathcal{L}(K_C) \simeq \{\text{holomorphe Differentialformen auf } C\}.$$

SATZ. *Ist $D \in \mathrm{Div}(C)$ über K definiert, so besitzt $\mathcal{L}(D)$ eine Basis $f_0, \ldots, f_n$ mit $f_i \in K(C)$.*

Wie wendet man $\mathcal{L}(D)$ an? Sei $D \in \mathrm{Div}(C)$ mit $\ell(D) > 0$. Wähle eine Basis $f_0, \ldots, f_n$ von $\mathcal{L}(D)$. Dann liefert

$$\phi = (f_0 : \cdots : f_n)$$

einen Morphismus $C \to \mathbf{P}^n$.

SATZ. *Ist $\deg D \geq 2g + 1$, so liefert $\mathcal{L}(D)$ einen Isomorphismus $\phi : C \to \phi(C) \subseteq \mathbf{P}^n$, $\phi(C)$ ist eine nichtsinguläre projektive Kurve in $\mathbf{P}^n$.*

Beispiel: Wir betrachten $C = \mathbf{P}^1$ und $D = 2\infty$. Dann ist $\mathcal{L}(D) = \overline{K} + \overline{K}x + \overline{K}x^2$, der zugehörige Morphismus also $\phi = (1 : x : x^2) : C \to \mathbf{P}^2$. Das Bild $\phi(C)$ ist die ebene Quadrik $\{x_0 x_2 = x_1^2\}$.

Literatur: [**13**], [**2a**].

KAPITEL 4

Elliptische Kurven

1. Einführung

DEFINITION. Eine elliptische Kurve über K besteht aus einer irreduziblen nichtsingulären projektiven Kurve E vom Geschlecht 1, die über K definiert ist, und einem Punkt $O \in E(K)$. Wir schreiben dafür (E, O) oder auch nur E.

Beispiel: Ist $C = \{f(x_0, x_1, x_2) = 0\}$ eine nichtsinguläre ebene Kubik, die über K definiert ist, so hat C Geschlecht 1. Ist $C(K) \neq \emptyset$, so wird C durch Wahl eines Punktes $O \in C(K)$ zu einer elliptischen Kurve über K.

LEMMA. *Sei C eine Kurve vom Geschlecht 1.*

1. *Die kanonische Klasse ist trivial, d.h. $K_E \sim 0$.*
2. *Für einen Divisor D mit $\deg D \geq 1$ gilt $\ell(D) = \deg(D)$.*
3. *Zu jedem Divisor D vom Grad 1 gibt es genau einen Punkt $P \in C$ mit $D \sim P$.*

Beweis:

1. Sei E eine elliptische Kurve. Ist ω eine von 0 verschiedene Differentialform, so gibt es wegen $\ell((\omega)) = 1$ eine Funktion $f \in \mathcal{L}((\omega))$ mit $(f\omega) = (f) + (\omega) \geq 0$ und wegen $\deg((f\omega)) = 0$ folgt $(f\omega) = 0$, also ist $f\omega$ ein ganzes Differential ohne Nullstellen und damit $K_E \sim 0$.
2. Dies ist der Satz von Riemann-Roch wegen $\deg(K_C - D) < 0$ und somit $\ell(K_C - D) = 0$.
3. Sei D ein Divisor vom Grad 1. Dann ist $\ell(D) = 1$, also gibt es eine Funktion $f \in \mathcal{L}(D) \setminus \{0\}$ mit $(f) + D \geq 0$. Da $(f) + D$ Grad 1 hat, gibt es einen Punkt P mit $(f) + D = P$, also $P \sim D$. Gilt für einen weiteren Punkt $Q \in C$ ebenfalls $D \sim Q$, so gibt es eine Funktion g mit $Q = (g) + D$, also ist $g \in \mathcal{L}(D)$. Da aber $\mathcal{L}(D)$ eindimensional ist, gibt es eine Konstante λ mit $g = \lambda f$ und damit $(g) = (f)$ und $P = Q$. ■

SATZ. *Sei (E, O) eine über K definierte elliptische Kurve. Dann ist*

$$\psi : E \to \mathrm{Pic}^0(E), \quad P \mapsto \textit{ Klasse von } P - O$$

eine Bijektion. Durch

$$P \oplus Q = \psi^{-1}(\psi(P) + \psi(Q))$$

wird dadurch E zu einer abelschen Gruppe mit O als neutralem Element. Wir denken uns (E, O) immer mit dieser Gruppenstruktur versehen. Außerdem gilt: $\psi(E(K)) = \mathrm{Pic}^0_K(E)$. Dann ist $E(K)$ eine Untergruppe von E.

Beweis:

1. Wir wollen zunächst zeigen, daß ψ injektiv ist. Seien $P, Q \in C$ mit $\psi(P) = \psi(Q)$. Dann ist $P - O \sim Q - O$, also $P \sim Q$, nach unserem Lemma folgt $P = Q$.
2. Wir zeigen die Surjektivität von ψ. Sei $D \in \mathrm{Div}^0(E)$. Dann ist $D + O$ ein Divisor vom Grad 1, also gibt es einen Punkt P mit $D + O \sim P$ und somit $D \sim P - O$, d.h. die Klasse von D ist das Bild von $\psi(P)$.
3. Natürlich gilt $\psi(E(K)) \subseteq \mathrm{Pic}^0_K(E)$. Ist $D \in \mathrm{Pic}^0_K(E)$ und $D \sim P - O$, so folgt für $\sigma \in G_K$ auch $D \sim \sigma(P) - O$, also $P \sim \sigma(P)$, was schließlich $P \in E(K)$ zeigt. ■

Bemerkung: Wann gilt $P \oplus Q = R$ auf einer elliptischen Kurve (E, O)? Genau dann, wenn $P - O + Q - O \sim R - O$ ist, was mit

$$P \oplus Q \sim P + Q - O$$

äquivalent ist.

Für nichtsinguläre ebene Kubiken hatten wir bereits geometrisch eine Gruppenstruktur definiert. Dies ist nichts anderes als die durch $E \simeq \mathrm{Pic}^0(E)$ definierte Gruppenstruktur.

SATZ. *Sei $C \subseteq \mathbf{P}^2$ eine nichtsinguläre ebene Kubik und $O \in C(K)$. Dann gilt*

$$P_1 \oplus P_2 = P_1 \oplus_g P_2$$

mit

$$P_1 \oplus P_2 = \psi^{-1}(\psi(P_1) + \psi(P_2)) \quad \text{und} \quad P_1 \oplus_g P_2 = \lambda(\lambda(P_1, P_2), O).$$

(Hier ist $\psi : E \to \mathrm{Pic}^0(E)$ wie oben definiert und $\lambda(P, Q)$ ist der dritte Punkt auf der Geraden durch P und Q.)

Beweis: Seien $P_1, P_2 \in C$. Sei $L = \{\ell = 0\}$ die Gerade durch P_1, P_2 mit $L \cdot C = P_1 + P_2 + Q$. Sei $M = \{m = 0\}$ die Gerade durch Q, O mit $M \cdot C = Q + O + P_3$. Der Punkt P_3 ist dann die geometrische Summe von P_1 und P_2, d.h. $P_3 = P_1 \oplus_g P_2$. Nun ist $\frac{\ell}{m}$ eine Funktion auf C mit Divisor

$$(\frac{\ell}{m}) = (P_1 + P_2 + Q) - (Q + O + P_3) = (P_1 - O) + (P_2 - O) - (P_3 - O),$$

d.h. $P_3 - O \sim (P_1 - O) + (P_2 - O)$ und damit $\psi(P_3) = \psi(P_1) + \psi(P_2)$, also ist $P_3 = P_1 \oplus P_2$, was wir zeigen wollten. ■

Da für eine elliptische Kurve (E, O) die Gruppe E nach Konstruktion isomorph zu $\mathrm{Pic}^0(E)$ ist, erhält man sofort:

SATZ. *Sei E eine Kurve vom Geschlecht 1 und $O_1, O_2 \in E(K)$. Dann sind (E, O_1) und (E, O_2) als Gruppen isomorph.*

Wir werden nun elliptische Kurven als ebene projektive Kurven realisieren.

SATZ. *Sei (E, O) eine elliptische Kurve über K. Dann gibt es Funktionen $x, y \in K(E)$, so daß $\phi : E \to \mathbf{P}^2$ mit $\phi = (1 : x : y)$ einen Isomorphismus auf eine (nichtsinguläre ebene projektive) Kurve C mit der Gleichung*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

liefert mit $a_i \in K$ und $\phi(O) = (0 : 0 : 1)$. Eine Gleichung dieser Form wird Weierstraßgleichung genannt.

Beweis:

1. Riemann-Roch besagt $\ell(n \cdot O) = n$ für $n \geq 1$. Also gibt es Funktionen $x, y \in K(E)$, die außerhalb O definiert sind mit $v_O(x) = -2$ und $v_O(y) = -3$, so daß gilt:

   $$\mathcal{L}(O) = \overline{K}, \quad \mathcal{L}(2O) = \overline{K} + \overline{K}x, \quad \mathcal{L}(3O) = \overline{K} + \overline{K}x + \overline{K}y.$$

   Nun ist $v_O(x^2) = -4$, $v_O(xy) = -5$, $v_O(x^3) = -6$ und damit

   $$\begin{aligned} \mathcal{L}(4O) &= \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2, \\ \mathcal{L}(5O) &= \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy, \\ \mathcal{L}(6O) &= \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy + \overline{K}x^3. \end{aligned}$$

   Nun ist auch $v_O(y^2) = -6$ und damit $y^2 \in \mathcal{L}(6O) \setminus \mathcal{L}(5O)$, also gibt es $A_i \in K$ mit

   $$y^2 = A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6x^3 \text{ und } A_6 \neq 0.$$

   Ersetzt man x durch $\frac{x}{A_6}$ und y durch $\frac{y}{A_6}$, so erhält man eine Gleichung der Form

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

   mit $a_i \in K$. Sei C die ebene Kurve mit der Gleichung

   $$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

   Dann liefert $\phi = (1 : x : y)$ also einen Morphismus $\phi : E \to C$.

2. Aus $v_O(x) = -2$ und $v_O(y) = -3$ folgt $v_O(\frac{1}{y}) = 3$, $v_O(\frac{x}{y}) = 1$ und damit $(\frac{1}{y})(O) = 0$, $(\frac{x}{y})(O) = 0$, was mit $\phi = (1 : x : y) = (\frac{1}{y} : \frac{x}{y} : 1)$ sofort $\phi(O) = (0 : 0 : 1)$ zeigt. Natürlich ist damit ϕ nicht konstant, also surjektiv.
3. Wir zeigen, daß die Kurve C nichtsingulär ist. Wäre C reduzibel, so würde man eine Gleichung vom Grad ≤ 2 zwischen den Funktionen x und y erhalten, was nicht sein kann. Also können wir annehmen, daß C irreduzibel ist. Wir beschränken uns auf den Fall, daß die Charakteristik verschieden von 2 und 3 ist. Nach Koordinatenwechsel über $\overline{K}$ erhält man dann eine Gleichung der Form $Y^2 = X^3$ oder $Y^2 = X^2 + X^3$. D.h. es gibt Funktionen $u, v \in \mathcal{L}(3O)$ mit $\mathcal{L}(3O) = \overline{K} + \overline{K}u + \overline{K}v$ und $v^2 = u^3$ oder $v^2 = u^2 + u^3$.
   (a) $v^2 = u^3$. Wir setzen $t = \frac{v}{u}$ und erhalten $u = t^2$, $v = t^3$. Damit ist t außerhalb von O definiert und wegen $t^2, t^3 \in \mathcal{L}(3O)$ folgt $v_O(t) = -1$, was nicht sein kann.
   (b) $v^2 = u^2 + u^3$. Sei $t = \frac{v}{u}$. Dann ist $u = 1 + t^2$ und $v = t + t^3$. Ebenso wie zuvor sieht man $t^2, t^3 \in \mathcal{L}(3O)$ und erhält damit wieder den Widerspruch $v_O(t) = -1$.

   Also ist C eine nichtsinguläre Kurve.
4. Da die Morphismen zwischen nichtsingulären Kurven den Abbildungen zwischen den Funktionenkörpern entsprechen, genügt es zu zeigen, daß $K(E) = \phi^* K(C)$ gilt. Nun wird $K(C)$ von den Koordinatenfunktionen X, Y erzeugt, aus $x = \phi^* X$, $y = \phi^* Y$ folgt also $\phi^* K(C) = K(x, y)$. Wir haben
$$K(x), K(y) \subseteq K(x, y) \subseteq K(E).$$
   Der Polstellendivisor von x hat Grad 2, der von y Grad 3, also ist $[K(E) : K(x)] = 2$, $[K(E) : K(y)] = 3$, woraus sofort $K(E) = K(x, y)$ folgt. Also ist ϕ ein Isomorphismus. ■

Jede elliptische Kurve läßt sich also durch eine Weierstraßgleichung
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K$$
beschreiben mit $O = (0 : 0 : 1)$. Umgekehrt liefert natürlich jede nichtsinguläre Kurve mit einer Weierstraßgleichung eine elliptische Kurve mit $O = (0 : 0 : 1)$ und $K(E) = K(x, y)$.

LEMMA. *Wird durch*
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K$$
eine nichtsinguläre ebene Kurve E beschrieben, so ist $O = (0 : 0 : 1)$ der einzige Punkte im Unendlichen, die Koordinatenfunktionen x, y sind regulär außerhalb von O und $v_O(x) = -2$, $v_O(y) = -3$.

Beweis: elementar. ■

Wir wollen nun die Addition auf einer elliptischen Kurve in Weierstraßscher Normalform ansehen. Wir werden ab jetzt statt $P \oplus Q$ einfach $P + Q$ schreiben, wenn keine Verwechslungen möglich sind.

SATZ. *Eine elliptische Kurve E sei gegeben durch die Gleichung*
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
mit $O = (0 : 0 : 1)$. Zunächst gilt für $(x_0, y_0) \in E$:
$$-(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$
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
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \quad \textit{falls } x_1 \neq x_2,$$
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \textit{falls } x_1 = x_2.$$
Dann gilt
$$x_2 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = -(\lambda + a_1)x_3 - \nu - a - 3.$$

Beweis: Wir schreiben $f = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Wir bemerken, daß $P + Q + R = O$ genau dann gilt, wenn die drei Punkte von einer Geraden ausgeschnitten werden.

1. Sei $P = (x_0, y_0)$ und $Q = -P$. Dann gilt $P + Q + O = O$, d.h. die Gerade $x = x_0$ durch P und O schneidet die Kurve in $Q = (x_0, y_0')$. Wir setzen $x = x_0$ in die Kurvengleichung ein. Dann gilt einerseits
$$f(x_0, y) = (y - y_0)(y - y_0'),$$
andererseits
$$f(x_0, y) = y^2 + (a_1 x_0 + a_3)y + (\dots),$$
so daß sich durch Koeffizientenvergleich $y_0 + y_0' = a_1 x_0 + a_3$ ergibt, also $-P = Q = (x_0, -y_0 - a_1 x_0 - a_3)$ wie behauptet.
2. Wir können den Fall $P_1 + P_2 = O$ wegen 1. bereits ausschließen. Ist $Q = -P_3$, so gilt $P_1 + P_2 + Q = O$ und $Q = (x_3, y_3')$. Wir berechnen die Gerade $y = \lambda x + \nu$ durch P_1 und P_2 (bzw. die Tangente in P_1, falls $P_1 = P_2$) und erhalten λ, ν wie im Satz angegeben. Einsetzen ergibt
$$f(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3),$$
woraus sich durch Koeffizientenvergleich bei x^3 sofort $c = -1$, durch Vergleich bei x^2 dann $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$ ergibt. Damit berechnet mit x_3. Nun ist $y_3' = \lambda x_3 + \nu$. Mit 1. erhält man schließlich $P_3 = (x_3, y_3)$. ■

SATZ. *Zwei elliptische Kurven E und E', die durch Weierstraßgleichungen beschrieben werden, sind genau dann isomorph über K mit festgehaltenem Nullpunkt, wenn sie durch einen Koordinatenwechsel*
$$X' = u^2 X + r, \quad Y' = u^3 Y + s u^2 X + t, \quad u, r, s \in K, u \neq 0$$
auseinander hervorgehen.

Beweis: Sei
$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad E' : y'^2 + a_1' x' y' + a_3' y' = x'^3 + a_2' x'^2 + a_4' x' + a_6'$$
und $\phi : E \to E'$ ein Isomorphismus über K mit $\phi((0:0:1)) = (0:0:1)$. Dann sind $\phi^* x'$ und $\phi^* y'$ Funktionen, die nur in $O = (0:0:1)$ einen Pol haben und zwar $v_O(\phi^*) = -2$ und $v_O(\phi^* y) = -3$. Also gibt es Darstellungen
$$\phi^* x' = c_0 + c_1 x, \quad \phi^* y' = c_2 + c_3 x + c_4 y$$
mit $c_i \in K$ und $c_1, c_4 \neq 0$. Wie früher folgt $c_1^3 = c_4^2$, also erfüllt $u = \frac{c_4}{c_1} \in K$ die Relationen $u^2 = c_1$, $u^3 = c_4$. Durch Umbenennung erhalten wir
$$\phi^* x' = u^2 x + r, \quad \phi^* y' = u^3 y + s u^2 x + t.$$
Daß umgekehrt ein solcher Koordinatenwechsel wieder eine Weierstraßgleichung ergibt, ist leicht zu sehen. ■

2. Weierstraßgleichungen in Charakteristik $\neq 2, 3$

Wir setzen jetzt voraus, daß die Charakteristik der Grundkörpers von 2 und 3 verschieden ist. Eine elliptische Kurve (E, O) über K läßt sich durch eine Weierstraßgleichung
$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in K$$
mit $O = (0:0:1)$ beschreiben. Wegen
$$y^2 + a_1 xy + a_3 y = (y + \frac{a_1}{2} x + \frac{a_3}{2})^2 + \text{Polynom in } x$$
und
$$x^3 + a_2 x^2 + a_4 x + a_6 = (x + \frac{a_2}{3})^3 + a_4'(x + \frac{a_2}{3}) + a_6'$$
läßt sich E durch Koordinatenwechsel auf die Gestalt
$$y^2 = x^3 + ax + b$$
bringen. Wir können also unsere elliptischen Kurven immer durch solch vereinfachte Weierstraßgleichungen beschreiben.

SATZ. *Die ebene Kurve $y^2 = x^3 + ax + b$ ist für $char(K) \neq 2, 3$ genau dann singulär, wenn $4a^3 + 27b^2 = 0$ gilt.*

Beweis: Die Kurve $x_0x_2^2 = x_1^3+ax_0^2x_1+bx_0^3$ hat im Unendlichen nur den Punkt $O = (0:0:1)$. Wählt man affine Koordinaten u, v mit $(u:v:1) = (x_0:x_1:x_2)$, so wird die Kurvengleichung $u = v^3 + au^2v + bu^3$, die Kurve ist also nichtsingulär in O mit Tangente $u = 0$ bzw. $x_0 = 0$.
Wir schreiben jetzt $f = x^3 + ax + b - y^2$. Dann ist $\frac{\partial f}{\partial x} = 3x^2 + a$ und $\frac{\partial f}{\partial y} = -2y$. Ist (x_0, y_0) singulärer Punkt, so gilt also

$$f(x_0, y_0) = \frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0,$$

was äquivalent ist mit

$$y_0 = 0, \quad x_0^3 + ax_0 + b = 3x_0^2 + a = 0.$$

Dies ist genau dann lösbar, wenn $4a^3 + 27b^2 = 0$ gilt. ■

SATZ. *Zwei elliptische Kurven mit Weierstraßgleichungen $y^2 = x^3 + ax + b$ und $y'^2 = x'^3 + a'x' + b'$ sind genau dann isomorph über K (unter Respektierung der Nullpunkte), wenn es ein $u \in K^*$ gibt mit*

$$a' = u^4a \quad \text{und} \quad b' = u^6b.$$

Dann ist $x = u^2x'$ und $y = u^3y'$ ein projektiver Koordinatenwechsel der Kurven.

Beweis: Wir wissen bereits, daß wir uns auf Koordinatenwechsel der Form

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

beschränken können. Aus $y'^2 = x'^3 + a'x' + b'$ erhält man durch Einsetzen

$$(u^3y + u^2sx + t)^2 = (u^2x + r)^3 + a'(u^2x + r) + b'$$

in $K(E)$. Die Relation $y^2 = x^3 + ax + b$ benutzend und $y \notin K(x)$ folgt sofort $s = t = 0$. Da dann auf der linken Seite kein Term x^2 mehr vorkommt, folgt auch $r = 0$ und somit

$$x' = u^2x \quad \text{und} \quad y' = u^3y.$$

Einsetzen ergibt jetzt:

$$u^6y^2 = u^6x^3 + a'u^2x + b'$$

und damit

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

Hat man umgekehrt eine solche Relation, erhält man durch obige Formeln natürlich sofort einen zugehörigen Koordinatenwechsel. ■

Ist E eine elliptische Kurve über einem Körper der Charakteristik $\neq 2, 3$, so läßt sich E durch eine Gleichung $y^2 = x^3 + ax + b$ beschreiben. Wird E durch eine weitere Gleichung $y^2 = x^3 + a'x + b'$ beschrieben, so gibt es ein $u \in K$ mit $a' = u^4a$, $b' = u^6b$. Dann ist aber

$$\frac{a'^3}{4a'^3 + 27b'^2} = \frac{a^3}{4a^3 + 27b^2}$$

und damit ist folgende Definition sinnvoll:

DEFINITION. Wird eine elliptische Kurve E durch eine Gleichung $y^2 = x^3 + ax + b$ beschrieben, so definieren wir die j-Invariante von E durch

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

SATZ. *Zwei elliptische Kurven E und E' sind genau dann isomorph über $\overline{K}$, wenn $j(E) = j(E')$ gilt.*

Beweis: E und E' werden durch Gleichungen $y^2 = x^3 + ax + b$ und $y^2 = x^3 + a'x + b'$ beschrieben.
$\Rightarrow$: Sind E und E' isomorph über $\overline{K}$, so gibt es $u \in \overline{K}^*$ mit $a' = u^4a$, $b' = u^6b$, woraus sofort $j(E') = j(E)$ folgt.
$\Leftarrow$: Sei $j(E) = j(E')$, d.h.

$$\frac{a^3}{4a^3 + 27b^2} = \frac{a'^3}{4a'^3 + 27b'^2}.$$

Wir suchen ein $u \in \overline{K}^*$ mit $a' = u^4a$ und $b' = u^6b$.

1. Ist $a = 0$, so auch $a' = 0$. Die Behauptung ergibt sich dann durch Wahl eines $u \in \overline{K}$ mit $b' = u^6 b$.
2. Ist $b = 0$, so auch $b' = 0$. Wir wählen $u \in \overline{K}$ mit $a' = u^4 a$.
3. Ist $ab \neq 0$, so auch $a'b' \neq 0$. Obige Gleichung liefert $a^3(4a'^3 + 27b'^2) = a'^3(4a^3 + 27b^2)$ und damit $a^3 b'^2 = a'^3 b^2$ bzw.
$$(\frac{b'}{b})^2 = (\frac{a'}{a})^3.$$
Setzt man $v = \frac{b'}{b}/\frac{a'}{a}$, so erhält man wie üblich $v^2 = \frac{a'}{a}$ und $v^3 = \frac{b'}{b}$. Wählt man $u \in \overline{K}$ mit $u^2 = v$, so ergibt sich schließlich die Behauptung. ■

Beispiel: Es ist $j(E) = 0$ genau dann, wenn E durch eine Gleichung $y^2 = x^3 + b$ beschrieben wird, $j(E) = 1728$, wenn E durch $y^2 = x^3 + ax$ beschrieben wird.

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.*
- *$j \neq 0, 1728$: $y^2 = x^3 - 3cu^2x + 2cu^3$ 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 $y^2 = x^3 - 3cu^2x + 2cu^3$ 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 $y^2 = x^3 - 3cu^2x + 2cu^3$ und E' durch $y^2 = x^3 - 3cu'^2x + 2cu'^3$. 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.
3. $K = \mathbf{F}_p$ mit $p \geq 5$. Die Gruppe K^* ist zyklisch von Ordnung $p - 1$, also
$$K^*/K^{*2} \simeq Z_2, \quad K^*/K^{*4} \simeq Z_{\gcd(4,p-1)}, \quad K^*/K^{*6} \simeq Z_{\gcd(6,p-1)},$$
insbesondere ist die Anzahl der K-Isomorphieklassen elliptischer Kurven gleich
$$\gcd(6, p-1) + \gcd(4, p-1) + 2(p-2),$$
d.h. ungefähr $2p$.

Beispiel: $K = \mathbf{F}_{1009}$. Wir wenden den Satz für $j = 100$ an und erhalten $c = 52$. Wegen $(\frac{11}{1009}) = -1$ ist 11 kein Quadrat in $\mathbf{F}_{1009}$, also sind 1 und 11 Repräsentanten von K^*/K^{*2}. Zu $j = 100$ findet man dann die beiden Kurven
$$y^2 = x^3 + 853x + 104 \quad \text{und} \quad y^2 = x^3 + 295x + 191.$$

Ein Automorphismus der elliptischen Kurve (E, O) ist ein Isomorphismus $\phi : E \to E$ mit $\phi(O) = O$. Wird E durch $y^2 = x^3 + ax + b$ beschrieben, so wird ϕ durch einen Koordinatenwechsel $x' = u^2 x, y' = u^3 y$

beschrieben, d.h. $\phi((x,y)) = (u^2x, u^3y)$. Da die Gleichung $y'^2 = x'^3 + ax' + b$ erfüllt sein muß, erhalten wir die Bedingung $u^4a = a$ und $u^6b = b$, d.h.

$$(u^4 - 1)a = (u^6 - 1)b = 0.$$

Wir unterscheiden 3 Fälle:

1. Ist $j = 0$, so ist $a = 0$, $b \neq 0$, die Bedingung lautet $u^6 = 1$, also gibt es 6 Automorphismen.
2. Ist $j = 1728$, so ist $a \neq 0$, $b = 0$, die Bedingung lautet $u^4 = 1$, also gibt es 4 Automorphismen.
3. Ist $j \neq 0, 1728$, so ist $a, b \neq 0$, also hat man die Bedingungen $u^4 = 1$ und $u^6 = 1$, was $u^2 = 1$ und damit $u = \pm 1$ liefert. Die Automorphismengruppe hat 2 Elemente. Der nichttriviale Automorphismus ist $(x, y) \mapsto (x, -y)$.

Damit erhalten wir folgenden Satz:

SATZ. *Für die Automorphismengruppe einer elliptischen Kurve in Charakteristik $\neq 2, 3$ gilt:*

- $\mathrm{Aut}(E) \simeq Z_6$ *für* $j(E) = 0$,
- $\mathrm{Aut}(E) \simeq Z_4$ *für* $j(E) = 1728$,
- $\mathrm{Aut}(E) \simeq Z_2$ *für* $j(E) \neq 0, 1728$.

3. Beliebige Charakteristik

Wir starten mit einer Gleichung

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

für die Kurve E und definieren

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= \frac{c_4^3}{\Delta}.
\end{aligned}$$

Man hat dann die Eigenschaften:

- E ist genau dann nichtsingulär, wenn $\Delta \neq 0$ gilt. Δ wird auch Diskriminante genannt.
- $j(E)$ ist wohldefiniert.
- $E \simeq_{\overline{K}} E' \iff j(E) = j(E')$.

4. Charakteristik 2

Sei K ein Körper der Charakteristik 2 und E eine elliptische Kurve über K mit der Gleichung

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

Man erhält

$$\Delta = a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_1^3a_3^3 + a_3^4 \quad \text{und} \quad j = \frac{a_1^{12}}{\Delta}.$$

Transformiert man mit den Gleichungen

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

so ergeben sich für die Koeffizienten der transformierten Gleichung $y'^2 + a'_1x'y' + a'_3y' = x'^3 + a_2x'^2 + a'_4x' + a'_6$

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

Wir betrachten zunächst den Fall $j \neq 0$. Dies bedeutet $a_1 \neq 0$. Durch Wahl von u erreicht man $a_1 = 1$, durch Wahl von r dann $a_3 = 0$, durch Wahl von t schließlich $a_4 = 0$. Wir erhalten also

$$y^2 + xy = x^3 + a_2x^2 + a_6 \quad \text{mit} \quad \Delta = a_6 \quad \text{und} \quad j = \frac{1}{a_6}.$$

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*
$$y^2 + xy = x^3 + ax^2 + \frac{1}{j} \quad \textit{mit} \quad a \in K$$
beschreiben.
2. *Zwei Kurven*
$$y^2 + xy = x^3 + ax^2 + \frac{1}{j} \quad \textit{und} \quad y^2 + xy = x^3 + a'x^2 + \frac{1}{j}$$
genau dann isomorph über K, wenn $s \in K$ existiert mit $a' = a + s + s^2$.

Beweis: Wir müssen nur noch die zweite Behauptung zeigen. Die obigen Transformationsformeln ergeben die Gleichungen

$$\begin{aligned} u &= 1, \\ u^2a' &= a + s + r + s^2, \\ 0 &= r, \\ 0 &= (t + rs) + r^2, \\ u^6\frac{1}{j} &= \frac{1}{j} + r^2a + r^3 + t^2 + rt, \end{aligned}$$

also

$$u = 1, \quad r = 0, \quad t = 0, \quad a' = a + s + s^2,$$

wie behauptet. ■

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*

$$y^2 + xy = x^3 + \frac{1}{j} \quad \textit{und} \quad y^2 + xy = x^3 + cx^2 + \frac{1}{j}$$

Repräsentanten der K-Isomorphieklassen elliptischer Kurven über K mit j-Invariante $j \neq 0$.

Durch Verwendung obiger Transformationsformeln erhält man sofort:

FOLGERUNG. *Eine elliptische Kurve E in Charakteristik 2 mit $j(E) \neq 0$ hat genau 2 Automorphismen, der nichttriviale ist $(x, y) \mapsto (x, x + y)$.*

Wir betrachten jetzt den Fall $j = 0$, d.h. $a_1 = 0$. Durch Wahl von r erreichen wir $a_2 = 0$ und erhalten dann

$$y^2 + a_3y = x^3 + a_4x + a_6 \quad \text{mit} \quad \Delta = a_3^4 \quad \text{und} \quad j = 0.$$

SATZ. *Eine elliptische Kurve in Charakteristik* 2 *mit j-Invariante* 0 *läßt sich durch eine Gleichung*

$$y^2 + a_3 y = x^3 + a_4 x + a_6$$

beschreiben. Zwei Kurven (mit j-Invariante 0*)*

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \text{ und } y^2 + a_3' y = x^3 + a_4' x + a_6'$$

sind genau dann isomorph über K*, wenn* $u, s, t \in K$ *existieren mit*

$$\begin{aligned} u^3 a_3' &= a_3, \\ u^4 a_4' &= a_4 + s a_3 + s^4, \\ u^6 a_6' &= a_6 + s^2 a_4 + t a_3 + s^6 + t^2, \end{aligned}$$

Beweis: Die Transformationsformeln ergeben die Bedingungen

$$\begin{aligned} 0 &= r + s^2, \\ u^3 a_3' &= a_3, \\ u^4 a_4' &= a_4 + s a_3 + r^2, \\ u^6 a_6' &= a_6 + r a_4 + r^3 + t a_3 + t^2, \end{aligned}$$

woraus sich $r = s^2$ und

$$\begin{aligned} u^3 a_3' &= a_3, \\ u^4 a_4' &= a_4 + s a_3 + s^4, \\ u^6 a_6' &= a_6 + s^2 a_4 + t a_3 + s^6 + t^2, \end{aligned}$$

ergibt, wie behauptet. ■

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*

$$y^2 + y = x^3.$$

SATZ. *Ist* E *eine elliptische Kurve in Charakteristik* 2 *mit j-Invariante* 0*, so gilt* $\#\mathrm{Aut}(E) = 24$*. Genauer gilt:* $\mathrm{Aut}(E)$ *ist semidirektes Produkt einer zyklischen Gruppe* Z_3 *mit einer Quaternionengruppe* $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ *als Normalteiler, wo* Z_3 *auf* Q_8 *durch Permutation von* i, j, k *operiert.*

Beweis: Da wir die Automorphismen über dem algebraischen Abschluß studieren, können wir E in der Form $y^2 + y = x^3$ annehmen. Wir haben dann die Gleichungen ($r = s^2$)

$$u^3 = 1, \quad s^4 + s = 0, \quad t^2 + t + s^6 = 0.$$

Dies ergibt 24 Lösungen und die zugehörigen Transformationen

$$(x, y) \mapsto (u^2 x + s^2, u^3 y + s u^2 x + t).$$

Die Gruppenstruktur muß man natürlich explizit nachrechnen. ■

Bemerkung: Sei $K = \mathbf{F}_{2^m}$. Man kann zeigen, daß es genau 3 für $m \equiv 1 \bmod 2$ bzw. 7 für $m \equiv 0 \bmod 2$ K-Isomorphieklassen elliptischer Kurven über K mit $j = 0$ gibt.

SATZ. *Sei* E *eine elliptische Kurve über* K *und* $E[2] = \{P \in E : 2P = 0\}$*. Dann gilt:*

- *Ist* $char(K) \neq 2$*, so ist* $E[2] \simeq Z_2 \times Z_2$*.*
- *Ist* $char(K) = 2$ *und* $j(E) \neq 0$*, so ist* $E[2] \simeq Z_2$*.*
- *Ist* $char(K) = 2$ *und* $j(E) = 0$*, so ist* $E[2] = \{0\}$*.*

Beweis: Es gilt $2P = 0$ genau dann, wenn $P = -P$ ist. Wird E durch eine Gleichung $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ beschrieben, so ist für $P = (x_0, y_0)$ dann $-P = (x_0, -y_0 - a_1 x_0 - a_3)$.

- Ist $char(K) \neq 2$, so können wir nach Koordinatenwechsel $a_1 = a_3 = 0$ annehmen. $P = -P$ liefert die Gleichung $y_0 = -y_0$, also $y_0 = 0$ und $x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6 = 0$, so daß es zusammen mit O genau 4 Elemente in $E[2]$ gibt und damit $E[2] \simeq Z_2 \times Z_2$.

- Ist $char(K) = 2$ und $j \neq 0$, so können wir $a_1 = 1$, $a_3 = 0$, $a_4 = 0$ erreichen. $P = -P$ liefert dann $(x_0, y_0) = -(x_0, y_0) = (x_0, -y_0 - x_0) = (x_0, y_0 + x_0)$ und damit $x_0 = 0$. Damit ist
$$E[2] = \{O, (0, \sqrt{a_6})\}.$$
- Ist $char(K) = 2$ und $j = 0$, so ist $a_1 = 0$ und $a_3 \neq 0$. Damit folgt die Gleichung
$$(x_0, y_0) = -(x_0, y_0) = (x_0, y_0 + a_3),$$
die offensichtlich keine Lösung hat. Also $E[2] = \{O\}$. ■

Literatu: [**13**].

KAPITEL 5

Isogenien

Wir wollen in diesem Abschnitt Abbildungen zwischen elliptischen Kurven studieren.

LEMMA. *Sei E eine elliptische Kurve und $P \in E$. Dann ist*

$$\tau_P : E \to E, \quad Q \mapsto Q + P$$

ein Isomorphismus mit Umkehrabbildung τ_{-P}. Man nennt τ_P die Translation um P.

Beweis: Die die Addition auf einer elliptischen Kurve durch algebraische Formeln beschrieben wird, ist klar, daß τ_P eine rationale Abbildung ist. Da E nichtsingulär ist, ist damit τ_P sogar ein Morphismus. Man rechnet sofort nach, daß $\tau_{-P} \circ \tau_P = id$ gilt. ■

Sei $\phi : E_1 \to E_2$ ein Morphismus elliptischer Kurven und $Q = \phi(O)$. Dann gilt für $\tilde{\phi} = \tau_{-Q} \circ \phi$ natürlich $\tilde{\phi}(O) = O$, d.h. $\phi = \tau_Q \circ \tilde{\phi}$: jeder Morphismus läßt sich also zerlegen in eine Translation und einen Morphismus, der die Nullpunkte respektiert.

DEFINITION. Ein Morphismus $\phi : E_1 \to E_2$ elliptischer Kurven heißt Isogenie, falls $\phi(O) = O$ gilt. Zwei elliptische Kurve E_1, E_2 heißen isogen, falls es eine Isogenie $\neq 0$ zwischen ihnen gibt.

LEMMA. *(Multiplikation mit m). Sei $m \in \mathbf{Z}$. Wir definieren $[m] : E \to E$ durch*

$$\begin{aligned} [m](P) &= P + \cdots + P \text{ (m-fache Summe) für } m \geq 0, \\ &= -[-m](P) \text{ für } m < 0. \end{aligned}$$

Dann ist $[m]$ eine Isogenie.

Beweis: Da die Addition auf E durch algebraische Formeln gegeben wird, sieht man durch Induktion, daß $[m]$ eine rationale Abbildung und damit ein Morphismus ist. Wegen $[m](O) = O$ ist dann $[m]$ eine Isogenie. ■

Ebenso einfach zeigt man:

LEMMA. *Sei K ein Körper der Charakteristik p und $q = p^e$. Sei E eine elliptische Kurve mit der Gleichung $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ und $E^{(q)}$ die elliptische Kurve mit der Gleichung $y^2 + a_1^q xy + a_3^q y = x^3 + a_2^q x^2 + a_4^q x + a_6^q$. Dann ist $\phi : E \to E^{(q)}$, $(x, y) \mapsto (x^q, y^q)$ eine Isogenie vom Grad q.*

Beispiel: Sei $char(K) \neq 2$, $a \in K$, $a \neq 0$ und $E : y^2 = x^3 + ax$, $E' : y^2 = x^3 - 4ax$. Durch Nachrechnen sieht man, daß die Zuordnung

$$(x, y) \mapsto (x + \frac{a}{x}, \frac{y}{x}(x - \frac{a}{x}))$$

eine rationale Abbildung $\phi : E \to E'$ liefert. Zunächst ist ϕ nicht definiert in $(0, 0)$ und $O = (0 : 0 : 1)$. Man rechnet allerdings ebenfalls nach, daß $\phi((0, 0)) = \phi(O) = O$ gilt. Also ist ϕ eine Isogenie.

Von fundamentaler Bedeutung ist folgender Satz:

SATZ. *Ist $\phi : E_1 \to E_2$ eine Isogenie, so gilt $\phi(P + Q) = \phi(P) + \phi(Q)$, d.h. Isogenien sind Gruppenhomomorphismen.*

Beweis: Wir haben Bijektionen

$$\lambda_i : E_i \to \mathrm{Pic}^0(E_i), \quad P \mapsto \text{ Klasse von } P - O,$$

die nach Definition auch Gruppenisomorphismen sind. Wir haben gesehen, daß auch

$$\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$$

ein Gruppenhomomorphismus ist. Da das folgende Diagramm kommutativ ist,

$$\begin{array}{ccc} E_1 & \xrightarrow{\lambda_1} & \mathrm{Pic}^0(E_1) \\ \phi \downarrow & & \downarrow \phi_* \\ E_2 & \xrightarrow{\lambda_2} & \mathrm{Pic}^0(E_2) \end{array}$$

folgt sofort, daß auch $\phi = \lambda_2^{-1} \circ \phi_* \circ \lambda_1$ ein Gruppenhomomorphismus ist. ■

DEFINITION. Sei E_1, E_2 elliptische Kurven über K. Dann ist

$$\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2 \text{ Isogenie }\}$$

mit $(\phi + \psi)(P) = \phi(P) + \psi(P)$ eine abelsche Gruppe.

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

erhält durch $(\phi\psi)(P) = \phi(\psi(P))$ zusätzlich eine Ringstruktur. $\mathrm{End}(E)$ heißt der Endomorphismenring von E. Analog definiert man $\mathrm{Hom}_K(E_1, E_2)$ bzw. $\mathrm{End}_K(E)$, indem man nur die über K definierten Isogenien betrachtet.

SATZ. *Sei E eine elliptische Kurve. Dann gilt:*

1. $\mathrm{End}(E)$ *ist nullteilerfrei.*
2. $\mathbf{Z} \to \mathrm{End}(E)$, $m \mapsto [m]$ *ist injektiver Ringhomomorphismus. Wir denken uns fortan* $\mathbf{Z} \subseteq \mathrm{End}(E)$.

Beweis:

1. Seien $\phi, \psi \in \mathrm{End}(E)$ mit $\phi\psi = 0$, d.h. $\phi(\psi(P)) = O$ für alle $P \in E_1$.
   1. Fall: ψ ist konstant, wegen $\psi(O) = O$ also $\psi = 0$.
   2. Fall: ψ ist nicht konstant und damit surjektiv. Dann folgt aber sofort $\phi = 0$.
2. Man sieht sofort, daß $\mathbf{Z} \to \mathrm{End}(E)$ ein Ringhomomorphismus ist. Wir nehmen an, er ist nicht injektiv. Nach 1. muß der Kern ein Primideal in $\mathbf{Z}$ sein, d.h. es gibt eine Primzahl p mit $[p] = 0$. Der Einfachkeit halber setzen wir $char(K) \neq 2$ voraus. Wir haben gesehen, daß es dann drei Punkte $P_1, P_2, P_3 \in E$ gibt mit $\{P \in E : 2P_0 = O\} = \{O, P_1, P_2, P_3\}$. Damit gilt:

   $$[2](P) = O \iff P \in \{(O, P_1, P_2, P_3\},$$

   Insbesondere ist $[2] \neq 0$. Wir schreiben jetzt $p = 2\ell + 1$ und erhalten

   $$[p](P_1) = (2\ell + 1)(P_1) = P_1 \neq O,$$

   also $[p] \neq 0$ und damit einen Widerspruch. Damit folgt die Behauptung. ■

Bemerkung: $\mathrm{Aut}(E) \subseteq \mathrm{End}(E)$, genauer gilt:

$$\mathrm{Aut}(E) = \mathrm{End}(E)^*.$$

Beispiel: Sei E eine elliptische Kurve in Charakteristik 2 mit $j(E) = 0$. Dann ist $\mathrm{Aut}(E)$ eine nichtabelsche Gruppe der Ordnung 24. Insbesondere ist damit $\mathrm{End}(E)$ nichtkommutativ.

SATZ. *Sei $\phi : E_1 \to E_2$ eine nichtkonstante Isogenie. Dann gilt für alle $Q \in E_2$*

$$\#\phi^{-1}(Q) = \deg_s \phi,$$

insbesondere ist $kern(\phi) = \phi^{-1}(O)$ eine endliche abelsche Gruppe der Ordnung $\deg_s \phi$.

Beweis: Sei $Q \in E_2$ und $P \in \phi^{-1}(Q)$. Dann sieht man sofort, daß

$$\phi^{-1}Q = P + \phi^{-1}O$$

gilt. Insbesondere hat man damit $\#\phi^{-1}Q = \#\phi^{-1}O$, d.h. alle Fasern haben gleiche Mächtigkeit. Da wir aber bereits wissen, daß es einen Punkt $Q_0 \in E_2$ gibt mit $\#\phi^{-1}(Q_0) = \deg_s \phi$, folgt die Behauptung. ■

FOLGERUNG. *Sei $\phi : E_1 \to E_2$ eine nichtkonstante separable Isogenie. Dann ist ϕ unverzweigt und $kern(\phi)$ hat Ordnung* $\deg\phi$.

