Diophantische Approximationen und Diophantische Gleichungen

Wolfgang M. Ruppert

Sommersemester 1993

29. Juli 1997[1]

[1] Im Sommersemester 1993 am Mathematischen Institut der Universität Erlangen-Nürnberg abgehaltene Vorlesung

Inhaltsverzeichnis

KAPITEL 1

Kettenbrüche

Ein Kettenbruch ist ein Ausdruck der Form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Man schreibt dafür auch

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots$$

oder

$$[a_0, a_1, a_2, a_3, \ldots].$$

Eine Kettenbruchentwicklung einer reellen Zahl kann man durch Iteration der Bildung $\alpha = \lfloor \alpha \rfloor + \frac{1}{\beta}$ gewinnen.

Beispiele:

- $$\frac{7}{5} = 1 + \cfrac{1}{2 + \frac{1}{2}}$$
- $$\frac{21}{13} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}}$$
- $$1 + \sqrt{2} = 2 + \frac{1}{1 + \sqrt{2}},$$

  woraus sich ergibt

  $$1 + \sqrt{2} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

  und daher auch

  $$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

- $\sqrt[3]{2} = [1; 3, 1, 5, 1, 1, 4, 1, 1, 8, \ldots]$
- $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, \ldots]$
- $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$

Wir denken uns zunächst die a_i's als Unbestimmte. Es gilt:

$$[a_0, \ldots, a_n] = [a_0, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}] \text{ und } [a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]}.$$

SATZ 1. *Definiert man*

$$p_0 = a_0, p_1 = a_1 a_0 + 1, p_n = a_n p_{n-1} + p_{n-2} (n \geq 2),$$

$$q_0 = 1, q_1 = a_1, q_n = a_n q_{n-1} + q_{n-2} (n \geq 2),$$

so gilt

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n].$$

Die a_i's heißen Teilquotienten, die $\frac{p_n}{q_n}$ Näherungsbrüche.

Beweis: durch Induktion, etc.

$$[a_0,\ldots,a_n]=[a_0,\ldots,a_{n-2},a_{n-1}+\frac{1}{a_n}]=\frac{(a_{n-1}+\frac{1}{a_n})p_{n-2}+p_{n-3}}{(a_{n-1}+\frac{1}{a_n})q_{n-2}+q_{n-3}}=\cdots=\frac{p_n}{q_n}$$

■

SATZ 2. *Es gilt:*

$$p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}\ \textit{d.h.}\ \frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^{n-1}}{q_{n-1}q_n}$$

und

$$p_nq_{n-2}-p_{n-2}q_n=(-1)^na_n\ \textit{d.h.}\ \frac{p_n}{q_n}-\frac{p_{n-2}}{q_{n-2}}=\frac{(-1)^na_n}{q_{n-2}q_n}$$

Beweis: mit obiger Formel und Induktion. ■

FOLGERUNG 1. *Sind die a_i's reell und $a_i>0$ für $i\geq 1$, so hat man*

$$\frac{p_0}{q_0}<\frac{p_2}{q_2}<\frac{p_4}{q_4}<\cdots<\frac{p_5}{q_5}<\frac{p_3}{q_3}<\frac{p_1}{q_1}.$$

Beweis: Durch Induktion sieht man $q_n>0$, der Rest folgt unmittelbar. ■

Wir betrachten jetzt die Kettenbruchentwicklungen reeller Zahlen. Sei α reell. Ist α nicht ganz, so können wir schreiben

$$\alpha=a_0+\frac{1}{\alpha_1}$$

mit $a_0\in\mathbf{Z}$ und $\alpha_1>1$ reell. So kann man induktiv weitermachen: Ist α_n keine ganze Zahl, so kann man schreiben

$$\alpha_n=a_n+\frac{1}{\alpha_{n+1}}$$

mit $a_n=\lfloor\alpha_n\rfloor$.

Kettenbruchentwicklungen rationaler Zahlen: Bricht der Kettenbruchalgorithmus ab, so ist natürlich α eine rationale Zahl. Sei umgekehrt α eine rationale Zahl. Ist $\alpha_n=\frac{a}{b}$, so ist $\alpha_n-a_n=\frac{c}{b}$ mit $0\leq c<b$, also $\alpha_{n+1}=\frac{b}{c}$. Insbesondere ist

$$\text{Nenner}(\alpha_{n+1})<\text{Nenner}(\alpha_n),$$

also muß irgendein α_m Nenner 1 haben, d.h. es ist ganzzahlig und damit bricht das Verfahren ab. Die endlichen Kettenbrüche gehören also genau zu den rationalen Zahlen.

Wir nehmen jetzt an, α ist eine irationale reelle Zahl. Dann haben wir dazu die Folge der Teilquotienten $a_i\in\mathbf{Z}$ mit $a_i\geq 1$ für $i\geq 1$. Außerdem ist $a_n<\alpha_n<a_n+1$.

SATZ 3. *Für eine irrationale reelle Zahl α gelten die Eigenschaften:*

1. $1=q_0\leq q_1<q_2<q_3<\ldots$ *und* $q_n\geq n$.
2. *Die Näherungsbrüche $\frac{p_n}{q_n}$ sind gekürzt.*
3. $$\frac{p_0}{q_0}<\frac{p_2}{q_2}<\cdots<\alpha<\cdots<\frac{p_3}{q_3}<\frac{p_1}{q_1}$$
4. $$\frac{1}{2q_nq_{n+1}}<\frac{1}{q_n(q_{