Beweis: Die Behauptung folgt sofort aus dem Kriterium, daß ϕ genau dann unverzweigt ist, wenn jede Faser genau $\deg\phi$ Elemente enthält. ■

Überlegungen:

1. Sei E eine elliptische Kurve und $P \in E$. Dann induziert $E \xrightarrow{\tau_P} E$ einen Körperhomomorphismus

   $$\overline{K}(E) \xrightarrow{\tau_P^*} \overline{K}(E), \quad f \mapsto (X \mapsto f(P+X)),$$

   der offensichtlich die Konstanten fest läßt. D.h. $\tau_P^* \in \mathrm{Aut}(\overline{K}(E)|\overline{K})$. Wegen $\tau_{P+Q}^* = \tau_P^* \circ \tau_Q^*$ ist

   $$E \to \mathrm{Aut}(\overline{K}(E)|\overline{K}), \quad P \mapsto \tau_P^*$$

   ein Gruppenhomomorphismus.
2. Sei nun $\phi : E_1 \to E_2$ eine nichtkonstante Isogenie mit Kern U. Für $P \in U$ und $g \in \overline{K}(E_2)$ gilt:

   $$\begin{aligned}(\tau_P^*(\phi^*g))(Q) &= (\phi^*g)(P+Q) = g(\phi(P+Q)) = \\ &= g(\phi(P)+\phi(Q)) = g(\phi(Q)) = (\phi^*g)(Q),\end{aligned}$$

   d.h. $\tau_P^*(\phi^*g) = \phi^*g$, τ_P^* läßt also die Elemente aus $\phi^*\overline{K}(E_2)$ fest. Damit erhalten wir einen Gruppenhomomorphismus

   $$U \to \mathrm{Aut}(\overline{K}(E_1)|\phi^*\overline{K}(E_2)),$$

   der offensichtlich injektiv ist. Die Galoistheorie liefert damit sofort folgenden Satz:

SATZ. *Ist $\phi : E_1 \to E_2$ eine nichtkonstante separable Isogenie, dann ist $\overline{K}(E_1)$ galoissch über $\phi^*\overline{K}(E_2)$ mit Galoisgruppe $Kern(\phi)$. Genauer:*

$$Kern(\phi) \to \mathrm{Gal}(\overline{K}(E_1)|\phi^*\overline{K}(E_2)), \quad P \mapsto \tau_P^*$$

ist ein Isomorphismus.

Der folgende Satz besagt, daß auch jede endliche Untergruppe $U \subseteq E$ als Kern einer separablen Isogenie auftritt.

SATZ. *Ist E eine elliptische Kurve und $U \subseteq E$ eine endliche Untergruppe, so gibt es eine elliptische Kurve E' und eine separable Isogenie $\phi : E \to E'$ mit $Kern(\phi) = U$. Man schreibt auch E/U für E'.*

Beweisidee: $\{\tau_P^* : P \in U\}$ ist eine endliche Untergruppe von $\mathrm{Aut}(\overline{K}(E)|\overline{K})$. Der Fixkörper ist der Funktionenkörper einer Kurve E'. Man man nun zeigen, daß E' eine elliptische Kurve ist, daß der durch die Körperinklusion $\overline{K}(E') \subseteq \overline{K}(E)$ gegebene Morphismus $\phi : E \to E'$ die gewünschte Isogenie ist. ■

Der letzte Satz geht allerdings wesentlich expliziter wie folgt:

SATZ. *Sei $char(K) \neq 2, 3$, $E : y^2 = x^3 + ax + b$ eine elliptische Kurve und $U \subseteq E$ eine endliche Untergruppe. Definiert man*

$$n = \#U, \quad p_i = \sum_{(u,v) \in U \setminus \{O\}} u^i, \quad A = -(5n-6)a - 15p_2, \quad B = -(14n-15)b - 21ap_1 - 35p_3$$

und

$$E' : y^2 = x^3 + Ax + B, \quad \phi(x,y) = (x + \sum_{P \in U\setminus\{O\}} \tau_P^* x - x(P), \quad y + \sum_{P \in U\setminus\{O\}} \tau_P^* y - y(P)),$$

so ist $\phi : E \to E'$ eine Isogenie mit Kern U.

Überlegung: Sei $\phi : E_1 \to E_2$ eine separable Isogenie vom Grad m, so daß auch $[m]$ separabel ist. Wegen $\#Kern(\phi) = m$ hat man $[m]Kern(\phi) = O$ und damit $Kern(\phi) \subseteq Kern([m])$. Die Galoistheorie liefert daher eine Inklusion der Funktionenkörper

$$\overline{K}(E_1) \subseteq \overline{K}(E_2) \subseteq \overline{K}(E_1),$$

so daß die Inklusion $\overline{K}(E_1) \subseteq \overline{K}(E_2)$ eine Morphismus $\psi : E_2 \to E_1$ liefert mit $\psi \circ \phi = [m]$. Allgemein gilt:

SATZ. *Sei $\phi : E_1 \to E_2$ eine nichtkonstante Isogenie vom Grad m. Dann gibt es genau eine Isogenie $\hat{\phi} : E_2 \to E_1$, so daß $\hat{\phi} \circ \phi = [m]$ gilt. $\hat{\phi}$ heißt die zu ϕ duale Isogenie. Man setzt $\hat{0} = 0$.*

Wir beweisen den Satz nicht. Die Eindeutigkeit ist aber trivial: Gilt $\psi_1 \circ \phi = [m] = \psi_2 \circ \phi$, so gilt $(\psi_1 - \psi_2) \circ \phi = 0$, da ϕ nichtkonstant sein sollte, folgt damit sofort $\psi_1 = \psi_2$.

Die wichtigsten Eigenschaften der dualen Isogenie finden sich in folgendem Satz:

SATZ. *Seien $\phi : E_1 \to E_2$, $\lambda : E_2 \to E_3$, $\psi : E_1 \to E_2$ Isogenien und $m \in \mathbf{Z}$. Dann gilt:*

1. $\phi \circ \hat{\phi} = [m]$.
2. $\lambda \hat{\circ} \phi = \hat{\phi} \circ \hat{\lambda}$.
3. $\phi \hat{+} \psi = \hat{\phi} + \hat{\psi}$.
4. $\hat{[m]} = [m]$ *und* $\deg[m] = m^2$.
5. $\deg \hat{\phi} = \deg \phi$.
6. $\hat{\hat{\phi}} = \phi$.

Beweis: Wir beweisen nur die Aussagen für $[m]$, die Multiplikation mit m. Zunächst ist $[1] = id$ und damit $\hat{[1]} = [1]$. Mit den Additionsformeln und Induktion folgt dann sofort $\hat{[m]} = [m]$. Sei nun $d = \deg[m]$. Dann gilt nach Definition

$$[d] = \hat{[m]} \circ [m] = [m] \circ [m] = [m^2],$$

also $d = m^2$, was wir zeigen wollten. ■

Wir haben erwähnt, daß ein Morphismus $\phi : C_1 \to C_2$ genau dann separabel ist, wenn die Abbildung $\Omega_{C_2} \xrightarrow{\phi^*} \Omega_{C_1}$ von 0 verschieden ist. Damit kann man folgende Separabilitätsaussagen zeigen:

LEMMA. *Sei E eine elliptische Kurve in Charakteristik p und $\phi : E \to E^{(q)}$ der q-te Frobeniusmorphismus. Dann ist $[m] + [n]\phi$ genau dann separabel, wenn $m \not\equiv 0 \bmod p$ gilt. Insbesondere ist $[m]$ separabel, falls p nicht m teilt, und ebenso $1 - \phi$.*

DEFINITION. Sei E eine elliptische Kurve und $m \geq 1$. Dann heißt

$$E[m] = \{P \in E : mP = O\}$$

die Gruppe der m-Teilungspunkte oder m-Torsionspunkte.

SATZ. *Sei E eine elliptische Kurve und $m \geq 1$. Dann gilt:*

1. *Ist $char(K) = 0$ oder $char(K) = p$ und $m \not\equiv 0 \bmod p$, so ist*
$$E[m] \simeq Z_m \times Z_m.$$
2. *Ist $char(K) = p$, so gibt es zwei Möglichkeiten:*
   - *$E[p^e] \simeq Z_{p^e}$ für alle $e \geq 1$,*
   - *$E[p^e] = \{O\}$ für alle $e \geq 1$.*

Beweis:

1. In diesem Fall ist $[m]$ separabel, also $\#E[m] = Kern([m]) = \deg[m] = m^2$. Nach dem Hauptsatz über endliche abelsche Gruppen gibt es natürliche Zahlen $d_1|d_2|\ldots|d_r$ mit $E[m] \simeq Z_{d_1} \times \cdots \times Z_{d_r}$. Natürlich gilt $d_1 \ldots d_r = m^2$ und $d_i|m$. Wir können o.E. $m \geq 2$ und $d_i \geq 2$ voraussetzen. Wäre $r \geq 3$, so gäbe es eine Primzahl q mit $q|d_1$, $q|d_2$, $q|d_3$, also hätte man $\#E[q] \geq q^3$, ein Widerspruch zu der eben bewiesenen Aussage im Fall $m = q$. Also ist $r \leq 2$, woraus sofort $d_1 = d_2 = m$ folgt.

2. Sei ϕ der p-te Frobeniusmorphismus. Dann ist ϕ rein inseparabel vom Grad p, d.h. $\deg_s \phi = 1$. Wir zerlegen $[p] = \hat{\phi} \circ \phi$ und erhalten
$$\#E[p^e] = \deg_s [p^e] = (\deg_s [p])^e = (\deg_s \hat{\phi} \deg_s \phi)^e = (\deg_s \hat{\phi})^e.$$
Nun ist $p = \deg \phi = \deg \hat{\phi} = \deg_i \hat{\phi} \deg_s \hat{\phi}$. Es gibt also zwei Möglichkeiten:
   - $\deg_s \hat{\phi} = p$. Dann folgt $\#E[p^e] = p^e$ für alle $e \geq 1$,
   - $\deg_s \hat{\phi} = 1$. Dann ist $\#E[p^e] = 1$ für alle $e \geq 1$. ■

DEFINITION. Eine elliptische Kurve E in Charakteristik p heißt supersingulär, falls $E[p] = 0$ gilt.

Das folgende Ergebnis haben wir bereits gezeigt:

SATZ. *Eine elliptische Kurve E in Charakteristik 2 ist genau dann supersingulär, wenn $j(E) = 0$ gilt, d.h. wenn E über dem algebraischen Abschluß zu $y^2 + y = x^3$ isomorph ist.*

In Charakteristik 2 gibt es also nur eine supersinguläre elliptische Kurve. Dies verallgemeinert sich in Charakteristik p wie folgt:

SATZ. *Sei $p > 2$ und $H_p(t) = \sum_{i=0}^{m} (\binom{m}{i})^2 t^i$ mit $m = \frac{p-1}{2}$. Dann ist die elliptische Kurve $y^2 = x(x-1)(x-\lambda)$ (mit $\lambda \neq 0, 1$) genau dann supersingulär, wenn $H_p(\lambda) = 0$ gilt. Insbesondere gibt es in Charakteristik p (bis auf $\overline{K}$-Isomorphie) nur endlich viele supersinguläre elliptische Kurven.*

Beispiel: Wir faktorisieren $H_p(t)$ in $\mathbf{F}_p[t]$:
$$\begin{aligned} H_3(t) &= t + 1, \\ H_5(t) &= t^2 + 4t + 1, \\ H_7(t) &= (t+1)(t+3)(t+5), \\ H_{19}(t) &= (t+1)(t+9)(t+17)(t^2+4t+1)(t^2+13t+6)(t^2+18t+16). \end{aligned}$$

Was hier bereits anklingt, gibt folgende allgemeine Aussage:

SATZ. *Ist E eine supersinguläre Kurve in Charakteristik p, so ist $j(E) \in \mathbf{F}_{p^2}$.*

Literatur: [**13**], [**10**].

KAPITEL 6

Endomorphismenringe elliptischer Kurven über $\mathbf{F}_q$

Sei E eine elliptische Kurve über einem Körper K.
$\mathrm{End}(E)$ ist nullteilerfrei und $\mathbf{Z} \subseteq \mathrm{End}(E)$, wobei wir jetzt der Einfachkeit halber m statt $[m]$ schreiben. Dann ist

$$\mathrm{End}^0(E) := \{\frac{\phi}{n} : \phi \in \mathrm{End}(E), n \in \mathbf{N}\} = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}(E)$$

mit den üblichen Bruchrechenregeln ein Ring und ein $\mathbf{Q}$-Vektorraum. Außerdem ist $\mathrm{End}(E) \subseteq \mathrm{End}^0(E)$. Ist $\phi \in \mathrm{End}(E)$, so gilt auch für die duale Abbildung $\hat{\phi} \in \mathrm{End}(E)$. Die Abbildung $\hat{}: \mathrm{End}(E) \to \mathrm{End}(E)$ erfüllt die folgenden Eigenschaften:

- $\hat{m} = m$ für $m \in \mathbf{Z}$,
- $\hat{\phi}\phi = \phi\hat{\phi} = \deg\phi$,
- $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$,
- $\widehat{\phi\psi} = \hat{\psi}\hat{\phi}$.

Ist $\phi \in \mathrm{End}(E)$, $\phi \neq 0$, so ist $n = \deg\phi \geq 1$ und aus $n = \phi\hat{\phi}$ ergibt sich in $\mathrm{End}^0(E)$ dann $\phi \cdot \frac{1}{n}\hat{\phi} = 1$, woraus sofort folgt, daß $\mathrm{End}^0(E)$ ein Schiefkörper (oder Körper) ist.

LEMMA. *Für $\phi \in \mathrm{End}(E)$ gilt:*

1. *$Sp\phi := \phi + \hat{\phi} \in \mathbf{Z}$ und $N\phi := \phi\hat{\phi} \in \mathbf{N}_0$.*
2. *ϕ ist quadratisch und ganz über $\mathbf{Z}$, es genügt der Gleichung $\phi^2 - Sp(\phi)\phi + N(\phi) = 0$.*
3. *$|Sp\phi| \leq 2\sqrt{N\phi}$, wobei $=$ genau dann gilt, wenn $\phi \in \mathbf{Z}$ ist.*
4. *Ist $\phi \notin \mathbf{Z}$, so ist $\mathbf{Q}(\phi) \subseteq \mathrm{End}^0(E)$ ein imaginärquadratischer Körper, d.h. es gibt eine quadratfreie natürliche Zahl $d \geq 2$ mit $\mathbf{Q}(\phi) \simeq \mathbf{Q}(\sqrt{-d})$. Der Ring $\mathbf{Z}[\phi]$ ist eine Ordnung in $\mathbf{Q}(\phi)$, d.h. es gibt eine natürliche Zahl f mit*

$$\mathbf{Z}[\phi] \simeq \begin{cases} \mathbf{Z} + \mathbf{Z}f\sqrt{-d} & \text{für } d \equiv 1, 2 \bmod 4, \\ \mathbf{Z} + \mathbf{Z}f\frac{1+\sqrt{-d}}{2} & \text{für } d \equiv 3 \bmod 4. \end{cases}$$

Beweis:

1. Wir wissen bereits, daß $N\phi = \phi\hat{\phi} = \deg\phi$ eine ganze Zahl ≥ 0 ist. Wegen
$$\deg(1+\phi) = (1+\hat{\phi})(1+\phi) = 1 + (\hat{\phi} + \phi) + \deg\phi \in \mathbf{Z}$$
ist dann auch $Sp(\phi) = \phi + \hat{\phi}$ eine ganze Zahl.
2. Wegen $0 = (\phi - \phi)(\phi - \hat{\phi}) = \phi^2 - Sp\phi\phi + N\phi$ ist ϕ Nullstelle des Polynoms $x^2 - Sp(\phi)x + N(\phi) \in \mathbf{Z}[x]$, das höchsten Koeffizienten 1 hat.
3. Für alle $m, n \in \mathbf{Z}$ gilt
$$m^2 + Sp(\phi)mn + N(\phi)n^2 = (m + n\phi)(m + n\hat{\phi}) = \deg(m + n\phi) \geq 0,$$
also gilt auch für alle $x \in \mathbf{Q}$
$$x^2 + Sp(\phi)x + N\phi \geq 0.$$
Daher muß die Diskriminante des quadratischen Polynoms ≤ 0 sein, d.h. $(Sp\phi)^2 - 4N\phi \leq 0$ und damit
$$|Sp\phi| \leq 2\sqrt{N\phi}.$$
Gilt $|Sp\phi| = 2\sqrt{N\phi}$, dann folgt $(\phi + \hat{\phi})^2 = 4\phi\hat{\phi}$ und damit $(\phi - \hat{\phi})^2 = 0$, also $\hat{\phi} = \phi$. Also ist $\phi = \frac{1}{2}Sp\phi \in \frac{1}{2}\mathbf{Z}$. Da aber ϕ ganz über $\mathbf{Z}$ ist, folgt auch $\phi \in \mathbf{Z}$.

4. Sei $\phi \notin \mathbf{Z}$. Dann ist $|Sp\phi| < 2\sqrt{N\phi}$, die Diskriminante der quadratischen Gleichung $x^2 - Sp(\phi)x + N(\phi) = 0$ für ϕ erfüllt $Sp\phi^2 - 4N\phi < 0$. Also ist $\mathbf{Q}(\phi)$ ein imaginärquadratischer Zahlkörper. Der Rest ist allgemeine Theorie. ■

Bemerkung: Sei D ein Schiefkörper mit $\mathbf{Q} \subseteq D$. Man sagt, $\alpha \in D$ ist ganz über $\mathbf{Z}$, wenn es ein Polynom $f(x) \in \mathbf{Z}[x]$ gibt, das höchsten Koeffizienten 1 hat und $f(\alpha) = 0$ erfüllt. Ein Unterring $R \subseteq D$ heißt eine Ordnung, wenn R ein endlich erzeugter $\mathbf{Z}$-Modul ist und $\mathbf{Q}R = D$ gilt. Für $\alpha \in D$ ist $\mathbf{Q}(\alpha)$ ein (kommutativer) Körper. Genau dann ist α ganz über $\mathbf{Z}$, wenn $\mathbf{Z}[\alpha]$ eine Ordnung in $\mathbf{Q}(\alpha)$ ist.

FOLGERUNG. *Sei E eine elliptische Kurve. Ist $F \subseteq \mathrm{End}^0(E)$ ein (kommutativer) Körper, so ist $F = \mathbf{Q}$ oder imaginärquadratisch, d.h. $F = \mathbf{Q}(\sqrt{-d})$ für eine quadratfreie natürliche Zahl d.*

Beweis: O.E. ist $F \neq \mathbf{Q}$. Dann gibt es ein $\phi \in F \setminus \mathbf{Q}$. Der Körper $\mathbf{Q}(\phi)$ ist quadratisch über $\mathbf{Q}$ und $\mathbf{Q}(\phi) \subseteq F$. Wäre $\mathbf{Q}(\phi) \neq F$, so gäbe es ein $\psi \in F \setminus \mathbf{Q}(\phi)$; da auch $\mathbf{Q}(\psi)$ quadratisch über $\mathbf{Q}$ ist, wäre $\mathbf{Q}(\phi, \psi)$ vom Grad 4 über $\mathbf{Q}$ (und kommutativ), nach dem Satz vom primitiven Element gäbe es ein λ mit $\mathbf{Q}(\lambda) = \mathbf{Q}(\phi, \psi)$. Da aber λ höchstens quadratisch über $\mathbf{Q}$ ist, erhält man einen Widerspruch. ■

Sei E eine elliptische Kurve über $\mathbf{F}_q$ und $\pi \in \mathrm{End}(E)$ der Frobeniusmorphismus $(x, y) \mapsto (x^q, y^q)$. Aus $\deg \pi = q$ folgt $N\pi = \pi\hat{\pi} = q$. Für einen Punkt $P \in E(\overline{\mathbf{F}}_q)$ gilt:

$$P \in E(\mathbf{F}_q) \iff \pi P = P \iff (1 - \pi)P = 0 \iff P \in Kern(1 - \pi),$$

d.h. $E(\mathbf{F}_q) = Kern(1 - \pi)$. Nun ist $1 - \pi$ separabel und damit

$$\#E(\mathbf{F}_q) = \deg(1 - \pi) = (1 - \pi)(1 - \hat{\pi}) = 1 - Sp\pi + N\pi = 1 + q - Sp\pi.$$

Unser Lemma liefert für den Frobeniusendomorphismus $|Sp(\pi)| \leq 2\sqrt{N\pi} = 2\sqrt{q}$, woraus wir erhalten $|\#E(\mathbf{F}_q) - (q + 1)| = |Sp\pi| \leq 2\sqrt{q}$. Wir formulieren dies als Satz:

SATZ (Hasse). *Ist E eine elliptische Kurve über $\mathbf{F}_q$ mit Frobenius $\pi(x, y) = (x^q, y^q)$, so gilt*

$$E(\mathbf{F}_q) = Kern(1 - \pi) \quad \textit{und} \quad \#E(\mathbf{F}_q) = 1 + q - Sp(\pi)$$

und

$$|\#E(\mathbf{F}_q) - (q + 1)| \leq 2\sqrt{q}$$

oder anders geschrieben:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbf{F}_q) \leq q + 1 + 2\sqrt{q}.$$

Die Aussage $\#E(\mathbf{F}_q) = q + 1 - Sp\pi$ kann man umgekehrt auch benutzen um den Frobenius auszurechnen.

Beispiel: Wir betrachten $E : y^2 + xy = x^3 + 1$ über $\mathbf{F}_2$. Dann ist

$$E(\mathbf{F}_2) = \{O, (0, 1), (1, 0), (1, 1)\},$$

also $\#E(\mathbf{F}_2) = 4$, $Sp(\pi) = 1 + 2 - 4 = -1$ und damit $\pi^2 + \pi + 2 = 0$ und $\pi = \frac{-1+\sqrt{-7}}{2}$.

Beispiel: Wir betrachten alle elliptischen Kurven über $\mathbf{F}_2$ und erhalten:

Kurve E	$j(E)$	$\#E(\mathbf{F}_2)$	$Sp(\pi)$	π
$y^2 + xy = x^3 + 1$	1	4	-1	$\frac{-1+\sqrt{-7}}{2}$
$y^2 + xy = x^3 + x^2 + 1$	1	2	1	$\frac{1+\sqrt{-7}}{2}$
$y^2 + y = x^3$	0	3	0	$\sqrt{-2}$
$y^2 + y = x^3 + x$	0	5	-2	$-1 + i$
$y^2 + y = x^3 + x + 1$	0	1	2	$1 + i$

Beispiel: Wir schreiben alle elliptischen Kurven über $\mathbf{F}_5$ auf, wo f_π das Minimalpolynom von π über $\mathbf{Q}$ ist:

$j(E)$	E	$\#E(\mathbf{F}_5)$	f_π	π
0	$y^2 = x^3 + 1$	6	$t^2 + 5$	$\sqrt{-5}$
0	$y^2 = x^3 + 2$	6	$t^2 + 5$	$\sqrt{-5}$
$1728 = 3$	$y^2 = x^3 + x$	4	$t^2 - 2t + 5$	$1 + 2i$
$1728 = 3$	$y^2 = x^3 + 2x$	2	$t^2 - 4t + 5$	$2 + i$
$1728 = 3$	$y^2 = x^3 + 3x$	10	$t^2 + 4t + 5$	$-2 + i$
$1728 = 3$	$y^2 = x^3 + 4x$	8	$t^2 + 2t + 5$	$-1 + 2i$
1	$y^2 = x^3 + 4x + 4$	8	$t^2 + 2t + 5$	$-1 + 2i$
1	$y^2 = x^3 + x + 2$	4	$t^2 - 2t + 5$	$1 + 2i$
2	$y^2 = x^3 + x + 1$	9	$t^2 + 3t + 5$	$\frac{-3+\sqrt{-11}}{2}$
2	$y^2 = x^3 + 4x + 3$	3	$t^2 - 3t + 5$	$\frac{3+\sqrt{-11}}{2}$
4	$y^2 = x^3 + 3x + 3$	5	$t^2 - t + 5$	$\frac{1+\sqrt{-19}}{2}$
4	$y^2 = x^3 + 2x + 4$	7	$t^2 + t + 5$	$\frac{-1+\sqrt{-19}}{2}$

Bemerkung: Ist E eine elliptische Kurve über $\mathbf{F}_q$ mit Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$, so ist $\pi^n : (x, y) \mapsto (x^{q^n}, y^{q^n})$ der zum Körper $\mathbf{F}_{q^n}$ gehörige Frobenius. Also folgt

$$\#E(\mathbf{F}_q^n) = \deg(1 - \pi^n) = 1 + q^n - Sp(\pi^n).$$

Kennt man also $\#E(\mathbf{F}_q)$, so kann man damit zunächst π und dann damit $\#E(\mathbf{F}_{q^n})$ ausrechnen.

Beispiel: Wir betrachten $E : y^2 + xy = x^3 + 1$ über $\mathbf{F}_2$. Der Frobenius ist $\pi = \frac{-1+\sqrt{-7}}{2}$. Aus

$$\pi^2 = \frac{-3 - \sqrt{-7}}{2}, \quad \pi^3 = \frac{5 - \sqrt{-7}}{2}, \quad \pi^4 = \frac{1 + 3\sqrt{-7}}{2}$$

ergibt sich

$$\#E(\mathbf{F}_4) = 8, \quad \#E(\mathbf{F}_8) = 4, \quad \#E(\mathbf{F}_{16}) = 16.$$

Wir wollen jetzt $\mathrm{End}(E)$ nochmals näher betrachten. Für eine elliptische Kurve E über einem endlichen Körper $\mathbf{F}_q$ haben wir natürlich immer den Frobenius π und damit $\mathbf{Q}(\pi) \subseteq \mathrm{End}^0(E)$. Das folgende Beispiel zeigt, daß $\pi \in \mathbf{Z}$ passieren kann.

Beispiel: $E : y^2 + y = x^3$ über $\mathbf{F}_2$ hat Frobenius $\pi = \sqrt{-2}$. Der Frobenius über $\mathbf{F}_4$ ist $\pi^2 = -2$, also $\mathbf{Z}[\pi^2] = \mathbf{Z}$.

LEMMA. *Ist E eine über $\mathbf{F}_q$ ($q = p^n$) definierte elliptische Kurve mit Frobenius π und $\pi \in \mathbf{Z}$, so ist $\pi = \pm\sqrt{q} = p^{\frac{n}{2}}$, insbesondere q also ein Quadrat. E ist in diesem Fall supersingulär.*

Beweis: Sei $\pi = m \in \mathbf{Z}$. Dann ist $q = \deg \pi = m^2$, was die erste Behauptung ergibt. Da π rein inseparabel ist, muß aber dann auch $[p]$ rein inseparabel sein und damit $E[p] = 0$, d.h. E ist supersingulär. ■

LEMMA. *Sei E eine elliptische Kurve über $\mathbf{F}_q$ mit Frobenius π. Ist $\pi \notin \mathbf{Z}$, so gilt* $\mathrm{End}^0_{\mathbf{F}_q}(E) = \mathbf{Q}(\pi)$.

Beweis: Ist $\phi \in \mathrm{End}_{\mathbf{F}_q}(E)$, so ist ϕ über $\mathbf{F}_q$ definiert, ϕ ist also Frobenius-invariant und damit $\pi\phi = \phi\pi$. Also ist $\mathbf{Q}(\pi, \phi) \subseteq \mathrm{End}^0(E)$ ein (kommutativer) Körper, also quadratisch und damit $\phi \in \mathbf{Q}(\pi)$. ■

FOLGERUNG. *Ist E eine über $\mathbf{F}_q$ definierte elliptische Kurve mit Frobenius π und gilt $\pi^n \notin \mathbf{Z}$ für alle $n \geq 1$, so ist* $\mathrm{End}^0(E) = \mathbf{Q}(\pi)$, *insbesondere imaginärquadratisch.*

Beweis: Da π^n der Frobenius zum Körper $\mathbf{F}_{q^n}$ ist und $\mathrm{End}^0(E) = \cup_{n\geq 1}\mathrm{End}^0_{\mathbf{F}_{q^n}}(E)$, folgt die Behauptung aus dem letzten Lemma. ■

Beispiel: Wir betrachten die elliptische Kurve $y^2 = x^3 + 2x$ über $\mathbf{F}_p$ für verschiedene $p \geq 3$. Wir haben einen Endomorphismus $\alpha : (x, y) \mapsto (-x, iy)$, der $\alpha^2 = -1$ erfüllt. Durch Berechnen von $\#E(\mathbf{F}_p)$ erhalten wir π:

p	3	5	7	11	13	17	19
$\#E(\mathbf{F}_p)$	4	2	8	12	10	20	20
$Sp\pi$	0	4	0	0	4	-2	0
π	$\sqrt{-3}$	$2+i$	$\sqrt{-7}$	$\sqrt{-11}$	$2+3i$	$-1+4i$	$\sqrt{-19}$

Für $p = 3, 7, 11, 19$ ist daher $\mathbf{Q}(\alpha, \pi)$ sicher nicht quadratisch, daher $\mathrm{End}^0(E)$ nichtkommutativ.

Man kann die Theorie noch weiterentwickeln und folgenden Satz erhalten:

SATZ. *Sei E eine elliptische Kurve über $\mathbf{F}_q$ mit Frobenius π und $p = char(\mathbf{F}_q)$. Dann gilt:*

1. *Die folgenden Aussagen sind äquivalent:*
   (a) *E ist supersingulär, d.h. $E[p] = 0$.*
   (b) *$\pi^n \in \mathbf{Z}$ für ein $n \in \mathbf{N}$.*
   (c) *$Sp(\pi) \equiv 0 \bmod p$.*
   (d) *$\mathrm{End}^0(E)$ ist eine Quaternionenalgebra. Genauer: Es gibt $i, j \in \mathrm{End}^0(E)$, so daß gilt*
   $$\mathrm{End}^0(E) = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}ij \quad \text{mit} \quad i^2 = -1, j^2 = -p, ji = -ij.$$
2. *Ist E nicht supersingulär, so ist $\mathrm{End}^0(E) = \mathbf{Q}(\pi)$ und imaginär quadratisch.*

FOLGERUNG. *Sei $p \geq 5$. Eine über $\mathbf{F}_p$ definierte elliptische Kurve E ist genau dann supersingulär, wenn $\#E(\mathbf{F}_p) = p + 1$ gilt.*

Beweis: E ist genau dann supersingulär, wenn $Sp(\pi) \equiv 0 \bmod p$ gilt, was wegen $|Sp(\pi)| \leq 2\sqrt{p}$ und $p \geq 5$ mit $Sp(\pi) = 0$ äquivalent ist. Mit $\#E(\mathbf{F}_p) = p + 1 - Sp(\pi)$ folgt die Behauptung. ■

Literatur: [**13**], [**2b**].

KAPITEL 7

Public-Key-Kryptographie

1. Einführung

Sowohl in der Codierungstheorie als auch in der Kryptographie geht es um Nachrichtenübertragung:

- In der Codierungstheorie geht es darum, einen Text so zu verschlüsseln, daß er gut rekonstruiert werden kann, wenn es auch Störungen bei der Übertragung gibt. Beispiele:
  - Signale eines Satelliten,
  - CD-Spieler,
  - Computernetze,
  - gesprochene Sprache.
- In der Kryptographie geht es darum, den Inhalt einer Nachricht vor Unbefugten zu schützen. Anwendungsbeispiele und Anwendungsgebiete:
  - Militärische oder diplomatische Informationen sollen vor dem Feind geheim gehalten werden. (Das war sicher der Ausgangspunkt der Kryptographie.)
  - Abhörsicherheit bei Mobiltelefonen oder bei Satellitenübertragung von Telefongesprächen.
  - Pay-TV: Nur wer zahlt, darf fernsehen.
  - Elektronische Bankgeschäfte.
  - Computernetze.
  - Nicht jeder soll leicht meine email lesen können.
  - Einkaufen per Internet mit Angabe der Kreditkartennummer.
  - Chipkarten, z.B. Telefonkarten.

Die Situation in der Kryptographie ist also folgende: A will einen Text T an B senden. A hat eine Verschlüsselungsfunktion bzw. -vorschrift f und macht aus T den Text $C = f(T)$. Dieser wird an B übermittelt. B wendet die Entschlüsselungsfunktion bzw. -vorschrift f^{-1} an auf C und erhält $T = f^{-1}(C)$, den ursprünglichen Text. Wichtig: f und f^{-1} werden geheimgehalten. Gewöhnlich liegt bei den Ver- und Entschlüsselungsfunktionen ein festgewähltes Verfahren zugrunde, das 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}.

Beispiel: Auf Gaius Julius Caesar (100–44 v.Chr.) soll folgendes Verfahren zurückgehen:

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
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 $f(a) = D$, ... $f^{-1}(A) = x$, ... Aus dem Text *heute ist donnerstag* wird dann *KHXWH LVW GRQQHUVWDJ*. Nummeriert man die Buchstaben durch von 0 bis 25, so wird die Verschlüsselungsfunktion

$$f(x) = x + 3 \bmod 26$$

und damit die Entschlüsselungsfunktion

$$f^{-1}(x) = x - 3 \bmod 26.$$

Bei den klassischen (oder symmetrischen) kryptographischen Verfahren, kann man aus f_K sofort f_K^{-1} berechnen. Alles hängt dann von der Geheimhaltung des Schlüssels K ab.

Public-Key-Kryptosysteme: (Die Idee geht auf Diffie und Hellman (1976) zurück.) Man braucht Verschlüsselungsfunktionen f_K mit folgenden Eigenschaften:

- Kennt man den Schlüssel K, so kann man schnell $f_K(T)$ für eine Nachricht T berechnen.
- Auch bei Kenntnis von K kann man $f_K^{-1}(C)$ für eine Nachricht C praktisch (d.h. in angemessener Zeit) nicht berechnen.

(Derartige Funktionen nennt man auch Einwegfunktionen.)
Wir denken uns ein System mit vielen Teilnehmern A, die paarweise vertraulich Informationen austauschen wollen.

- Jeder Teilnehmer A hat eine Verschlüsselungsfunktion f_A und die zugehörige Entschlüsselungsfunktion f_A^{-1}.
- In einer Liste (Telefonbuch) findet man die Daten (A, f_A). Die Verschlüsselungsfunktion f_A ist also allgemein bekannt, man nennt den zugehörigen Schlüssel den öffentlichen Schlüssel von A. Allerdings ist f_A^{-1} nur A selbst bekannt; der zugehörige Schlüssel heißt der private Schlüssel von A.

Was kann man damit machen?

- Will A einen Text T an B senden, so sendet er $f_B(T)$. Mit $f_B^{-1}(f_B(T)) = T$ erfährt B den ursprünglichen Text. Da andere Teilnehmer C die Funktion f_B^{-1} nicht kennen, können sie T aus der Kenntnis von $f_B(T)$ nicht berechnen.
- Wie kann B sicher sein, daß die Nachricht T von A stammt? (Authentifikation, wichtig z.B. bei Bankgeschäften) A nimmt ein Wort P und schreibt an den Schluß seines Textes $f_B(f_A^{-1}(P))$. B erhält dann am Schluß nach Entschlüsselung den unverständlichen Text $f_A^{-1}(P)$. B wendet jetzt f_A an und erhält P, was verständlich ist. Da f_A^{-1} nur A bekannt ist, kann der Text nur von A kommen.

Ein Vorteil eines solches Systems ist, daß es viele Teilnehmer haben kann, daß auch neue Teilnehmer unproblematisch hinzugefügt werden können.
Zieht man klassische Kryptosysteme vor, so kann man dennoch Public-Key-Kryptosysteme zum Schlüsselaustausch benutzen.

Frage: Gibt es Verschlüsselungsfunktionen f, so daß f^{-1} sich nicht aus f praktisch erschließen läßt?

2. RSA

Das wohl bekannteste Public-Key-Verfahren geht auf Rivest, Shamir und Adleman (1977) zurück. Wir beginnen mit der Mathematik.

LEMMA. *Seien p und q verschiedene Primzahlen, d eine natürliche Zahl mit $ggT(d,(p-1)(q-1)) = 1$ und $n = pq$. Dann ist*

$$f : \mathbf{Z}/(n) \to \mathbf{Z}/(n), \quad x \mapsto x^d$$

bijektiv. Ist e eine natürliche Zahl mit $de \equiv 1 \bmod (p-1)(q-1)$, so ist die Umkehrabbildung gegeben durch $f^{-1}(x) = x^e$.

Beweis: Wir wollen zeigen, daß für alle $x \in \mathbf{Z}$ gilt $x^{de} \equiv x \bmod pq$. Wegen des chinesischen Restsatzes genügt es, $x^{de} \equiv x \bmod p$ und $x^{de} \equiv x \bmod q$ zu zeigen. Wir schreiben $de = 1 + \ell(p-1)(q-1)$. Ist $x \equiv 0 \bmod p$, so gilt natürlich $x^{de} \equiv x \bmod p$. Ist $x \not\equiv 0 \bmod p$, so gilt $x^{p-1} \equiv 1 \bmod p$, da $(\mathbf{Z}/(p))^*$ Ordnung $p-1$ hat, also folgt

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

woraus schließlich die Aussage mod$p$ folgt. Analog folgt die Aussage mod$q$ und damit die Behauptung. ■

Bemerkungen:

1. Potenzieren $x^d \bmod n$ geht schnell.
2. Es ist leicht, sich große Primzahlen p und q zu verschaffen.
3. Faktorisierung einer Zahl $n = pq$ ist i.a. schwer.
4. Hat man $n = pq$ und eine Bijektion $\mathbf{Z}/(n) \xrightarrow{x \mapsto x^d} \mathbf{Z}/(n)$, so kennt man heute nur einen Weg um die Umkehrabbildung zu bestimmen, nämlich über die Faktorisierung von n und das Berechnen eines e mit $de \equiv 1 \bmod (p-1)(q-1)$.

Bevor man mit dem RSA-Verfahren beginnt, muß man sich einigen, wie man Text in Zahlen umsetzt. Eine Möglichkeit ist folgende:
Sei $\mathbf{A}$ die Menge der verwendeten Buchstaben und Sonderzeichen, $N = \#\mathbf{A}$ und $w : \mathbf{A} \to \{0, 1, \ldots, N-1\}$ eine Bijektion. Man wählt eine Zahl $k \geq 1$. Jeder Text T wird in Worte T_i bestehend aus k Buchstaben zerlegt:

$$T = T_1 T_2 T_3 \ldots$$

Ist $T_i = (t_0 t_1 \ldots t_{k-1})$, so setzt man

$$W(T_i) = w(t_0) + w(t_1)N + w(t_2)N^2 + \cdots + w(t_{k-1})N^{k-1}.$$

Dann gilt $0 \leq W(T_i) \leq N^k - 1$. Der Text T gibt dann eine Folge von Zahlen

$$W(T_1), W(T_2), W(T_3), \ldots,$$

die alle zwischen 0 und $N^{k-1} - 1$ liegen.

Wir denken uns jetzt eine Gruppe von Leuten, die sich auf ein Alphabet mit N Buchstaben und eine Wortlänge k wie oben geeinigt haben. Jeder muß dann folgendes tun:

- Wähle zwei große Primzahlen p und q mit $n = pq > N^k$.
- Teste (mit allen gängigen Faktorisierungsverfahren), ob sich N faktorisieren läßt. Wenn ja, wähle andere Primzahlen p und q.
- Wähle ein $d \in \mathbf{N}$ (mit $ggT(d, (p-1)(q-1)) = 1$) und bestimme dazu mit dem erweiterten euklidischen Algorithmus ein $e \in \mathbf{N}$ mit $de \equiv 1 \bmod (p-1)(q-1)$.
- Gib das Paar (n, d) als öffentlichen Schlüssel bekannt. Der private Schlüssel ist dann (n, e). Die Verschlüsselungsfunktion ist $f(x) \equiv x^d \bmod n$ und $f^{-1}(x) \equiv x^e \bmod n$.

Beispiel: Wir legen ein Alphabet $\mathbf{A}$ mit $N = 28$ Zeichen zugrunde und durch folgende Tabelle definierte Funktion $w : \mathbf{A} \to \{0, \ldots, 27\}$:

	A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Wir wollen den Text

HEUTE IST DER LETZTE DONNERSTAG IM JUNI.

mit dem öffentlichen Schlüssel

$$(944981483009, 1001)$$

verschlüsseln. Wir haben 5 Worte T_i. So ist $T_1 =$ HEUTE IS und $W(T_1) = w(H) + w(E) \cdot 28 + w(U) \cdot 28^2 + \cdots + w(S) \cdot 28^7 = 260706183396$. Man erhält folgende Tabelle mit $f(x) \equiv x^d \bmod n$:

Wort T_i	$W(T_i)$	$f(W(T_i))$
HEUTE IS	260706183396	629033489210
T DER LE	73258502932	313684161661
TZTE DON	196198321388	929649924795
NERSTAG	3403166970	505668424024
IM JUNI.	368900155381	255511526881

Durch Faktorisieren von $n = 944981483009 = 123457 \cdot 7654337$ kann man leicht den privaten Schlüssel errechnen. Man erhält: $e = 326634267737$.

Bemerkung: Wie berechnet man $x^d \bmod n$? Ist $d = d_0 + d_1 \cdot 2 + \cdots + d_r \cdot 2^r$ die Binärentwicklung von d mit $d_i \in \{0, 1\}$, so ist

$$x^d = \prod_{i=0}^{r} (x^{2^i})^{d_i}.$$

Definiert man rekursiv x_i und y_i durch

$$x_0 = x, \quad y_0 = x^{d_0} \quad \text{und} \quad x_{i+1} = x_i^2 \bmod n, \quad y_{i+1} = y_i x_{i+1}^{d_{i+1}} \bmod n,$$

so sieht man schnell, daß $y_r \equiv x^d \bmod n$ gilt. Man beachte, daß $d_i = 0, 1$ ist. Man braucht also $O(\log d)$ Schritte. Dies läßt sich auch einfach programmieren.
Ein Programm für ein beliebiges Monoid G, $g \in G$ und $d \in \mathbf{N}$ sieht z.B. so aus:

1. Setze $y \leftarrow 1$, $D \leftarrow d$, $z \leftarrow g$.
2. Ist $D \equiv 1 \bmod 2$, so setze $y \leftarrow yz$.
3. Setze $D \leftarrow \lfloor D/2 \rfloor$. Ist $D = 0$, so gib y als Ergebnis g^d aus und höre auf. Sonst setze $z \leftarrow z^2$ und gehe zu 2.

Worauf beruht also die Sicherheit von RSA:

- Man kann leicht große Primzahlen p und q produzieren.
- Es ist im allgemeinen schwer eine große Zahl $n = pq$ zu faktorisieren.
- Man kennt außer der Faktorisierung von $n = pq$ keinen Weg, um zu gegebenem n und d ein e mit $de \equiv 1 \bmod (p-1)(q-1)$ zu berechnen.

Literatur: [**3**], [**4**].

KAPITEL 8

ECM - Faktorisierung mit elliptischen Kurven

Jede natürliche Zahl n besitzt eine eindeutige Primfaktorzerlegung $n = p_1^{e_1} \dots p_r^{e_r}$. Um diese zu bestimmen kann man iterativ so vorgehen:

- Entscheide, ob n zusammengesetzt oder eine Primzahl ist.
- Ist n zusammengesetzt, bestimme einen nichttrivialen Teiler von n.

Wir werden beide Probleme getrennt voneinander behandeln.

Die numerischen Rechnungen wurden auf einem Notebook mit einem 75-MH5-Pentium-Prozessor und unter Verwendung von Ubasic durchgeführt. Angegebene Rechenzeiten beziehen sich auf diese Situation.

1. Primzahltests

Ein Primzahltest soll entscheiden, ob eine natürliche Zahl n zusammengesetzt oder eine Primzahl ist.

Naive Methode: Teilt keine der Zahlen

$$2, \quad 3, \quad 5, \quad 7, \quad 9, \quad 11, \quad \dots, \quad \lfloor \sqrt{n} \rfloor$$

die Zahl n, so ist n prim.

Beispiel: Mit der naiven Methode braucht man mehr als 2 Minuten um zu sehen, daß $p = 10^{15} + 37$ prim ist. Extrapoliert man dies, so würde man sehen, daß man für $p = 10^{50} + 151$ mehr als 10^{29} Jahre bräuchte.

Die naive Methode ist also für größere Zahlen nicht geeignet. Die Anzahl der Rechenschritte ist $O(\sqrt{n}) = O(e^{\frac{1}{2}\log n})$. Ein weiteres Problem ist, daß der Nachweis für einen Außenstehenden nicht nachprüfbar ist.

Ist p eine ungerade Primzahl, so ist $\mathbf{Z}/(p)$ ein Körper, die multiplikative Gruppe $(\mathbf{Z}/(p))^*$ also zyklisch von Ordnung $p-1$. Daher gilt $a^{p-1} \equiv 1 \bmod p$ für alle $1 \leq a \leq p-1$. Damit erhalten wir sofort folgenden Test:

Fermat-Test: Sei n eine ungerade natürliche Zahl. Ist a eine ganze Zahl mit $1 \leq a \leq n-1$ und $a^{n-1} \equiv 1 \bmod n$, so sagt man, n hat den Fermat-Test bzgl. a bestanden.

Nun ist klar:

- Ist n eine Primzahl, so besteht n den Fermat-Test (für jede Zahl a).
- Hat n den Fermat-Test nicht bestanden, so ist n zusammengesetzt.

Beispiel: Wir probieren $n = 10^{500} + i$ für $i = 1, 3, 5, 7, 9, \dots$.

- Man findet, $2^{n-1} \not\equiv 1 \bmod n$ für $i = 1, 3, 5, 9, \dots 959$. Also sind die entsprechenden Zahlen nicht prim, d.h. zusammengesetzt. Allerdings liefert obiges Kriterium noch keinen expliziten Teiler von n.
- Für $n = 10^{500} + 961$ gilt $2^{n-1} \equiv 1 \bmod n$ (in weniger als 3 Sekunden) und ebenso $a^{n-1} \equiv 1 \bmod n$ für $a = 3, 5, 7, 11, 13, 17, 19$. Ist n damit schon prim?

Bemerkungen:

1. Eine zusammengesetzte ungerade natürliche Zahl $n \geq 3$ heißt Carmichaelzahl, wenn für alle $a \in \mathbf{Z}$ mit $ggT(a, n) = 1$ gilt $a^{n-1} \equiv 1 \bmod n$.
2. Die erste Carmichaelzahl ist $561 = 3 \cdot 11 \cdot 17$, eine weitere ist $56052361 = 211 \cdot 421 \cdot 631$.

3. Man kann zeigen: Sind $6m+1$, $12m+1$ und $18m+1$ Primzahlen, so ist $n = (6m+1)(12m+1)(18m+1)$ eine Carmichael-Zahl, insbesondere besteht sie den Fermat-Test für $a = 2, 3, \ldots, 6m$.
4. Es wurde 1994 bewiesen, daß es unendlich viele Carmichaelzahlen gibt. Man kann also den Fermat-Test nicht so einfach benutzen um zu zeigen, daß eine Zahl Primzahl ist.

Sei p eine ungerade Primzahl und $p-1 = 2^\ell q$ mit einer ungeraden Zahl q. Die multiplikative Gruppe $(\mathbf{Z}/(p))^*$ ist zyklisch von der Ordnung $p-1 = 2^\ell q$. Das einzige Element der Ordnung 2 ist daher $-1 \equiv p-1$. Sei $a \in (\mathbf{Z}/(p))^*$, für $b = a^q$ gilt dann $b^{2^\ell} = 1$, also gilt

$$b = 1 \quad \text{oder} \quad -1 \in \{b, b^2, b^4, b^8, \ldots, b^{2^{\ell-1}}\}.$$

Das führt zu folgendem Test:

Miller-Test: Sei n eine ungerade natürliche Zahl und $n-1 = 2^\ell q$ mit q ungerade. Sei weiter $2 \le a \le n-1$. Ist

$$a^q \equiv 1 \bmod n \quad \text{oder} \quad (a^q)^{2^i} \equiv -1 \bmod n \text{ für ein } i \text{ mit } 0 \le i \le \ell - 1,$$

so sagt man, n hat den Test bzgl. a bestanden.

Für den Miller-Test gilt nun offensichtlich:

- Ist n eine Primzahl, so besteht n den Miller-Test.
- Hat n den Test nicht bestanden, so ist n zusammengesetzt.

Beispiel: Für die Carmichael-Zahl $n = 56052361$ gilt:

$$n - 1 = 2^3 \cdot q \text{ mit } q \text{ ungerade.}$$

Nun ist

$$\begin{aligned} 2^q &\equiv 40874919, \\ 40874919^2 &\equiv 1065129, \\ 1065129^2 &\equiv 1, \end{aligned}$$

also hat n den Miller-Test für $a = 2$ nicht bestanden.

Man kann nun zeigen:

- Ist n zusammengesetzt, so besteht n den Test höchstens für $\frac{1}{4}$ der a's zwischen 1 und $n-1$.
- Besteht n den Test für ℓ verschiedene (unabhängige) a's, so sollte die Wahrscheinlichkeit, daß n nicht prim ist $< (\frac{1}{4})^\ell$ sein.
- In der Praxis macht man den Test für einige a's. Besteht n diese Tests, so nennt man n wahrscheinlich prim bzw. eine wahrscheinliche Primzahl.

Als Ergebnis des Miller-Tests erhalten wir also eine der Aussagen:

- n ist wahrscheinlich prim.
- n ist zusammengesetzt.

Die *isprime*-Funktion von Maple hat früher so funktioniert.

Beispiel: Wir betrachten nochmals $n = 10^{500} + 961$. Es ist $n - 1 = 2^6 \cdot q$ mit $q \equiv 1 \bmod 2$. Nachfolgend sind die Exponenten e mit $(a^q)^e \equiv -1 \bmod n$ angegeben:

a	2	3	5	7	11	13	17	19
e	4	32	4	16	4	32	16	32

n besteht also den Miller-Test für alle Primzahlen ≤ 19. Wir nennen n wahrscheinlich prim.

Beispiel: Folgende Zahlen $n \geq 30000$ bestehen den Test mit $a = 2$, obwohl sie zusammengesetzt sind:

$$\begin{aligned} 2047 &= 23 \cdot 89 \\ 3277 &= 29 \cdot 113 \\ 4033 &= 37 \cdot 109 \\ 4681 &= 31 \cdot 151 \\ 8321 &= 53 \cdot 157 \\ 15841 &= 7 \cdot 31 \cdot 73 \\ 29341 &= 13 \cdot 37 \cdot 61 \end{aligned}$$

Keine dieser Zahlen besteht aber den Test für $a = 3$.

Bemerkung: Man kann zeigen: Gilt die verallgemeinerte Riemannsche Vermutung und besteht n den Miller-Test für $a = 2, 3, \ldots, [2(\log n)^2]$, so ist n prim.

Man kann also sehr schnell sehen, ob eine Zahl n zusammengesetzt oder wahrscheinlich prim ist. Ist n wahrscheinlich prim und will man sicher sein, daß n prim ist, so muß man noch einen Primzahlbeweis machen: Dazu gibt es auch verschiedene gängige Methoden:

- Der Jacobi-Summen-Test
- Primzahlbeweise mit elliptischen Kurven

Wir wollen dies aber vorerst nicht machen.

Hier ist das Ubasic-Programm *wprim.ub*:

```
 10  print:print "Das Programm testet, ob eine ungerade Zahl n>10"
 20  print "wahrscheinlich prim ist. Als Basis wurde 2,3,5 und 7 gewaehlt."
 30  print:input "n";N
 40  clr time
 50  L0=0:Q=N-1
 60  if Q@2=0 then Q=Q\2:L0=L0+1:goto 60
 70  A=2:L=L0:gosub 120
 80  A=3:L=L0:gosub 120
 90  A=5:L=L0:gosub 120
100  A=7:L=L0:gosub 120
110  print "wahrscheinlich prim":print "Zeit in Millisekunden:";time1000:goto 30
120  A=fnPower(A,Q,N)
130  if A=1 or A=N-1 then goto 180
140  if L=1 then print "nicht prim":print "Zeit in Millsekunden:";time1000:goto 30
150  A=(A^2)@N:L=L-1
160  if A=N-1 then goto 180
170  goto 140
180  return
190  fnPower(A0,B0,M0)
200  ' Funktion berechnet a0^b0 mod m0
210  A1=A0:B1=B0:N1=1
220  while B1<>0
230  if B1@2=1 then N1=(N1*A1)@M0
240  B1=B1\2
250  A1=(A1^2)@M0
260  wend
270  return(N1)
```

2. Faktorisierung

Um einen konkreten Hintergrund zu haben, wollen wir versuchen, die Zahlen $n = 11^{50} + i$ für $i = 1, \ldots, 10$ zu faktorisieren.

Kleine Teiler: Als erstes sucht man naiv durch Probieren, ob eine Zahl n kleine Teiler 2, 3, 5, 7, ..., 10^5 hat.
Ein Ubasic-Programm *kt.ub* tut dies:

```
 10  print:print "Das Programm bestimmt durch naives Suchen alle"
 20  print "Primteiler < 10^5 einer natuerlichen Zahl n.":print
 30  input "n=";N:print "Teiler:"
 40  clr time
 50  if N@2=0 then N=N\2:print 2:goto 50
 60  for I=3 to 100000 step 2
 70  if N@I=0 then N=N\I:print I:goto 70
 80  next
 90  print "Rest:";N
100  print "Zeit in Millisekunden:";time1000:print
110  goto 30
```

Beispiele:

- $11^{50}+3 = 2^2 \cdot n_{52}$. Einige Miller-Tests ergeben, daß n_{52} wahrscheinlich prim ist. Wir geben uns damit zufrieden.
- $11^{50}+4 = 5 \cdot 1409 \cdot n_{49}$. Ein Miller-Test ergibt, daß n_{49} zusammengesetzt ist.
- $11^{50}+8 = 3 \cdot 59 \cdot n_{50}$. Ein Miller-Test ergibt, daß n_{50} zusammengesetzt ist.

Wir nehmen von jetzt an, daß die kleinen Teiler jeweils schon entfernt wurden.

Die Idee von Pollard: Sei p ein Primteiler der Zahl n mit

$$p-1 = q_1^{e_1} \dots q_r^{e_r} \qquad \text{(Primfaktorzerlegung)}$$

und

$$q_i^{e_i} \leq K \text{ für alle } i.$$

Dann wird $(\mathbf{Z}/(p))^*$ annulliert von $p-1 = q_1^{e_1} \dots q_r^{e_r}$, also auch von $kgV(1 \dots K)$, d.h. für $a \in (\mathbf{Z}/(p))^*$ gilt

$$a^{kgV(1\dots K)} \equiv 1 \bmod p$$

und damit gilt auch

$$p | ggT(a^{kgV(1\dots K)} - 1, n).$$

Natürlich muß man $a^{kgV(1\dots K)} - 1$ nur modulo n berechnen, was sehr schnell geht. Durch Wahl von K und a kann man so versuchen, Teiler von n zu finden.

Hier ist das Ubasic-Programm *poll.ub*:

```
 10  print:print "Pollard-Methode mit Basis 2: Man waehlt ein k0, berechnet"
 20  print "dann k=kgV(1..k0) und versucht durch Bildung von ggT(2^k-1,n)"
 30  print "einen nichttrivalen Teiler der Zahl n zu finden. "
 40  ' Man fange z.B. mit k0=1000 an.
 50  print:input "k0=";K0
 60  K=1:for I=2 to K0:K=lcm(K,I):next
 70  print:input "n=";N
 80  clr time
 90  print "ggT=";gcd(fnPower(2,K,N)-1,N):print "Zeit in Millisekunden:";time1000
100  goto 70
110  fnPower(A0,B0,M0)
120  ' Funktion berechnet a0^b0 mod m0
130  A1=A0:B1=B0:N1=1
140  while B1<>0
150  if B1@2=1 then N1=(N1*A1)@M0
160  B1=B1\2
170  A1=(A1^2)@M0
```

```
180   wend
190   return(N1)
```

Beispiele: Wir wenden die Pollardsche Methode für $K = 5000$ und $a = 2$ an. $kgV(1 \ldots 5000)$ ist eine Zahl mit 2171 Dezimalstellen. Wir geben nur die Fälle an, wo wir Erfolg hatten.

- Wir haben $11^{50} + 8 = 3 \cdot 59 \cdot n_{50}$, wo n_{50} zusammengesetzt ist. Wir berechnen $ggT((2^{kgV(1\ldots5000)} - 1) \bmod n, n)$ und erhalten in weniger als 2 Sekunden den Teiler $p = 2891796499$, wobei tatsächlich wegen
$$p - 1 = 2 \cdot 3^3 \cdot 31 \cdot 823 \cdot 2099$$
die Gruppe $(\mathbf{Z}/(p))^*$ von $kgV(1 \ldots 5000)$ annulliert wird. Also ist
$$n^{50} + 8 = 3 \cdot 59 \cdot 2891796499 \cdot n_{41}$$
und n_{41} ist zusammengesetzt.
- Bei $11^{50} + 5$ finden wir den Teiler 1235243182721, der sich in 435923 und 2833627 zerlegt.
- Bei $11^{50} + 9$ finden wir den Primteiler 2731049.

Wann funktioniert die Pollardsche Methode für festes K und p? Dann, wenn $(\mathbf{Z}/(p))^*$ von $kgV(1 \ldots K)$ annulliert wird, d.h. wenn gilt
$$\#(\mathbf{Z}/(p))^* | kgV(1 \ldots K).$$

3. Lenstras ECM-Verfahren

Pollards Faktorisierungsmethode liefert einen Teiler p, wenn $(\mathbf{Z}/(p))^*$ speziell gebaut ist, genauer: wenn es von $kgV(1 \ldots K)$ annulliert wird. Dies hat man aber nicht im Griff: entweder es funktioniert oder es funktioniert nicht. Lenstra kam auf die Idee, einer Zahl noch andere Testobjekte zuzuordnen, nämlich elliptische Kurven. Davon gibt es nämlich bei fester Primzahl p viele.

Vorbereitungen:

- Wir betrachten elliptische Kurven E_a, die durch $y^2 = x^3 + ax + 1$ gegeben sind. Der Punkt $P = (1 : 0 : 1)$ liegt auf E_a.
- Wir schreiben die Additionsgesetze auf E_a in homogener Form:
$$(x_0 : x_1 : x_2) + (y_0 : y_1 : y_2) = (z_0 : z_1 : z_2).$$

Sei jetzt n eine zusammengesetzte natürliche Zahl (ohne kleine Teiler) und p ein Primteiler von n.

- Wir wählen eine Zahl K und berechnen $L = kgV(1 \ldots K)$.
- Wir wählen ein $a \in \mathbf{Z}$ und berechnen den Punkt $L \cdot P = (z_0 : z_1 : z_2)$ modulo n, was unproblematisch ist, wenn wir uns die Kurve über $\mathbf{F}_p$ definiert denken wegen $n = 0$ in $\mathbf{F}_p$.
- Ist $ggT(z_0, n) \neq 1$, so haben wir einen nichttrivialen Teiler von n gefunden. Ist $ggT(z_0, n) = 1$, so wählen wir ein anderes a (oder K) und probieren weiter.

Wann funktioniert das? Ist $\#E_a(\mathbf{F}_p) | kgV(1 \ldots K)$, so folgt $kgV(1 \ldots K) \cdot P = (0 : 0 : 1)$ in $E_a(\mathbf{F}_p)$, also $z_0 \equiv 0 \bmod p$ und damit $p | ggT(z_0, n)$.

Es ist nicht schwer, dazu ein entsprechendes Programm zu schreiben, wenn man die Additionstheoreme hat. Hier ist ein Ubasic-Programm *ecm.ub*:

```
 10   print:print "Faktorisierungsversuch mit elliptischen Kurven y^2=x^3+ax+1."
 20   print "Man waehlt ein k0, bildet dann k=kgV(1..k0). Fuer eine natuerliche "
 30   print "Zahl n wird dann bei variierendem a der Punkt k(1:0:1) berechnet - "
 40   print "hoffend dabei einen nichttrivialen Teiler von n zu erhalten.":print
 50   input "k0=";K0
 60   K=1:for I=2 to K0:K=lcm(K,I):next
 70   print:input "n=";N
 80   input "Startwert fuer a=";A:A=A-1:clr time
 90   A=A+1:print "a=";A
100   ' Gestartet wird mit dem Punkt (1:0:1)
```

```
110   A0=1:A1=0:A2=1
120   K0=K:P0=0:P1=0:P2=1:B0=A0:B1=A1:B2=A2
130   while K0>0
140   if K0@2=1 then X0=P0:X1=P1:X2=P2:Y0=B0:Y1=B1:Y2=B2:gosub 210:P0=Z0:P1=Z1:P2=Z2
150   K0=K0\2
160   X0=B0:X1=B1:X2=B2:gosub 340:B0=Z0:B1=Z1:B2=Z2
170   wend
180   if gcd(N,P0)>1 or gcd(N,P1)>1 or gcd(N,P2)>1 then print "ggT's sind: ";gcd(N,P0),gcd(N,P1),g
190   goto 90
200   ' Addition zweier Punkte: (x0:x1:x2)+(y0:y1:y2)=(z0:z1:z2)
210   Z0=(A*X0^2*Y0*Y1-A*X0*X1*Y0^2-X0^2*Y2^2+X2^2*Y0^2+3*X0*X1*Y1^2-3*X1^2*Y0*Y1)@N
220   Z1=(-3*X0^2*Y0*Y1+3*X0*X1*Y0^2-A*X0^2*Y1^2+A*X1^2*Y0^2-X0*X1*Y2^2+X2^2*Y0*Y1+2*X0*X2*Y1*Y2-2
230   Z2=(3*X0^2*Y0*Y2-3*X0*X2*Y0^2+A*X0^2*Y1*Y2-A*X1*X2*Y0^2+2*A*X0*X1*Y0*Y2-2*A*X0*X2*Y0*Y1-X0*X
240   if Z0<>0 or Z1<>0 or Z2<>0 then goto 320
250   Z0=(3*X0^2*Y0*Y1-3*X0*X1*Y0^2+A*X0^2*Y1^2-A*X1^2*Y0^2+X0*X1*Y2^2-X2^2*Y0*Y1+2*X0*X2*Y1*Y2-2*
260   Z1=(A^2*X0^2*Y0*Y1-A^2*X0*X1*Y0^2-3*X0^2*Y1^2+3*X1^2*Y0^2-A*X0*X1*Y1^2+A*X1^2*Y0*Y1+X1^2*Y2^
270   Z2=(-A^2*X0^2*Y0*Y2+A^2*X0*X2*Y0^2+3*X0^2*Y1*Y2-3*X1*X2*Y0^2+6*X0*X1*Y0*Y2-6*X0*X2*Y0*Y1+2*A
280   if Z0<>0 or Z1<>0 or Z2<>0 then goto 320
290   Z0=(6*X0*X2*Y0^2+6*X0^2*Y0*Y2+2*A*X1*X2*Y0^2+2*A*X0^2*Y1*Y2+4*A*X0*X2*Y0*Y1+4*A*X0*X1*Y0*Y2+
300   Z1=(2*A^2*X0*X2*Y0^2+2*A^2*X0^2*Y0*Y2-6*X1*X2*Y0^2-6*X0^2*Y1*Y2-12*X0*X2*Y0*Y1-12*X0*X1*Y0*Y
310   Z2=(-2*X0^2*Y0^2*A^3-18*X0^2*Y0^2-6*A*X0*X1*Y0^2-6*A*X0^2*Y0*Y1-2*A^2*X1^2*Y0^2-2*A^2*X0^2*Y
320   return
330   ' Verdoppelung eines Punktes: 2 (x0:x1:x2)=(z0:z1:z2)
340   Z0=(8*X0*X2^3)@N
350   Z1=(2*X2*(A^2*X0^3-9*X0^2*X1-3*A*X0*X1^2+X2^2*X1))@N
360   Z2=(-X0^4*A^3-9*X0^4-6*A*X0^3*X1-6*A^2*X1^2*X0^2+18*X0*X1^3+3*A*X1^4+X2^4)@N
370   return
```

Beispiel: Wir haben $n = 11^{50} + 4 = 5 \cdot 1409 \cdot n_{49}$, wo n_{49} zusammengesetzt ist.
Wir wenden ECM mit $K = 200$ an auf n_{49} und erhalten nach weniger als 16 Sekunden bei $a = 24$ den Teiler $p = 272824957$, der sich als prim herausstellt:

$$n_{49} = 272824957 \cdot n_{40},$$

wo n_{40} zusammengesetzt ist. Man rechnet nach, daß die Ordnung von P in $E_a(\mathbf{F}_p)$ $2^6 \cdot 11 \cdot 23 \cdot 41 \cdot 137$ ist, was natürlich mit $kgV(1 \ldots K) \cdot P = (0 : 0 : 1)$ in $E_a(\mathbf{F}_p)$ zusammenpaßt.
Wir wenden ECM mit $K = 2000$ an auf n_{40} und erhalten bei $a = 209$ den Teiler 26121051523381013, der sich als prim herausstellt. Damit ist

$$n_{40} = 26121051523381013 \cdot n_{24}$$

und auch n_{24} ist wahrscheinlich prim. Die Ordnung von P in $E_a(\mathbf{F}_p)$ ist nun

$$2 \cdot 3 \cdot 11^2 \cdot 71 \cdot 109 \cdot 491 \cdot 1109 \cdot 1423,$$

was wieder gut mit $kgV(1 \ldots 2000) \cdot P = (0 : 0 : 1)$ in $E_a(\mathbf{F}_p)$ zusammenpaßt.

Bemerkung: Das ECM-Faktorisierungsverfahren ist probabilistisch: es ist nicht klar, nach wievielen Versuchen man ans Ziel kommt.

Im letzten Beispiel haben wir die Ordnung eines Punktes $P \in E(\mathbf{F}_p)$ benutzt. Das folgende Beispiel zeigt, wie man sie erhält:

Beispiel: Wir betrachten E mit $y^2 = x^3 + 209x + 1$ über $\mathbf{F}_p$ mit $p = 26121051523381013$ und haben $P = (1 : 0 : 1) \in E(\mathbf{F}_p)$.

- Wir wissen, daß $kgV(1 \ldots 2000) \cdot P = O$ ergibt. Nun ist

$$kgV(1 \ldots 2000) = \prod_{p \leq 2000} p^{\lfloor \frac{\log 2000}{\log p} \rfloor}$$

und $ord(P)|kgV(1\ldots2000)$. Durch Ausprobieren erhält man dann schnell

$$ord(P) = 2 \cdot 3 \cdot 11^2 \cdot 71 \cdot 109 \cdot 491 \cdot 1109 \cdot 1423.$$

- Wir können jetzt auch leicht $\#E(\mathbf{F}_p)$ bestimmen: Wir haben $\#E(\mathbf{F}_p) = k \cdot ord(P)$ und $p+1-2\sqrt{p} < \#E(\mathbf{F}_p) < p+1+2\sqrt{p}$, also

$$\frac{p+1-2\sqrt{p}}{ord(P)} < k < \frac{p+1+2\sqrt{p}}{ord(P)},$$

was durch Einsetzen $5.99 < k < 6.01$ ergibt, also $k = 6$ und damit

$$\#E(\mathbf{F}_p) = 2^2 \cdot 3^2 \cdot 11^2 \cdot 71 \cdot 109 \cdot 491 \cdot 1109 \cdot 1423.$$

In der nachfolgenden Tabelle haben wir die Ergebnisse zusammengestellt.

Zahl	Teiler
$11^{50}+1$	2, 61, 101 (kleine Teiler)
	212601841 ($K = 100, a = 15$)
	2248313994601 ($K = 1000, a = 142$)
	19930999065427108197278845 01 (Rest)
$11^{50}+2$	3, 163, 809 (kleine Teiler)
	245581177 ($K = 100, a = 61$)
	15178363 ($K = 200, a = 3$)
	5370524233 ($K = 1000, a = 4$)
	1482313913618372313841 (Rest)
$11^{50}+3$	2^2 (kleine Teiler)
	2934771321992382912666662399758957998474553474680751 (Rest)
$11^{50}+4$	5, 1409 (kleine Teiler)
	272824957 ($K = 200, a = 24$)
	26121051523381013 ($K = 2000, a = 209$)
	233818305715254943423129 (Rest)
$11^{50}+5$	2, 3^2, 7 (kleine Teiler)
	435923 ($K = 50, a = 9$)
	2833627 ($K = 100, a = 2$)
	325883458070321 ($K = 2000, a = 1073$)
	231445601127662433889841 (Rest)
$11^{50}+6$	31, 269 (kleine Teiler)
	26148409049261 ($K = 2000, a = 89$)
	1852932030385921853 ($K = 5000, a = 409$)
	29054641769971661 (Rest)
$11^{50}+7$	2^6, 53, 233, 337, 2381, 3229 (kleine Teiler)
	57327783672588827906923873380813 4431 (Rest)
$11^{50}+8$	3, 59 (kleine Teiler)
	2891796499 ($K = 100, a = 188$)
	2464252583113 ($K = 1000, a = 69$)
	93069642023927273191527574 91 (Rest)
$11^{50}+9$	2, 5, 13, 761 (kleine Teiler)
	2731049 ($K = 100, a = 48$)
	13958966513 ($K = 1000, a = 89$)
	2275445411957 ($K = 2000, a = 43$)
	136790856853997617 3 (Rest)
$11^{50}+10$	5087 (kleine Teiler)
	3525195553434041 ($K = 5000, a = 207$)
	65462005556211885695330365314 8933 (Rest)

DEFINITION. Sei $K \in \mathbf{N}$. Eine natürliche Zahl $n = q_1^{e_1} \dots q_r^{e_r}$ (Primfaktorzerlegung) heißt K-glatt, wenn eine der äquivalenten Bedingungen erfüllt ist:

- für alle $i = 1, \dots, r$ gilt $q_i^{e_i} \leq K$,
- $n | kgV(1 \dots K)$,
- $kgV(1 \dots K)$ annulliert die zyklische Gruppe Z_n.

Damit können wir jetzt sagen für einen Primteiler p von n:

- Pollard funktioniert mit K für p, wenn $p-1 = \#(\mathbf{Z}/(p))^*$ K-glatt ist.
- ECM funktioniert mit K und E_a für p, wenn $\#E_a(\mathbf{F}_p)$ K-glatt ist.

Nun ist

$$p + 1 - 2\sqrt{p} \leq E(\mathbf{F}_p) \leq p + 1 + 2\sqrt{p}$$

und jede natürliche Zahl in diesem Intervall tritt auch als Punkteanzahl einer elliptischen Kurve über $\mathbf{F}_p$ auf. Gibt es also viele K-glatte Zahlen in dem Intervall, so ist die Chance, daß ECM funktioniert groß.

Beispiel: Für $p = 435923$ gibt es 2641 Zahlen im Intervall $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$. In der folgenden Tabelle ist jeweils die Anzahl der K-glatten Zahlen dieses Intervalls angegeben:

K	30	100	500	1000	3000	6000
Anzahl	4	101	577	845	1245	1464

Beispiel: Für $K = 100$ geben wir in der folgenden Tabelle den Anteil der K-glatten Zahlen im Intervall $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ an:

p	10^3+9	10^4+7	10^5+3	10^6+3	10^7+19	10^8+7
Anteil	47.2%	20.4%	7.8%	2.5%	0.7%	0.2%

Beispiel: $p = 435923$ und $E_a : y^2 = x^3 + ax + 1$. In der folgenden Tabelle ist jeweils das kleinste K angegeben, so daß $\#E_a(\mathbf{F}_p)$ K-glatt ist.

a	$\#E_a(\mathbf{F}_p)$	K
1	$435023 = 31 \cdot 14033$	14033
2	$437038 = 2 \cdot 7 \cdot 19 \cdot 31 \cdot 53$	53
3	$436137 = 3 \cdot 13 \cdot 53 \cdot 211$	211
4	$436903 = 359 \cdot 1217$	1217
5	$436988 = 2^2 \cdot 107 \cdot 1021$	1021
6	$436197 = 3 \cdot 145399$	145399
7	$435540 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 61$	61
8	$435639 = 3 \cdot 145213$	145213
9	$435160 = 2^3 \cdot 5 \cdot 11 \cdot 23 \cdot 43$	43
10	$434877 = 3 \cdot 17 \cdot 8527$	8527

Bemerkung: Die vorstehenden Überlegungen machen verständlich, daß man mit ECM kleinere Primteiler schneller findet.

Bemerkung: (Der größte mit ECM gefundene Primfaktor) Man kannte folgende Faktorisierung

$$2^{1071} + 1 = \text{ bekannte Faktoren } \cdot c_{142},$$

wobei c_{142} eine zusammengesetzte Zahl mit 142 Dezimalstellen ist. Am 24. Juni 1998 wurde mit ECM ein 49-stelliger Primteiler p_{49} von c_{142} gefunden.

Es gibt viele Faktorisierungmethoden, was natürlich auch daran liegt, daß bis jetzt keine optimale gefunden wurde. Siehe z.B. [**8a**] oder [**1**]. Moderne Faktorisierungsmethoden sind:

- MPQS (multiple polynomial quadratic sieve)
- NFS (number field sieve)

Literatur: [**8a**], [**5**].

KAPITEL 9

Diskrete Logarithmen

Sei G eine endliche abelsche Gruppe, die wir multiplikativ schreiben. Sind $g, a \in G$ und gibt es ein $x \in \mathbf{N}_0$ mit $g^x = a$, so heißt x diskreter Logarithmus von a zur Basis g. Manchmal schreibt man $x = \log_g a$ oder $x = \mathrm{ind}_g a$. Natürlich ist x nur modulo $ord(g)$ bestimmt.

Beispiele:

1. Zu $p = 10^6 + 3$ betrachten wir $G = \mathbf{F}_p^*$. Durch Probieren findet man:
   - $2^x \equiv 3 \bmod p$ wird gelöst von $x = 254277$.
   - $3^x \equiv 2 \bmod p$ hat keine Lösung.
2. Wir betrachten $G = \mathbf{F}_{1024}^*$. Dabei ist $\mathbf{F}_{1024} = \mathbf{F}_2[x]/(x^{10} + x^3 + 1)$, wir arbeiten also mit

   $$\mathbf{F}_{1024} = \{x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_9\alpha^9 : x_i \in \mathbf{F}_2\} \quad \text{und der Relation} \quad \alpha^{10} = 1 + \alpha^3.$$

   Durch Probieren findet man

   $$\alpha^{949} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^8 + \alpha^9.$$

Wir haben bereits gesehen, wie man für $g \in G$ und $x \in \mathbf{N}_0$ schnell die Potenz g^x berechnen kann: Es ist

$$g^x = \prod_{x_i=1} g^{2^i}, \text{ wo } x = \sum_i x_i \cdot 2^i \text{ und } x_i \in \{0, 1\}.$$

Hat G die Ordnung n, so braucht man also höchstens $O(\log n)$ Schritte zur Berechnung.
Sind aber $g, a \in G$ gegeben, so ist zunächst nicht klar, wie man $\log_g a$ außer durch Probieren berechnen kann. Das ergibt im allgemeinen dann $O(n)$ Schritte.

Um einen Eindruck von der Schwierigkeit des Berechnens von Logarithmen zu geben, geben wir zwei Beispiele, die kürzlich in der Zahlentheorieliste erschienen:

1. Am 26. Mai 1998 teilten A. Joux und R. Lercier mit, daß sie einen neuen Rekord für das allgemeine diskrete Logarithmusproblem aufgestellt haben: Für die 90-stellige Primzahl $p = \lfloor 10^{89}\pi \rfloor + 156137$ und $a = \lfloor 10^{89}e \rfloor$ haben sie die diskreten Logarithmen $\log_2 a$, $\log_2(a+1)$, $\log_2(a+2)$, $\log_2(a+3)$ und $\log_2(a+4)$ berechnet.
2. Am 30. Juni 1998 teilte D. J. Bernstein mit, daß er demjenigen \$100 zahlt, der als erster eine 500-stellige Primzahl p und $x, y \in \mathbf{N}$ angibt mit $4^x \equiv 9 \bmod p$ und $4^y \equiv 25 \bmod p$.

Potenzieren ist einfach, die Berechnung diskreter Logarithmen scheint schwierig zu sein. Dies benutzt man nun zur Konstruktion von kryptographischen Verfahren. Wir skizzieren im folgenden einige davon.

1. Public-Key-Kryptosysteme

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

- 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.
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: Man einigt sich auf $p = 10^6 + 3$ und $g = 2$. A's öffentlicher Schlüssel ist $g^a = 491373$, B's öffentlicher Schlüssel ist $g^b = 911253$. Was ist der vereinbarte Schlüssel g^{ab}? (Lösung: $a = 38628$, $b = 729944$, $g^{ab} = 609491$.)

Das Massey-Omura-Kryptosystem zur Nachrichtenübertragung. Man einigt sich auf einen Körper $\mathbf{F}_q$ und darauf, Nachrichten mit Elementen aus $\mathbf{F}_q$ zu verschlüsseln.

- Jeder Teilnehmer wählt sich eine (zufällige) Zahl e_A zwischen 0 und $q-1$ und berechnet sich d_A mit $d_A e_A \equiv 1 \bmod q-1$. (Dann ist $x \mapsto x^{d_A}$ invers zu $x \mapsto x^{e_A}$ in $\mathbf{F}_q$.) A hält die Zahlen e_A und d_A geheim. (A hat also keinen öffentlichen Schlüssel.)

Wie kann A eine Nachricht T an B verschlüsselt senden?

- A sendet T^{e_A} an B, womit B natürlich nichts anfangen kann.
- B berechnet $T^{e_A e_B}$ und sendet dies an A zurück.
- A berechnet $T^{e_B} = T^{e_A e_B d_A}$ und sendet es an B.
- B kann nun aus $T = T^{e_B d_B}$ die gewünschte Nachricht T berechnen.

Wir bemerken dazu noch folgendes:

1. Vorteilhaft ist, daß man außer $\mathbf{F}_q$ und g nichts kennen muß um an dem System teilzunehmen. Man braucht also keine Teilnehmerlisten mit öffentlichen Schlüsseln.
2. Um eine Nachricht von A nach B zu übermitteln, braucht es 3 Übertragungen.
3. Stellt A nicht sicher, daß die Nachricht T wirklich an B geht, könnte dies ein Außenstehender C ausnutzen: Er fängt T^{e_A} auf, schickt $T^{e_A e_C}$ zurück, fängt dann wieder $T^{e_C} = T^{e_A e_C d_A}$ auf und berechnet sich daraus $T = T^{e_C d_C}$. Man muß also auf andere Weise sicherstellen, daß die Nachricht den richtigen Empfänger erreicht.

Das ElGamal-Kryptosystem. Man einigt sich auf einen Körper $\mathbf{F}_q$, ein Element $g \in \mathbf{F}_q^*$ und darauf, wie man Nachrichten in Elemente aus $\mathbf{F}_q$ übersetzt.

- Jeder Teilnehmer A wählt sich eine (zufällige) Zahl d_A mit $1 \le d_A \le q-2$ als geheimen Schlüssel und gibt $g^{d_A} \in \mathbf{F}_q$ als öffentlichen Schlüssel bekannt.

Wie kann ein Teilnehmer A eine Nachricht T verschlüsselt an B schicken?

- A wählt eine zufällige Zahl k, holt sich g^{d_B}, den öffentlichen Schlüssel von B, berechnet $(g^{d_B})^k$ und schickt dann das Paar
$$(g^k, T \cdot g^{d_B k})$$
an B.
- B berechnet $(g^k)^{d_B} = g^{d_B k}$ und damit die Nachricht T.

Das Verfahren ist sicher, solange man den diskreten Logarithmus von g^{d_B} zur Basis g nicht berechnen kann und solange man keinen Weg kennt, aus der Kenntnis von g, g^k und g^{d_B} den Wert $g^{d_B k}$ zu berechnen.

DSA - Digital Signature Algorithm. Das NIST - National Institute of Standards and Technology der US-Regierung hat 1991 einen Digital Signature Standard (DSS) vorgeschlagen, der auf nachfolgendem Algorithmus beruht.
Jeder Teilnehmer A muß folgendes tun:

- A sucht sich eine ungefähr 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 zwischen 512 und 1024, möglichst ein Vielfaches von 64.
- A bestimmt einen Erzeuger g der zyklischen Untergruppe der Ordnung q von $\mathbf{F}_p^*$: Ist $g \in \mathbf{Z}$ mit $g^{\frac{p-1}{q}} \not\equiv 0, 1 \bmod p$, so liefert g einen solchen Erzeuger.
- A wählt eine Zufallszahl x mit $0 < x < q$ als geheimen Schlüssel. Der öffentliche Schlüssel wird $y = g^x \bmod p$.

(q, p und g können allen Teilnehmern der Benutzergruppe gemeinsam sein.)
Wie signiert A eine Nachricht T an B?

- A berechnet einen Hash-Wert H der Nachricht T mit $0 < H < q$. (Hashfunktionen werden kurz im nächsten Abschnitt vorgestellt.)
- A wählt eine Zufallszahl k mit $0 < k < q$ und berechnet dann
$$r = (g^k \bmod p) \bmod q.$$
- A bestimmt eine ganze Zahl s mit
$$sk \equiv H + xr \bmod q.$$
- Kurz:
$$r = (g^k \bmod p) \bmod q \quad \text{und} \quad s = (k^{-1}(H + xr) \bmod q.$$
- Die Signatur ist dann das Paar (r, s) von Zahlen mod$q$.

Wie kann der Empfänger B sehen, daß die Nachricht T wirklich von A stammt?

- B berechnet sich ebenfalls den Hash-Wert H der Nachricht T.
- Dann berechnet B
$$u_1 = s^{-1}H \bmod q \quad \text{und} \quad u_2 = s^{-1}r \bmod q.$$
- Dann berechnet B den Wert $g^{u_1}y^{u_2}$. Gilt
$$g^{u_1}y^{u_2} \equiv r \bmod q$$
ist B zufrieden. (Warum?)

Ein Vorteil ist, daß die Signatur (r, s) recht kurz ist.

Wir wollen jetzt Verfahren vorstellen, wie man in einer endlichen abelschen Gruppe G diskrete Logarithmen berechnen kann.

2. Die naive Methode zur Berechnung diskreter Logarithmen

Ist G eine Gruppe mit n Elementen, sind $g, a \in G$, so kann man natürlich für jedes x mit $0 \le x \le n-1$ testen, ob $g^x = a$ gilt. Die Laufzeit ist $O(n)$.

Ein Ubasic-Programm *dlnaiv.ub* zur Berechnung von $g^x = a$ in $\mathbf{F}_p^*$ kann in etwa so aussehen:

```
10   ' Programm dlnaiv: Berechnet das erste x mit g^x=a mod p
20   input "p,g,a=";P,G,A:clr time
30   H=1:X=0
40   if H=A then print "x=";X:goto 60
50   H=(G*H)@P:X=X+1:if X<P then goto 40
60   print time:goto 20
```

Beispiel: $p = 10^7 + 19$. Wir haben $p - 1 = 2 \cdot 7^2 \cdot 67 \cdot 1523$. Durch Probieren findet man
$$ord(2) = \frac{p-1}{7}, \quad ord(3) = \frac{p-1}{2}, \quad ord(6) = p - 1,$$
d.h. 6 ist ein Erzeuger von $\mathbf{F}_p^*$. Dies nennt man auch eine Primitivwurzel modulo p. Wir finden mit obigem Programm
$$\begin{aligned} 6^x &\equiv 2 \bmod p \text{ für } x = 3619301 \text{ in 1'16"}, \\ 6^x &\equiv 3 \bmod p \text{ für } x = 6380718 \text{ in 2'15"}, \\ 6^x &\equiv 5 \bmod p \text{ für } x = 6033274 \text{ in 2'7"}. \end{aligned}$$

Braucht man also (bei allgemeinem a) für $p \approx 10^7$ mehr als eine Minute, so braucht man für $p \approx 10^{10}$ mehr als 16 Stunden, für $p \approx 10^{11}$ mehr als 6 Tage.

3. Die Baby-Step-Giant-Step-Methode nach Shanks

Sei wieder G eine Gruppe mit n Elementen. Wir wollen die Gleichung $g^x = a$ lösen. Man geht folgendermaßen vor:

- Berechne $m = \lceil \sqrt{n} \rceil$, d.h. die kleinste natürliche Zahl $\geq \sqrt{n}$.
- Berechne die Mengen
$$S = \{(i, ag^i) : i = 0, \ldots, m\} \quad \text{und} \quad T = \{(i, g^{mi}) : i = 0, \ldots, m\}.$$
- Suche Elemente $(i, ag^i) \in S$ und $(j, g^{mj}) \in T$, die das gleiche zweite Element haben, d.h. mit $ag^i = g^{mj}$. Das kann man z.B. so machen, daß man S und T nach dem zweiten Eintrag sortiert (nach Wahl einer geeigneten Ordnung auf G) und dann vergleicht.
- Gilt $ag^i = g^{mj}$, so ist $x = mj - i$ eine Lösung von $g^x = a$.

Bemerkungen:

1. Jedes Element x des Intervalls $0 \leq x \leq n$ läßt sich als $x = mj - i$ schreiben. Existiert ein diskreter Logarithmus, so kann man ihn also mit obigem Verfahren finden.
2. Um die Mengen S und T zu berechnen braucht man $O(m)$ Schritte. Es gibt Sortieralgorithmen, z.B. heapsort, so daß man zum Sortieren und Vergleichen von S und T nur $O(m \log m)$ Schritte braucht. Auf diese Weise wird die Laufzeit $O(\sqrt{n} \log n)$, allerdings braucht man auch $O(\sqrt{n})$ Speicherplatz.
3. Der Algorithmus funktioniert auch, wenn $m \geq \lceil \sqrt{n} \rceil$ gilt, d.h. man muß die Gruppenordnung nicht genau kennen. Zum Ausprobieren kann man den Algorithmus auch mit einem beliebigen m starten.
4. Die Baby-Step-Giant-Step-Methode wird auch an anderen Stellen in der Zahlentheorie verwendet. Die Idee geht auf Shanks zurück.

4. Pollards Monte-Carlo-Methode

Wir betrachten zuerst den Fall $G = \mathbf{F}_p^*$, wo p eine ungerade Primzahl ist. Wir wollen die Gleichung $g^x = a$ in $\mathbf{F}_p$ lösen, wobei wir annehmen, daß g eine Primitivwurzel modulo p ist. Sei $n = p - 1$.

1. Schritt: Wir suchen $s, t \in \mathbf{N}$ mit $a^s \equiv g^t \bmod p$. Dazu definieren wir eine Folge $x_0, x_1, x_2, \cdots \in \mathbf{F}_p^*$ durch

$$x_0 = 1 \quad \text{und} \quad x_{i+1} = \begin{cases} ax_i & \text{für } 0 < x_i < \frac{1}{3}p, \\ x_i^2 & \text{für } \frac{1}{3}p < x_i < \frac{2}{3}p, \\ gx_i & \text{für } \frac{2}{3}p < x_i < p. \end{cases}$$

Schreibt man $x_i = a^{e_i} g^{f_i}$, so hat man

$$e_0 = 0 \quad \text{und} \quad e_{i+1} = \begin{cases} e_i + 1 \bmod n & \text{für } 0 < x_i < \frac{1}{3}p, \\ 2e_i \bmod n & \text{für } \frac{1}{3}p < x_i < \frac{2}{3}p, \\ e_i & \text{für } \frac{2}{3}p < x_i < p, \end{cases}$$

$$f_0 = 0 \quad \text{und} \quad f_{i+1} = \begin{cases} f_i & \text{für } 0 < x_i < \frac{1}{3}p, \\ 2f_i \bmod n & \text{für } \frac{1}{3}p < x_i < \frac{2}{3}p, \\ f_i + 1 \bmod n & \text{für } \frac{2}{3}p < x_i < p. \end{cases}$$

Die Folge $x_0, x_1, x_2, \ldots$ ist ein random walk in $\mathbf{F}_p^*$, man erwartet daher, daß es ein $i \leq 3\sqrt{n}$ gibt mit $x_i = x_{2i}$. Ist aber $x_i = x_{2i}$, so haben wir mit $s = e_i - e_{2i} \bmod n$ und $t = f_{2i} - f_i \bmod n$ eine Lösung von $a^s = g^t$. Der Vorteil ist nun, daß man die Folge $x_0, x_1, x_2, \ldots$ nicht speichern muß. Man berechnet einfach sukzessiv für $i = 0, 1, 2, \ldots$

$$(x_i, e_i, f_i, x_{2i}, e_{2i}, f_{2i})$$

und testet dann, ob $x_i = x_{2i}$ gilt.

2. Schritt: Wir nehmen an, wir haben eine Relation $a^s \equiv g^t \bmod p$ gefunden.

1. Ist $ggT(s, n) = 1$, so gibt es ein $u \in \mathbf{N}$ mit $us \equiv 1 \bmod n$ und damit $a \equiv g^{tu}$, was unser Problem löst.

2. Ist $d = ggT(s,n) > 1$, so können wir mit dem erweiterten euklidischen Algorithmus $u, v \in \mathbf{N}$ finden mit $d = us + vn$. Dann ist $a^d \equiv g^{tu}$, also ist g^{tu} eine d-te Potenz und damit $tu = dk$ für ein $k \in \mathbf{N}$. Aus $a^d \equiv g^{dk}$ folgt $a \equiv g^{k+\frac{n}{d}i}$ für ein i mit $0 \le i \le d-1$, da $g^{\frac{n}{d}}$ eine primitive d-te Einheitswurzel ist. Indem man für $i = 0, 1, 2, \ldots, d-1$ ausprobiert, ob $a \equiv g^{k+\frac{n}{d}i}$ gilt, kann man die Lösung finden.

Das Ubasic-Programm *dlpoll.ub* führt das Verfahren aus:

```
10   print "Programm dlpoll zum Berechnen diskreter Logarithmen"
20   print "mit Pollards Monte-Carol-Methode. Einzugeben sind "
30   print "p,g,a, als Ergebnis erhaelt man Relationen a^s=g^t (p)."
40   input "p,g,a=";P,G,A:print "p=";P;"g=";G;"a=";A
50   X=1:E=0:F=0:Xx=1:Ee=0:Ff=0:Az=0:Z=0:clr time
60   Z=Z+1
70   I=(X*3)\P
80   if I=0 then X1=(A*X)@P:E1=(E+1)@(P-1):F1=F
90   if I=1 then X1=(X*X)@P:E1=(2*E)@(P-1):F1=(2*F)@(P-1)
100  if I=2 then X1=(G*X)@P:E1=E:F1=(F+1)@(P-1)
110  I=(Xx*3)\P
120  if I=0 then Xx1=(A*Xx)@P:Ee1=(Ee+1)@(P-1):Ff1=Ff
130  if I=1 then Xx1=(Xx*Xx)@P:Ee1=(2*Ee)@(P-1):Ff1=(2*Ff)@(P-1)
140  if I=2 then Xx1=(G*Xx)@P:Ee1=Ee:Ff1=(Ff+1)@(P-1)
150  I=(Xx1*3)\P
160  if I=0 then Xx2=(A*Xx1)@P:Ee2=(Ee1+1)@(P-1):Ff2=Ff1
170  if I=1 then Xx2=(Xx1*Xx1)@P:Ee2=(2*Ee1)@(P-1):Ff2=(2*Ff1)@(P-1)
180  if I=2 then Xx2=(G*Xx1)@P:Ee2=Ee1:Ff2=(Ff1+1)@(P-1)
190  X=X1:E=E1:F=F1:Xx=Xx2:Ee=Ee2:Ff=Ff2
200  if X=Xx then print "s=";(E-Ee)@(P-1);"t=";(Ff-F)@(P-1);"ggT(s,p-1)=";gcd(E-Ee,P-1);"nach";Z;
210  goto 60
```

Beispiel: Wir wollen die Gleichung $2^x \equiv 3 \bmod p$ für $p = 10^{12} + 547$ lösen. Mit obigem Programm erhalten wir nach 528798 Versuchen (für i) und 1'44"

$$s = 273935841518, \quad t = 488473193126, \quad ggT(s, p-1) = 2.$$

Wie oben beschrieben erhält man schnell

$$3^2 \equiv 2^{2k} \bmod p \quad \text{mit} \quad k = 626279696105.$$

Nun ist

$$2^k \equiv 1000000000544 \quad \text{und} \quad 2^{k+\frac{n}{2}} = 3,$$

so daß

$$k + \frac{n}{2} \equiv 1126279696378$$

unser gesuchter diskreter Logarithmus ist.

Beispiele: Im folgenden ist p eine Primzahl, so daß $p - 1 = 2q$ gilt mit einer Primzahl q. Weiter ist g eine Primitivwurzel modulo p und $a \in \mathbf{F}_p^*$. Es werden Relationen $a^2 \equiv g^t \bmod p$ bestimmt mit obigem Programm. (Die Zeiten beziehen sich auf einen 486-PC mit 50 MHz.)

p	g	a	s	t	$ggT(s,p-1)$	Versuche	Zeit
$10^{13}+259$	2	3	5591785064514	7287067539592	2	2536935	0:18:50
$10^{14}+5083$	2	3	57235676284350	58444219663308	2	11513945	1:22:07
$10^{15}+5719$	11	2	172130302390902	191270124335536	2	25714488	3:13:52

Bemerkungen:

1. Das Verfahren ist nicht deterministisch, die Laufzeit ist $O(\sqrt{n})$. Ein Vorteil ist, daß man kaum Speicherplatz braucht.

2. Das Verfahren läßt sich leicht auch für andere Gruppen G durchführen, man muß nur G in drei disjunkte Mengen S_1, S_2, S_3 aufteilen, die ungefähr gleich groß sind. Bei der Definition von x_{i+1} wird dann danach unterschieden, ob $x_i \in S_1$, $x_i \in S_2$ oder $x_i \in S_3$ gilt.

5. Das Silver-Pohlig-Hellman-Verfahren

Sei wieder G eine Gruppe mit n Elementen. Wir wollen die Gleichung $g^x = a$ lösen.

Beispiel: Wir wollen $g^x = a$ in $\mathbf{F}_p^*$ lösen, wobei wir annehmen, daß g eine Primitivwurzel modulo p ist und $p-1$ sich faktorisieren läßt

$$n = \#\mathbf{F}_p = p - 1 = q_1 \cdot q_2 \cdot \ldots q_r$$

mit paarweise verschiedenen Primzahlen q_i.

1. $g^{\frac{n}{q_i}}$ ist eine primitive q_i-te Einheitswurzel. Wegen $1 = a^n = (a^{\frac{n}{q_i}})^{q_i}$ gibt es also ein x_i mit
$$a^{\frac{n}{q_i}} = g^{\frac{n}{q_i} x_i} \quad \text{und} \quad 0 \le x_i \le q_i - 1,$$
wobei wir x_i durch Probieren in $O(q_i)$ Schritten finden können.
2. Mit dem chinesischen Restsatz bestimmen wir ein x mit $x \equiv x_i \bmod q_i$ für $i = 1, 2, \ldots, r$.
3. Nun gilt
$$(a^{-1} g^x)^{\frac{n}{q_i}} = a^{-\frac{n}{q_i}} g^{\frac{n}{q_i} x_i} = 1$$
für alle $i = 1, \ldots, r$. Daraus folgt schnell $a^{-1} g^x = 1$, d.h. x ist der diskrete Logarithmus von a zur Basis g.

Beispiel: $p = 10^{10} + 19$ und $g = 2$. Dann ist

$$p - 1 = 2 \cdot 131 \cdot 521 \cdot 73259.$$

Wir wollen die Gleichung $2^x \equiv 3 \bmod p$ lösen. Nach dem eben geschilderten Verfahren erhalten wir

$$\begin{aligned} x &\equiv 0 \bmod 2, \\ x &\equiv 92 \bmod 131, \\ x &\equiv 223 \bmod 521, \\ x &\equiv 55292 \bmod 73259, \end{aligned}$$

woraus man mit dem chinesischen Restsatz $x = 5181957398$ erhält.

Das allgemeine Verfahren geht für eine endliche abelsche Gruppe G und die Gleichung $g^x = a$ folgendermaßen:

1. Bestimme die Primfaktorzerlegung
$$n = \#G = q_1^{e_1} \ldots q_r^{e_r}.$$
2. Wir betrachten ein festes $q = q_i$: Speichere die Werte $\zeta_{q,j} = g^{\frac{n}{q} j}$ für $j = 0, 1, \ldots, q-1$, was den q-ten Einheitswurzeln entspricht.
3. Bestimme das x_0 mit
$$a^{\frac{n}{p}} = \zeta_{p,x_0}.$$
4. Bilde rekursiv für $i = 1, 2, \ldots, e-1$ den Wert
$$a_i = a g^{-(x_0 + x_1 q + \cdots + x_{i-1} q^{i-1})}$$
und bestimme ein x_i mit
$$a_i^{\frac{n}{q^{i+1}}} = \zeta_{q,x_i} \quad \text{und} \quad 0 \le x_i \le q - 1.$$
5. Für das gesuchte x hat man dann
$$x \equiv x_0 + x_1 q_i + \cdots + x_{e_i - 1} q_i^{e_i - 1} \bmod q_i^{e_i},$$
woraus man mit dem chinesischen Restsatz x berechnen kann.

Bemerkungen:

1. Die Laufzeit des Verfahrens ist

$$O(\sum_{i=1}^{r} e_i(\log n + q_i)),$$

das Verfahren funktioniert also nur vernünftig, wenn die Gruppenordnung glatt ist, d.h. keine großen Primzahlen in $n = \#G$ auf gehen.

Beispiel: $p = 10^{10} + 259$. Hier ist $p - 1 = 2 \cdot q$ mit q prim. $g = 2$ ist Primitivwurzel. Das dargestellte Verfahren ist hier fast ebenso schlecht wie die naive Methode.

6. Die Index-Calculus-Methode

Sei p eine ungerade Primzahl, $G = \mathbf{F}_p^*$ und $n = \#G = p - 1$. Sei g eine Primitivwurzel modulo p. Wir wollen die Gleichung $g^x = a$ lösen.

1. Schritt: Seien $q_1, q_2, \ldots, q_m$ die ersten m Primzahlen. Wir wollen Relationen

$$\prod_{j=1}^{m} q_j^{a_{ij}} \equiv g^{b_i} \text{ für } i = 1, 2, \ldots, m, \ldots$$

Dies geschieht wie folgt:

1. Wähle b mit $1 \leq b \leq n$ zufällig.
2. Berechne $x \equiv g^b \bmod p$ mit $1 \leq x \leq n$.
3. Faktorisiere

$$x = q_1^{a_1} q_2^{a_2} \ldots q_m^{a_m} \cdot \tilde{x} \text{ mit } \tilde{x} \in \mathbf{N}$$

durch Division durch $q_1, \ldots, q_m$, solange es geht.
4. Ist $\tilde{x} > 1$, fängt man von vorne an. Ist $\tilde{x} = 1$, haben wir eine gewünschte Relation

$$q_1^{a_1} q_2^{a_2} \ldots q_m^{a_m} \equiv g^b \bmod p.$$

(Weshalb funktioniert das?)

Ein Ubasic-Programm *dlindex.ub* sieht so aus:

```
10   print "Index-Calculus-Methode zur Berechnung des diskreten"
20   print "Logarithmus im Koerper F_p mit Basis g und den"
30   print "ersten m Primzahlen als Basiselemente. (Schritt 1)"
40   print "Es werden Relationen q1^a1*...qm^am=g^b (p) erzeugt"
50   print "und dann a1,...,am,b ausgegeben.":print
60   input "p=";P:input "g=";G:input "m=";M
70   print "p=";P;"g=";G;"m=";M
80   dim Q(M):for I=1 to M:Q(I)=prm(I):next:dim A(M)
90   Z=0:Az=1:clr time
100  B=int(rnd*P):Z=Z+1
110  for I=0 to M:A(I)=0:next I
120  X=modpow(G,B,P)
130  for I=1 to M
140  if X@Q(I)=0 then X=X\Q(I):A(I)=A(I)+1:goto 140
150  next I
160  if X=1 then goto 170 else goto 100
170  A(0)=B:print "Relation Nr.";Az;"nach";Z;"Versuchen und Zeit";time:Az=Az+1
180  for I=1 to M:print A(I);:next I:print A(0)
190  goto 100
```

Beispiel: $p = 10^7 + 79$, $g = 11$, $p - 1 = 2 \cdot 11 \cdot 23 \cdot 19763$. Wir wählen $m = 2$, d.h. $q_1 = 2$, $q_2 = 3$ und erhalten

a_{i1}	a_{i2}	b_i	
10	6	3324384	nach 59359 Versuchen und 12 Sekunden
9	3	6528940	nach 93848 Versuchen und 20 Sekunden
2	13	4941490	nach 152252 Versuchen und 33 Sekunden
2	9	4169762	nach 188961 Versuchen und 41 Sekunden

2. Schritt: Wir haben also jetzt einige Relationen

$$\prod_{j=1}^{m} q_j^{a_{ij}} \equiv g^{b_i} \text{ für } i = 1, 2, \ldots, m, \ldots$$

Schreiben wir $q_i \equiv g^{\ell_i}$, so werden die Relationen zu

$$\sum_{j=1}^{m} a_{ij}\ell_j \equiv b_i \bmod n \text{ für } i = 1, 2, \ldots, m, \ldots$$

Dies ist ein lineares Gleichungssystem über dem Ring $\mathbf{Z}/(n)$. Hat man genügend Relationen, so erhält man eine eindeutige Lösung, d.h. die Logarithmen von $q_1, \ldots, q_m$ bzgl. g.

Beispiel: Wir betrachten wieder $p = 10^7 + 79$, $g = 11$, $m = 2$, $n = p - 1 = 2 \cdot 11 \cdot 23 \cdot 19763$. Die aus obigen Relationen hervorgehenden linearen Gleichungen sind:

$$\begin{aligned} 10\ell_1 + 6\ell_2 &\equiv 3324384 \bmod n, \\ 9\ell_1 + 3\ell_2 &\equiv 6528940 \bmod n, \\ 2\ell_1 + 13\ell_2 &\equiv 4941490 \bmod n, \\ 2\ell_1 + 9\ell_2 &\equiv 4169762 \bmod n. \end{aligned}$$

Da 3 invertierbar ist modulo n, erhält man aus der zweiten Gleichung

$$\ell_2 = -3\ell_1 - 1157046,$$

wodurch die erste Gleichung zu $8\ell_1 \equiv -10266660 \bmod n$ wird, sie läßt sich allerdings nicht eindeutig lösen. Die dritte Gleichung ergibt

$$37\ell_1 \equiv -19983088 \bmod n,$$

womit wir schließlich

$$\ell_1 \equiv 6216726 \quad \text{und} \quad \ell_2 \equiv 192932$$

erhalten.

Bemerkung: Den 2. Schritt haben wir nicht programmiert, sondern die bei den Beispielen aufgetretenen linearen Gleichungssysteme jeweil gesondert mit Maple gelöst.

3. Schritt: Wir können jetzt schnell die Gleichung $g^x \equiv a \bmod p$ lösen.
Wir erzeugen eine Relation

$$\prod_{j=1}^{m} q_j^{e_j} \equiv a \cdot g^e$$

wie im 1. Schritt durch zufällige Wahl von e im Intervall $[1, n]$ und haben dann sofort

$$a \equiv g^{\sum_{j=1}^{m} \ell_j e_j - e}.$$

Ein Ubasic-Programm *dlindex3.ub* für den dritten Schritt kann so aussehen:

```
10  print "Index-Calculus-Methode zur Berechnung des diskreten"
20  print "Logarithmus im Koerper F_p mit Basis g und den"
30  print "ersten m Primzahlen als Basiselemente: 3. Schritt."
40  input "p=";P:input "g=";G:input "m=";M
50  print "p=";P;"g=";G;"m=";M
60  dim L(M):for I=1 to M:print I;"-ter Logarithmus":input L(I):next
70  dim Q(M):for I=1 to M:Q(I)=prm(I):next:dim E(M)
80  input "a=";A:print "a=";A:Z=0:clr time
```

```
 90  Ee=int(rnd*P):Z=Z+1
100  for I=0 to M:E(I)=0:next I
110  X=(A*modpow(G,Ee,P))@P
120  for I=1 to M
130  if X@Q(I)=0 then X=X\Q(I):E(I)=E(I)+1:goto 130
140  next I
150  if X=1 then goto 160 else goto 90
160  Y=-Ee:for I=1 to M:Y=Y+E(I)*L(I):next:Y=Y@(P-1)
170  print "Logarithmus=";Y
180  print "nach";Z;"Versuchen und Zeit";time:Az=Az+1
190  for I=1 to M:print E(I);:next I:print Ee
200  goto 80
```

Beispiel: Wir betrachten wieder $p = 10^7 + 79$ mit $g = 11$ und $m = 2$.

a	Logarithmus	e_1	e_2	e	
2	6216726	0	1	3976284	nach 34873 Versuchen und 7 Sekunden
3	192932	10	7	3324384	nach 24486 Versuchen und 5 Sekunden
5	4825802	4	5	1005606	nach 26689 Versuchen und 5 Sekunden
7	8668806	1	4	8319726	nach 13766 Versuchen und 3 Sekunden
100001	6776838	19	2	1725962	nach 131888 Versuchen und 29 Sekunden
99999	3319872	0	13	9188322	nach 1639 Versuchen und 0 Sekunden

Man kann natürlich jetzt die bekannten Logarithmen wieder benutzen. So findet man z.B. für $m = 4$ und $a = 10^5 + 1$ jetzt nach 5777 Versuchen und einer Sekunde den Logarithmus mit $e_1 = 2, e_2 = 4, e_3 = 2, e_4 = 1, e = 4748596$.

Bemerkungen:

1. Eine wesentliche Vorarbeit in der Index-Calculus-Methode ist der 1. Schritt. Man muß m geeignet wählen. Ist m zu klein, findet man schwer Relationen, ist m zu groß, 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 Verfahren.
3. Es ist nicht klar, ob man das Index-Calculus-Verfahren in irgendeiner Verfahren auch bei elliptischen Kurven verwenden kann.
4. Sei
$$L(p) = e^{\sqrt{\log p \log\log p}}.$$
Wählt man m so, daß $q_m \approx L(p)^{\frac{1}{2}}$, dann kann man die Laufzeit für die ersten beiden Schritte durch $L(p)^{2+o(1)}$ abschätzen. Dies ist subexponentiell.

Beispiel: $p = 10^{12} + 547$, $g = 2$. Wir wenden die Index-Calculus-Methode an.

- Im 1. Schritt haben wir $m = 10$ gewählt. Nach 1 Stunde und 50 Minuten hatten wir 20 Relationen.
- Die ersten 12 Relationen genügten um daraus die ersten 10 Logarithmen (zur Basis 2) zu berechnen (2. Schritt):

$$\begin{aligned}
\log 2 &= 1,\\
\log 3 &= 126279695832,\\
\log 5 &= 624340846355,\\
\log 7 &= 468022953033,\\
\log 11 &= 669715915915,\\
\log 13 &= 403120760399,\\
\log 17 &= 444516793734,\\
\log 19 &= 292184457190,\\
\log 23 &= 483221903637,\\
\log 29 &= 134591997338.
\end{aligned}$$

- Für den 3. Schritt haben wir nun $m = 10$ gewählt und so die Logarithmen der Primzahlen von 31 bis 47 berechnet. (Minimalzeit zur Berechnung eines Logarithmus: 6'20", Maximalzeit: 14'4".)
- Die berechneten Logarithmen wurden nun für den 3. Schritt mit $m = 15$ verwendet um die Logarithmen der nächsten Primzahlen zu berechnen, die dann wieder für den 3. Schritt verwendet wurden, u.s.w. Wir haben dies solange fortgesetzt, bis wir die Logarithmen für die ersten 100 Primzahlen berechnet hatten.
- Wir hatten also nun $m = 100$ für den 3. Schritt. Wir haben nun damit die Logarithmen für 1000 zufällige Werte von a berechnet. Durchschnittlich brauchte man 0.8 Sekunden (bei 402 Versuchen), das Maximum lag bei 5.2 Sekunden (und ungefähr 2500 Versuchen).

Literatur: [**11**], [**3**], [**4**], [**5a**].

KAPITEL 10

Kryptosysteme mit elliptischen Kurven - ECC

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 q eine große Auswahl an Gruppen $E(\mathbf{F}_q)$ zur Verfügung, während es nur eine Gruppe $\mathbf{F}_q^*$ gibt.
- Man kannte keine schnellen Algorithmen zur Berechnung diskreter Logarithmen in $E(\mathbf{F}_q)$, wenn die Gruppenordnung $\#E(\mathbf{F}_q)$ nicht glatt ist.

Die Idee ist also, die Schwierigkeit des Berechnens von diskreten Logarithmen in $E(\mathbf{F}_q)$ kryptographisch zu nutzen. Inzwischen gibt es kommerzielle Kryptosysteme, die mit elliptischen Kurven arbeiten. (Beispielsweise werden von Certicom solche vertrieben. Nähere Informationen findet man unter http://www.certicom.com.)

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 geht das? Wir denken uns Text bzw. Worte gegeben durch Zahlen m mit $0 \leq m < M$. Wir skizzieren ein probabilistisches Verfahren, wie man den Zahlen m des Intervalls $[0, M-1]$ Punkte einer elliptischen Kurve zuordnen kann.

- Wir wählen eine natürliche Zahl k, z.B. $k = 30$. (Die Wahrscheinlichkeit, daß das Verfahren für die Zahl m nicht funktioniert, ist dann ungefähr 0.5^k.)
- Wir nehmen eine Primzahl p mit $p > Mk$ und eine elliptische Kurve E über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$.
- Sei jetzt m vorgegeben mit $0 \leq m < M$ und $j = 0$.
  1. Sei $x = mk + j$ und $y_2 = x^3 + ax + b$.
  2. Wir testen, ob y_2 ein Quadrat ist in $\mathbf{F}_p$, z.B. durch Berechnen des Legendresymbols $(\frac{y_2}{p})$.
  3. Ist y_2 kein Quadrat und $j < k-1$, ersetzen wir j durch $j+1$ und gehen zurück zu 1. Ist y_2 kein Quadrat und $j = k-1$, ist das Verfahren fehlgeschlagen und wir hören auf. (Da ungefähr die Hälfte der Zahlen in $\mathbf{F}_p$ Quadrate sind, ist die Wahrscheinlichkeit, daß y_2 für k verschiedene x-Werte kein Quadrat ist, ungefähr $(\frac{1}{2})^k$.)
  4. Ist y_2 ein Quadrat, so berechnen wir ein $y \in \mathbf{F}_p$ mit $y^2 = y_2$. Wir ordnen jetzt der Zahl m den Punkt $(x, y) \in E(\mathbf{F}_p)$ zu und sind fertig.

  Ist umgekehrt $P = (x, y)$ gegeben, so schreiben wir $x = mk + j$ mit $0 \leq j \leq k-1$. Dann ist $m = [\frac{x}{k}]$.

Beispiel: Wir wollen $M = 10^{10}$ benutzen und setzen $k = 30$. Die Primzahl $p = 3 \cdot 10^{11} + 77$ erfüllt dann $p > Mk$. Wir wählen die elliptische Kurve E mit der Gleichung $y^2 = x^3 + x + 1$. Wir haben 10^6 Zahlen m im Intervall $0 \leq m \leq M-1$ zufällig gefällt und das j bestimmt, für das das dargestellte Verfahren funktioniert. Die Tabelle gibt die Anzahlen zu gegebenem j wieder:

j	0	1	2	3	4	5	6	7	8	9	10
#	498841	250915	124760	62927	31327	15593	7908	3856	1991	931	494

j	11	12	13	14	15	16	17	18	19	20	21	22
#	225	130	53	20	10	7	2	1	4	3	1	1

Wir haben einige Kryptosysteme kennengelernt, denen die Schwierigkeit der Logarithmenberechnung in $\mathbf{F}_q^*$ zugrunde liegt. Das kann man unmittelbar auf elliptische Kurven übertragen - man muß in der Formulierung nur Multiplikation durch Addition, Potenzieren durch Multiplizieren ersetzen, da wir die Verknüpfung in $E(\mathbf{F}_q)$ additiv schreiben. Man erhält dann z.B.

- das Analogon zum Diffie-Hellman-Schlüsselaustausch,
- das Analogon zum Massey-Omura-Kryptosystem für Nachrichtenübertragung,
- das Analogon zum ElGamal-Kryptosystem.

Bevor wir ein weiteres Kryptosystem mit elliptischen Kurven explizit beschreiben, erwähnen wir noch den Begriff der Hashfunktion.

Hash-Funktionen: Eine Hash-Funktion H berechnet zu einer beliebig langen Nachricht M einen Wert h fester Bitlänge m, wobei folgende Bedingungen erfüllt sein sollen:

- Für jedes M läßt sich $H(M)$ schnell berechnen.
- Man kann praktisch keine $M \neq M'$ finden mit $H(M) = H(M')$.
- Zu h im Bild von H kann man praktisch kein M finden mit $h = H(M)$.

Bemerkungen:

1. Wir nehmen an, A sendet eine Nachricht M an B, B empfängt M'. Wie kann B sicher sein, daß $M' = M$ ist? A sendet ebenfalls $H(M)$, B berechnet $H(M')$. Ist jetzt $H(M) \neq H(M')$, so stimmt etwas nicht.
2. Bei einem Multiusercomputersystem ist es besser, nicht die Paßwörter selbst, sondern die Hashwerte der Paßwörter zu speichern.
3. Hashfunktionen sind z.B. MD5 von Rivest und SHA.

Digitale Signaturen: Hier sind einige Eigenschaften, die eine eigenhändige Unterschrift hat bzw. haben sollte:

- 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.

Digitale Signaturen sollen nun die gleichen Funktionen erfüllen wie eine eigenhändige Unterschrift. Wir geben ein Beispiel:

ECDSA: (Das Analogon zu DSA für elliptische Kurven. Es wird zur Zeit diskutiert, ob ECDSA zu einem Standard für digitale Signaturen werden soll.)
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.
ECDSA-Schlüsselerzeugung: Jeder Benutzer A wählt sich eine Zufallszahl x_A mit $1 < x_A < q - 1$ und berechnet $Q_A = x_A P$. Der öffentliche Schlüssel von A ist Q_A, der private x_A.
ECDSA-Signatur-Erzeugung: A unterschreibt eine Nachricht m folgendermaßen:

1. A wählt eine Zufallszahl k mit $1 < k < q - 1$.
2. A berechnet $kP = (x_1, y_1)$ (mit $0 \leq x_1 \leq p - 1$) und $r = x_1 \bmod q$ (mit $0 \leq r \leq q - 1$). Ist $r = 0$, geht A zurück zu 1.
3. A berechnet den Hashwert $H(m)$ der Nachricht m und $s = k^{-1}(H(m) + x_A r) \bmod q$, wo $k-1$ das Inverse zu k modulo q meint. Im Fall $s = 0$, geht A zurück zu 1.
4. Die Signatur für die Nachricht m ist das Paar (r, s), die A seiner Nachricht an B dann hinzufügt.

ECDSA-Signatur-Verifikation: B erhält also eine Nachricht m und eine Signatur (r, s). Um zu sehen, daß die Signatur (r, s) gültig ist, geht B folgendermaßen vor:

1. B holt sich A's öffentlichen Schlüssel Q_A, überprüft, ob r und s im Intervall $[1, q-1]$ liegen; dann berechnet B die Werte $w = s^{-1} \bmod q$, $H(m)$, $u_1 = H(m)w \bmod q$, $u_2 = rw \bmod q$ und den Punkt $u_1P + u_2Q_A = (x_0, y_0)$ und schließlich $v = x_0 \bmod q$.
2. B akzeptiert die Unterschrift nur dann, falls $v = r$ gilt.

Warum gilt $v = r$, wenn alles richtig gelaufen ist? Es ist

$$(x_0, y_0) = u_1P + u_2Q_A = H(m)wP + rwx_AP = (H(m) + x_Ar)wP = skwP = kP = (x_1, y_1),$$

also $x_0 = y_0$ und damit $r = v$. Natürlich sollte man sich jetzt noch überlegen, daß die gewünschten Eigenschaften einer digitalen Signatur auch erfüllt sind.

Wichtige Fragen:

- Was sind kryptographisch geeignete elliptische Kurven? Wie kann man solche konstruieren?
- Wie berechnet man diskrete Logarithmen in $E(\mathbf{F}_q)$? Folgende Methoden kann man im Prinzip verwenden:
  - die naive Methode,
  - die Baby-Step-Giant-Step-Methode, die allerdings viel Speicherplatz benötigt;
  - die Pollardsche Monte-Carlo-Methode: dazu braucht man die Gruppenordnung $\#E(\mathbf{F}_q)$;
  - das Silver-Pohlig-Hellman-Verfahren: dazu braucht man ebenfalls die Gruppenordnung $\#E(\mathbf{F}_q)$, es funktioniert nur, wenn $\#E(\mathbf{F}_q)$ glatt ist, d.h. keinen großen Primteiler hat.

  Ein Analogon zur Index-Calculus-Methode ist für elliptische Kurven nicht bekannt.
- Wie berechnet man $\#E(\mathbf{F}_q)$?

Im folgenden geben wir noch Beispiele für die Logarithmenberechnung in $E(\mathbf{F}_p)$, wobei wir uns auf Kurven der Gestalt $y^2 = x^3 + ax + 1$ beschränken.

Das folgende Programm dlecnaiv.ub berechnet auf naive Weise diskrete Logarithmen.

```
 10  print "Diskrete Logarithmen fuer elliptische Kurven: Naive Methode."
 20  print "Es werden Kurven y^2=x^3+ax+1 betrachtet ueber F_p betrachtet."
 30  print "Vorzugegeben sind zwei Punkte P und Q, fuer die man xP=Q loesen will."
 40  input "p,a=";P,A
 50  input "Basispunkt P: Px,Py=";P1,P2:P0=1:X0=P0:X1=P1:X2=P2
 60  if (P1^3+A*P1+1-P2^2)@P>0 then print "Kein Punkt der Kurve!":goto 50
 70  input "Punkt Q: Qx,Qy=";Q1,Q2:Q0=1
 80  if (Q1^3+A*Q1+1-Q2^2)@P>0 then print "Kein Punkt der Kurve!":goto 70
 90  clr time
100  R0=0:R1=0:R2=1:X=0
110  if (R0*Q1-R1*Q0)@P=0 and (R0*Q2-R2*Q0)@P=0 and (R1*Q2-R2*Q1)@P=0 then print "x=";X,"Zeite=";
120  Y0=R0:Y1=R1:Y2=R2:gosub 150:X=X+1:R0=Z0:R1=Z1:R2=Z2
130  if R0>0 then goto 110
140  print "Q ist kein Vielfaches von P.":goto 40
150  ' Addition zweier Punkte: (x0:x1:x2)+(y0:y1:y2)=(z0:z1:z2)
160  Z0=(A*X0^2*Y0*Y1-A*X0*X1*Y0^2-X0^2*Y2^2+X2^2*Y0^2+3*X0*X1*Y1^2-3*X1^2*Y0*Y1)@P
170  Z1=(-3*X0^2*Y0*Y1+3*X0*X1*Y0^2-A*X0^2*Y1^2+A*X1^2*Y0^2-X0*X1*Y2^2+X2^2*Y0*Y1+2*X0*X2*Y1*Y2-2
180  Z2=(3*X0^2*Y0*Y2-3*X0*X2*Y0^2+A*X0^2*Y1*Y2-A*X1*X2*Y0^2+2*A*X0*X1*Y0*Y2-2*A*X0*X2*Y0*Y1-X0*X
190  if Z0<>0 or Z1<>0 or Z2<>0 then goto 270
200  Z0=(3*X0^2*Y0*Y1-3*X0*X1*Y0^2+A*X0^2*Y1^2-A*X1^2*Y0^2+X0*X1*Y2^2-X2^2*Y0*Y1+2*X0*X2*Y1*Y2-2*
210  Z1=(A^2*X0^2*Y0*Y1-A^2*X0*X1*Y0^2-3*X0^2*Y1^2+3*X1^2*Y0^2-A*X0*X1*Y1^2+A*X1^2*Y0*Y1+X1^2*Y2^
220  Z2=(-A^2*X0^2*Y0*Y2+A^2*X0*X2*Y0^2+3*X0^2*Y1*Y2-3*X1*X2*Y0^2+6*X0*X1*Y0*Y2-6*X0*X2*Y0*Y1+2*A
230  if Z0<>0 or Z1<>0 or Z2<>0 then goto 270
240  Z0=(6*X0*X2*Y0^2+6*X0^2*Y0*Y2+2*A*X1*X2*Y0^2+2*A*X0^2*Y1*Y2+4*A*X0*X2*Y0*Y1+4*A*X0*X1*Y0*Y2+
250  Z1=(2*A^2*X0*X2*Y0^2+2*A^2*X0^2*Y0*Y2-6*X1*X2*Y0^2-6*X0^2*Y1*Y2-12*X0*X2*Y0*Y1-12*X0*X1*Y0*Y
260  Z2=(-2*X0^2*Y0^2*A^3-18*X0^2*Y0^2-6*A*X0*X1*Y0^2-6*A*X0^2*Y0*Y1-2*A^2*X1^2*Y0^2-2*A^2*X0^2*Y
270  return
```

Beispiel: Wir betrachten $p = 10^7 + 19$ und E über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + x + 1$. Es ist $\#E(\mathbf{F}_p) = 9998581$, eine Primzahl. Durch Probieren finden wir folgende Punkte auf E:

$$P_1 = (1, 2075579), P_2 = (2, 4127806), P_4 = (4, 1887063), P_7 = (7, 1983045), P_8 = (8, 63008).$$

Mit obigem Programm und $P_0 = (0, 1)$ findet man

$$\log_{P_0} P_1 = 2346532 \text{ in } 13'30'' \text{ und } \log_{P_0} P_8 = 5083795 \text{ in } 29'13''.$$

Das Überprüfen selbst braucht (selbst mit Maple) keine Zeit.

Ein Programm dlecpoll.ub für die Pollardsche Monte-Carlo-Methode ist folgendes:

```
 10  print "Programm dlecpoll zum Berechnen diskreter Logarithmen"
 20  print "fuer elliptische Kurven y^2=x^3+a*x+1 ueber F_p mit"
 30  print "Pollards Monte-Carlo-Methode."
 40  input "p,a=";P,A
 50  input "#E(F_p)=";N
 60  input "Punkt P: Px,Py=";P1,P2:P0=1
 70  input "Punkt Q: Qx,Qy=";Q1,Q2:Q0=1
 80  X0=0:X1=0:X2=1:E=0:F=0:Xx0=0:Xx1=0:Xx2=1:Ee=0:Ff=0:Z=0:clr time
 90  Z=Z+1
100  I=(X0+X1+X2)\P:Y0=X0:Y1=X1:Y2=X2
110  if I=0 then gosub 270:E=(E+1)@N
120  if I=1 then gosub 400:E=(2*E)@N:F=(2*F)@N
130  if I=2 then gosub 450:F=(F+1)@N
140  X0=Z0:X1=Z1:X2=Z2
150  I=(Xx0+Xx1+Xx2)\P:Y0=Xx0:Y1=Xx1:Y2=Xx2
160  if I=0 then gosub 270:Ee=(Ee+1)@N
170  if I=1 then gosub 400:Ee=(2*Ee)@N:Ff=(2*Ff)@N
180  if I=2 then gosub 450:Ff=(Ff+1)@N
190  Xx0=Z0:Xx1=Z1:Xx2=Z2
200  I=(Xx0+Xx1+Xx2)\P:Y0=Xx0:Y1=Xx1:Y2=Xx2
210  if I=0 then gosub 270:Ee=(Ee+1)@N:
220  if I=1 then gosub 400:Ee=(2*Ee)@N:Ff=(2*Ff)@N
230  if I=2 then gosub 450:Ff=(Ff+1)@N
240  Xx0=Z0:Xx1=Z1:Xx2=Z2
250  if (X0*Xx1-X1*Xx0)@P=0 and (X0*Xx2-X2*Xx0)@P=0 and (X1*Xx2-X2*Xx1)@P=0 then print "s=";(E-Ee)
260  goto 90
270  ' Addition zweier Punkte: (q0:q1:q2)+(y0:y1:y2)=(z0:z1:z2)
280  Z0=(A*Q0^2*Y0*Y1-A*Q0*Q1*Y0^2-Q0^2*Y2^2+Q2^2*Y0^2+3*Q0*Q1*Y1^2-3*Q1^2*Y0*Y1)@P
290  Z1=(-3*Q0^2*Y0*Y1+3*Q0*Q1*Y0^2-A*Q0^2*Y1^2+A*Q1^2*Y0^2-Q0*Q1*Y2^2+Q2^2*Y0*Y1+2*Q0*Q2*Y1*Y2-2
300  Z2=(3*Q0^2*Y0*Y2-3*Q0*Q2*Y0^2+A*Q0^2*Y1*Y2-A*Q1*Q2*Y0^2+2*A*Q0*Q1*Y0*Y2-2*A*Q0*Q2*Y0*Y1-Q0*Q
310  if Z0<>0 or Z1<>0 or Z2<>0 then goto 390
320  Z0=(3*Q0^2*Y0*Y1-3*Q0*Q1*Y0^2+A*Q0^2*Y1^2-A*Q1^2*Y0^2+Q0*Q1*Y2^2-Q2^2*Y0*Y1+2*Q0*Q2*Y1*Y2-2*
330  Z1=(A^2*Q0^2*Y0*Y1-A^2*Q0*Q1*Y0^2-3*Q0^2*Y1^2+3*Q1^2*Y0^2-A*Q0*Q1*Y1^2+A*Q1^2*Y0*Y1+Q1^2*Y2^
340  Z2=(-A^2*Q0^2*Y0*Y2+A^2*Q0*Q2*Y0^2+3*Q0^2*Y1*Y2-3*Q1*Q2*Y0^2+6*Q0*Q1*Y0*Y2-6*Q0*Q2*Y0*Y1+2*A
350  if Z0<>0 or Z1<>0 or Z2<>0 then goto 390
360  Z0=(6*Q0*Q2*Y0^2+6*Q0^2*Y0*Y2+2*A*Q1*Q2*Y0^2+2*A*Q0^2*Y1*Y2+4*A*Q0*Q2*Y0*Y1+4*A*Q0*Q1*Y0*Y2+
370  Z1=(2*A^2*Q0*Q2*Y0^2+2*A^2*Q0^2*Y0*Y2-6*Q1*Q2*Y0^2-6*Q0^2*Y1*Y2-12*Q0*Q2*Y0*Y1-12*Q0*Q1*Y0*Y
380  Z2=(-2*Q0^2*Y0^2*A^3-18*Q0^2*Y0^2-6*A*Q0*Q1*Y0^2-6*A*Q0^2*Y0*Y1-2*A^2*Q1^2*Y0^2-2*A^2*Q0^2*Y
390  return
400  ' Verdoppelung eines Punktes: 2 (y0:y1:y2)=(z0:z1:z2)
410  Z0=(8*Y0*Y2^3)@P
420  Z1=(2*Y2*(A^2*Y0^3-9*Y0^2*Y1-3*A*Y0*Y1^2+Y2^2*Y1))@P
430  Z2=(-Y0^4*A^3-9*Y0^4-6*A*Y0^3*Y1-6*A^2*Y1^2*Y0^2+18*Y0*Y1^3+3*A*Y1^4+Y2^4)@P
440  return
```

```
450   ' Addition zweier Punkte: (p0:p1:p2)+(y0:y1:y2)=(z0:z1:z2)
460   Z0=(A*P0^2*Y0*Y1-A*P0*P1*Y0^2-P0^2*Y2^2+P2^2*Y0^2+3*P0*P1*Y1^2-3*P1^2*Y0*Y1)@P
470   Z1=(-3*P0^2*Y0*Y1+3*P0*P1*Y0^2-A*P0^2*Y1^2+A*P1^2*Y0^2-P0*P1*Y2^2+P2^2*Y0*Y1+2*P0*P2*Y1*Y2-2
480   Z2=(3*P0^2*Y0*Y2-3*P0*P2*Y0^2+A*P0^2*Y1*Y2-A*P1*P2*Y0^2+2*A*P0*P1*Y0*Y2-2*A*P0*P2*Y0*Y1-P0*P
490   if Z0<>0 or Z1<>0 or Z2<>0 then goto 570
500   Z0=(3*P0^2*Y0*Y1-3*P0*P1*Y0^2+A*P0^2*Y1^2-A*P1^2*Y0^2+P0*P1*Y2^2-P2^2*Y0*Y1+2*P0*P2*Y1*Y2-2*
510   Z1=(A^2*P0^2*Y0*Y1-A^2*P0*P1*Y0^2-3*P0^2*Y1^2+3*P1^2*Y0^2-A*P0*P1*Y1^2+A*P1^2*Y0*Y1+P1^2*Y2^
520   Z2=(-A^2*P0^2*Y0*Y2+A^2*P0*P2*Y0^2+3*P0^2*Y1*Y2-3*P1*P2*Y0^2+6*P0*P1*Y0*Y2-6*P0*P2*Y0*Y1+2*A
530   if Z0<>0 or Z1<>0 or Z2<>0 then goto 570
540   Z0=(6*P0*P2*Y0^2+6*P0^2*Y0*Y2+2*A*P1*P2*Y0^2+2*A*P0^2*Y1*Y2+4*A*P0*P2*Y0*Y1+4*A*P0*P1*Y0*Y2+
550   Z1=(2*A^2*P0*P2*Y0^2+2*A^2*P0^2*Y0*Y2-6*P1*P2*Y0^2-6*P0^2*Y1*Y2-12*P0*P2*Y0*Y1-12*P0*P1*Y0*Y
560   Z2=(-2*P0^2*Y0^2*A^3-18*P0^2*Y0^2-6*A*P0*P1*Y0^2-6*A*P0^2*Y0*Y1-2*A^2*P1^2*Y0^2-2*A^2*P0^2*Y
570   return
```

Beispiel: Wir betrachten wieder E mit $y^2 = x^3 + x + 1$ über $\mathbf{F}_p$ mit $p = 10^7 + 19$. Die Gruppenordnung ist $n = \#E(\mathbf{F}_p) = 9998581$, eine Primzahl. Sei

$$P_0 = (0, 1), \quad P_1 = (1, 2075579), \quad P_8 = (8, 63008).$$

Nach 2561101 Versuchen und 37 Minuten findet man

$$s = 3460064, \quad t = 3168616, \quad ggT(s, n) = 1 \quad \text{für} \quad sP_1 = tP_0,$$

was den oben berechneten Logarithmus liefert. Nach 7190102 Versuchen und 1 Stunde und 44 Minuten findet man

$$s = 25132, \quad t = 4067922, \quad ggT(s, n) = 1 \quad \text{für} \quad sP_8 = tP_0,$$

was den oben berechneten Logarithmus liefert.

Beispiel: Wir betrachten E mit der Gleichung $y^2 = x^3 + 3x + 1$ über $\mathbf{F}_p$ mit $p = 10^7 + 19$. Die Gruppenordnung ist

$$n = \#E(\mathbf{F}_p) = 9999846 = 2 \cdot 3^2 \cdot 347 \cdot 1601 = 18 \cdot 347 \cdot 1601.$$

Wir betrachten die Punkte

$$P = (2, 4417259) \quad \text{und} \quad Q = (1, 866032)$$

in $E(\mathbf{F}_p)$. Mit der naiven Methode findet man nun (sofort)

$$\begin{aligned} x \cdot \frac{n}{18} \cdot P = \frac{n}{18} \cdot Q \quad &\text{impliziert} \quad x \equiv 14 \bmod 18, \\ x \cdot \frac{n}{347} \cdot P = \frac{n}{347} \cdot Q \quad &\text{impliziert} \quad x \equiv 81 \bmod 347, \\ x \cdot \frac{n}{1601} \cdot P = \frac{n}{1601} \cdot Q \quad &\text{impliziert} \quad x \equiv 854 \bmod 1601, \end{aligned}$$

woraus mit dem chinesischen Restesatz sofort

$$x = \log_P Q = 5553122$$

folgt. Dieses Verfahren funktioniert, weil $\#E(\mathbf{F}_p)$ recht glatt ist.

Das letzte Beispiel zeigt nochmals, daß bei kryptographisch geeigneten elliptischen Kurven $\#E(\mathbf{F}_q)$ mindestens einen großen Primteiler haben muß.

1993 haben Menezes, Okamoto und Vanstone gezeigt, daß man die Berechnung von Logarithmen in $E(\mathbf{F}_q)$ auf die Berechnung von Logarithmen in $\mathbf{F}_{q^k}^*$ zurückführen kann. Wir werden dies im nächsten Paragraphen behandeln. Dies wird ebenfalls Auswirkung auf die Eignung elliptischer Kurven für kryptographische Zwecke haben.

Verwendete Literatur: [**3**], [**4**], [**11**].

KAPITEL 11

Die Weil-Paarung

Sei C eine projektive nichtsinguläre irreduzible Kurve über einem Körper K. Ist $f \in \overline{K}(C)^*$ und $D = \sum_i n_i P_i$ ein Divisor, so daß D und (f) disjunkten Träger haben (d.h. f ist definiert in allen P_i), so definieren wir

$$f(D) = \prod_i f(P_i)^{n_i}.$$

Natürlich gilt $f(D_1 + D_2) = f(D_1)f(D_2)$ und $(fg)(D) = f(D)g(D)$, sofern die Ausdrücke definiert sind. Ohne Beweis geben wir folgenden wichtigen Satz an:

SATZ (Weilsches Reziprozitätsgesetz). *Sind $f, g \in \overline{K}(C)^*$, so daß* $\mathrm{div}(f)$ *und* $\mathrm{div}(g)$ *disjunkte Träger haben, dann gilt:*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

Beispiel: Wir betrachten $\mathbf{P}^1$ mit $\overline{K}(\mathbf{P}^1) = \overline{K}(x)$. Für $f = x - a$ und $g = \frac{x-b}{x-c}$ ist

$$\mathrm{div}(f) = (a) - (\infty) \quad \text{und} \quad \mathrm{div}(g) = (b) - (c).$$

Sind a, b, c paarweise verschieden, so erhält man

$$\begin{aligned} f(\mathrm{div}(g)) &= f((b) - (c)) = \frac{f(b)}{f(c)} = \frac{b-a}{c-a}, \\ g(\mathrm{div}(f) &= g((a) - (\infty)) = \frac{g(a)}{g(\infty)} = \frac{\frac{a-b}{a-c}}{1}, \end{aligned}$$

also $f(\mathrm{div}(g)) = g(\mathrm{div}(g))$.

Sei jetzt E eine elliptische Kurve über einem Körper K. Da wir Addition in E und in $\mathrm{Div}E$ benutzen, schreiben wir für einen Punkt $P \in E$, den wir als Divisor auffassen (P). So meint $(P) + (Q)$ den Divisor, der aus den beiden Punkten P und Q besteht, während $(P + Q)$ nur aus einem Punkt, der Summe von P und Q auf E, besteht. Die Addition auf E war so definiert, daß gilt

$$(P + Q) - (O) \sim [(P) - (O)] + [(Q) - (O)], \text{ also } (P + Q) \sim (P) + (Q) - (O).$$

Sei $m \in \mathbf{N}$, so daß $ggT(m, p) = 1$, falls $p = char(K)$ ist. Wir wollen eine Abbildung, die sogenannte Weil-Paarung,

$$e_m : E[m] \times E[m] \to \overline{K}^*$$

definieren.

- Seien $P, Q \in E[m]$. Nach Definition bedeutet das, daß die Klassen der Divisoren $(P) - (O)$ und $(Q) - (O)$ (in $\mathrm{Pic}^0(E)$) von m annulliert werden. Anders ausgedrückt:

  $$m((P) - (O)) \sim m((Q) - (O)) \sim 0.$$

- Seien A und B Divisoren mit

  $$A \sim (P) - (O) \quad \text{und} \quad B \sim (Q) - (O),$$

  so daß A und B disjunkten Träger haben. (Wir werden später explizit Beispiele für solche Divisoren A und B angeben.)

- Dann gilt
$$mA \sim m((P)-(O)) \sim 0 \quad \text{und} \quad mB \sim m((Q)-(O)) \sim 0,$$
also gibt es Funktionen f_A und f_B mit
$$mA = (f_A) \quad \text{und} \quad mB = (f_B).$$
Da A und B disjunkte Träger haben, gilt das natürlich auch für (f_A) und (f_B).
- Wir definieren jetzt:
$$e_m(P,Q) = \frac{f_A(B)}{f_B(A)}.$$

Wir müssen jetzt sehen, daß $e_m(P,Q)$ nicht von der Wahl von A, B, f_A und f_B abhängen.

- Seien A' und B' andere Divisoren mit $A' \sim P-O$ und $B' \sim Q-O$. Dann gibt es Funktionen g,h mit $A' = A + \mathrm{div}(g)$ und $B' = B + \mathrm{div}(h)$. Weiter gilt
$$mA' = mA + m\mathrm{div}(g) = (f_A) + (g^m) = (f_A g^m) \quad \text{und} \quad mB' = (f_B h^m),$$
also können wir $f_{A'} = f_A g^m$ und $f_{B'} = f_B h^m$ wählen. Damit erhält man:
$$\begin{aligned}\frac{f_{A'}(B')}{f_{B'}(A')} &= \frac{(f_A g^m)(B+\mathrm{div}(h))}{(f_B h^m)(A+\mathrm{div}(g))} = \frac{f_A(B) f_A(\mathrm{div}(h)) g(B)^m g(\mathrm{div}(h))^m}{f_B(A) f_B(\mathrm{div}(g)) h(A)^m h(\mathrm{div}(g))^m} = \\ &= \frac{f_A(B)}{f_B(A)} \cdot \frac{f_A(\mathrm{div}(h))}{h(mA)} \cdot \frac{g(mB)}{f_B(\mathrm{div}(g))} \cdot \frac{g(\mathrm{div}(h))^m}{h(\mathrm{div}(g))^m} = \frac{f_A(B)}{f_B(A)},\end{aligned}$$
da die letzten drei Produkte nach dem Weilschen Reziprozitätsgesetz 1 sind.
- f_A ist durch A nur bis auf eine Konstante bestimmt. Da aber B Grad 0 hat, gilt für jedes $c \in \overline{K}^*$ offensichtlich $c(B) = 1$ und damit $(f_A)(B) = (cf_A)(B)$. Analog: $f_B(A) = (c'f_B)(A)$. Damit folgt schließlich, daß $e_m(P,Q)$ wohldefiniert ist.

Wir geben nun die wichtigsten Eigenschaften der Weil-Paarung e_m ohne Beweis an:

SATZ. *Für die Weil-Paarung auf einer elliptischen Kurve gilt:*

1. *e_m ist bilinear, d.h. $e_m(P_1+P_2,Q) = e_m(P_1,Q)e_m(P_2,Q)$ und $e_m(P,Q_1+Q_2) = e_m(P,Q_1)e_m(P,Q_2)$.*
2. *Aus der Bilinearität folgt sofort $(e_m(P,Q))^m = 1$, d.h. $e_m(P,Q)$ ist eine m-te Einheitswurzel. Anders geschrieben:*
$$e_m : E[m] \times E[m] \to \mu_m,$$
wo $\mu_m \subseteq \overline{K}^*$ die Gruppe der m-ten Einheitswurzeln bezeichnet.
3. *e_m ist alternierend, d.h. $e_m(P,P) = 1$, woraus sofort folgt, daß gilt $e_m(Q,P) = e_m(P,Q)^{-1}$.*
4. *e_m ist nicht ausgeartet, d.h. gilt $e_m(P,Q) = 1$ für alle $Q \in E[m]$, so ist $Q = O$.*
5. *Für $\sigma \in G_K$ gilt:*
$$e_m(\sigma P, \sigma Q) = \sigma e_m(P,Q).$$
6. *Ist $P \in E[mm']$ und $Q \in E[m]$, so gilt*
$$e_{mm'}(P,Q) = e_m(m'P,Q).$$

LEMMA. *Hat $P \in E[m]$ die Ordnung m, so gibt es einen Punkt $P' \in E[m]$, so daß $e_m(P,P')$ eine primitive m-te Einheitswurzel ist.*

Beweis: Offensichtlich ist $G_P = \{e_m(P,Q) \subseteq \mu_m : Q \in E[m]\}$ eine Untergruppe von μ_m, insbesondere zyklisch von einer Ordnung m' mit $m'|m$. Dann erhält man für alle $Q \in E[m]$ die Aussage $1 = (e_m(P,Q))^{m'} = e_m(m'P,Q)$, was wegen der Nichtausgeartetheit von e_m sofort $m'P = O$ und damit $m = m'$ liefert. Insbesondere gibt es einen Punkt $P' \in E[m]$, so daß $e_m(P,P')$ eine primitive m-te Einheitswurzel ist. ■

SATZ. *Gilt $E[m] \subseteq E(K)$, so folgt $\mu_m \subseteq K^*$.*

Beweis: Nach dem letzten Lemma gibt es $P, P' \in E[m]$, so daß $\zeta_m = e_m(P,P')$ eine primitive m-te Einheitswurzel ist. Wegen $E[m] \subseteq E(K)$ folgt für jedes $\sigma \in G_K$
$$\sigma\zeta_m = \sigma e_m(P,P') = e_m(\sigma P, \sigma P') = e_m(P,P') = \zeta_m,$$
also $\zeta_m \in K$. ■

Beispiele:

1. Ist E eine über $\mathbf{R}$ definierte elliptische Kurve, so folgt aus $E[m] \subseteq E(\mathbf{R})$ sofort $\mu_m \subseteq \mathbf{R}^*$, also $m|2$. D.h. höchstens die 2-Teilungspunkte sind alle über $\mathbf{R}$ definiert.
2. Sei E eine über $\mathbf{F}_q$ definierte elliptische Kurve mit $E[m] \subseteq E(\mathbf{F}_{q^k})$. Dann folgt $\mu_m \subseteq \mathbf{F}_{q^k}^*$, was äquivalent ist mit $m|(q^k-1)$. Insbesondere ist $m|(q-1)$ eine notwendige Bedingung für $E[m] \subseteq E(\mathbf{F}_q)$.
3. Ist ℓ eine Primzahl und $E[\ell] \subseteq E(\mathbf{F}_{1009})$, so folgt wegen $1009-1 = 2^4 \cdot 3^2 \cdot 7$ sofort $\ell \in \{2,3,7\}$.

Für die Kryptographie ist folgender Satz wichtig:

SATZ. *Sei E eine elliptische Kurve über $\mathbf{F}_q$, $P \in E(\mathbf{F}_q)$, $ord(P) = m$ und $ggT(m,q) = 1$.*

1. *Sei $P' \in E[m]$, so daß $e_m(P,P')$ eine primitive m-te Einheitswurzel ist. Dann ist*
$$E[m] = \mathbf{Z}/(m) \cdot P + \mathbf{Z}/(m) \cdot P'.$$
Ist $P' \in E(\mathbf{F}_{q^k})$, so gilt $m|q^k-1$.
2. *Für $Q \in E(\mathbf{F}_q)$ gilt:*
$$Q \in < P > \quad \Longleftrightarrow \quad mQ = O \text{ und } e_m(P,Q) = 1.$$
3. *Für $Q \in < P >$ und $x \in \mathbf{N}_0$ gilt:*
$$Q = xP \quad \Longleftrightarrow \quad e_m(Q,P') = e_m(P,P')^x.$$

Beweis:

1. Sei $E[m] = \mathbf{Z}/(m)P_1 + \mathbf{Z}/(m)P_2$. Dann gibt es $a,b,c,d \in \mathbf{Z}/(m)$ mit $P = aP_1 + bP_2$, $P' = cP_1 + dP_2$ und damit
$$e_m(P,P') = e_m(aP_1 + bP_2, cP_1 + dP_2) = e_m(P_1,P_2)^{ad-bc}.$$
Also ist $ad - bc \in (\mathbf{Z}/(m))^*$, so daß auch P_1, P_2 Linearkombinationen von P, P' sind, also $E[m] = \mathbf{Z}/(m)P + \mathbf{Z}/(m)P'$. Die Aussage $m|q^k-1$ wurde schon erwähnt.
2. Jedes $Q \in E[m]$ schreibt sich als $Q = xP + yP'$ mit $0 \le x,y \le m-1$. Nun ist $e_m(P,Q) = e_m(P,P')^y$, was die Behauptung liefert.
3. $Q = xP$ liefert natürlich $e_m(Q,P') = e_m(P,P')^x$. Sei umgekehrt $e_m(Q,P') = e_m(P,P')^x$. Die Bilinearität liefert $e_m(Q - xP, P') = 1$, wegen $Q \in < P >$ gilt $e_m(Q - xP, P) = 1$. Da e_m nichtausgeartet ist, folgt nun $Q - xP = O$, was zu zeigen war. ■

Der letzte Satz reduziert die Berechnung von Logarithmen in $E(\mathbf{F}_q)$ auf die Berechnung von Logarithmen in $\mathbf{F}_{q^k}^*$. Wir müssen untersuchen, ob dies eine Vereinfachung ist. Es stellen sich zwei Fragen:

- Wie berechnet man die Weil-Paarung?
- Wie findet man einen Punkt $P' \in E[m]$, so daß $e_m(P,P')$ eine primitive m-te Einheitswurzel ist?

Zur Berechnung der Weil-Paarung $e_m(P,Q)$ gehen wir in zwei Schritten vor.

1. Schritt: Man braucht zunächst trägerfremde Divisoren A und B mit $A \sim (P) - (O)$ und $B \sim (Q) - (O)$. Nun gilt $(P+S) \sim (P) + (S) - (O)$, also $(P+S) - (S) \sim (P) - (O)$. Man kann offensichtlich leicht Punkte $S, T \in E$ wählen, so daß
$$A = (P+S) - (S) \sim (P) - (O) \quad \text{und} \quad B = (Q+T) - (T) \sim (Q) - (O)$$
disjunkte Träger haben. Dann gilt also
$$e_m(P,Q) = \frac{f_A((Q+T) - (T))}{f_B((P+S) - (S))} = \frac{f_A(Q+T) f_B(S)}{f_A(T) f_B(P+S)}.$$

2. Schritt: Wie findet bzw. berechnet man eine Funktion f_A mit $\mathrm{div}(f_A) = mA$, falls $A = (P+S) - (S)$ ist?

Seien P, Q Punkte einer elliptischen Kurve E (in Weierstraßscher Normalform). Wir schreiben $\ell(P,Q)$ für eine Linearform, so daß $\ell(P,Q) = 0$ die Gerade durch P und Q bzw. im Fall $P = Q$ die Tangente ist.

Z.B. ist dann $\ell(O,O) = x_0$. Bezeichnet $(\ell(P,Q))$ den zu $\ell(P,Q) = 0$ gehörigen Divisor vom Grad 3, so gilt nach Konstruktion der Addition auf E:

$$(\ell(P,Q)) = (P) + (Q) + (-(P+Q)) \quad \text{und} \quad (\ell(P+Q,O)) = (P+Q) + (O) + (-(P+Q)),$$

woraus wir sofort folgende Formel erhalten: Für Punkte P, Q auf E gilt:

$$[(P) - (O)] + [(Q) - (O)] = (P+Q) - (O) + \mathrm{div}(\frac{\ell(P,Q)}{\ell(P+Q,O)}).$$

Da $E \to \mathrm{Pic}^0(E), P \mapsto$ Klasse von $(P) - (O)$ bijektiv ist, folgt nun sofort folgendes Lemma:

LEMMA. 1. *Jeder Divisor D vom Grad 0 hat eine eindeutige Darstellung*

$$D = (P) - (O) + \mathrm{div}(f),$$

wobei f natürlich nur bis auf eine Konstante eindeutig bestimmt ist. (Wir benutzen diese Darstellung als Normalform für Divisoren vom Grad 0.)

2. *Für zwei Divisoren $D_i = (P_i) - (O) + \mathrm{div}(f_i)$ gilt:*

$$D_1 + D_2 = (P_1 + P_2) - (O) + \mathrm{div}(f_1 f_2 \frac{\ell(P_1, P_2)}{\ell(P_1 + P_2, O)}).$$

Mit dem letzten Lemma kann man jetzt rekursiv die Normalform von $d(P) - d(O)$ berechnen. Man erhält dann eine Darstellung

$$d(P) - d(O) = (dP) - (O) + \mathrm{div}(L_{d,P}).$$

Benutzt man das square-and-multiply-Verfahren, so braucht man zur Berechnung dieser Normalform $O(\log d)$ Schritte.
Wir geben ein Beispiel für $d = 7$:

$$\begin{aligned}
2(P) - 2(O) &= [(P) - (O)] + [(P) - (O)] = (2P) - (O) + \mathrm{div}(\frac{\ell(P,P)}{\ell(2P,O)}),\\
4(P) - 4(O) &= [2(P) - 2(O)] + [2(P) - 2(O)] = 2(2P) - 2(O) + 2\mathrm{div}(\frac{\ell(P,P)}{\ell(2P,O)}) =\\
&= (4P) - (O) + \mathrm{div}(\frac{\ell(2P,2P)}{\ell(4P,O)}) + 2\mathrm{div}(\frac{\ell(P,P)}{\ell(2P,O)}) =\\
&= (4P) - (O) + \mathrm{div}(\frac{\ell(2P,2P)\ell(P,P)^2}{\ell(4P,O)\ell(2P,O)^2}),\\
6(P) - 6(O) &= [2(P) - 2(O)] + [4(P) - 4(O)] =\\
&= [(2P) - (O) + \mathrm{div}(\frac{\ell(P,P)}{\ell(2P,O)})] + [(4P) - (O) + \mathrm{div}(\frac{\ell(2P,2P)\ell(P,P)^2}{\ell(4P,O)\ell(2P,O)^2})] =\\
&= (6P) - (O) + \mathrm{div}(\frac{\ell(2P,4P)}{\ell(6P,O)}) + \mathrm{div}(\frac{\ell(P,P)^3\ell(2P,2P)}{\ell(2P,O)^3\ell(4P,O)}) =\\
&= (6P) - (O) + \mathrm{div}(\frac{\ell(P,P)^3\ell(2P,2P)\ell(2P,4P)}{\ell(2P,O)^3\ell(4P,O)\ell(6P,O)}),\\
7(P) - 7(O) &= [(P) - (O)] + [6(P) - 6(O)] =\\
&= (7P) - (O) + \mathrm{div}(\frac{\ell(P,6P)}{\ell(7P,O)}) + \mathrm{div}(\frac{\ell(P,P)^3\ell(2P,2P)\ell(2P,4P)}{\ell(2P,O)^3\ell(4P,O)\ell(6P,O)}) =\\
&= (7P) - (O) + \mathrm{div}(\frac{\ell(P,P)^3\ell(2P,2P)\ell(2P,4P)\ell(P,6P)}{\ell(2P,O)^3\ell(4P,O)\ell(6P,O)\ell(7P,O)}).
\end{aligned}$$

Damit folgt nun sofort für $P \in E[m]$:

$$\begin{aligned}
m(P+S) - m(S) &= [m(P+S) - m(O)] - [m(S) - m(O)] =\\
&= [(mP + mS) - (O) + \mathrm{div}(L_{m,P+S})] - [(mS) - (O) + \mathrm{div}(L_{m,S})] =\\
&= \mathrm{div}(\frac{L_{m,P+S}}{L_{m,S}}).
\end{aligned}$$

Für unsere Problemstellung $P, Q \in E[m]$, $A = (P+S) - (S)$ und $B = (Q+T) - (T)$ können wir also wählen

$$f_A = \frac{L_{m,P+S}}{L_{m,S}} \quad \text{und} \quad f_B = \frac{L_{m,Q+T}}{L_{m,T}}.$$

Damit erhält man schließlich

$$e_m(P,Q) = \frac{L_{m,P+S}(Q+T)L_{m,Q+T}(S)L_{m,S}(T)L_{m,T}(P+S)}{L_{m,S}(Q+T)L_{m,T}(S)L_{m,P+S}(T)L_{m,Q+T}(P+S)}.$$

Wählt man S und T nicht zu speziell, kann man damit sofort $e_m(P,Q)$ berechnen. Die Schrittzahl läßt sich durch $O(\log m)$ abschätzen.

Beispiel: Wir betrachten die elliptische Kurve E mit der Gleichung $y^2 = x^3 - 48x + 1$ über $\mathbf{F}_p$ mit $p = 1009$. Wegen $p - 1 = 2^4 \cdot 2^3 \cdot 7$ liegen die 7-ten Einheitswurzeln in $\mathbf{F}_p$. (Dies ist eine notwendige Bedingung dafür, daß $E[7] \subseteq E(\mathbf{F}_p)$ gelten kann.) Man findet $\#E(\mathbf{F}_p) = 980 = 2^2 \cdot 5 \cdot 7^2$. Durch Probieren finden wir Punkte auf E. Wir geben einige an mit der jeweiligen Ordnung:

P	(0,1)	(2,448)	(3,231)	(4,138)	(6,470)	(7,131)	(11,472)	(12,12)	(69,481)
$ord(P)$	35	28	140	70	140	7	70	140	7

Durch Probieren sieht man sofort, daß

$$E[7] = \mathbf{Z}/(7) \cdot (7,131) + \mathbf{Z}/(7) \cdot (69,481)$$

gilt. Sei $P = (7,131)$ und $Q = (69,481)$. Wir wollen $e_7(P,Q)$ berechnen. Probeweise wählen wir $S = (0,1)$ und $T = (2,448)$. Die Bestimmung der Funktionen $\ell(P,P)$ etc. ist leicht. Man erhält dann:

$$\begin{aligned}
L_{7,P+S} &= \frac{(770+736x+y)^3(805+539x+y)(188+520x+y)(520+150x+y)}{(298+x)^3(484+x)(239+x)(44+x)},\\
L_{7,S} &= \frac{(1008+24x+y)^3(17+4x+y)(602+271x+y)(1008+528x+y)}{(433+x)^3(127+x)(665+x)(44+x)},\\
L_{7,Q+T} &= \frac{(617+489x+y)^3(273+687x+y)(94+616x+y)(645+309x+y)}{(102+x)^3(39+x)(796+x)(632+x)},\\
L_{7,T} &= \frac{(642+464x+y)^3(919+148x+y)(863+393x+y)(359+101x+y)}{(634+x)^3(35+x)(268+x)(632+x)}
\end{aligned}$$

und damit

$$f_A = \frac{L_{7,P+S}}{L_{7,S}} \quad \text{und} \quad f_B = \frac{L_{7,Q+T}}{L_{7,T}},$$

womit man dann sofort durch Einsetzen

$$e_7(P,Q) = 105$$

berechnet. (Wie es sein sollte ist $105^7 \equiv 1 \bmod 1009$.)

Bemerkung: Bei der Berechnung von $e_m(P,Q)$ muß man nicht $L_{m,P+S}$ etc. explizit berechnen, sondern nur die Auswertung an zwei Punkten. Dies macht das Programmieren deutlich einfacher und schneller. Wir skizzieren dies kurz:

1. Sei $P \in E[m]$, $mP = (L_{m,P})$ und $R_1, R_2 \in E$ Punkte. Wir wollen $\frac{L_{m,P}(R_1)}{L_{m,P}(R_2)}$ berechnen.
2. Ein Divisor D vom Grad 0 hat eine eindeutige Darstellung $D = (P) - (O) + \mathrm{div}(f)$. Für die 'meisten' Divisoren ist dann die Abbildung
$$\alpha(D) = (P, \frac{f(R_1)}{f(R_2)})$$
definiert.
3. Ist $D_i = (P_i) - (O) + \mathrm{div}(f_i)$, so gilt
$$\alpha(D_1 + D_2) = (P_1 + P_2, \frac{f_1(R_1)}{f_1(R_2)} \cdot \frac{f_2(R_1)}{f_2(R_2)} \cdot \frac{\ell(P_1,P_2)(R_1)}{\ell(P_1,P_2)(R_2)} \cdot \frac{\ell(P_1+P_2,O)(R_2)}{\ell(P_1+P_2,O)(R_1)}),$$
wenn R_1, R_2 nicht auf einer der auftretenden Geraden liegen.

4. Mit dem square-and-multiply-Verfahren berechnet man nun für $P \in E[m]$ in $O(\log m)$ Schritten
$$\alpha(m(P) - m(O)) = (O, \frac{L_{m,P}(R_1)}{L_{m,P}(R_2)}),$$
was wir haben wollten.

Das unten angegebene Maple-Programm funktioniert auf (ähnliche) Weise.

Fazit: Die Weil-Paarung $e_m(P,Q)$ läßt sich schnell berechnen. Wesentlich geht die Arithmetik in $\mathbf{F}_{q^k}$ ein.

Wie wendet man das nun auf die Logarithmenberechnung in $E(\mathbf{F}_q)$ an? (Das Reduktionsverfahren geht auf Menezes, Okamoto und Vanstone zurück.) Seien $P, Q \in E(\mathbf{F}_q)$ gegeben. Wir suchen $\log_P Q$. Sei außerdem noch $ord(P) = m$ und $ggT(m,q) = 1$ bekannt.

1. Bestimme ein (möglichst kleines) k mit $E[m] \subseteq E(\mathbf{F}_{q^k})$.
2. Bestimme dann ein $P' \in E[m]$, so daß $e_m(P,P')$ eine primitive m-te Einheitswurzel ist. Dann gilt
$$E[m] = \mathbf{Z}/(m)P + \mathbf{Z}/(m)P'.$$
3. Es muß gelten $mQ = O$, sonst können wir sofort aufhören.
4. Es muß weiter gelten $e_m(P,Q) = 1$.
5. Sei $g = e_m(P,P')$ und $a = e_m(Q,P')$. Wir müssen jetzt in $\mathbf{F}_{q^k}^*$ den diskreten Logarithmus $\log_g a$ bestimmen. Er ist identisch mit $\log_P Q$.

Einige Bemerkungen dazu:

zu 1.: Eine notwendige Bedingung ist $m | q^k - 1$, d.h. $q^k \equiv 1 \bmod p$.

zu 2.: Berechne $N = \#E(\mathbf{F}_{q^k})$, zerlege $N = m'u$ mit $ggT(m,u) = 1$. (Dann gilt $m | m'$.) Wähle einen zufälligen Punkt P''' und setze $P'' = \frac{N}{u}P'''$. Dann wird P'' von m' annulliert, also $ord(P'') | m'$. Berechne $ord(P'')$. Ist $ord(P'') \not\equiv 0 \bmod m$, wähle einen anderen Punkt P'''. Gilt $m | ord(P'')$, setze $P' = \frac{ord(P'')}{m}P''$. Der Punkt P' hat also Ordnung m. Teste jetzt, ob $e_m(P,P')$ eine primitive m-te Einheitswurzel ist. Wenn nein, wähle einen anderen Punkt P'''.

Beispiel: Für die Kurve $E : y^2 = x^3 + x + 1$ über $\mathbf{F}_p$ mit $p = 10^7 + 19$ ist $\#E(\mathbf{F}_p) = 9998581$ eine Primzahl. Wählt man $m = 9998581$ und sucht die kleinste Zahl $k \geq 1$ mit $p^k \equiv 1 \bmod m$, so findet man (mit $m - 1 = 2^2 \cdot 3 \cdot 5 \cdot 166643$) $k = \frac{m-1}{3}$. Der Reduktionsprozeß liefert also ein Problem in $\mathbf{F}_{p^k}$, was nicht machbar ist. Allein zur Beschreibung dieses Körpers bräuchte man ein (über $\mathbf{F}_p$ irreduzibes) Polynom vom Grad $k = 3332860$.

Bemerkung: Sucht man also nach kryptographisch geeigneten Kurven E über $\mathbf{F}_q$ mit einem Punkt $P \in E(\mathbf{F}_q)$ und $ord(P) = m$ (und $ggT(m,q) = 1$) und wählt man q und m so, daß das kleinste k mit $q^k \equiv 1 \bmod m$ schon sehr groß ist, dann kann man sicher sein, daß man die Logarithmenberechnung in $E(\mathbf{F}_q)$ praktisch nicht mehr auf eine Berechnung in $\mathbf{F}_{q^k}^*$ zurückführen kann.

Wir werden jetzt eine Klasse von Kurven betrachten, bei denen der Reduktionsprozeß sinnvoll sein kann.

SATZ. *Sei $p \geq 5$ eine Primzahl und E eine elliptische Kurve über $\mathbf{F}_p$. Dann gilt:*

1. *E ist genau dann supersingulär, wenn $\#E(\mathbf{F}_p) = p + 1$ gilt.*
2. *Ist E supersingulär, so gilt*
$$E(\mathbf{F}_p) \subseteq E[p+1] = E(\mathbf{F}_{p^2}).$$

Beweis: Die erste Aussage kennen wir bereits. Sei jetzt E supersingulär und π der Frobeniusendomorphismus. Die Spur s des Frobenius ist 0 wegen $p + 1 = \#E(\mathbf{F}_p) = p + 1 - s$, also erfüllt π die Gleichung
$$\pi^2 + p = 0.$$
Dann gilt
$$\#E(\mathbf{F}_{p^2}) = (1 - \pi^2)(1 - \overline{\pi^2}) = (p+1)^2.$$
Ist $P \in E[p+1]$, so ist $\pi^2 P = (-p)P = (-p + p + 1)P = P$, also $P \in E(\mathbf{F}_{p^2})$. D.h.
$$E[p+1] \subseteq E(\mathbf{F}_{p^2}).$$
Da beide Mengen gleichmächtig sind, folgt die Behauptung. ■

Bemerkung: Allgemein kann man zeigen: Ist E über $\mathbf{F}_q$ supersingulär und $P \in E(\mathbf{F}_q)$ mit $ord(P) = m$, so gibt es ein $k \leq 6$ mit $E[m] \subseteq E(\mathbf{F}_{q^k})$. Der Reduktionsprozeß macht also aus einem Logarithmenproblem in $E(\mathbf{F}_q)$ ein Logarithmenproblem in $\mathbf{F}_{q^k}^*$ mit einem $k \leq 6$. Die Reduktion kann hier durchaus sinnvoll sein.

Mit dem folgenden Lemma, das wir später beweisen werden, erhält man leicht Beispiele für supersinguläre elliptische Kurven:

LEMMA. *Ist p eine Primzahl mit $p \equiv 3 \bmod 4$, so ist für alle $a \in \mathbf{F}_p^*$ die Kurve $y^2 = x^3 + ax$ supersingulär (über $\mathbf{F}_p$).*

Wir geben jetzt Beispiele für den Reduktionsprozeß.

Beispiel: Sei $p = 1063$ und E mit der Gleichung $y^2 = x^3 + 342x + 1$. Wegen $\#E(\mathbf{F}_p) = 1064 = 2^3 \cdot 7 \cdot 19$ ist E supersingulär. Durch Probieren findet man folgende Punkte der Ordnung 7

$$P = (129, 616) = 152 \cdot (12, 287), \quad Q = (236, 959) = 152 \cdot (2, 256).$$

Wir schreiben $\mathbf{F}_{p^2} = \mathbf{F}_p(w)$ mit $w^2 = 3$. Durch Probieren findet man den Punkt $(1, 115w) \in E(\mathbf{F}_{p^2})$. Dann hat auch

$$P' = (950, 324w) = 152 \cdot (1, 115w)$$

die Ordnung 7. Wir benutzen unsere Formeln und die Punkte $S = (0, 1)$, $T = (2, 256)$ und erhalten

$$e_7(P, Q) = 1, \quad e_7(P, P') = 255 + 985w, \quad e_7(Q, P') = 363 + 614w,$$

(7-te Einheitswurzeln). Nun ist

$$363 + 614w = (255 + 985w)^2 \quad \text{und damit} \quad 2P = Q.$$

Beispiel: Wir betrachten die elliptische Kurve E mit der Gleichung $y^2 = x^3 + x$ über $\mathbf{F}_p$ mit $p = 10^{10} + 1251$. Es gilt $\#E(\mathbf{F}_p) = p + 1$, da E supersingulär ist. Außerdem ist $p + 1 = 4q$ mit einer Primzahl q. Wir wählen $m = p + 1$. Einige Punkte auf E:

P	Punkt	$ord(P)$
P_0	$(0, 0)$	2
P_3	$(3, 5394836499)$	m
P_5	$(5, 4773453646)$	$\frac{m}{2}$
P_6	$(6, 9298634306)$	$\frac{m}{2}$
P_7	$(7, 7398289296)$	m

Unser eigentlicher Wunsch ist es, den Logarithmus von P_7 zur Basis P_3 auszurechnen. Für die Berechnung der Weil-Paarungen benutzen wir jeweils $S = P_0$ und $T = P_5$. Natürlich gilt $e_m(P_3, P_7) = 1$. Um das Logarithmenreduktionsverfahren anzuwenden, müssen wir den Grundkörper erweitern. Wir wählen $\mathbf{F}_{p^2} = \mathbf{F}_p(w)$ mit $w^2 = 2$. Man findet wieder schnell ein paar Punkte:

P_1	$(1, w)$	m
P_2	$(2, 8888606940w)$	$\frac{m}{2}$
P_4	$(4, 8388997221w)$	m

Wir suchen einen Punkt $P' \in E(\mathbf{F}_{p^2}) \setminus E(\mathbf{F}_p)$, so daß $e_m(P_3, P')$ Ordnung m hat. Wir probieren P_1 und P_4, die aber beide nicht funktionieren. Warum?

- $e_m(P_3, P_1) = -1$. Warum? Schreibt man $P_1 = xP_3 + yP'$, so daß $e_m(P_3, P')$ eine primitive m-te Einheitswurzel ist, so ist
$$-1 = e_m(P_3, P_1) = e_m(P_3, P')^y,$$
also ist $y = \frac{m}{2}$, d.h. yP' ist ein 2-Teilungspunkt. Die 2-Teilungspunkte sind O, P_0 und
$$P_a = (491599629w, 0) \quad \text{und} \quad P_b = (9508401622w, 0)$$
und tatsächlich ist
$$P_1 + P_a = (-1, 983199258) \quad \text{und} \quad P_1 + P_b = (-1, 9016801993).$$

- $e_m(P_3, P_4)$ hat Ordnung $\frac{m}{2}$, d.h. P_4 kann nicht als Punkt P' genommen werden. Auch bei anderen Punkten der Gestalt (a, bw) mit $a, b \in \mathbf{F}_p$ passiert Ähnliches. Weshalb? $\frac{m}{2}P_4$ ist ein 2-Teilungspunkt und wegen
$$\sigma(\frac{m}{2}P_4) = \frac{m}{2}(-P_4) = -\frac{m}{2}P_4 = \frac{m}{2}P_4$$
(mit $\sigma w = -w$) ist $\frac{m}{2}P_4 \in E(\mathbf{F}_p)$, also $\frac{m}{2}P_4 = P_0$. Damit folgt jetzt
$$1 = e_2(P_0, P_0) = e_2(\frac{m}{2}P_3, \frac{m}{2}P_4) = e_{2\cdot\frac{m}{2}}(P_3, \frac{m}{2}P_4) = e_m(P_3, P_4)^{\frac{m}{2}}.$$

Als nächsten Punkt probieren wir:
$$P_s = (1 + w, 3330076431 + 6628225183w) \quad \text{mit} \quad ord(P) = m.$$
Nun ist tatsächlich
$$e_m(P_3, P_s) = 2110109965 + 695098701w$$
eine primitive m-te Einheitswurzel. Wegen
$$e_m(P_7, P_s) = 6919527600 + 2773843306w$$
gilt also für $x \in \mathbf{N}$
$$P_7 = xP_3 \quad \Longleftrightarrow \quad 6919527600 + 2773843306w = (2110109965 + 695098701w)^x.$$
Man muß jetzt also Logarithmen in $\mathbf{F}_{p^2}$ berechnen, was wir nicht tun werden.

Mit dem folgenden Maple-Programm *weil* wurde das letzte Beispiel berechnet:

```
# Weil-Paarung auf der elliptischen Kurve y^2=x^3+a*x+b ueber F_p
#
# Eingabe von a,b,p

# Beispiel
p:=10^10+1251; a:=1; b:=0;
alias(w=RootOf(X^2-2,X) mod p);
P0:=[1,0,0];
P1:=[1,1,w];
P2:=[1,2,8888606940*w];
P3:=[1,3,5394836499];
P4:=[1,4,8388997221*w];
Ps:=[1,1+w,6628225183*w+3330076431];

# Additionstheoreme
Z1:=proc(Px,Py)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
za0 := a*x0^2*y0*y1-a*x0*x1*y0^2-x0^2*y2^2+x2^2*y0^2+3*x0*x1*y1^2
-3*x1^2*y0*y1;
za1 := -3*b*x0^2*y0*y1+3*b*x0*x1*y0^2-a*x0^2*y1^2+a*x1^2*y0^2
-x0*x1*y2^2+x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
za2 := 3*b*x0^2*y0*y2-3*b*x0*x2*y0^2+a*x0^2*y1*y2-a*x1*x2*y0^2
+2*a*x0*x1*y0*y2-2*a*x0*x2*y0*y1-x0*x2*y2^2+x2^2*y0*y2+3*x1^2*y1*y2
-3*x1*x2*y1^2;
[Normal(za0) mod p,Normal(za1) mod p,Normal(za2) mod p];
end;

Z2:=proc(Px,Py)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
zb0 := 3*b*x0^2*y0*y1-3*b*x0*x1*y0^2+a*x0^2*y1^2-a*x1^2*y0^2+x0*x1*y2^2
-x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
```

```
zb1 := a^2*x0^2*y0*y1-a^2*x0*x1*y0^2-3*b*x0^2*y1^2+3*b*x1^2*y0^2
-a*x0*x1*y1^2+a*x1^2*y0*y1+x1^2*y2^2-x2^2*y1^2;
zb2 := -a^2*x0^2*y0*y2+a^2*x0*x2*y0^2+3*b*x0^2*y1*y2-3*b*x1*x2*y0^2
+6*b*x0*x1*y0*y2-6*b*x0*x2*y0*y1+2*a*x0*x1*y1*y2-2*a*x1*x2*y0*y1
-a*x0*x2*y1^2+a*x1^2*y0*y2+x1*x2*y2^2-x2^2*y1*y2;
[Normal(zb0) mod p,Normal(zb1) mod p,Normal(zb2) mod p];
end;

Z3:=proc(Px,Py)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
zc0 := 6*b*x0*x2*y0^2+6*b*x0^2*y0*y2+2*a*x1*x2*y0^2+2*a*x0^2*y1*y2
+4*a*x0*x2*y0*y1+4*a*x0*x1*y0*y2+2*x2^2*y0*y2+2*x0*x2*y2^2+6*x1*x2*y1^2
+6*x1^2*y1*y2;
zc1 := 2*a^2*x0*x2*y0^2+2*a^2*x0^2*y0*y2-6*b*x1*x2*y0^2-6*b*x0^2*y1*y2
-12*b*x0*x2*y0*y1-12*b*x0*x1*y0*y2-4*a*x1*x2*y0*y1-4*a*x0*x1*y1*y2
-2*a*x1^2*y0*y2-2*a*x0*x2*y1^2+2*x2^2*y1*y2+2*x1*x2*y2^2;
zc2 := -2*x0^2*y0^2*a^3-18*x0^2*y0^2*b^2-6*a*b*x0*x1*y0^2
-6*a*b*x0^2*y0*y1-2*a^2*x1^2*y0^2-2*a^2*x0^2*y1^2-8*a^2*x0*x1*y0*y1
+18*b*x1^2*y0*y1+18*b*x0*x1*y1^2+6*a*x1^2*y1^2+2*x2^2*y2^2;
[Normal(zc0) mod p,Normal(zc1) mod p,Normal(zc2) mod p];
end;

Z:=proc(Px,Py)
ZD:=Z1(Px,Py);
if ZD=[0,0,0] then ZD:=Z3(Px,Py);
  if ZD=[0,0,0] then ZD:=Z2(Px,Py); fi;
fi;
ZD;
end;

M:=proc(k,P)
P1:=P;k1:=k;Q1:=[0,0,1];
while k1<>0 do
   if k1 mod 2=1 then Q1:=Z(Q1,P1); fi;
   k1:=trunc(k1/2);
   P1:=Z3(P1,P1);
od;
Q1;
end;

# Normalform eines Punktes
NF:=proc(Q)
if Q[1]=0 then QQ:=[0,Q[2],1]; fi;
if Q[1]<>0 then QQ:=[1,Normal(Q[2]/Q[1]) mod p,Normal(Q[3]/Q[1]) mod p]; fi;
QQ;
end;

# ausgewertete Geradengleichung
ell:=proc(P,Q,R)
if Normal(P[1]*Q[2]-P[2]*Q[1]) mod p=0 and
   Normal(P[1]*Q[3]-P[3]*Q[1]) mod p=0 and
   Normal(P[2]*Q[3]-P[3]*Q[2]) mod p=0
   then LL:=(2*R[1]*a*P[1]*P[2]+3*R[1]*b*P[1]^2-R[1]*P[3]^2
```

```
            +3*R[2]*P[2]^2+R[2]*a*P[1]^2-2*P[1]*P[3]*R[3]);
   else LL:=(P[1]*Q[2]*R[3]-P[1]*Q[3]*R[2]-Q[1]*P[2]*R[3]
            +Q[1]*P[3]*R[2]+R[1]*P[2]*Q[3]-R[1]*P[3]*Q[2]);
fi;
if LL=0 then ERROR('Geradenauswertung',P,Q,R); fi;
Normal(LL) mod p;
end;

V:=proc(D1,D2)
P1:=D1[1]; P2:=D2[1]; f1:=D1[2]; f2:=D2[2]; R:=D1[3];
if D1[3]<>D2[3] then ERROR('Divisoren',D1,D2); fi;
P:=Z(P1,P2);
f:=Normal(f1*f2*ell(P1,P2,R)/ell(P,[0,0,1],R)) mod p;
[P,f,R];
end;

unprotect(W);

W:=proc(d,P,R)
y:=[[0,0,1],1,R]; dd:=d; z:=[P,1,R];
while dd>0 do
   if dd mod 2=1 then y:=V(y,z); fi;
   dd:=trunc(dd/2);
   z:=V(z,z);
od;
y[2];
end;

e:=proc(m,P,Q,S,T)
fAQT:=Normal(W(m,Z(P,S),Z(Q,T))/W(m,S,Z(Q,T))) mod p;
fAT:=Normal(W(m,Z(P,S),T)/W(m,S,T)) mod p;
fBPS:=Normal(W(m,Z(Q,T),Z(P,S))/W(m,T,Z(P,S))) mod p;
fBS:=Normal(W(m,Z(Q,T),S)/W(m,T,S)) mod p;
Normal(fAQT*fBS/fAT/fBPS) mod p;
end;
```

Verwendete Literatur: [**13**], [**6**], [**7**].

KAPITEL 12

Elliptische Kurven über $\mathbf{F}_p$ mit p Punkten

Sei E eine über $\mathbf{F}_p$ definierte elliptische Kurve, so daß $E(\mathbf{F}_p)$ eine Untergruppe der Ordnung p enthält. Für $p \geq 7$ folgt dann $\#E(\mathbf{F}_p) = p$. Wie kann man Logarithmen in $E(\mathbf{F}_p)$ berechnen? Die Weil-Paarung ist für diesen Fall nicht definiert. Sind also solche Kurven kryptographisch geeignet?

Beispiele: In der folgenden Tabelle sind Beispiele für elliptische Kurven $y^2 = x^3 + ax + b$ angegeben, die über $\mathbf{F}_p$ definiert sind und p rationale Punkte haben.

p	a	b
5	3	2
7	0	5
11	1	5
19	0	10
101	1	32
1009	1	79
10007	777	1

Das folgende Lemma gibt eine Möglichkeit, auch für große Primzahlen p elliptische Kurven mit p rationalen Punkten zu konstruieren. (Der Beweis folgt in einem späteren Kapitel.)

LEMMA. *Sei $p \geq 5$ eine Primzahl mit $p = 3m^2 - 3m + 1$, $m \geq 2$ und $E_b : y^2 = x^3 + b$ mit $b \in \mathbf{F}_p^*$. Dann gilt*

$$\#E_b(\mathbf{F}_p) \in \{p - 3m + 2, p - 3m + 3, p, p + 2, p + 3m - 1, p + 3m\} = A.$$

Außerdem gibt es zu jedem $N \in A$ eine elliptische Kurve E_b mit $N = \#E_b(\mathbf{F}_p)$.

Wie kann man dann b finden? Man wähle $b = 1, 2, 3, \ldots$, bestimme einen Punkt $P \in E_b(\mathbf{F}_p) \setminus \{O\}$ und berechne pP. Ist $pP = O$, so hat man eine gewünschte Kurve, ist $pP \neq O$, so wähle man ein anderes b.

Beispiel: Das kleinste Beispiel mit $p = 3n^2 - 3n + 1$ und $p \geq 10^{50}$:

$$n = 577350269189625764509149 7, \quad p = 100000000000000000000000301202957353700719569828537.$$

Durch Probieren findet man, daß für $E : y^2 = x^3 + 41$ und $P = (2, 7) \in E(\mathbf{F}_p)$ gilt $pP = O$. Also ist $\#E(\mathbf{F}_p) = p$.

Sei nun E eine elliptische Kurve über $\mathbf{F}_p$ mit $\#E(\mathbf{F}_p) = p$. Nach Semaev gibt es einen Isomorphismus von Gruppen

$$\lambda : E(\mathbf{F}_p) \to \mathbf{F}_p,$$

der sich schnell berechnen läßt. Damit läßt sich die Berechnung von Logarithmen in $E(\mathbf{F}_p)$ auf die Berechnung von Logarithmen in $\mathbf{F}_p$ zurückführen. In $\mathbf{F}_p$ ist aber Logarithmenberechnung nichts anderes als Division, was trivial ist.

Wir erinnern zunächst an einige Tatsachen, wobei E eine beliebige elliptische Kurve über einem Körper K sein kann: Der Raum der Differentialformen Ω_E ist ein 1-dimensionaler $\overline{K}(E)$-Vektorraum. Ist $R \in E$ ein Punkt und t in R uniformisierend, so läßt sich jedes $\omega \in \Omega_E$ schreiben als $\omega = g dt$ mit $g \in \overline{K}(E)$. Man schreibt auch $g = \frac{\omega}{dt}$. Ist g definiert in P, so heißt ω ganz oder holomorph in P. In diesem Fall kann man einsetzen: $g(R) = \frac{\omega}{dt}(R) \in \overline{K}$.

SATZ. *Sei E eine elliptische Kurve mit der Gleichung $y^2 = x^3 + ax + b$ über $\mathbf{F}_p$, so daß gilt $\#E(\mathbf{F}_p) = p$. Sei weiter $R \in E(\mathbf{F}_p)$ und t uniformisierend in R. Dann gilt:*

$$\lambda : E(\mathbf{F}_p) \to \mathbf{F}_p, \quad P \mapsto \frac{dL_{p,P}}{L_{p,P}dt}(R)$$

ist ein Gruppenisomorphismus. (Dabei ist $L_{p,P}$ eine Funktion mit $(L_{p,P}) = p(P) - p(O)$.)

Beweis: Wir müssen zunächst zeigen, daß λ wohldefiniert ist. Anschließend zeigen wir die Eigenschaften von λ. Da p fest ist, schreiben wir L_P statt $L_{p,P}$.

1. L_P ist durch $p(P) - p(O) = (L_P)$ natürlich nur bis auf eine Konstante festgelegt. Dies spielt aber wegen $\frac{d(cL_P)}{cL_P} = \frac{dL_P}{L_P}$ keine Rolle.
2. Es ist $v_P(L_P) \equiv 0 \bmod p$, also können wir schreiben $L_P = t^{pm}u$ mit $m \in \mathbf{Z}$ und einer Einheit u (in R). Nun ist
$$\frac{dL_P}{L_P} = \frac{d(t^{pm}u)}{t^{pm}u} = \frac{t^{pm}du}{t^{pm}u} = \frac{du}{u},$$
da sich p-Potenzen beim Ableiten wie Konstanten verhalten. Schreibt man $du = gdt$, so wissen wir, daß auch g in R definiert ist. Also ist $\frac{dL_P}{L_P} = \frac{g}{u}dt$ ganz in R und damit
$$\frac{dL_P}{L_P dt}(R) = \frac{g}{u}(R)$$
wohldefiniert. Da alle auftretenden Größen über $\mathbf{F}_p$ definiert sind, ist $\frac{dL_P}{L_P dt}(R) \in \mathbf{F}_p$.
3. Da bei der letzten Betrachtung $R \in E$ beliebig war, folgt sofort, daß $\frac{dL_P}{L_P}$ eine holomorphe Differentialform ist.
4. Sind $P, Q \in E(\mathbf{F}_p) = E[p]$, so gilt
$$[(P) - (O)] + [(Q) - (O)] = (P + Q) - (O) + \operatorname{div}(\frac{\ell(P,Q)}{\ell(P+Q,O)})$$
nach einer früheren Formel, wo $\ell(P,Q)$ die Gleichung einer Geraden durch P und Q bzw. die Tangente ist. Multiplikation mit p liefert
$$\operatorname{div}(L_P) + \operatorname{div}(L_Q) = \operatorname{div}(L_{P+Q}) + \operatorname{div}(\frac{\ell(P,Q)^p}{\ell(P+Q,O)^p})$$
und damit o.E.
$$L_P L_Q = L_{P+Q}(\frac{\ell(P,Q)}{\ell(P+Q,O)})^p.$$
Logarithmisches Ableiten ergibt
$$\frac{dL_P}{L_P} + \frac{dL_Q}{L_Q} = \frac{dL_{P+Q}}{L_{P+Q}}$$
und damit die Additivität
$$\lambda(P + Q) = \lambda(P) + \lambda(Q).$$
Natürlich gilt auch $\lambda(O) = 0$.
5. Es bleibt nur noch die Injektivität zu zeigen. Sei also $\frac{dL_P}{L_P dt}(R) = 0$. Bei elliptischen Kurven haben aber holomorphe Differentiale keine Nullstellen (wegen $\deg((\omega)) = 0$), also ist $dL_P = 0$. Dann ist aber L_P eine p-Potenz: $L_P = cf^p$ mit einer Funktion f und einer Konstanten c. Aus
$$p(P) - p(O) = \operatorname{div}(L_P) = \operatorname{div}(f^p) = p\operatorname{div}(f)$$
folgt jetzt $(P) - (O) = \operatorname{div}(f)$. Dies ist aber bei einer elliptischen Kurve nur für $P = O$ möglich. Dies zeigt die Injektivität und damit die Behauptung. ■

Beispiel: Wir betrachten E über $\mathbf{F}_7$ mit der Gleichung $y^2 = x^3 + 5$. Die Gruppe $E(\mathbf{F}_7)$ hat 7 Elemente. Es ist $P = (3, 2) \in E(\mathbf{F}_7)$. Mit dem bei der Weil-Paarung erläuterten Algorithmus erhält man $7(P) - 7(P) = (L_P)$ mit
$$L_P = \frac{(5 + 5x + 5x^2 + 2x^3 + 6x^5 + 2x^6 + 6x^7) + (5 + 4x + 6x^2 + 6x^3 + 6x^4 + 2x^5 + 2x^6)y}{1 + 6x + 4x^2 + x^4}.$$

Wir betrachten L_P im Punkt $R = (5, 2)$. In R ist $t = x - 5$ ein lokaler Parameter. Für die Funktionen x und y hat man dann

$$x = 5 + t, \quad y = 2 + 3t + 5t^2 + 5t^3 + 2t^4 \bmod t^5,$$

woraus für L_P folgt

$$L_P = 5 + 5t + 4t^2 + 4t^3 \bmod t^4$$

und damit

$$\frac{dL_P}{L_P} = (1 + 2t + t^2 + \dots)dt.$$

Man erhält also $\frac{1}{L_P}\frac{dL_P}{dt}(R) = 1$.

Für die Praxis ist es natürlich nicht sinnvoll, zunächst die Funktionen $L_{p,P}$ zu berechnen um $\frac{dL_{p,P}}{L_{p,P}dt}(R)$ zu erhalten. Wir skizzieren eine andere Möglichkeit. Mit dem im letzten Kapitel vorgestellten Algorithmus erhält man $L_{p,P}$ in der Gestalt

$$L_{p,P} = \frac{\ell_{a1}\ell_{a2}\dots\ell_{ar}}{\ell_{b1}\ell_{b2}\dots\ell_{br}},$$

wo die ℓ_i's Geradengleichungen liefern. Logarithmisches Ableiten ergibt

$$\frac{dL_{p,P}}{L_{p,P}} = \frac{d\ell_{a1}}{\ell_{a1}} + \frac{d\ell_{a2}}{\ell_{a2}} + \dots + \frac{d\ell_{ar}}{\ell_{ar}} - \frac{d\ell_{b1}}{\ell_{b1}} - \frac{d\ell_{b2}}{\ell_{b2}} - \dots - \frac{d\ell_{br}}{\ell_{br}}.$$

Jetzt gilt folgendes Lemma:

LEMMA. *Sei E eine elliptische Kurve mit der Gleichung $y^2 = x^3 + ax + b$ und $R = (r, s) \in E$ mit $s \neq 0$. Dann ist $t = x - r$ uniformisierend in R. Sei $\ell = A + Bx + Cy$. Gilt $\ell(R) \neq 0$, so ist*

$$\frac{d\ell}{\ell dt}(R) = \frac{B + C\frac{3r^2+a}{2s}}{A + Br + Cs}.$$

Beweis: Wir rechnen in $\overline{K}(E)$ und Ω_E. Aus $y^2 = x^3 + ax + b$ folgt $2ydy = (3x^2 + a)dx$ und damit

$$dy = \frac{3x^2 + a}{2y}dx.$$

Nun ist wegen $dx = dt$

$$d\ell = Bdx + Cdy = (B + C\frac{3x^2 + a}{2y})dt$$

und somit

$$\frac{d\ell}{\ell dt} = \frac{B + C\frac{3x^2+a}{2y}}{A + Bx + Cy}.$$

Da die Funktionen y und $A + Bx + Cy$ Einheiten in R sind, erhält man durch Einsetzen sofort die Behauptung. ■

Wir definieren jetzt zu $R \in E$ mit Ortsuniformisierender t eine Zuordnung $D \mapsto \beta(D)$ für die 'meisten' Divisoren D vom Grad 0: Jeder Divisor D vom Grad 0 läßt sich schreiben als $D = (P) - (O) + \mathrm{div}(f)$, wobei P eindeutig, f bis auf eine Konstante eindeutig bestimmt ist. Setze

$$\beta(D) = (P, \frac{df}{fdt}(R)).$$

$\beta(D)$ ist nicht definiert, wenn f eine Pol- oder Nullstelle in R hat. Ist $D_i = (P_i) - (O) + \mathrm{div}(f_i)$, so ist

$$D_1 + D_2 = (P_1 + P_2) + \mathrm{div}(f_1 f_2 \frac{\ell(P_1, P_2)}{\ell(P_1 + P_2, O)})$$

und somit

$$\beta(D_1 + D_2) = (P_1 + P_2, \frac{df_1}{f_1 dt}(R) + \frac{df_2}{f_2 dt}(R) + \frac{d\ell(P_1, P_2)}{\ell(P_1, P_2)dt}(R) - \frac{d\ell(P_1 + P_2, O)}{\ell(P_1 + P_2, O)dt}(R)).$$

Man kann also $\beta(D_1+D_2)$ einfach aus $\beta(D_1)$ und $\beta(D_2)$ berechnen, wenn ℓ nicht auf einer der auftretenden Geraden liegt. Mit dem square-and-multiply-Verfahren kann man damit

$$\beta(p(P)-p(O)) = (O, \frac{dL_{p,P}}{L_{p,P}dt}(R)) = (O, \lambda(P))$$

mit $O(\log p)$ Schritten berechnen.

Das nachfolgende Maple-Programm *semaev* funktioniert auf diese Weise:

```
# Programm Semaev zur Berechnung von lambda:E(F_p)->F_p im Fall
# #E(F_p)=p
#
# Eingabe von a,b,p

# Beispiel
p:=10000000000000000000000030120295735370071956982853 7; a:=0; b:=41;
P2 :=[1, 2 , 7 ];
P3 :=[1, 3 , 14170827109783283898659709835881829432757361581090 ];
P12 :=[1, 12 , 689466899262715825551900331381880415993407669131 ];
P1000 :=[1, 1000 , 615989375811297385372583801200754529729521933903 28 ];

# Additionstheoreme
Z1:=proc(Px,Py)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
za0 := a*x0^2*y0*y1-a*x0*x1*y0^2-x0^2*y2^2+x2^2*y0^2+3*x0*x1*y1^2
-3*x1^2*y0*y1;
za1 := -3*b*x0^2*y0*y1+3*b*x0*x1*y0^2-a*x0^2*y1^2+a*x1^2*y0^2
-x0*x1*y2^2+x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
za2 := 3*b*x0^2*y0*y2-3*b*x0*x2*y0^2+a*x0^2*y1*y2-a*x1*x2*y0^2
+2*a*x0*x1*y0*y2-2*a*x0*x2*y0*y1-x0*x2*y2^2+x2^2*y0*y2+3*x1^2*y1*y2
-3*x1*x2*y1^2;
[za0 mod p,za1 mod p,za2 mod p];
end;

Z2:=proc(Px,Py)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
zb0 := 3*b*x0^2*y0*y1-3*b*x0*x1*y0^2+a*x0^2*y1^2-a*x1^2*y0^2+x0*x1*y2^2
-x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
zb1 := a^2*x0^2*y0*y1-a^2*x0*x1*y0^2-3*b*x0^2*y1^2+3*b*x1^2*y0^2
-a*x0*x1*y1^2+a*x1^2*y0*y1+x1^2*y2^2-x2^2*y1^2;
zb2 := -a^2*x0^2*y0*y2+a^2*x0*x2*y0^2+3*b*x0^2*y1*y2-3*b*x1*x2*y0^2
+6*b*x0*x1*y0*y2-6*b*x0*x2*y0*y1+2*a*x0*x1*y1*y2-2*a*x1*x2*y0*y1
-a*x0*x2*y1^2+a*x1^2*y0*y2+x1*x2*y2^2-x2^2*y1*y2;
[zb0 mod p,zb1 mod p,zb2 mod p];
end;

Z3:=proc(Px,Py)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
zc0 := 6*b*x0*x2*y0^2+6*b*x0^2*y0*y2+2*a*x1*x2*y0^2+2*a*x0^2*y1*y2
+4*a*x0*x2*y0*y1+4*a*x0*x1*y0*y2+2*x2^2*y0*y2+2*x0*x2*y2^2+6*x1*x2*y1^2
+6*x1^2*y1*y2;
zc1 := 2*a^2*x0*x2*y0^2+2*a^2*x0^2*y0*y2-6*b*x1*x2*y0^2-6*b*x0^2*y1*y2
-12*b*x0*x2*y0*y1-12*b*x0*x1*y0*y2-4*a*x1*x2*y0*y1-4*a*x0*x1*y1*y2
```

```
-2*a*x1^2*y0*y2-2*a*x0*x2*y1^2+2*x2^2*y1*y2+2*x1*x2*y2^2;
zc2 := -2*x0^2*y0^2*a^3-18*x0^2*y0^2*b^2-6*a*b*x0*x1*y0^2
-6*a*b*x0^2*y0*y1-2*a^2*x1^2*y0^2-2*a^2*x0^2*y1^2-8*a^2*x0*x1*y0*y1
+18*b*x1^2*y0*y1+18*b*x0*x1*y1^2+6*a*x1^2*y1^2+2*x2^2*y2^2;
[zc0 mod p,zc1 mod p,zc2 mod p];
end;

Z:=proc(Px,Py)
ZD:=Z1(Px,Py);
if ZD=[0,0,0] then ZD:=Z3(Px,Py);
  if ZD=[0,0,0] then ZD:=Z2(Px,Py); fi;
fi;
ZD;
end;

M:=proc(k,P)
P1:=P;k1:=k;Q1:=[0,0,1];
while k1<>0 do
   if k1 mod 2=1 then Q1:=Z(Q1,P1); fi;
   k1:=trunc(k1/2);
   P1:=Z3(P1,P1);
od;
Q1;
end;

# Normalform eines Punktes
NF:=proc(Q)
if Q[1]=0 then QQ:=[0,Q[2],1]; fi;
if Q[1]<>0 then QQ:=[1,(Q[2]/Q[1]) mod p,Q[3]/Q[1] mod p]; fi;
QQ;
end;

# Koeffizienten der Geradengleichung durch P und Q
ellc:=proc(P,Q)
if (P[1]*Q[2]-P[2]*Q[1]) mod p=0 and
   (P[1]*Q[3]-P[3]*Q[1]) mod p=0 and
   (P[2]*Q[3]-P[3]*Q[2]) mod p=0
   then LL:=[P[3]^2-2*a*P[1]*P[2]-3*b*P[1]^2,-3*P[2]^2-a*P[1]^2,
            2*P[1]*P[3]];
   else LL:=[P[2]*Q[3]-P[3]*Q[2],-P[1]*Q[3]+Q[1]*P[3],
            P[1]*Q[2]-Q[1]*P[2]];
fi;
LL mod p;
end;

# Auswertung von dl/l in R
dll:=proc(P,Q,R)
if R[1]<>1 then ERROR('R[1]'); fi;
r:=R[2]; s:=R[3];
A:=ellc(P,Q)[1]; B:=ellc(P,Q)[2]; C:=ellc(P,Q)[3];
(B+C*(3*r^2+a)/(2*s))/(A+B*r+C*s) mod p;
end;
```

```
V:=proc(D1,D2)
P1:=D1[1]; P2:=D2[1]; df1:=D1[2]; df2:=D2[2]; R:=D1[3];
if D1[3]<>D2[3] then ERROR('Divisoren',D1,D2); fi;
P:=Z(P1,P2);
df:=(df1+df2+dll(P1,P2,R)-dll(Z(P1,P2),[0,0,1],R)) mod p;
[P,df,R];
end;

unprotect(W);

W:=proc(d,P,R)
y:=[[0,0,1],0,R]; dd:=d; z:=[P,0,R];
while dd>0 do
   if dd mod 2=1 then y:=V(y,z); fi;
   dd:=trunc(dd/2);
   z:=V(z,z);
od;
y[2];
end;

# Semaev-Funktion lambda(P) mit Basispunkt R
S:=proc(P,R)
W(p,P,R);
end;
```

Beispiel: Wir betrachten $p = 10^{10} + 510297$ und $E : y^2 = x^3 + 11$ über $\mathbf{F}_p$. Es ist $\#E(\mathbf{F}_p) = p$, also können wir das skizzierte Reduktionsverfahren benutzen. Wir nehmen

$$P = (1, 2207053721), \quad Q = (2, 2044983766) \quad \text{und} \quad R = (104, 3271333276).$$

Dann berechnet man mit dem oben angegebenen Programm

$$\lambda(P) = 8968829585 \quad \text{und} \quad \lambda(Q) = 3586566048.$$

Mit

$$x = \frac{\lambda(Q)}{\lambda(P)} = 786328117$$

gilt dann $xP = Q$, d.h. $x = \log_P Q$.

Um die Qualität des Verfahrens zu zeigen, nehmen wir noch ein größeres Beispiel:

Beispiel: Wir betrachten E mit der Gleichung $y^2 = x^3 + 41$ über $\mathbf{F}_p$ mit

$$p = 10000000000000000000000030120295735370071956982853 7.$$

(Es ist $p \geq 10^{50}$.) Wieder ist $\#E(\mathbf{F}_p) = p$. Wir wählen Punkte

$$\begin{aligned} P &= (2, 7), \\ Q_1 &= (3, 14170827109783283898659709835881829432757361581090), \\ R &= (12, 68946688992627158255519003313818804159934076691 31), \\ Q_2 &= (1000, 61598937581129738537258380120075452972952193390328). \end{aligned}$$

Wir berechnen

$$\begin{aligned} \lambda(P) &= 331147226845344346036049839432037168668178928219 6, \\ \lambda(Q_1) &= 106659645578242980192182524986453340273534391705 6, \\ \lambda(Q_2) &= 196307442800852114758405099868120561424103226437 58 \end{aligned}$$

und erhalten sofort

$$\begin{aligned}\log_P Q_1 &= \frac{\lambda(Q_1)}{\lambda(P)} = 359175687695712378713295052736447700502513477602 98,\\ \log_P Q_2 &= \frac{\lambda(Q_2)}{\lambda(P)} = 293581904578418220080342357175953179048716632828 13.\end{aligned}$$

Fazit: Die Berechnung von Logarithmen in $E(\mathbf{F}_p)$ mit $\#E(\mathbf{F}_p) = p$ ist leicht vermöge des oben skizzierten Verfahrens. Kryptographisch sind solche Kurven also absolut ungeeignet.

Verwendete Literatur: [**12**], [**9**]

KAPITEL 13

Wie bestimmt man $\#E(\mathbf{F}_p)$?

Wir wollen uns jetzt einigen Fragen zuwenden, die von zentraler Bedeutung bei der Verwendung elliptischer Kurven in der Kryptographie sind.

- Wie bestimmt man bei einer über $\mathbf{F}_p$ definierten elliptischen Kurve E mit einer Gleichung $y^2 = x^3 + ax + b$ die Anzahl $\#E(\mathbf{F}_p)$?
- Wie kann man sich Punkte auf einer vorgegebenen elliptischen Kurve verschaffen?
- Kann man zu einer Zahl N mit $p+1-2\sqrt{p} < N < p+1+2\sqrt{p}$ eine elliptische Kurve E über $\mathbf{F}_p$ konstruieren mit $\#E(\mathbf{F}_p) = N$?

1. Punkte auf elliptischen Kurven

Sei E eine elliptische Kurve über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$, wobei wir uns p als große Primzahl vorstellen können. Wie findet man dann Punkte in $E(\mathbf{F}_p)$?

Sei $x_0 \in \mathbf{F}_p$. Gibt es dann ein $y_0 \in \mathbf{F}_p$ mit $(x_0, y_0) \in E(\mathbf{F}_p)$? Diese Frage ist schnell mit Hilfe des Legendre-Symbols zu beantworten: Genau dann gibt es ein solches y_0, wenn für das Legendre-Symbol gilt:

$$(\frac{x_0^3 + ax_0 + b}{p}) \neq -1.$$

Wir erinnern an einige Eigenschaften des Legendre-Symbols:

- Das Legendre-Symbol $(\frac{m}{p})$ wird für eine ungerade Primzahl p und $m \in \mathbf{Z}$ definiert durch

$$(\frac{m}{p}) = \begin{cases} 0 & \text{falls } m \equiv 0 \bmod p, \\ 1 & \text{falls } m \text{ ein Quadrat modulo } p \text{ ist}, \\ -1 & \text{falls } m \text{ kein Quadrat modulo } p \text{ ist} \end{cases}$$

- Eine Verallgemeinerung des Legendre-Symbols ist das Jacobi-Symbol, das in gleicher Weise geschrieben wird, aber für $m, n \in \mathbf{Z}$, $n \geq 1$, $n \equiv 1 \bmod 2$ definiert ist durch

$$(\frac{m}{n}) = \prod_i (\frac{m}{p_i})^{e_i} \text{ mit der Primfaktorzerlegung } n = \prod_i p_i^{e_i},$$

  wo $(\frac{m}{p_i})$ das Legendre-Symbol ist. Natürlich gilt dann auch

$$(\frac{m}{n}) = (\frac{m \bmod n}{n}).$$

- Das Jacobi-Symbol ist multiplikativ:

$$(\frac{m_1 m_2}{n}) = (\frac{m_1}{n})(\frac{m_2}{n})$$

  und es gelten die Formeln

$$(\frac{-1}{n}) = \begin{cases} 1 & \text{für } n \equiv 1 \bmod 4, \\ -1 & \text{für } n \equiv 3 \bmod 4, \end{cases} \qquad (\frac{2}{n}) = \begin{cases} 1 & \text{für } n \equiv 1, 7 \bmod 8, \\ -1 & \text{für } n \equiv 3, 5 \bmod 8. \end{cases}$$

- Von fundamentaler Bedeutung ist das quadratische Reziprozitätsgesetz:

$$(\frac{m}{n}) = \begin{cases} (\frac{n}{m}) & \text{falls } m \equiv 1 \bmod 4 \text{ oder } n \equiv 1 \bmod 4, \\ -(\frac{n}{m}) & \text{falls } m \equiv n \equiv -1 \bmod 4. \end{cases}$$

- Mit den angegebenen Formeln ist es möglich, das Legendre-Symbol schnell zu berechnen.

Ist jetzt $(\frac{x_0^3+ax_0+b}{p}) = 0$, so ist $(x_0, 0) \in E(\mathbf{F}_p)$. Gilt $(\frac{x_0^3+ax_0+b}{p}) = 1$, so weiß man, daß ein $y_0 \in \mathbf{F}_p^*$ existiert mit $(x_0, y_0) \in E(\mathbf{F}_p)$, aber wie man ein y_0 findet, ist nicht klar. Natürlich kann man ausprobieren. Das aber braucht i.a. $O(p)$ Schritte, ist also für größere Primzahlen p unbrauchbar. Wir stellen jetzt einen Algorithmus vor, wie man schnell Quadratwurzeln modulo p berechnen kann. Wir beginnen mit einem Beispiel, das die Grundidee zeigt.

Beispiel: Wir wollen $x^2 \equiv -1 \bmod p$ für eine ungerade Primzahl p untersuchen. Das Legendre-Symbol zeigt, daß die Gleichung genau im Fall $p \equiv 1 \bmod 4$ lösbar ist. Sei also $p \equiv 1 \bmod 4$. Die zyklische Gruppe $\mathbf{F}_p^*$ hat Ordnung $p - 1 = 4m$, also liegen die 4-ten Einheitswurzeln alle in $\mathbf{F}_p$: $\pm 1, \pm i$, wo $i \in \mathbf{F}_p$ die Gleichung $i^2 + 1 = 0$ erfüllt. Wir suchen also i (oder $-i$). Nun ist

$$\alpha : \mathbf{F}_p^* \to \{1, -1, i, -i\}, \quad x \mapsto x^{\frac{p-1}{4}}$$

ein Gruppenhomomorphismus. Wählt man also zufällig $y \in \mathbf{F}_p^*$, so ist die Wahrscheinlichkeit, daß $\alpha(y) = \pm i$ ist $\frac{1}{2}$. Nach ein paar Versuchen wird man also eine Lösung der Gleichung $x^2 \equiv -1 \bmod p$ haben.

Algorithmus zur Berechnung von Quadratwurzeln modulo p: Sei $p \geq 3$ eine Primzahl und $a \in \mathbf{F}_p^*$, wo wir bereits wissen, daß $(\frac{a}{p}) = 1$ ist. Wir werden Folgen $b_i, x_i \in \mathbf{F}_p^*$ konstruieren, so daß $ab_i = x_i^2$ gilt und b_i gegen 1 'konvergiert'. Also erhalten wir schließlich ein x mit $a = x^2$.

1. Sei $p - 1 = 2^e q$ mit $q \equiv 1 \bmod 2$ und $e \geq 1$. Die 2-Sylowgruppe G von $\mathbf{F}_p^*$ ist dann zyklisch von der Ordnung 2^e. Ist $n \in \mathbf{F}_p^*$, so ist $n^q \in G$. Das Element n^q erzeugt genau dann G, wenn gilt $(\frac{n}{p}) = -1$. Dies ist leicht nachzuprüfen. Durch Probieren zufälliger n's erhält man so schnell einen Erzeuger z von G. Also $ord(z) = 2^e$, wo ord sich auf $\mathbf{F}_p^*$ bezieht.
2. Wir wollen Folgen $b_i, x_i \in \mathbf{F}_p^*$ konstruieren mit $ab_i = x_i^2$ und $b_i \in G$.
3. Wir wählen $b_0 = a^q \in G$. Dann ist $ab_0 = x_0^2$ mit $x_0 = a^{\frac{q+1}{2}}$.
4. Ist $b_i = 1$, so ist $x = x_i$ eine Lösung der Gleichung $x^2 = a$. Sonst ist $b_i \in G$ und ein Quadrat, also kann man schreiben
$$b_i = z^{2^{e_i} u_i} \text{ mit } u_i \equiv 1 \bmod 2 \text{ und } e_i \geq 1.$$
5. Wie bestimmt man e_i? Es ist
$$b_i^{2^{e-e_i}} \equiv 1, \text{ aber } b_i^{2^{e-e_i-1}} \not\equiv 1, \text{ also } b_i^{2^{e-e_i-1}} = -1,$$
da -1 das einzige Element der Ordnung 2 in G ist. Durch sukzessives Quadrieren bestimmen wir also ein d_i mit $b_i^{2^{d_i}} = -1$. Dann ist $d_i = e - e_i - 1$, also $e_i = e - 1 - d_i$.
6. Wir definieren nun
$$b_{i+1} = b_i z^{2^{e_i}} = z^{2^{e_i}(u_i+1)} = z^{2^{e_{i+1}} u_{i+1}} \text{ mit } 2^{e_i}(u_i + 1) = 2^{e_{i+1}} u_{i+1} \text{ und } e_{i+1} > e_i.$$
Dann ist
$$ab_{i+1} = x_i^2 (z^{2^{e_i-1}})^2 = (x_i z^{2^{e_i-1}})^2,$$
also können wir
$$x_{i+1} = x_i z^{2^{e_i-1}}$$
setzen.
7. So erhält man also Folgen $b_0, b_1, \ldots$ und $x_0, x_1, \ldots$. Wegen $e_{i+1} > e_i$ gilt schließlich $e_i \geq e$ und damit $b_i = 1$.

Das folgende Ubasic-Programm *sqrmp.ub* berechnet x mit $x^2 \equiv a \bmod p$ nach der eben skizzierten Idee.

```
10   input "p=";P
20   input "a=";A
30   Q=P-1:E=0
40   if Q@2=0 then Q=Q\2:E=E+1:goto 40
50   N=2
60   if kro(N,P)=1 then N=N+1:goto 60
70   Z=modpow(N,Q,P)
80   Y=Z:R=E:X=modpow(A,(Q-1)\2,P):B=(A*X*X)@P:X=(A*X)@P
90   if B@P=1 then print "x=";X:goto 20
100  M=1:Bb=(B*B)@P
```

```
110   if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 110
120   if M=R then print A;" ist kein quadratischer Rest modulo ";P:goto 20
130   T=modpow(Y,2^(R-M-1),P):Y=(T*T)@P:R=M:X=(X*T)@P:B=(B*Y)@P:goto 90
```

Das folgende Ubasic-Programm *punkte.ub* wendet den eben beschriebenen Quadratwurzelalgorithmus auf die Konstruktion von Punkten auf elliptischen Kurven an. Es läuft sehr schnell.

```
10    print "Fuer die elliptische Kurve y^2=x^3+ax+b ueber F_p wird"
20    print "zu vorgegebenem x0 der naechste x-Wert bestimmt, so"
30    print "dass (x,y) auf E liegt."
40    input "p,a,b=";P,A,B
50    Q=P-1:E=0
60    if Q@2=0 then Q=Q\2:E=E+1:goto 60
70    N=2
80    if kro(N,P)=1 then N=N+1:goto 80
90    Z=modpow(N,Q,P)
100   input "Startwert fuer x=";X
110   Ae=(X^3+A*X+B)@P
120   if Ae=0 then Y=0:print "x,y=";X;Y:goto 100
130   if kro(Ae,P)=-1 then X=X+1:goto 110
140   Ye=Z:R=E:Y=modpow(Ae,(Q-1)\2,P):Be=(Ae*Y*Y)@P:Y=(Ae*Y)@P
150   if Be@P=1 then print "x,y=";X;Y:goto 100
160   M=1:Bb=(Be*Be)@P
170   if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 170
180   T=modpow(Ye,2^(R-M-1),P):Ye=(T*T)@P:R=M:Y=(Y*T)@P:Be=(Be*Ye)@P:goto 150
```

Beispiel: Bei der Kurve $y^2 = x^3 + x + 3$ über $\mathbf{F}_p$ mit $p = 10^{500} + 961$ findet das Programm bei Vorgabe von x_0 den nächsten Punkt $(x, y) \in E(\mathbf{F}_p)$ in zwei Sekunden.

2. Elementare (naive) Bestimmung von $\#E(\mathbf{F}_p)$

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

$$\#E(\mathbf{F}_p) = 1 + \sum_{x \in \mathbf{F}_p} (1 + (\frac{x^3 + ax + b}{p})) = p + 1 + \sum_{x \in \mathbf{F}_p} (\frac{x^3 + ax + b}{p}).$$

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.

Ein entsprechendes Ubasic-Programm *anzahl.ub* sieht so aus:

```
10    print "Bestimmung der Anzahl der Punkte auf der elliptischen Kurve"
20    print "y^2=x^3+a*x+b ueber dem Koerper mit p Elementen"
30    input "p,a,b=";P,A,B:clr time
40    N=P+1
50    for X=0 to P-1:N=N+kro(X^3+A*X+B,P):next
```

```
60   print "p=";P,"a=";A,"b=";B,"N=";N,"Zeit=";time
70   goto 30
```

Beispiel: Wir betrachten die elliptische Kurve $y^2 = x^3 + x + 1$ über verschiedenen Körpern $\mathbf{F}_p$. Mit obigem Programm erhält man:

p	$\#E(\mathbf{F}_p)$	Rechenzeit
$10^3 + 9$	1034	0 Sekunden
$10^4 + 7$	10065	0 Sekunden
$10^5 + 3$	100181	3 Sekunden
$10^6 + 3$	1000727	42 Sekunden
$10^7 + 19$	9998581	7 Minuten, 48 Sekunden

Es ist klar, daß man auf diese Weise $\#E(\mathbf{F}_p)$ für größere p nicht berechnen kann.

3. Bestimmung von $\#E(\mathbf{F}_p)$ durch Studium von $ord(P)$

Gegeben sei eine elliptische Kurve E durch eine Gleichung $y^2 = x^3+ax+b$ über $\mathbf{F}_p$. Man kann versuchen, $\#E(\mathbf{F}_p)$ folgendermaßen zu erhalten:

- Wähle einen Punkt $P \in E(\mathbf{F}_p)$. Berechne
$$M = \{m \in \mathbf{N} : p+1-2\sqrt{p} < m < p+1+2\sqrt{p} \text{ und } mP = O\}.$$
Dazu braucht man $O(\sqrt{p})$ Schritte. (Man berechnet zunächst $(p+1-[2\sqrt{p}])P$ mit dem square-and-multiply-Verfahren und addiert dann jeweils P.)
- Jedenfalls gilt $\#E(\mathbf{F}_p) \in M$. Enthält M also nur ein Element, so ist dies die Gruppenordnung und man ist fertig.
- Ist $\#M \geq 2$ und sind $m_1 < m_2$ die beiden kleinsten Elemente von M, so gilt $ord(P) = m_2 - m_1$, denn
$$M = \{n \cdot ord(P) : n \in \mathbf{N} \text{ mit } p+1-2\sqrt{p} < n \cdot ord(P) < p+1+2\sqrt{p}\},$$
man kann also nach Bestimmung von m_2 aufhören, weil man keine neue Information mehr erhält. Man probiere nun sein Glück mit einem neuen Punkt P.

Ein entsprechendes Ubasic-Programm *ordnung.ub* sieht so aus:

```
10   print "Fuer die elliptische Kurve y^2=x^3+ax+b ueber F_p soll"
20   print "die Gruppenordnung bestimmt werden, indem die Ordnung"
30   print "von Punkten bestimmt wird. Dazu wird ein Punkt P bestimmt"
40   print "und getestet, welche Zahlen m des Intervalls [p+1-isqrt(4*p),p+1+isqrt(4*p)]"
50   print "mP=O erfuellen."
60   input "p,a,b=";P,A,B:clr time:X=-1
70   Q=P-1:E=0
80   if Q@2=0 then Q=Q\2:E=E+1:goto 80
90   N=2
100  if kro(N,P)=1 then N=N+1:goto 100
110  Z=modpow(N,Q,P)
120  X=X+1
130  Ae=(X^3+A*X+B)@P
140  if Ae=0 then Y=0:goto 210
150  if kro(Ae,P)=-1 then goto 120
160  Ye=Z:R=E:Y=modpow(Ae,(Q-1)\2,P):Be=(Ae*Y*Y)@P:Y=(Ae*Y)@P
170  if Be@P=1 then goto 210
180  M=1:Bb=(Be*Be)@P
190  if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 190
200  T=modpow(Ye,2^(R-M-1),P):Ye=(T*T)@P:R=M:Y=(Y*T)@P:Be=(Be*Ye)@P:goto 170
210  print "P=(";X;",";Y;")"
220  P0=1:P1=X:P2=Y
230  M=P+1-isqrt(4*P):Oo=0:Oz=0
```

```
240   N=M:U0=P0:U1=P1:U2=P2:gosub 480:Q0=V0:Q1=V1:Q2=V2
250   if Q0=0 and Q1=0 then Oz=1:Oo=M
260   for I=M+1 to P+1+isqrt(4*P)
270   X0=Q0:X1=Q1:X2=Q2:Y0=P0:Y1=P1:Y2=P2:gosub 300:Q0=Z0:Q1=Z1:Q2=Z2
280   if Q0=0 and Q1=0 then Oz=Oz+1:if Oz=1 then Oo=I else print "ord(P)=";I-Oo:cancel for:goto 120
290   next I:print "Gruppenordnung=";Oo:print "Zeit=";time:goto 60
300   ' Addition (x0:x1:x2)+(y0:y1:y2)=(z0:z1:z2)
310   Z0=(A*X0^2*Y0*Y1-A*X0*X1*Y0^2-X0^2*Y2^2+X2^2*Y0^2+3*X0*X1*Y1^2-3*X1^2*Y0*Y1)@P
320   Z1=(-3*B*X0^2*Y0*Y1+3*B*X0*X1*Y0^2-A*X0^2*Y1^2+A*X1^2*Y0^2-X0*X1*Y2^2+X2^2*Y0*Y1+2*X0*X2*Y1*
330   Z2=(3*B*X0^2*Y0*Y2-3*B*X0*X2*Y0^2+A*X0^2*Y1*Y2-A*X1*X2*Y0^2+2*A*X0*X1*Y0*Y2-2*A*X0*X2*Y0*Y1-
340   if Z0>0 or Z1>0 or Z2>0 then return
350   Z0=(6*B*X0*X2*Y0^2+6*B*X0^2*Y0*Y2+2*A*X1*X2*Y0^2+2*A*X0^2*Y1*Y2+4*A*X0*X2*Y0*Y1+4*A*X0*X1*Y0
360   Z1=(2*A^2*X0*X2*Y0^2+2*A^2*X0^2*Y0*Y2-6*B*X1*X2*Y0^2-6*B*X0^2*Y1*Y2-12*B*X0*X2*Y0*Y1-12*B*X0
370   Z2=(-2*X0^2*Y0^2*A^3-18*X0^2*Y0^2*B^2-6*A*B*X0*X1*Y0^2-6*A*B*X0^2*Y0*Y1-2*A^2*X1^2*Y0^2-2*A^
380   if Z0>0 or Z1>0 or Z2>0 then return
390   Z0=(3*B*X0^2*Y0*Y1-3*B*X0*X1*Y0^2+A*X0^2*Y1^2-A*X1^2*Y0^2+X0*X1*Y2^2-X2^2*Y0*Y1+2*X0*X2*Y1*Y
400   Z1=(A^2*X0^2*Y0*Y1-A^2*X0*X1*Y0^2-3*B*X0^2*Y1^2+3*B*X1^2*Y0^2-A*X0*X1*Y1^2+A*X1^2*Y0*Y1+X1^2
410   Z2=(-A^2*X0^2*Y0*Y2+A^2*X0*X2*Y0^2+3*B*X0^2*Y1*Y2-3*B*X1*X2*Y0^2+6*B*X0*X1*Y0*Y2-6*B*X0*X2*Y
420   return
430   ' Verdopplung eines Punktes 2(x0:x1:x2)=(z0:z1:z2)
440   Z0=(12*B*X0^3*X2+12*A*X1*X2*X0^2+4*X2^3*X0+12*X1^3*X2)@P
450   Z1=(4*A^2*X0^3*X2-36*B*X1*X2*X0^2-12*A*X1^2*X2*X0+4*X2^3*X1)@P
460   Z2=(-2*X0^4*A^3-18*X0^4*B^2-12*A*B*X0^3*X1-12*A^2*X1^2*X0^2+36*B*X1^3*X0+6*A*X1^4+2*X2^4)@P
470   return
480   ' Multiplikation n(u0:u1:u2)=(v0:v1:v2)
490   N1=N:V0=0:V1=0:V2=1
500   while N1>0
510   if N1@2=1 then X0=U0:X1=U1:X2=U2:Y0=V0:Y1=V1:Y2=V2:gosub 300:V0=Z0:V1=Z1:V2=Z2
520   N1=N1\2
530   X0=U0:X1=U1:X2=U2:gosub 430:U0=Z0:U1=Z1:U2=Z2
540   wend
550   return
```

Beispiele: Wir betrachten die Kurve $y^2 = x^3 + 5x + 7$ über verschiedenen Körpern $\mathbf{F}_p$. Interessanterweise funktioniert das Verfahren gleich beim ersten gewählten Punkt.

p	P	$\#E(\mathbf{F}_p) = ord(P)$	Rechenzeit
$10^8 + 7$	$(1, 64521804)$	99987600	15”
$10^8 + 37$	$(0, 57886846)$	99985860	14”
$10^9 + 7$	$(0, 978874217)$	999981750	45”
$10^9 + 9$	$(0, 121078727)$	1000012992	45”
$10^{10} + 19$	$(1, 6243000782)$	10000113575	3’9”
$10^{10} + 33$	$(0, 2002716843)$	10000067374	2’48”
$10^{11} + 3$	$(2, 99999999998)$	100000134900	10’16”
$10^{12} + 39$	$(0, 89541225401)$	1000001558752	29’52”
$10^{12} + 61$	$(1, 499693076180)$	1000000227912	32’8”

Bemerkungen:

1. Bei den behandelten Beispielen hat das vorgestellte Verfahren immer funktioniert.
2. Es gibt einen Satz von Mestre, der besagt, daß das Verfahren (mit einer kleinen Modifikation) für $p > 229$ immer funktioniert (siehe [**11a**]). Genauer: Ist $E : y^2 = x^3 + ax + b$ und u mit $(\frac{u}{p}) = -1$, so gilt für $E' : y^2 = x^3 + au^2x + bu^3$:

$$E \simeq_{\overline{\mathbf{F}}_p} E', \quad \text{aber} \quad E \not\simeq_{\mathbf{F}_p} E'.$$

Wir werden später die folgende Formel beweisen:

$$\#E(\mathbf{F}_p) + \#E'(\mathbf{F}_p) = 2(p+1),$$

kennt man also $\#E(\mathbf{F}_p)$, so auch $\#E'(\mathbf{F}_p)$ und umgekehrt. Der Satz von Mestre besagt nun: funktioniert das Verfahren für E nicht, dann funktioniert es für E'.

3. Für die Kurven $y^2 = x^3 + b$ funktioniert das Verfahren über $\mathbf{F}_{229}$ nicht.
4. Zur Bestimmung der Menge $M = \{m \in [p+1-2\sqrt{p}, p+1+2\sqrt{p}] : mP = O\}$ kann man auch das baby-step-giant-step-Verfahren verwenden. Dann hat man $O(\sqrt[4]{p})$ Schritte, braucht aber entsprechend viel Speicherplatz.

4. Elliptische Kurven, bei denen man Informationen über $\mathrm{End}(E)$ hat

Wir beginnen mit den Fällen $j(E) = 1728$ und $j(E) = 0$.

4.1. Elliptische Kurven mit $j = 1728$. Wir betrachten also $E : y^2 = x^3 + ax$ über $\mathbf{F}_p$ mit $p \geq 5$. Dann erfüllt der Automorphismus

$$\varphi : (x, y) \mapsto (-x, iy) \quad (\text{mit } i \in \mathbf{F}_p \text{ oder } i \in \mathbf{F}_{p^2} \text{ und } i^2 = -1)$$

die Gleichung $\varphi^2 = -1$ in $\mathrm{End}(E)$. Natürlich haben wir auch den Frobeniusautomorphismus $\pi : (x, y) \mapsto (x^p, y^p)$, der einer Gleichung $\pi^2 - s\pi + p = 0$ genügt (mit $s = Sp(\pi)$). Wir unterscheiden zwei Fälle:

Der Fall $p \equiv 3 \bmod 4$: Dann gilt mit $i^p = i^3 = -i$:

$$\pi\varphi(x, y) = \pi(-x, iy) = (-x^p, i^p y^p) = (-x^p, -iy^p) = -(-x^p, iy^p) = -\varphi(x^p, y^p) = -\varphi\pi(x, y),$$

also $\pi\varphi = -\varphi\pi$, d.h. $\mathrm{End}(E)$ ist nicht kommutativ, damit E supersingulär. Wir formulieren dies als Satz:

Satz. *Ist $p \geq 7$ eine Primzahl mit $p \equiv 3 \bmod 4$, so ist für $a \in \mathbf{F}_p^*$ die elliptische Kurve E mit der Gleichung $y^2 = x^3 + ax$ supersingulär und insbesondere*

$$\#E(\mathbf{F}_p) = p + 1.$$

Beispiele: Im folgenden geben wir einige Primzahlen p an, so daß $p + 1 = 4q$ mit einer Primzahl q gilt:

$$10^{10} + 1251, \quad 10^{20} + 12651, \quad 10^{30} + 651, \quad 10^{40} + 1107, \quad 10^{50} + 25803,$$

$$10^{60} + 90603, \quad 10^{70} + 130827, \quad 10^{80} + 32403.$$

$p+1$ ist dann jeweils die Anzahl der rationalen Punkte auf der supersingulären Kurve $y^2 = x^3 + ax$ über $\mathbf{F}_p$.

Der Fall $p \equiv 1 \bmod 4$: Wegen $i^p = i$ gilt in diesem Fall mit analoger Rechnung wie oben

$$\pi\varphi = \varphi\pi.$$

Damit ist $\mathbf{Q}(\varphi, \pi)$ ein kommutativer Teilkörper von $\mathrm{End}(E) \otimes \mathbf{Q}$, da es aber (in jedem Fall) nur quadratische gibt, folgt $\pi \in \mathbf{Z}[\varphi]$. Wäre E supersingulär, so würde π der Gleichung $\pi^2 + p = 0$ genügen, was aber für Elemente aus $\mathbf{Z}[\varphi]$ unmöglich ist. Also ist E nicht supersingulär und damit $\mathrm{End}(E) = \mathbf{Z}[\varphi]$. Mit dem Isomorphismus $\mathbf{Z}[\varphi] \simeq \mathbf{Z}[i]$ identifizieren wir jetzt

$$\mathrm{End}(E) = \mathbf{Z}[i] \quad (\text{wo } ((x, y) \mapsto (-x, iy)) \mapsto i).$$

(Man beachte, daß i hier in zwei Bedeutungen vorkommt.) Wir schreiben $\pi = u + iv$ mit $u, v \in \mathbf{Z}$. Zunächst gilt

$$p = \deg \pi = \pi\hat{\pi} = \pi\overline{\pi} = u^2 + v^2.$$

Wir werden gleich sehen, wie man $m, n \in \mathbf{Z}$ konstruieren kann mit $p = m^2 + n^2$. Dann gilt

$$p = \pi\overline{\pi} = (m + ni)(m - ni).$$

Nun ist $\mathbf{Z}[i]$ faktoriell, die Einheiten sind $\pm 1, \pm i$, also folgt

$$\pi \in \{m \pm ni, -m \pm ni, n \pm mi, -n \pm mi\}.$$

Somit erhalten wir

$$\#E(\mathbf{F}_p) = p + 1 - (\pi + \overline{\pi}) \in \{p + 1 - 2m, p + 1 + 2m, p + 1 - 2n, p + 1 + 2n\}.$$

SATZ. *Ist E die elliptische Kurve $y^2 = x^3 + ax$ über $\mathbf{F}_p$ mit $p \equiv 1 \bmod 4$, so ist* $\mathrm{End}(E) = \mathbf{Z}[i]$. *Schreibt man $p = m^2 + n^2$, so gilt $\pi \in \{\pm m \pm ni, \pm n \pm mi\}$ und*

$$\#E(\mathbf{F}_p) \in \{p+1-2m, p+1+2m, p+1-2n, p+1+2n\}.$$

Bemerkung: Hat man $y^2 = x^3 + ax$ über $\mathbf{F}_p$ mit $p \equiv 1 \bmod 4$ gegeben, so bestimmt man die Gruppenordnung am einfachsten, indem man sich einen Punkt $P \in E(\mathbf{F}_p)$ wählt und testet, von welcher der Zahlen $p+1 \pm 2m, p+1 \pm 2n$ er annulliert wird. (Man kann auch zeigen, daß jede der möglichen Anzahlen realisiert wird.)

Beispiel: Wir betrachten $y^2 = x^3 + x$ über $\mathbf{F}_p$ mit $p = 10^{100} + 949$. Mit nachfolgendem Programm findet man sofort $p = m^2 + n^2$ mit

$$\begin{aligned} m &= 99697921470138519447541656418848509184628524016382, \\ n &= 77668819055070508451725982180298333694401232778 95. \end{aligned}$$

Also wissen wir $\#E(\mathbf{F}_p) \in \{p+1-2m, p+1+2m, p+1-2n, p+1+2n\}$. Wir wählen einen Punkt auf E, z.B.

$$\begin{aligned} P_3 = (&3, 54623271714330180818642066289896420475604228765190 \\ &52593537076380366897011836382568451797420914806202). \end{aligned}$$

(Der Punkt $(0,0)$ ist ungeeignet wegen $2 \cdot (0,0) = O$.) Nun rechnet man nach:

$$(p+1-2m)P_3 \neq O, \quad (p+1+2m)P_3 \neq O, \quad (p+1-2n)P_3 \neq O, \quad (p+1+2n)P_3 = O,$$

woraus sofort $\#E(\mathbf{F}_p) = p+1+2n$ folgt.

Mit dem sogenannten Cornacchia-Algorithmus ist es möglich, sehr schnell ganzzahlige Lösungen der Gleichung $x^2 + dy^2 = p$ (mit $d \geq 1$) zu bestimmen. Wir werden darauf nicht näher eingehen. (Siehe [**1**].) Das folgende Ubasic-Programm corna.ub berechnet auf diese Weise Lösungen der Gleichung $x^2 + dy^2 = p$.

```
 10  input "p=";P
 20  input "d=";D
 30  K=kro(-D,P):if K=-1 then print "keine Loesung mod p":goto 20
 40  Q=P-1:E=0:A=(-D)@P
 50  if Q@2=0 then Q=Q\2:E=E+1:goto 50
 60  N=2
 70  if kro(N,P)=1 then N=N+1:goto 70
 80  Z=modpow(N,Q,P)
 90  Y=Z:R=E:X=modpow(A,(Q-1)\2,P):B=(A*X*X)@P:X=(A*X)@P
100  if B@P=1 then print "x=";X:goto 150
110  M=1:Bb=(B*B)@P
120  if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 120
130  if M=R then print A;" ist kein quadratischer Rest modulo ";P:goto 20
140  T=modpow(Y,2^(R-M-1),P):Y=(T*T)@P:R=M:X=(X*T)@P:B=(B*Y)@P:goto 100
150  if 2*X<P then X=P-X
160  A=P:B=X:L=isqrt(P)
170  if B>L then R=A@B:A=B:B=R:goto 170
180  if (P-B^2)@D<>0 then print "keine Loesung":goto 20
190  C=(P-B^2)\D:Y=isqrt(C):X=B
200  if Y*Y<>C then print "keine Loesung":goto 20
210  print "x=";X,"y=";Y:goto 20
```

4.2. Elliptische Kurven mit $j = 0$. Wir betrachten jetzt Kurven $E : y^2 = x^3 + b$ über $\mathbf{F}_p$ mit $p \geq 5$. Ist $\zeta \in \mathbf{F}_{p^2}$ eine primitive 3-te Einheitswurzel, d.h. gilt $\zeta^2 + \zeta + 1 = 0$, so ist

$$\varphi : (x, y) \mapsto (\zeta x, y)$$

ein Automorphismus der Ordnung 3. Daneben gibt es den Frobeniusendomorphimus $\pi(x,y) = (x^p, y^p)$. Es gilt:

$$\begin{aligned} \varphi\pi(x,y) &= \varphi(x^p,y^p) = (\zeta x^p, y^p), \\ \pi\varphi(x,y) &= \pi(\zeta x, y) = (\zeta^p x^p, y^p). \end{aligned}$$

- Ist $p \equiv 2 \bmod 3$, so ist $\zeta^p = \zeta^2 \neq \zeta$, also $\pi\varphi \neq \varphi\pi$, der Endomorphismenring $\mathrm{End}(E)$ ist nichtkommutativ, E also supersingulär und damit $\#E(\mathbf{F}_p) = p+1$.
- Ist $p \equiv 1 \bmod 3$, so ist $\zeta^p = \zeta$ und somit $\varphi\pi = \pi\varphi$. Wie im Fall $j = 1728$ zeigt man nun $\mathrm{End}(E) = \mathbf{Z}[\varphi] \simeq \mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$. Wir schreiben $\zeta = \frac{-1+\sqrt{-3}}{2}$ und haben dann $\overline{\zeta} = \zeta^2 = -1-\zeta$. Ist $\pi = u + v\zeta$ mit $u, v \in \mathbf{Z}$, so gilt $p = \pi\overline{\pi} = u^2 - uv + v^2$. Hat man umgekehrt $m, n \in \mathbf{Z}$ mit $p = m^2 - mn + n^2$, so unterscheidet sich (wegen der eindeutigen Primfaktorzerlegung in $\mathbf{Z}[\zeta]$) π von $m + n\zeta$ oder $m + n\overline{\zeta}$ nur um eine Einheit, d.h. um $\pm 1, \pm\zeta, \pm\zeta^2$. Dies ergibt folgende Möglichkeiten (o.E. bis auf Konjugation):

$$\begin{aligned} \pi &= \pm(m+n\zeta) \quad \text{und} \quad Sp(\pi) = \pm(2m-n), \\ \pi &= \pm\zeta(m+n\zeta) \quad \text{und} \quad Sp(\pi) = \pm(-m-n), \\ \pi &= \pm\zeta^2(m+n\zeta) \quad \text{und} \quad Sp(\pi) = \pm(-m+2n). \end{aligned}$$

  Mit der Formel $\#E(\mathbf{F}_p) = p + 1 - Sp(\pi)$ ergeben sich dann die Aussagen des folgenden Satzes:

Satz. *Sei E eine durch $y^2 = x^3 + b$ über $\mathbf{F}_p$ definierte elliptische Kurve.*

1. *Ist $p \equiv 2 \bmod 3$, so ist E supersingulär und damit $\#E(\mathbf{F}_p) = p+1$.*
2. *Ist $p \equiv 1 \bmod 3$, so ist $\mathrm{End}(E) = \mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$. Schreibt man $p = m^2 - mn + n^2$ mit $m, n \in \mathbf{Z}$, so gilt*

$$\#E(\mathbf{F}_p) \in \{p+1-2m+n, p+1+2m-n, p+1-m-n, p+1+m+n, p+1+m-2n, p+1-m+2n\}.$$

Bemerkungen:

1. Wieder gibt es einen Algorithmus, mit dem man schnell zu $p \equiv 1 \bmod 3$ eine Darstellung $p = m^2 - mn + n^2$ findet. (Siehe [**11a**] und das folgende Programm.)
2. Zu vorgegener Kurve $y^2 = x^3 + b$ über $\mathbf{F}_p$ findet man schnell die Gruppenordnung durch Wahl eines Punktes $P \in E(\mathbf{F}_p)$ und Testen, welche der möglichen Zahlen (für die Gruppenordnung) den Punkt P annullieren.

Das folgende Ubasic-Programm *corna2.ub* benutzt den verallgemeinerten Cornacchia-Algorithmus um zu gegebener imaginärquadratischer Diskriminante D und Primzahl p Zahlen $u, v \in \mathbf{Z}$ mit

$$p = \frac{u + v\sqrt{D}}{2} \cdot \frac{u - v\sqrt{D}}{2}$$

zu bestimmen bzw. festzustellen, daß eine solche Darstellung nicht existiert.

```
 10  print "Cornacchia-Algorithmus:"
 20  input "Imaginaerquadratische Diskriminante=";D
 30  input "p=";P
 40  if D@P=0 then print "p ist verzweigt":goto 30
 50  if kro(D,P)=-1 then print "p ist traege":goto 30
 60  ' Verfahren nach sqrmp.ub
 70  A=D
 80  Q=P-1:E=0
 90  if Q@2=0 then Q=Q\2:E=E+1:goto 90
100  N=2
110  if kro(N,P)=1 then N=N+1:goto 110
120  Z=modpow(N,Q,P)
130  Y=Z:R=E:X=modpow(A,(Q-1)\2,P):B=(A*X*X)@P:X=(A*X)@P
140  if B@P=1 then 190
150  M=1:Bb=(B*B)@P
160  if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 160
```

```
170   T=modpow(Y,2^(R-M-1),P):Y=(T*T)@P:R=M:X=(X*T)@P:B=(B*Y)@P:goto 140
180   ' Verfahren sqrmp.ub beendet
190   if (X-D)@2=1 then X=X+P
200   L=isqrt(4*P):X0=2*P:X1=X
210   if X1>L then X2=X0@X1:X0=X1:X1=X2:goto 210
220   if (X1^2-4*P)@D>0 then print "kein Hauptideal":goto 30
230   Q=(X1^2-4*P)\D:V=isqrt(Q)
240   if V^2<>Q then print "kein Hauptideal":goto 30
250   print "Hauptideal (u+v*sqrt(D))/2 mit u,v=";X1;V:goto 30
```

Beispiel: Wir betrachten Kurven $E_b : y^2 = x^3 + b$ über $\mathbf{F}_p$ mit $p = 10^{10} + 33$. Mit dem Cornacchia-Algorithmus findet man

$$m = 109088 \quad \text{und} \quad n = 21759 \quad \text{mit} \quad p = m^2 - mn + n^2.$$

Dann ist

$$\#E(\mathbf{F}_p) \in \{9999803617, 9999869187, 9999934464, 10000065604, 10000130881, 10000196451\}.$$

Wir betrachten die Kurven mit $1 \le b \le 30$. Wir wählen jeweils den ersten Punkt P mit einer x-Koordinate ≥ 1 und probieren, von welchen der obigen Zahlen er annulliert wird. Bei diesen Beispielen passiert das jeweils nur bei einer Zahl. (Punkte mit x-Koordinate 0 sind ungeeignet, da solche Punkte 3-Teilungspunkte sind.) Hier ist das Ergebnis:

$\#E_b(\mathbf{F}_p)$	b
9999803617	20, 30
9999869187	4, 6, 9, 11, 14, 21
9999934464	1, 8, 12, 13, 17, 18, 22, 27, 28
10000065604	10, 15, 29
10000130881	5
10000196451	2, 3, 7, 16, 19, 23, 24, 25, 26

Man sieht auch, daß die Anzahl $\#E_b(\mathbf{F}_p)$ nur von $\overline{b} \in \mathbf{F}_p^*/\mathbf{F}_p^{*6} = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{10}, \overline{20}\}$ abhängt.

4.3. Elliptische Kurven über Q mit komplexer Multiplikation. Sei E eine über $\mathbf{C}$ definierte elliptische Kurve. Im allgemeinen ist dann $\mathrm{End}(E) = \mathbf{Z}$. Ist $\mathrm{End}(E) \neq \mathbf{Z}$, so ist $\mathrm{End}(E)$ Ordnung in einem imaginärquadratischen Zahlkörper, man sagt, E hat komplexe Multiplikation. Es gibt dazu die Theorie der komplexen Multiplikation, auf die wir nicht eingehen wollen.
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}	$y^2 = x^3 - 264x - 1694$
$\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$	$-2^{15} \cdot 3^3$	$y^2 = x^3 - 152x - 722$
$\mathbf{Z}[\frac{1+\sqrt{-43}}{2}]$	$-2^{18} \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 3440x - 77658$
$\mathbf{Z}[\frac{1+\sqrt{-67}}{2}]$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$y^2 = x^3 - 29480x - 1948226$
$\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$y^2 = x^3 - 8697680x - 9873093538$

Sei jetzt E durch eine Gleichung $y^2 = x^3 + ax + b$ aus der obigen Tabelle gegeben mit $a, b \neq 0$ und Endomorphismenring $\mathbf{Z}[\omega]$ und j-Invariante j. Wir wollen E über $\mathbf{F}_p$ mit einer hinreichend großen Primzahl p betrachten.

- Ist $u \in \mathbf{F}_p$ mit $(\frac{u}{p}) = -1$ und definiert man E' durch die Gleichung $y^2 = x^3 + au^2x + bu^3$, so bilden E und E' ein Repräsentantensystem (bzgl. $\mathbf{F}_p$-Isomorphie) der über $\mathbf{F}_p$-definierten elliptischen Kurven mit j-Invariante j.
- Gibt es kein $\pi \in \mathbf{Z}[\omega]$ mit $p = \pi\overline{\pi}$, so ist E supersingulär und damit $\#E(\mathbf{F}_p) = p + 1$.
- Gibt es ein $\pi \in \mathbf{Z}[\omega]$ mit $p = \pi\overline{\pi}$, so ist E nicht supersingulär, $\pm\pi$ ist (bis auf Konjugation) der Frobeniusendomorphismus. Damit gilt

$$\#E(\mathbf{F}_p) = p + 1 \pm Sp(\pi).$$

- Ob es ein $\pi \in \mathbf{Z}[\omega]$ gibt, kann man schnell mit dem Cornacchia-Algorithmus (Programm *corna2.ub*) sehen bzw. explizit bestimmen.
- Wir schreiben $\#E(\mathbf{F}_p) = p+1-s$ und $\#E'(\mathbf{F}_p) = p+1-s'$. Dann ist nach unserer Anzahlformel

$$s = -\sum_{x \in \mathbf{F}_p} (\frac{x^3 + ax + b}{p}) = \sum_{x \in \mathbf{F}_p} (\frac{u^3}{p})(\frac{x^3 + ax + b}{p}) = \sum_{x \in \mathbf{F}_p} (\frac{x^3 + au^2x + bu^3}{p}) = -s',$$

  also

$$\#E(\mathbf{F}_p) = p + 1 - s \quad \text{und} \quad \#E'(\mathbf{F}_p) = p + 1 + s.$$

  D.h. Ist π der Frobenius von E, so $-\pi$ der von E' (bzw. umgekehrt).

Wir geben ein Beispiel, das zeigen soll, wie schnell man in diesem Fall $\#E(\mathbf{F}_p)$ berechnen kann.

Beispiel: Wir betrachten E mit der Gleichung $y^2 = x^3 - 35x - 98$ und Endomorphismenring $\mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$.

- $p = 10^{100} + 267$. Der Cornacchia-Algorithmus zeigt, daß es kein $\pi \in \mathbf{Z}[\frac{1+\sqrt{-7}}{2}]$ gibt mit $p = \pi\overline{\pi}$. Also ist E supersingulär über $\mathbf{F}_p$ und damit $\#E(\mathbf{F}_p) = p + 1$. (Sicherheitshalber haben wir für ein paar Punkte die Richtigkeit der Beziehung $(p + 1)P = O$ überprüft.)

- $p = 10^{100} + 949$. Der Cornacchia-Algorithmus liefert $p = N(\frac{m+n\sqrt{-7}}{2})$ mit

$$\begin{aligned} m &= 42325959994171622650565228296262404195440861980822, \\ n &= 73880708008220718780302597336179440975963604218004. \end{aligned}$$

Wegen $(\frac{2}{p}) = -1$ ist E' mit der Gleichung $y^2 = x^3 - 35 \cdot 2^2 x - 98 \cdot 2^3$ eine zu E über $\mathbf{F}_p$ nichtisomorphe Kurve mit gleicher j-Invariante. Damit gilt:

$$\{\#E(\mathbf{F}_p), \#E'(\mathbf{F}_p)\} = \{p+1-m, p+1+m\}.$$

Der Punkt $P = (3, *)$ auf E erfüllt $(p+1+m)P = O$, $(p+1-m)P \neq O$, der Punkt $P' = (0, *)$ auf E' erfüllt $(p+1+m)P' \neq O$, $(p+1-m)P' = O$, also folgt

$$\#E(\mathbf{F}_p) = p+1+m \quad \text{und} \quad \#E'(\mathbf{F}_p) = p+1-m$$

und für die Frobeniusendomorphismen

$$\pi = \frac{-m+n\sqrt{-7}}{2} \quad \text{und} \quad \pi' = \frac{m+n\sqrt{-7}}{2}.$$

Bemerkungen:

1. Durch Reduktion (modulo p) von Kurven mit komplexer Multiplikation erhält man also Kurven E, bei denen man sehr schnell die Gruppenordnung $\#E(\mathbf{F}_p)$ berechnen kann. Dies kann man zur Konstruktion von Beispielen benutzen.
2. Es zeigt sich, daß jede elliptische Kurve über $\mathbf{C}$ mit komplexer Multiplikation schon über einem Zahlkörper definiert ist, wobei das Reduktionsverhalten (modulo einem Primideal) ähnlich wie bei den dargestellten Beispielen über $\mathbf{Q}$ ist. Auf solche Weise kann man versuchen bei vorgegebenem N und p (mit $|p+1-N| < 2\sqrt{p}$) eine elliptische Kurve E über $\mathbf{F}_p$ zu konstruieren mit $\#E(\mathbf{F}_p) = N$.

5. Der Schoof-Algorithmus

Wir werden jetzt einen Algorithmus behandeln, der auf Schoof zurückgeht, und für beliebige elliptische Kurven im Prinzip mit polynomialer Laufzeit funktioniert.

Sei E eine elliptische Kurve über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$. Wir stellen uns vor, daß p eine hinreichend große Primzahl ist. Ist $\pi : (x, y) \mapsto (x^p, y^p)$ der Frobeniusendomorphismus, so genügt π in $\mathrm{End}(E)$ einer Gleichung $\pi^2 - s\pi + p = 0$ und dann ist

$$\#E(\mathbf{F}_p) = p + 1 - s.$$

Für s gilt die Abschätzung

$$|s| < 2\sqrt{p}.$$

Bestimmt man nun s modulo genügend vieler Primzahlen, so kann man mit dieser Abschätzung und dem chinesischen Restsatz s und damit $\#E(\mathbf{F}_p)$ berechnen.

Wie findet man $s \equiv \#E(\mathbf{F}_p) \bmod 2$? Da die nichttrivialen 2-Teilungspunkte genau die Punkte $(x_0, 0)$ mit $x_0^3 + ax_0 + b = 0$ sind, gilt

$$\#E(\mathbf{F}_p) \equiv s \equiv 0 \bmod 2 \quad \Longleftrightarrow \quad \text{das Polynom } x^3 + ax + b \text{ hat eine Nullstelle in } \mathbf{F}_p.$$

(Eine äquivalente Bedingung ist $ggT(x^p - x, x^3 + ax + b) \neq 1$ in $\mathbf{F}_p[x]$.)

Sei jetzt ℓ eine ungerade Primzahl mit $\ell < p$. Für alle $P \in E[\ell]$ gilt

$$\pi^2(P) - s\pi(P) + pP = O,$$

mit $s' \equiv s \bmod \ell$ und $p' \equiv p \bmod \ell$ dann natürlich auch

$$\pi^2(P) - s'\pi(P) + p'P = O.$$

Angenommen wir finden ein t mit $0 \leq t \leq \ell - 1$, so daß für alle $P \in E[\ell]$ gilt

$$\pi^2(P) - t\pi(P) + pP = O.$$

Dies liefert $(t - s)\pi(P) = O$ und damit $t \equiv s \bmod \ell$. Wir müssen jetzt sehen, wie man praktisch ein solches t finden kann. Dazu brauchen wir die sogenannten n-Teilungspolynome.

Die Teilungspolynome ψ_n: (Mehr dazu findet man als Übungsaufgabe in [**13**, Aufgabe III.3.7].) Man definiert rekursiv Polynome $\psi_n \in \mathbf{Z}[a,b,x,y]$ durch

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4+6ax^2+12bx-a^2,\\
\psi_4 &= 4y(x^6+5ax^4+20bx^3-5a^2x^2-4abx-8b^2-a^3),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3-\psi_{m-1}\psi_{m+1}^3 \quad (m\geq 2),\\
2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2) \quad (m\geq 2).
\end{aligned}$$

Eliminiert man alle höheren Potenzen von y mit der Relation $y^2=x^3+ax+b$, so stellt man fest, daß für ungerade n's die Polynome ψ_n Polynome in $\mathbf{Z}[a,b,x]$ sind.
Nun gilt für $P\in E$:

$$P\in E[n] \quad\Longleftrightarrow\quad \psi_n(P)=0.$$

Für ungerades n gilt außerdem

$$\psi_n(x)=nx^{\frac{n^2-1}{2}}+\dots$$

(wie es sein sollte, da für $ggT(p,n)=1$ die Menge $E[n]$ genau n^2 Elemente enthält). Leider werden die ψ_n's schnell sehr groß und unhandlich. (Wir benutzen im nachfolgenden Programm nur ψ_3, ψ_5, ψ_7 und ψ_{11}.)

Der Algorithmus: Sei jetzt ℓ eine ungerade Primzahl und $f=y^2-(x^3+ax+b)$. Für $x_0,y_0\in\overline{\mathbf{F}_p}$ gilt:

$$(x_0,y_0)\in E[\ell] \quad\Longleftrightarrow\quad f(x_0,y_0)=\psi_\ell(x_0)=0.$$

Um alle ℓ-Teilungspunkte zu betrachten, werden wir mit Polynomen rechnen und zwar modulo f und modulo ψ_ℓ.

- Man muß ψ_ℓ explizit berechnen um damit rechnen zu können.
- Wir betrachten den Ring
$$R=\mathbf{F}_p[x,y]/(f,\psi_\ell).$$
Indem man die höheren Potenzen von y mit $y^2=x^3+ax+b$ eliminiert und höhere Potenzen von x mit $\psi_\ell(x)$ kann man jedes Element aus R eindeutig in der Form
$$g(x)+h(x)y \text{ mit } g(x),h(x)\in\mathbf{F}_p[x] \text{ und } \deg g,\deg h\leq\frac{\ell^2-1}{2}-1$$
schreiben. Wir benutzen dies als Normalform. (R hat also Dimension ℓ^2-1 über $\mathbf{F}_p$.)
- Mit dem square-and-multiply-Verfahren kann man die Normalform der Polynome x^p, y^p, x^{p^2}, y^{p^2} im Ring R in $O(\log p)$ Schritten bestimmen.
- Man schreibt die Additionsgesetze auf E in homogener Form, damit man auch Elemente aus R, also Polynome, einsetzen kann und nicht invertieren muß.
- Der Punkt $(1:x:y)$ liegt formal auf E, da er die Definitionsgleichung für E erfüllt. Wir berechnen mit den Additionsgesetzen den Punkt
$$-((1:x^{p^2}:y^{p^2})+(p \bmod \ell)(1:x:y))$$
und addieren nacheinander den Punkt $(1:x^p:y^p)$ um
$$-((1:x^{p^2}:y^{p^2})+(p \bmod \ell)(1:x:y))+t(1:x^p:y^p)$$
für $t=0,1,2,\dots$ zu erhalten. Gilt
$$-((1:x^{p^2}:y^{p^2})+(p \bmod \ell)(1:x:y))+t(1:x^p:y^p)=(0:0:*),$$
so hören wir auf. Dann gilt nämlich auch für alle ℓ-Teilungspunkte P
$$-(\pi^2(P)+(p \bmod \ell)P)+t\pi(P)=O,$$
(die Umkehrung gilt ebenso), also folgt nach unserer Vorüberlegung
$$s\equiv t \bmod \ell$$
und wir haben $s \bmod \ell$ bestimmt.

Beispiel: Wir betrachten $y^2 = x^3 + 5x + 7$ über $\mathbf{F}_p$ mit $p = 97$. Wir rechnen in $\mathbf{F}_{97}[x,y]/(f,\psi_3)$, d.h. modulo $f = y^2 - (x^3 + 5x + 7)$ und $\psi_3 = 3x^4 + 30x^2 + 84x - 25$. Man berechnet (mit der square-and-multiply-Methode):

$$\begin{aligned} x^p &= 61 + 60x + 33x^2 + 32x^3, \\ x^{p^2} &= 12 + 57x + 32x^2 + 53x^3, \\ y^p &= 35xy + 92x^2y + 51x^3y, \\ y^{p^2} &= 3y + 33xy + 90x^2y + 46x^3y. \end{aligned}$$

Mit den Additionsformeln erhält man nun ($p \equiv 1 \bmod 3$)

$$(1 : x^{p^2} : y^{p^2}) + (1 : x : y) = (35 + 62x + 2x^2 + x^3 : 12 + 91x + 6x^2 + 26x^3 : 34y + 11xy + 3x^2y + 77x^3y),$$

also

$$-((1 : x^{p^2} : y^{p^2}) + (1 : x : y)) = (35 + 62x + 2x^2 + x^3 : 12 + 91x + 6x^2 + 26x^3 : -(34y + 11xy + 3x^2y + 77x^3y)).$$

Nun ist

$$(1 : x^p : y^p) = (1 : 61 + 60x + 33x^2 + 32x^3 : 35xy + 92x^2y + 51x^3y).$$

Wir addieren jetzt

$$\begin{aligned} (-((1 : x^{p^2} : y^{p^2}) + (1 : x : y))) + (1 : x^p : y^p) \quad = \quad & (54y + 35xy + 14x^2y + x^3y : \\ & 84y + 77xy + 75x^2y + 18x^3y : \\ & 61 + 70x + 53x^2 + 76x^3), \end{aligned}$$

dazu wieder $(1 : x^p : y^p)$:

$$(-((1 : x^{p^2} : y^{p^2}) + (1 : x : y))) + 2(1 : x^p : y^p) = (0 : 0 : 75y + 54xy + 41x^2y + 93x^3y),$$

also gilt für die Spur des Frobenius $s \equiv 2 \bmod 3$.

Bemerkungen:

1. Hat man mit dem vorgestellten Algorithmus s modulo den Primzahlen 2, 3, 5, ... , ℓ_n bestimmt, so kennt man mit dem chinesischen Restsatz s modulo $2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot \ell_n$.
2. Ist n so gewählt, daß gilt
$$2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot \ell_n > 4\sqrt{p},$$
so ist s dadurch (wegen $|s| < 2\sqrt{p}$) eindeutig bestimmt. Z.B. ist
$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 > 4\sqrt{333503} \quad \text{und} \quad 2 \cdot 3 \cdot 5 \cdot \cdots \cdot 127 \cdot 131 > 4\sqrt{10^100 + 267}.$$
3. Praktisch ist das kaum zu machen. So ist für $\ell = 131$ ein Element aus R ein Polynom mit 17160 Koeffizienten (in $\mathbf{F}_p$).
4. Das nachfolgende Maple-Programm *schoof* funktioniert für $\ell = 3, 5, 7, 11$. Zusammen mit dem einfachen Fall $\ell = 2$ hat man dann s modulo 2310 bestimmt. (Für weitere ℓ's muß man zuerst ψ_ℓ berechnen, was irgendwann Speicherprobleme gibt.)

Das Maple-Programm *schoof*:

```
# Schoof-Algorithmus
# spur(p,a,b) berechnet die Spur des Frobenius fuer y^2=x^3+ax+b
# ueber F_p modulo der Primzahlen 2, 3, 5, 7, 11, also modulo 2310

# psi-Polynome
psi_polynom:=proc(ell,a,b)
psi3 := 3*x^4+6*a*x^2+12*b*x-a^2;
psi5 := 380*x^9*b-105*x^8*a^2-300*x^6*a^3-240*x^6*b^2-125*x^4*a^4
-50*a^5*x^2-1600*b^3*x^3+5*x^12+a^6+62*x^10*a+240*x^7*a*b
-696*x^5*b*a^2-1920*a*x^4*b^2-80*a^3*x^3*b-240*b^2*x^2*a^2
-100*b*x*a^4-256*b^4-32*b^2*a^3-640*a*b^3*x;
psi7 := -2954*x^20*a^2-19852*x^18*a^3-35231*x^16*a^4-82264*x^14*a^5
-111916*x^12*a^6+308*x^22*a-42168*x^10*a^7-42896*x^18*b^2
```

```
-829696*x^15*b^3-928256*x^12*b^4+3944*x^21*b+15673*x^8*a^8
+14756*x^6*a^9-1555456*x^9*b^5+1302*x^4*a^10+196*a^11*x^2
-2809856*b^6*x^6+160*b^2*a^9-802816*b^7*x^3+3328*b^4*a^6-112*x^19*a*b
-571872*x^16*a*b^2-2132480*x^13*a*b^3-92568*x^17*a^2*b
-31808*x^15*a^3*b-615360*x^14*a^2*b^2-161840*x^13*a^4*b
-297472*x^12*a^3*b^2-608160*x^11*a^5*b-425712*x^9*b*a^6
-2603776*x^11*b^3*a^2-1192800*x^10*b^2*a^4-3727360*x^9*a^3*b^3
-831936*x^8*a^5*b^2-53824*x^7*a^7*b-190400*x^6*b^2*a^6
-3293696*x^10*b^4*a-7069440*x^8*b^4*a^2-1314560*x^7*b^3*a^4
+57288*x^5*a^8*b-168448*a^5*x^5*b^3+134400*a^7*x^4*b^2+1680*a^9*x^3*b
+152320*b^3*x^3*a^6-7127040*b^5*x^7*a-2293760*b^4*x^6*a^3
-3698688*b^5*x^5*a^2+394240*b^4*x^4*a^4+7*x^24-a^12+3696*a^8*b^2*x^2
+392*a^10*b*x+831488*b^5*a^3*x^3+96768*b^4*a^5*x^2+7168*b^3*a^7*x
-3039232*b^6*a*x^4+544768*b^6*x^2*a^2+64512*b^5*x*a^4+65536*b^8
+229376*b^7*a*x+24576*b^6*a^3;
psi11 := 2111496782872576*x^33*b^9+1111020726813184*x^30*b^10+
20424226112536576*x^27*b^11-1462749167616*x^36*b^8-1634430741504*x^45*b^5-
35141520150528*x^42*b^6-77988692508672*x^39*b^7+16930281984*x^48*b^4+
1197743580033*x^40*a^10+2175830922716*x^38*a^11+998244352*b^10*a^15+
42282700345442304*x^32*b^8*a^2+130243629815169024*x^30*b^8*a^3+
169511083234099200*x^28*b^8*a^4+123221468589981696*x^26*b^8*a^5+
165600081563811840*x^24*b^8*a^6+1093351076471808*x^37*b^5*a^4+14783574589808640
*x^34*b^6*a^4+1519633647310592*x^36*b^4*a^6+3386894377405440*x^34*b^4*a^7+
4486098469205760*x^32*b^4*a^8+4024768800701440*x^30*b^4*a^9+1988257877760*x^40*
b^4*a^4+4610221329494528*x^28*b^4*a^10+3281869637544 96*x^38*b^4*a^5+
8088356319031296*x^26*b^4*a^11-15884231074560*x^44*b^4*a^2-39603044659200*x^42*
b^4*a^3+1125721483476480*x^20*b^4*a^14-48050571999232*x^18*b^4*a^15-
341167409915904*x^16*b^4*a^16-151880699435520*x^14*b^4*a^17+8749729799247360*x^
24*b^4*a^12-25134055161600*x^12*b^4*a^18+1808735095860*x^41*a^8*b+
85885200592752*x^38*a^8*b^2+75058846822367232*x^31*a^4*b^7-5734532100*x^49*a^4*
b+11*x^60-a^30+3223489742187*x^36*a^12+5384207244702*x^34*a^13+50897017743*x^44
*a^8+8608181312269*x^32*a^14+387221579866*x^42*a^9+9712525647792*x^30*a^15-
5391243935*x^48*a^6-7864445336*x^46*a^7-1084042069649*x^24*a^18-1642552094436*x
^22*a^19-948497199067*x^20*a^20-291359180310*x^18*a^21+6610669151537*x^28*a^16-
28366041*x^52*a^4-57392757037*x^16*a^22+1890240552750*x^26*a^17-815789634*x^50*
a^5-14323974808*x^14*a^23+12742754241085440*b^13*x^21+15942213691244544*b^14*x^
18+18675888971317248*b^15*x^15+18560019830145024*b^12*x^24+89980928*b^8*a^18+
92884*x^57*b-207691*x^56*a^2-5092956*x^54*a^3-18457648*x^54*b^2-3970900032*x^51
*b^3-443200472352*x^46*a^4*b^2-7789571940480*x^43*a^4*b^3+110981172112 80*x^39*a
^9*b+203202938229632*x^36*a^9*b^2+5962766981124096*x^35*a^5*b^5+
33390044082683904*x^32*a^5*b^6+84439317922578432*x^29*a^5*b^7-86607991008*x^47*
a^5*b-1209317982336*x^44*a^5*b^2-9557248141056*x^41*a^5*b^3+2484788737993605 12*
b^12*x^20*a^2+584930706648465408*b^12*x^18*a^3+611846930477088768*b^12*x^16*a^4
+197479223814782976*b^12*x^14*a^5+13273668654202880*b^12*x^12*a^6+
22769096958541824 0*b^9*x^25*a^4+374997489467523072*b^10*x^22*a^4+
287054394295320576*b^8*x^22*a^7+249703530359095296*b^8*x^20*a^8+
108590684152135680*b^8*x^18*a^9+20789634448687104*b^8*x^16*a^10-
6411647711969280*b^8*x^14*a^11-60554950410240*b^8*a^14*x^8-15006649810944*b^8*a
^15*x^6-1224232796160*b^8*a^16*x^4-3360817152*b^8*a^17*x^2-62300709729730 56*b^8
*a^12*x^12+51268590648924*a^16*x^25*b+98825462385072*a^16*x^22*b^2+
13979863796557824*a^12*x^21*b^5+7803897920028672*a^12*x^18*b^6-2281284842225664
*a^12*x^15*b^7+21881962779708*a^12*x^33*b+228527539349824*a^12*x^30*b^2+
2255812306139392*a^12*x^27*b^3+60469774025613312*a^10*b^6*x^22+
32404861810556928*a^11*b^6*x^20-791973571952640*a^13*b^6*x^16-21403307126784 00*
```

```
a^14*b^6*x^14+15192241694510284 8*a^8*b^7*x^23+15950299769733120 0*a^8*b^9*x^17+
45182255843450880*a^8*b^6*x^26+503225791523136*a^14*b^2*x^26+297065794700928*a^
15*b^2*x^24-12667429015296*a^17*b^2*x^20-38179759168144*a^18*b^2*x^18+
471864748244736*a^13*b^2*x^28-16041862868064*a^19*b^2*x^16+932995178009664*a^8*
b^3*x^35+221777475716016*a^10*b^2*x^34+143196317262240*a^11*b^2*x^32+
136836734751805 44*a^8*b^5*x^29-103824645408*a^22*b^2*x^10-10552508736*a^23*b^2*
x^8-567533296*a^24*b^2*x^6+35528064*a^25*b^2*x^4-2159701514784*a^20*b^2*x^14+
133584*a^26*b^2*x^2+3281719656112128*a^13*b^5*x^19-315551058223104*a^14*b^5*x^
17-941487299444736*a^15*b^5*x^15-337684970929152*a^16*b^5*x^13+1249116471313920
*a^14*b^3*x^23+62562364976922624*a^10*b^7*x^19+23545425241755648*a^10*b^5*x^25+
11352247866960*a^17*b*x^23-7456485707880*a^18*b*x^21-7937009545520*a^19*b*x^19+
99590466344160*a^14*b*x^29-2713640947116*a^20*b*x^17+945102972133 76*a^15*b*x^27
-362014866400*a^21*b*x^15+57726168969920*a^13*b*x^31+10970879311068 16*a^10*b^3*
x^31-3227582820*a^24*b*x^9-143619344*a^25*b*x^7+15049320*a^26*b*x^5+75504*a^27*
b*x^3-52266299888*a^22*b*x^13+20748049857304*a^10*b*x^37+2420*a^28*b*x+
12351444798529536*x^33*b^5*a^6+14844388818665472*x^31*b^5*a^7-2673823072800*x^
42*b^2*a^6+31436860716800*x^39*b^3*a^6-628796468686848*x^38*b^6*a^2+
3508796085239808*x^35*b^7*a^2-5093605*a^26*x^8+2923492*a^27*x^6+33033*a^28*x^4+
1210*a^29*x^2-3974726283*a^24*x^12-171670990030848*x^41*b^5*a^2+189877131718 56*
x^35*b*a^11-324283434992*x^45*b*a^6-566667724128*x^43*b*a^7+825344784*x^50*b^2*
a^2-368122723584*x^47*b^3*a^2-68708376*x^53*b*a^2+15256015886712832*x^27*b^5*a^
9+10220448106176*x^40*b^2*a^7+331673723009024*x^37*b^3*a^7+17226965836185 60*x^
36*b^6*a^3+29873243216412672*x^33*b^7*a^3-186037635108864*x^39*b^5*a^3-
22204466592*x^48*b^2*a^3-3788155075584*x^45*b^3*a^3+528546480*x^51*b*a^3+
25423850464911360*x^23*b^5*a^11+1297970806784640*x^33*b^3*a^9-28833867360*x^11*
b*a^23-263706866024448*x^40*b^6*a-320769528397824*x^37*b^7*a+43138933810790 40*x
^34*b^8*a-41152339058688*x^43*b^5*a-1080820224*x^52*b^2*a-20898768000*x^49*b^3*
a-941626532352*x^46*b^4*a-1166288*x^55*b*a+38062193222631424*x^30*b^6*a^6+
67707257092440064*x^27*b^7*a^6+35266831327264768*x^28*b^6*a^7+34147605159084032
*x^31*b^9*a+147500109762396160*x^29*b^9*a^2+257174099696025600*x^27*b^9*a^3+
63310950733578240*x^24*b^6*a^9+99839427702423552*x^25*b^7*a^7+
23393513759676825 6*x^26*b^10*a^2+4316326921280*x^19*a^16*b^3+1291255568373760*x
^29*a^11*b^3-119780969793408*x^17*a^17*b^3+2325912473482752*x^25*a^13*b^3+
688436877648199680*b^11*x^19*a^4+25967186671986 2784*b^9*x^23*a^5+
605161656460247040*b^10*x^20*a^5+619360631509745664*b^11*x^17*a^5-
1556136760442880*b^9*a^12*x^9-85759818203136*b^10*a^12*x^6-7527584497664*b^11*a
^12*x^3+2189417605654118 40*b^11*x^23*a^2+443293524875542528*b^9*x^21*a^6+
390512814850048000*b^9*x^19*a^7+29752608815893708 8*b^10*x^24*a^3+
385265794075852800*b^11*x^21*a^3+29953024007864320*b^9*x^15*a^9-
13328365876936704*b^9*x^13*a^10-8833585594236928*b^9*x^11*a^11+
524118330003423232*b^10*x^18*a^6+2006867715104440 32*b^11*x^15*a^6+
192024785574690816*b^10*x^16*a^7+339253710381121536*b^13*x^17*a^2+
35817435826225152*b^10*x^14*a^8+461704421185683456*b^13*x^15*a^3-
20276728484069376*b^10*x^12*a^9+29540701981114368*b^11*x^13*a^7+
239256381004185600*b^14*x^14*a^2-24503719286538240*b^11*x^11*a^8+
179002445534330880*b^13*x^13*a^4-11199999971950592*b^10*x^10*a^10+
823012227400335 36*b^12*x^22*a+45256640*a^24*b^3*x^3+391298058567680*a^15*x^21*b
^3-58381169969408*a^18*x^15*b^3-52072062592*a^21*x^12*b^2-9301616163840*a^19*x^
13*b^3-56376025216*a^20*x^11*b^3+4581548430289920*a^13*x^22*b^4-624027579648*a^
20*b^4*x^8-59583777792*a^20*b^5*x^5+13632357004738560*a^11*b^7*x^17-23047290112
*a^22*b^3*x^7-482141440*a^22*b^4*x^4+88828822836740096*x^28*b^10*a+
131488957649584128*x^21*a^9*b^7-289368456960*x^9*a^21*b^3-910333952*a^23*x^5*b^
3+106682294181298176*b^11*x^25*a-47087388450816*b^5*x^11*a^17-1808216295424*b^5
*x^9*a^18-1004104273920*b^5*x^7*a^19-327758520320*x^10*a^19*b^4-664500689076224
```

```
*x^12*a^15*b^6-63093370081280*x^10*b^6*a^16-41962809856*a^21*x^6*b^4-
5843472678912*a^17*x^8*b^6-1289989550080*b^6*x^6*a^18-3947866625015808*b^7*x^13
*a^13-1510102436806656*b^8*x^10*a^13+9750868547076096*b^16*x^12+
1764870781403136*b^17*x^9+2794*x^58*a-385382514*a^25*x^10+1120*a^27*b^2-
336618061824000*b^16*x^4*a^4-44220983279616*b^16*a^5*x^2+93137212727623680*b^13
*x^19*a+118780165449842688*b^14*x^16*a-26748489853566976*b^12*a^7*x^10-
9602950376718336*b^12*a^8*x^8-5912997440520192*b^13*a^7*x^7-287533833388032*b^
13*a^8*x^5-40202236067840*b^13*a^9*x^3-469312015958016*b^12*a^9*x^6+
5597639466811392*b^15*a^3*x^9-12634896203776*b^10*a^13*x^4-224365903872*b^10*a^
14*x^2-7367329201520640*b^16*a^3*x^6+2660456019787776*b^13*x^11*a^5-
1210475712872448*b^10*x^8*a^11+128519978751098880*b^14*x^12*a^3-
11802673099571200*b^11*x^9*a^9+3697129323233280*b^14*x^10*a^4-774328949932032*b
^11*x^7*a^10-23446475576967168*b^14*a^5*x^8-83045004607488*b^11*a^11*x^5-
27352712630763520*b^13*x^9*a^6-2822560165134336*b^14*x^6*a^6+61355931400667136*
b^15*x^11*a^2-15266727541604352*b^15*x^7*a^4-1065272148492288*b^15*a^5*x^5-
105213813850112*b^15*x^3*a^6-66121826828288*b^12*x^4*a^10-2764549652480*b^12*a^
11*x^2+16315558555287552*b^16*a*x^10+3127358961745920*b^16*x^8*a^2+2626945024*b
^9*x*a^16-22145925120*b^11*a^13*x-180356414177280*b^14*a^7*x^4+687126047883264*
b^17*a*x^7-15900774236160*b^14*a^8*x^2-117922622078976*b^17*a^3*x^3-
2588628328906752*b^17*x^5*a^2-488686747648*b^13*x*a^10-597172252835840*b^18*a*x
^4-3307124817920*b^15*a^7*x-46866683133952*b^18*x^2*a^2-10204842295296*b^17*x*a
^4-12094627905536*b^19*a*x+370855936*a^21*b^5*x^3-63017781297152*a^15*b^7*x^9-
11367867236352*a^16*b^7*x^7-1414933217280*a^17*b^7*x^5-1115918945353728*a^14*b^
7*x^11+33623040*a^23*b^4*x^2-15356238233600*a^14*b^9*x^5-706685698048*a^15*b^9*
x^3-54748897280*a^19*b^6*x^4-72682580213760*a^13*b^9*x^7+170368*a^25*b^3*x-
1099511627776*b^20+73338729095233536*x^13*b^15*a+4244635648*b^12*a^12+
41575283425280*b^18*x^6-66520453480448*b^19*x^3-214748364800*b^16*a^6-
13421772800*b^14*a^9-824633720832*b^18*a^3+75520*a^24*b^4+3817472*a^21*b^6-
26763984896*a^18*b^7*x^3+657907712*a^20*b^6*x^2+15679488*a^22*b^5*x+377749504*a
^19*b^7*x;
if ell=3 then psi3 elif ell=5 then psi5 elif ell=7 then psi7 elif
   ell=11 then psi11 fi;
end;

spur2:=proc(p,a,b)
g:=x;k:=p;h:=1;
while k<>0 do
   if k mod 2=1 then
      h:=Rem(expand(h*g),x^3+a*x+b,x) mod p;
   fi;
   k:=trunc(k/2);
   g:=Rem(expand(g^2),x^3+a*x+b,x) mod p;
od;
if (Gcd(h-x,x^3+a*x+b) mod p)=1 then 1; else 0; fi;
end;

# Normalform eines Punktes im Ring F_p[x,y]/(y^2-(x^3+ax+b),psi.ell)
N:=proc(Pz,p,a,b,ell)
f:=y^2-(x^3+a*x+b); psi:=psi_polynom(ell,a,b);
z0:=op(1,Pz); z1:=op(2,Pz); z2:=op(3,Pz);
z0:=Rem(Rem(z0,f,y) mod p,psi,x) mod p;
z1:=Rem(Rem(z1,f,y) mod p,psi,x) mod p;
z2:=Rem(Rem(z2,f,y) mod p,psi,x) mod p;
[z0,z1,z2];
```

```
end;

# Additionstheoreme
Z1:=proc(Px,Py,p,a,b,ell)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
za0 := a*x0^2*y0*y1-a*x0*x1*y0^2-x0^2*y2^2+x2^2*y0^2+3*x0*x1*y1^2
-3*x1^2*y0*y1;
za1 := -3*b*x0^2*y0*y1+3*b*x0*x1*y0^2-a*x0^2*y1^2+a*x1^2*y0^2
-x0*x1*y2^2+x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
za2 := 3*b*x0^2*y0*y2-3*b*x0*x2*y0^2+a*x0^2*y1*y2-a*x1*x2*y0^2
+2*a*x0*x1*y0*y2-2*a*x0*x2*y0*y1-x0*x2*y2^2+x2^2*y0*y2+3*x1^2*y1*y2
-3*x1*x2*y1^2;
N([za0,za1,za2],p,a,b,ell);
end;

Z2:=proc(Px,Py,p,a,b,ell)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
zb0 := 3*b*x0^2*y0*y1-3*b*x0*x1*y0^2+a*x0^2*y1^2-a*x1^2*y0^2+x0*x1*y2^2
-x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
zb1 := a^2*x0^2*y0*y1-a^2*x0*x1*y0^2-3*b*x0^2*y1^2+3*b*x1^2*y0^2
-a*x0*x1*y1^2+a*x1^2*y0*y1+x1^2*y2^2-x2^2*y1^2;
zb2 := -a^2*x0^2*y0*y2+a^2*x0*x2*y0^2+3*b*x0^2*y1*y2-3*b*x1*x2*y0^2
+6*b*x0*x1*y0*y2-6*b*x0*x2*y0*y1+2*a*x0*x1*y1*y2-2*a*x1*x2*y0*y1
-a*x0*x2*y1^2+a*x1^2*y0*y2+x1*x2*y2^2-x2^2*y1*y2;
N([zb0,zb1,zb2],p,a,b,ell);
end;

Z3:=proc(Px,Py,p,a,b,ell)
x0:=op(1,Px); x1:=op(2,Px); x2:=op(3,Px);
y0:=op(1,Py); y1:=op(2,Py); y2:=op(3,Py);
zc0 := 6*b*x0*x2*y0^2+6*b*x0^2*y0*y2+2*a*x1*x2*y0^2+2*a*x0^2*y1*y2
+4*a*x0*x2*y0*y1+4*a*x0*x1*y0*y2+2*x2^2*y0*y2+2*x0*x2*y2^2+6*x1*x2*y1^2
+6*x1^2*y1*y2;
zc1 := 2*a^2*x0*x2*y0^2+2*a^2*x0^2*y0*y2-6*b*x1*x2*y0^2-6*b*x0^2*y1*y2
-12*b*x0*x2*y0*y1-12*b*x0*x1*y0*y2-4*a*x1*x2*y0*y1-4*a*x0*x1*y1*y2
-2*a*x1^2*y0*y2-2*a*x0*x2*y1^2+2*x2^2*y1*y2+2*x1*x2*y2^2;
zc2 := -2*x0^2*y0^2*a^3-18*x0^2*y0^2*b^2-6*a*b*x0*x1*y0^2
-6*a*b*x0^2*y0*y1-2*a^2*x1^2*y0^2-2*a^2*x0^2*y1^2-8*a^2*x0*x1*y0*y1
+18*b*x1^2*y0*y1+18*b*x0*x1*y1^2+6*a*x1^2*y1^2+2*x2^2*y2^2;
N([zc0,zc1,zc2],p,a,b,ell);
end;

Z:=proc(Px,Py,p,a,b,ell)
ZZ:=Z1(Px,Py,p,a,b,ell);
if ZZ=[0,0,0] then ZZ:=Z3(Px,Py,p,a,b,ell);
   if ZZ=[0,0,0] then ZZ:=Z2(Px,Py,p,a,b,ell); fi;
fi;
if ZZ=[0,0,0] then print('Vorsicht'); else ZZ; fi;
end;

# Multiplikation k.P
M:=proc(k,P,p,a,b,ell)
```

```
P1:=P;k1:=k;Q1:=[0,0,1];
while k1<>0 do
   if k1 mod 2=1 then Q1:=Z(Q1,P1,p,a,b,ell); fi;
   k1:=trunc(k1/2);
   P1:=Z3(P1,P1,p,a,b,ell);
od;
Q1;
end;

# Potenzieren von Elementen in obigem Ring
pow:=proc(g,k,p,a,b,ell)
f:=y^2-(x^3+a*x+b); psi:=psi_polynom(ell,a,b);
g1:=g;k1:=k;h1:=1;
while k1<>0 do
   if k1 mod 2=1 then
      h1:=Rem(Rem(expand(h1*g1),f,y) mod p,psi,x) mod p;
   fi;
   k1:=trunc(k1/2);
   g1:=Rem(Rem(expand(g1^2),f,y) mod p,psi,x) mod p;
od;
h1;
end;

# Spur des Frobenius modulo ell
spur_ell:=proc(p,a,b,ell)
P:=[1,x,y];
piP:=[1,pow(x,p,p,a,b,ell),pow(y,p,p,a,b,ell)];
pi2P:=[1,pow(x,p^2,p,a,b,ell),pow(y,p^2,p,a,b,ell)];
pP:=M(p mod ell,P,p,a,b,ell);
LS:=Z(pi2P,pP,p,a,b,ell);
L:=[op(1,LS),op(2,LS),-op(3,LS)];
t:=0;
while op(1,L)<>0 do L:=Z(L,piP,p,a,b,ell); t:=t+1; od;
t;
end;

spur:=proc(p,a,b)
st:=time(); s2:=spur2(p,a,b);
print('s','ist',s2,'modulo',2,'mit',time()-st,'Sekunden');
st:=time(); s3:=spur_ell(p,a,b,3);
print('s','ist',s3,'modulo',3,'mit',time()-st,'Sekunden');
st:=time(); s5:=spur_ell(p,a,b,5);
print('s','ist',s5,'modulo',5,'mit',(time()-st)/60,'Minuten');
st:=time(); s7:=spur_ell(p,a,b,7);
print('s','ist',s7,'modulo',7,'mit',(time()-st)/60,'Minuten');
print('s','ist',chrem([s2,s3,s5,s7],[2,3,5,7]),'modulo',2*3*5*7);
st:=time(); s11:=spur_ell(p,a,b,11);
print('s','ist',s11,'modulo',11,'mit',(time()-st)/60,'Minuten');
print('s','ist',chrem([s2,s3,s5,s7,s11],[2,3,5,7,11]),'modulo',2310);
end;
```

Beispiel: Wir betrachten die elliptische Kurve $y^2 = x^3 + 5x + 7$ über $\mathbf{F}_p$ mit $p = 10007$. Sei s die Spur des Frobenius. Dann ist $N = E(\mathbf{F}_p) = p + 1 - s$. Der Satz von Hasse liefert die Abschätzung $|s| \leq 2\sqrt{p}$,

also $|s| \leq 200$. Mit dem Schoof-Algorithmus erhalten wir

$$s \equiv 0 \bmod 2, \quad s \equiv 1 \bmod 3, \quad s \equiv 2 \bmod 5, \quad s \equiv 1 \bmod 7, \quad s \equiv 10 \bmod 11,$$

woraus mit dem chinesischen Restsatz folgt

$$s \equiv 2122 \bmod 2310.$$

Die Abschätzung $|s| \leq 200$ zeigt dann, daß nur $s = -188$ möglich ist. Also $\#E(\mathbf{F}_p) = p + 1 - s = 1198$.

Beispiel: Wir betrachten $E : y^2 = x^3 + 5x + 7$ über $\mathbf{F}_p$ mit $p = 10^5 + 3$. Der Schoof-Algorithmus ergibt

$$s \equiv 0 \bmod 2, \quad s \equiv 1 \bmod 3, \quad s \equiv 4 \bmod 5, \quad s \equiv 6 \bmod 7, s \equiv 0 \bmod 11,$$

also

$$s \equiv 2134 \bmod 2310.$$

Der Satz von Hasse liefert $|s| \leq 632$, also bleibt nur die Möglichkeit $s = -176$ und damit

$$\#E(\mathbf{F}_p) = 100180.$$

Beispiel: Wir betrachten $E : y^2 = x^3 + 5x + 7$ über $\mathbf{F}_p$ mit $p = 10^{10} + 19$. Mit dem Schoof-Algorithmus erhält man

$$s \equiv 1 \bmod 2, \quad s \equiv 1 \bmod 3, \quad s \equiv 0 \bmod 5, \quad s \equiv 6 \bmod 7, \quad s \equiv 9 \bmod 11,$$

also

$$s \equiv 1945 \bmod 2310.$$

Der Satz von Hasse liefert $|s| \leq 200000$. Also folgt

$$s = 1945 + 2310i \quad \text{für ein } i \text{ mit } -87 \leq i \leq 85.$$

Wir wählen einen Punkt auf E: $P_1 = (1, 6243000782)$ und berechnen jetzt für $-87 \leq i \leq 85$ den Punkt $(p + 1 - (1945 + 2310i))P_1$. Man findet

$$(p + 1 - (1945 + 2310i))P_1 = O \quad \Longleftrightarrow \quad i = -50.$$

Also folgt für die Spur des Frobenius $s = 1945 - 50 \cdot 2310 = -113555$. Die Gruppenordnung ist dann $\#E(\mathbf{F}_p) = p + 1 - s = 5^2 \cdot 17 \cdot 23529679$. Dieses Beispiel zeigt, wie man mit dem Schoof-Algorithmus Informationen gewinnen kann, die helfen, auf andere Weise weiterzumachen.

Beispiel: Wir betrachten $E : y^2 = x^3 + 5x + 7$ über verschiedenen Körpern $\mathbf{F}_p$. Die Tabelle gibt eine Kongruenz für die Spur s des Frobenius und die Rechenzeiten zur Berechnung modulo 3, 5, 7, 11 mit

obigem Schoof-Algorithmus.

p	$s \equiv$	Zeit $\ell = 3$	$\ell = 5$	$\ell = 7$	$\ell = 11$
$10^{10} + 19$	1945 mod 2310	15”	0.88’	4.03’	30.3’
$10^{11} + 3$	134 mod 210	13”	1.03’	2.28’	
$10^{12} + 39$	118 mod 210	15”	1.20’	5.03’	
$10^{13} + 37$	175 mod 210	17”	0.93’	3.40’	
$10^{14} + 31$	165 mod 210	17”	1.00’	4.90’	
$10^{15} + 37$	30 mod 210	18”	1.10’	3.87’	
$10^{16} + 61$	78 mod 210	20”	1.35’	4.02’	
$10^{17} + 3$	208 mod 210	21”	1.42’	5.02’	
$10^{18} + 3$	183 mod 210	20”	1.50’	4.90’	
$10^{19} + 51$	16 mod 210	21”	1.32’	5.38’	
$10^{20} + 39$	96 mod 2310	23”	1.67’	6.95’	53.42’
$10^{30} + 57$	3 mod 210	35”	2.72’	10.37’	
$10^{40} + 121$	20 mod 210	61”	3.58’	18.25’	
$10^{50} + 151$	204 mod 210	74”	6.37’	22.95’	

Diese Zahlen machen deutlich: das Hauptproblem ist nicht die Größe der Primzahl, sondern die Größe der Polynome ψ_ℓ.

6. Kombination des Schoof-Algorithmus mit anderen Algorithmen

Der Schoof-Algorithmus funktioniert zwar theoretisch gut, praktisch kommt man allerdings nicht allzu weit damit. Man kann aber versuchen, Informationen, die man mit dem Schoof-Algorithmus gewinnt, für andere Algorithmen auszunutzen. In dieser Hinsicht gibt es praktikable Vorschläge von Atkin und Elkies. Wir werden den Schoof-Algorithmus mit einem früher behandelten Algorithmus kombinieren.

Sei $E : y^2 = x^3 + ax + b$ über $\mathbf{F}_p$ gegeben, s die Spur des Frobenius und damit $\#E(\mathbf{F}_p) = p + 1 - s$. Man kann folgendermaßen vorgehen:

- Mit dem Schoof-Algorithmus bestimmt man s_0, L mit $s \equiv s_0 \bmod L$.
- Man wählt einen Punkt $P \in E(\mathbf{F}_p)$ und berechnet die Menge
$$M' = \{p + 1 - (s_0 + Li) : (p + 1 - (s_0 + Li))P = O \text{ und } |s_0 + Li| < 2\sqrt{p}\}.$$
(Die Anzahl der Schritte zur Berechnung von M' ist ungefähr $\frac{4\sqrt{p}}{L}$, während die Berechnung der früheren Menge M ungefähr $4\sqrt{p}$ Schritte braucht.)
- Enthält M' nur ein Element, so ist dies die Gruppenordnung $\#E(\mathbf{F}_p)$ und wir sind fertig.
- Gilt $\#M' \geq 2$, so wählen wir einen neuen Punkt P.

Das folgende Programm *ordnung2.ub* nutzt die Vorgabe einer Kongruenz $s \equiv s_0 \bmod L$ aus:

```
10   print "Fuer die elliptische Kurve y^2=x^3+ax+b ueber F_p soll"
20   print "die Gruppenordnung bestimmt werden, indem die Ordnung"
30   print "von Punkten bestimmt wird. Dazu wird ein Punkt P bestimmt"
40   print "und getestet, welche Zahlen m des Intervalls [p+1-isqrt(4*p),p+1+isqrt(4*p)]"
50   print "mP=O erfuellen. Man kann auch eine Kongruenz fuer die"
60   print "Spur des Frobenius eingeben."
70   input "p,a,b=";P,A,B:X=-1
80   input "s0 mod L: s0,L=";S0,L:clr time
90   Q=P-1:E=0
```

```
100   if Q@2=0 then Q=Q\2:E=E+1:goto 100
110   N=2
120   if kro(N,P)=1 then N=N+1:goto 120
130   Z=modpow(N,Q,P)
140   X=X+1
150   Ae=(X^3+A*X+B)@P
160   if Ae=0 then Y=0:goto 230
170   if kro(Ae,P)=-1 then goto 140
180   Ye=Z:R=E:Y=modpow(Ae,(Q-1)\2,P):Be=(Ae*Y*Y)@P:Y=(Ae*Y)@P
190   if Be@P=1 then goto 230
200   M=1:Bb=(Be*Be)@P
210   if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 210
220   T=modpow(Ye,2^(R-M-1),P):Ye=(T*T)@P:R=M:Y=(Y*T)@P:Be=(Be*Ye)@P:goto 190
230   print "P=(";X;",";Y;")"
240   P0=1:P1=X:P2=Y
250   N=L:U0=P0:U1=P1:U2=P2:gosub 520:LP0=V0:LP1=V1:LP2=V2
260   M=P+1-S0-L*int((2*sqrt(P)-S0)/L):Oo=0:Oz=0
270   N=M:U0=P0:U1=P1:U2=P2:gosub 520:Q0=V0:Q1=V1:Q2=V2
280   if Q0=0 and Q1=0 then Oz=1:Oo=M
290   for I=int((2*sqrt(P)-S0)/L)-1 to -int((2*sqrt(P)+S0)/L) step -1
300   X0=Q0:X1=Q1:X2=Q2:Y0=LP0:Y1=LP1:Y2=LP2:gosub 340:Q0=Z0:Q1=Z1:Q2=Z2
310   if Q0=0 and Q1=0 then Oz=Oz+1:if Oz=1 then Oo=P+1-S0-L*I else print "ord(P) teilt ";P+1-S0-L
320   next I:if Oz=0 then print "Spur stimmt nicht!":goto 80
330   print "Gruppenordnung=";Oo:print "Zeit=";time:goto 70
340   ' Addition (x0:x1:x2)+(y0:y1:y2)=(z0:z1:z2)
350   Z0=(A*X0^2*Y0*Y1-A*X0*X1*Y0^2-X0^2*Y2^2+X2^2*Y0^2+3*X0*X1*Y1^2-3*X1^2*Y0*Y1)@P
360   Z1=(-3*B*X0^2*Y0*Y1+3*B*X0*X1*Y0^2-A*X0^2*Y1^2+A*X1^2*Y0^2-X0*X1*Y2^2+X2^2*Y0*Y1+2*X0*X2*Y1*
370   Z2=(3*B*X0^2*Y0*Y2-3*B*X0*X2*Y0^2+A*X0^2*Y1*Y2-A*X1*X2*Y0^2+2*A*X0*X1*Y0*Y2-2*A*X0*X2*Y0*Y1-
380   if Z0>0 or Z1>0 or Z2>0 then return
390   Z0=(6*B*X0*X2*Y0^2+6*B*X0^2*Y0*Y2+2*A*X1*X2*Y0^2+2*A*X0^2*Y1*Y2+4*A*X0*X2*Y0*Y1+4*A*X0*X1*Y0
400   Z1=(2*A^2*X0*X2*Y0^2+2*A^2*X0^2*Y0*Y2-6*B*X1*X2*Y0^2-6*B*X0^2*Y1*Y2-12*B*X0*X2*Y0*Y1-12*B*X0
410   Z2=(-2*X0^2*Y0^2*A^3-18*X0^2*Y0^2*B^2-6*A*B*X0*X1*Y0^2-6*A*B*X0^2*Y0*Y1-2*A^2*X1^2*Y0^2-2*A^
420   if Z0>0 or Z1>0 or Z2>0 then return
430   Z0=(3*B*X0^2*Y0*Y1-3*B*X0*X1*Y0^2+A*X0^2*Y1^2-A*X1^2*Y0^2+X0*X1*Y2^2-X2^2*Y0*Y1+2*X0*X2*Y1*Y
440   Z1=(A^2*X0^2*Y0*Y1-A^2*X0*X1*Y0^2-3*B*X0^2*Y1^2+3*B*X1^2*Y0^2-A*X0*X1*Y1^2+A*X1^2*Y0*Y1+X1^2
450   Z2=(-A^2*X0^2*Y0*Y2+A^2*X0*X2*Y0^2+3*B*X0^2*Y1*Y2-3*B*X1*X2*Y0^2+6*B*X0*X1*Y0*Y2-6*B*X0*X2*Y
460   return
470   ' Verdopplung eines Punktes 2(x0:x1:x2)=(z0:z1:z2)
480   Z0=(12*B*X0^3*X2+12*A*X1*X2*X0^2+4*X2^3*X0+12*X1^3*X2)@P
490   Z1=(4*A^2*X0^3*X2-36*B*X1*X2*X0^2-12*A*X1^2*X2*X0+4*X2^3*X1)@P
500   Z2=(-2*X0^4*A^3-18*X0^4*B^2-12*A*B*X0^3*X1-12*A^2*X1^2*X0^2+36*B*X1^3*X0+6*A*X1^4+2*X2^4)@P
510   return
520   ' Multiplikation n(u0:u1:u2)=(v0:v1:v2)
530   N1=N:V0=0:V1=0:V2=1
540   while N1>0
550   if N1@2=1 then X0=U0:X1=U1:X2=U2:Y0=V0:Y1=V1:Y2=V2:gosub 340:V0=Z0:V1=Z1:V2=Z2
560   N1=N1\2
570   X0=U0:X1=U1:X2=U2:gosub 470:U0=Z0:U1=Z1:U2=Z2
580   wend
590   return
```

In folgendem Beispiel sind Rechenzeiten angegeben, die veranschaulichen, was man durch Verwendung des Schoof-Algorithmus gewinnt.

Beispiel: Wir betrachten die Kurve $y^2 = x^3 + 5x + 7$ über verschiedenen Körpern $\mathbf{F}_p$. Mit dem Schoof-Algorithmus berechnen wir eine Kongruenz $s \equiv s_0 \bmod 210 = 2 \cdot 3 \cdot 5 \cdot 7$. Dann benutzen wir obiges Verfahren und erhalten folgende Rechenzeiten:

p	$10^{10}+19$	$10^{11}+3$	$10^{12}+39$	$10^{13}+37$	$10^{14}+31$	$10^{15}+37$	$10^{16}+61$	$10^{17}+3$
Zeit	0”	3”	10”	35”	1’51”	6’33”	20’28”	1h6’56”

Verwendete Literatur: [**1**], [**5**], [**10a**], [**11a**]

KAPITEL 14

Hyperelliptische Kryptosysteme

Wir haben einige Public-Key-Kryptosysteme angesprochen, deren Sicherheit darauf beruht, daß es schwierig ist, diskrete Logarithmen in geeignet gewählten Gruppen $\mathbf{F}_q^*$ oder $E(\mathbf{F}_q)$ zu berechnen:

- Schlüsselaustausch nach Diffie-Hellman,
- Massey-Omura-Kryptosystem für Nachrichtenübertragung,
- ElGamal-Kryptosystem,
- Signatur-Verfahren DSA, ECDSA.

Gefahren für solche Systeme gibt es von verschiedenen Seiten:

- Fortschritte in der Computertechnologie führen dazu, daß man immer größere Schlüssellängen braucht. Für die Praxis will man natürlich keine zu großen Schlüssellängen aus Geschwindigkeitsgründen.
- Fortschritte in der Theorie sind gefährlicher, weil sie nicht vorhersagbar sind. Zudem haben elliptische Kurven eine so reichhaltige Struktur, daß es ist nicht klar, wann jemand die nächste Idee zur schnellen Logarithmusberechnung hat, die dazu führt, daß man gewisse Klassen elliptischer Kurven für die Kryptographie ausschließen muß. So haben wir gesehen, daß die Semaev-Reduktion von Logarithmen in $E(\mathbf{F}_p)$ zu einer Division in $\mathbf{F}_p$ führt, was extrem schnell auszuführen ist. Über die Sicherheit solcher Kryptosysteme läßt sich also theoretisch wenig aussagen, sie werden aber praktisch benutzt.

Es ist naheliegend, auch andere Klassen endlicher abelscher Gruppen G auf ihre Tauglichkeit für die Kryptographie hin zu untersuchen. Es gibt zwei wichtige Bedingungen:

- Quadrieren und Multiplizieren sollte schnell möglich sein, so daß man mit der square-and-multiply-Methode schnell Potenzieren kann.
- Es sollten keine schnellen Verfahren zur Logarithmenberechnung bekannt sein.

Wir werden diese Fragen im Bereich der Kurven über einem endlichen Körper anschauen.

Sei C eine (irreduzible nichtsinguläre projektive) Kurve über einem Körper $K = \mathbf{F}_q$ mit Geschlecht $g(C) \geq 2$. Die Kurve C selbst besitzt keine Gruppenstrukur, die mit der algebraischen Struktur verträglich ist. Aber

$$\mathrm{Pic}^0(C) = \{\text{Divisoren vom Grad } 0\}/\{\text{Hauptdivisoren}\}$$

und $\mathrm{Pic}^0_K(C)$ sind in natürlicher Weise Gruppen. Man kann $\mathrm{Pic}^0(C)$ auch mit der Struktur einer g-dimensionalen irreduziblen nichtsingulären projektiven Varietät versehen und erhält dann die sogenannte Jacobische Varietät $\mathrm{Jac}(C)$ von C. Die Frage ist nun: Kann man mit $\mathrm{Pic}^0(C)$ vernünftig rechnen? Genauer:

- Kann man für die Elemente aus $\mathrm{Pic}^0(C)$ bzw. $\mathrm{Pic}^0_K(C)$ gute Repräsentanten finden?
- Kann man die Addition praktisch schnell ausführen?

Wir gehen in ähnlicher Weise wie bei den elliptischen Kurven vor.

Sei $P_0 \in C$ ein festgewählter Punkt und sei E die Menge der effektiven Divisoren vom Grad g, d.h.

$$E = \{P_1 + \cdots + P_g \in \mathrm{Div}(C) : P_1, \ldots, P_g \in C\}.$$

Wir definieren

$$\psi : E \to \mathrm{Pic}^0(C), \quad P_1 + \cdots + P_g \mapsto \text{ Klasse von } (P_1 + \cdots + P_g) - gP_0.$$

LEMMA. *ψ ist surjektiv.*

Beweis: Sei $d \in \mathrm{Pic}^0(C)$ und $D \in \mathrm{Div}^0(C)$ ein Repräsentant von d. Dann ist nach Riemann-Roch

$$\ell(D + gP_0) = \deg(D + gP_0) + 1 - g + \ell(K - D - gP_0) = 1 + \ell(K - D - gP_0) \geq 1,$$

also gibt es eine Funktion f mit $D + gP_0 + (f) \geq 0$. Wegen $\deg(D + gP_0 + (f)) = g$ gibt es also Punkte $P_1, \ldots, P_g \in C$ mit $D + gP_0 + (f) = P_1 + \cdots + P_g$, d.h. $D \sim (P_1 + \cdots + P_g) - gP_0$ und damit $\psi(P_1 + \cdots + P_g) = d$. ■

LEMMA. *$\psi(P_1 + \cdots + P_g) = \psi(Q_1 + \cdots + Q_g)$ gilt genau dann, wenn es Punkte $R_1, \ldots, R_{g-2} \in C$ gibt, so daß $P_1 + \cdots + P_g + R_1 + \cdots + R_{g-2}$ und $Q_1 + \cdots + Q_g + R_1 + \cdots + R_{g-2}$ effektive kanonische Divisoren sind.*

Beweis: Sei $\psi(P_1 + \cdots + P_g) = \psi(Q_1 + \cdots + Q_g)$ mit $P_1 + \cdots + P_g \neq Q_1 + \cdots + Q_g$. Dann gibt es eine Funktion f mit $Q_1 + \cdots + Q_g = P_1 + \cdots + P_g + (f)$, also sind $1, f \in \mathcal{L}(P_1 + \cdots + P_g)$. Wegen

$$\ell(P_1 + \cdots + P_g) = 1 + \ell(K - (P_1 + \cdots + P_g))$$

ist also $\ell(K - (P_1 + \cdots + P_g)) \geq 1$. Es gibt somit eine Funktion g und Punkte $R_1, \ldots, R_{g-2}$ mit

$$K - (P_1 + \cdots + P_g) + (g) = R_1 + \cdots + R_{g-2}.$$

Wegen

$$\begin{aligned} P_1 + \cdots + P_g + R_1 + \cdots + R_{g-2} &= K + (g), \\ Q_1 + \cdots + P_g + R_1 + \cdots + R_{g-2} &= K + (f) + (g) \end{aligned}$$

und der Tatsache, daß Divisoren, die zu kanonischen Divisoren äquivalent sind, ebenfalls kanonisch sind, folgt die Behauptung der einen Richtung. Die Umkehrung folgt daraus, daß kanonische Divisoren linear äquivalent sind. ■

Beispiel: Sei $C \subseteq \mathbf{P}^2$ eine ebene Quartik. C hat Geschlecht 3, die effektiven kanonischen Divisoren sind genau die Geradenschnitte. $\psi(P_1 + P_2 + P_3) = \psi(Q_1 + Q_2 + Q_3)$ gilt also genau dann, wenn es einen Punkt $R \in C$ gibt, so daß $P_1 + P_2 + P_3 + R$ und $Q_1 + Q_2 + Q_3 + R$ Geradenschnitte sind, was sich leicht überprüfen läßt.

Auch im allgemeinen Fall wird für die 'meisten' $D \in E$ gelten $\psi^{-1}(\psi(D)) = \{D\}$, bei den Ausnahmen kommen effektive kanonische Divisoren ins Spiel. Es ist also wichtig, eine gute Beschreibung der effektiven kanonischen Divisoren zu besitzen.

Das nächste Problem ist die Addition in $\mathrm{Pic}^0(C)$. Sind $D_1, D_2 \in E$ gegeben, so muß man ein $D \in E$ bestimmen mit

$$\psi(D_1) + \psi(D_2) = \psi(D).$$

Anders geschrieben: $D_1 - gP_0 + D_2 + gP_0 \sim D - gP_0$ oder

$$D \sim D_1 + D_2 - gP_0.$$

Dies ist ein Riemann-Roch-Problem: Bestimme $\mathcal{L}(D_1 + D_2 - gP_0)$ bzw. einen zu $D_1 + D_2 - gP_0$ linear äquivalenten Divisor. Es gibt zwar effektive Versionen des Satzes von Riemann-Roch, diese sind aber i.a. nicht so gebaut, daß man sie für unsere Zwecke einsetzen könnte. Hier steckt also noch eine Herausforderung für die Theorie.

Wir werden jetzt eine Klasse von Kurven betrachten, bei denen man die obigen Probleme gut lösen kann. Der Einfachkeit halber setzen wir $char(K) \neq 2$ voraus.

DEFINITION. Eine irreduzible nichtsinguläre projektive Kurve C vom Geschlecht $g(C) \geq 2$ heißt hyperelliptisch, wenn es einen Morphismus $\phi : C \to \mathbf{P}^2$ vom Grad 2 gibt.

Ist C hyperelliptisch, so ist $K(C)$ eine quadratische Erweiterung von $K(\mathbf{P}^1) = K(x)$, also kann man schreiben

$$K(C) = K(x,y) \text{ mit einer Relation } y^2 = f(x) \text{ bzw. } K(C) = \mathrm{Quot}(K[x,y]/(y^2 - f(x))).$$

Dabei kann man erreichen, daß $f(x)$ normiert, separabel und vom Grad $2g+1$ ist. Die ebene Kurve $C_0 = \{y^2 = f(x)\} \subseteq \mathbf{P}^2$ ist im Endlichen nichtsingulär, im Unendlichen gibt es genau einen Punkt $\infty = (0:0:1)$, der allerdings singulär ist. Der Morphismus

$$\varphi : C \to C_0 \text{ mit } \varphi = (1 : x : y)$$

ist nun bijektiv, ja sogar ein Isomorphismus außerhalb von $\varphi^{-1}(\infty)$ bzw. ∞. Wir können also auf C_0 rechnen, wobei man mit ∞ etwas vorsichtig sein muß. Wir denken uns also

$$C = \{(x,y) : y^2 = f(x)\} \cup \{\infty\}.$$

Hier sind einige Eigenschaften:

- Sei $P = (u,v) \in C$. Ist $v \neq 0$, so ist $x - u$ uniformisierend in P, ist $v = 0$, so ist y uniformisierend. Damit sieht man leicht
$$\sum_{P \neq \infty} v_P(x) = 2 \quad \text{und} \quad \sum_{P \neq \infty} v_P(y) = 2g+1,$$
was schließlich
$$v_\infty(x) = -2 \quad \text{und} \quad v_\infty(y) = -(2g+1)$$
liefert, also ist $\frac{x^g}{y}$ uniformisierend in ∞.
- Es gibt einen Automorphismus $\sigma : C \to C$ mit $\sigma(x,y) = (x,-y)$. Dies nennt man auch die hyperelliptische Involution.
- Man kann zeigen, daß sich alle effektiven kanonischen Divisoren in der Form
$$\sum_{i=1}^{g-1} (P_i + \sigma P_i)$$
schreiben lassen, wobei $P_1, \ldots, P_{g-1}$ Punkte auf C sind.

Wir wollen jetzt eine Normalform für die Divisoren vom Grad 0 auf C herleiten. Als Basispunkt wählen wir ∞. Für $P = (u,v)$ gilt

$$P + \sigma P = (x-u) + 2\infty, \quad \text{d.h.} \quad P + \sigma P - 2\infty \sim 0.$$

Mit den vorstehenden Überlegungen läßt sich dann jede Klasse in $\mathrm{Pic}^0(C)$ eindeutig durch einen Divisor

$$D = \sum m_i P_i - (\sum m_i)\infty$$

darstellen, der folgende Bedingungen erfüllt:

- $m_i \geq 0$.
- Ist $P_i = \sigma P_i$, so ist $m_i \leq 1$.
- Ist $P_i \neq \sigma P_i$, so ist $\sigma P_i \neq P_j$ für alle j.
- $\sum m_i \leq g$.

Ein Divisor mit diesen Eigenschaft heißt reduziert.

Ein reduzierter Divisor $D = \sum m_i P_i - (\sum m_i)\infty$ mit $P_i = (u_i, v_i)$ kann auch in folgender Weise durch ein Paar von Polynomen $[a(x), b(x)]$ beschrieben werden:

- Sei $a(x) = \prod (x - u_i)^{m_i}$ (mit $\deg a(x) \leq g$).
- Sei $b(x)$ ein Polynom mit den Eigenschaften
$$\deg b(x) < \deg a(x), \qquad b(u_i) = v_i \quad \text{und} \quad b(x)^2 - f(x) \equiv 0 \bmod a(x).$$
(Ist $a(x)$ separabel, so folgt die dritte Eigenschaft aus der zweiten.)

Umgekehrt liefert jedes solche Paar von Polynomen einen reduzierten Divisor. Man kann dann schreiben:

$$\mathrm{Pic}^0_K(C) \simeq \{[a(x), b(x)] : a, b \in K[x], \deg b < \deg a \leq g, a \text{ normiert }, a(x) | b(x)^2 - f(x)\}.$$

Mit dieser Darstellung ist es nicht schwer, ein Additionsgesetz für reduzierte Divisoren herzuleiten. Die obige Darstellung besitzt nämlich ein Analogon zur Darstellung von Idealklassen in imaginärquadratischen Zahlkörpern. Man überträgt jetzt einfach die im zahlentheoretischen Fall bekannten Algorithmen auf den vorliegenden Fall. Wir führen dies nicht weiter aus. Das nachfolgende Programm nach Algorithmen von Koblitz [**4**] macht genau das:

Das Maple-Programm *hypell*:

```
# Rechnen auf der Jacobischen einer hyperelliptischen Kurven y^2=f(x)
# vom Geschlecht g ueber F_p --- p, f, g sind vorzugeben.

# Reduktion von Divisoren
red:=proc(D)
a:=D[1]; b:=D[2];
while degree(a,x)>g do
  aa:=Quo(f-b^2,a,x) mod p;
  bb:=Rem(-b,aa,x) mod p;
  a:=aa; b:=bb;
od;
a:=(a/lcoeff(a,x)) mod p;
[a,b];
end;

# Addition zweier Divisoren
add:=proc(D1,D2)
a1:=D1[1]; b1:=D1[2]; a2:=D2[1]; b2:=D2[2];
d1:=Gcdex(a1,a2,x,'e1','e2') mod p;
d:=Gcdex(d1,b1+b2,x,'c1','c2') mod p;
s1:=(c1*e1) mod p; s2:=(c1*e2) mod p; s3:=c2;
d:=(s1*a1+s2*a2+s3*(b1+b2)) mod p;
a:=Quo(a1*a2,d^2,x) mod p;
b:=Rem(Quo(s1*a1*b2+s2*a2*b1+s3*(b1*b2+f),d,x) mod p,a,x) mod p;
red([a,b]);
end;

# Multiplikation
mult:=proc(m,D)
Dy:=[1,0]; Dz:=D; n:=m;
while n>0 do
  if n mod 2=1 then Dy:=add(Dz,Dy); fi;
  n:=trunc(n/2);
  Dz:=add(Dz,Dz);
od;
Dy;
end;
```

Beispiel: Wir betrachten die durch $y^2 = x^5 + x + 1$ über $\mathbf{F}_p$, $p = 101$, definierte hyperelliptische Kurve C vom Geschlecht 2. Durch explizites Rechnen findet man

$$\#C(\mathbf{F}_p) = 104 \quad \text{und} \quad \#C(\mathbf{F}_{p^2}) = 10250.$$

Damit kann man das Zählerpolynom $P(T)$ der Zeta-Funktion $Z(C/\mathbf{F}_p, T) = \frac{P(T)}{(1-T)(1+pT)}$ berechnen (siehe [**4**]) und erhält

$$P(T) = 1 + 2T + 26T^2 + 202T^3 + 10201T^4.$$

Nun ist

$$\#\mathrm{Pic}^0_{\mathbf{F}_p}(C) = P(1) = 10432 = 2^6 \cdot 163.$$

Der Punkt $(17, 44) \in C(\mathbf{F}_p)$ liefert den Divisor $(17, 44) - \infty \simeq [x - 17, 44]$. Dann ist

$$163((17, 44) - \infty) \simeq 163 \cdot [x - 17, 44] = [(x - 40)(x - 65), 50x + 42] \simeq (40, 22) + (65, 60) - 2\infty.$$

Auch $[x^2+77x+91, 5]$ repräsentiert einen reduzierten Divisor, und zwar von Ordnung $2^3 \cdot 163$ in $\mathrm{Pic}^0_{\mathbf{F}_p}(C)$.

Bemerkung: Am Institut für Experimentelle Mathematik in Essen wurde (1995?) von U. Krieger ein Signaturverfahren *signature.c* programmiert, das in $\mathrm{Pic}^0(C)$ der hyperelliptischen Kurve

$$C : y^2 = x^5 - 140x^3 + 240x^2 + 3810x - 6928$$

vom Geschlecht 2 über $\mathbf{F}_p$ mit

$$p = 153946287550700989943 \approx 1.5 \cdot 10^{20}$$

arbeitet, und zwar in einer Untergruppe der (primen) Ordnung

$$N = 59248648645708686479341865505391744126 79 \approx 5.9 \cdot 10^{39}.$$

Folgende Divisoren sind in dieser Untergruppe:

$$\begin{aligned} D_1 &= (9, 8485222533513363208) - \infty \simeq [x - 9, 8485222533513363208], \\ D_2 &= (10, 76034844529428485443) - \infty \simeq [x - 10, 76034844529428485443]. \end{aligned}$$

Was ist z.B $\log_{D_1} D_2$?

Literatur: [**4**], [**1a**].

Literaturverzeichnis

[1] H. Cohen, A Course in Computational Algebraic Number Theory, Springer 1993.

[1a] G. Frey, Tran van Trung, Proceedings der Tagung: Datensicherheit in Netzen und Einsatz von Chipkarten, Institut für Experimentelle Mathematik, Universität GH Essen, Preprint **19** (1995).

[2] W. Fulton, Algebraic Curves, Benjamin/Cummings 1969.

[2a] R. Hartshorne, Algebraic Geometry, Springer 1977.

[2b] D. Husemöller, Elliptic Curves, Springer 1987.

[3] N. Koblitz, A Course in Number Theory and Cryptography, Second Edition, Springer 1994.

[4] N. Koblitz, Algebraic Aspects of Cryptography, Springer 1998.

[5] H. W. Lenstra, Jr., Elliptic Curves and Number-Theoretic Algorithms, Proceedings of the International Congress of Mathematics, Berkeley, California, USA, 1986, 99–120.

[5a] K. S. McKurley, The Discrete Logarithm Problem, in Cryptology and Computational Number Theory, Proceedings of Symposia in Applied Mathematics **42**, 1990, 49–74.

[6] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Acad. Publ. 1993.

[7] Menezes, Okamoto, Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory **39** (1993), 1639–1646.

[8] Pollard, Monte Carlo methods for index computations mod p, Math. Comp. **32** (1978), 918–924.

[8a] H. Riesel, Prime Numbers and Computer Methods for Factorization, Birkhäuser 1985.

[9] H.-G. Rück, On the Discrete Logarithm in the Divisor Class Group of Curves, preprint, 1997.

[10] W. Ruppert, Elliptische Kurven, Vorlesungsskript, Sommersemester 1992, Universität Erlangen.

[10a] W. Ruppert, Diophantische Geometrie, Vorlesungsskript, Wintersemester 1995/96, Universität Erlangen.

[11] B. Schneier, Angewandte Kryptographie, Addison-Wesley 1996.

[11a] R. Schoof, Counting points elliptic curves over finite fields, Journal de Théorie des Nombres de Bordeaux **7** (1995), 219–254.

[12] I. A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, Math. Comp. **67** (1998), 353–356.

[13] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer 1986.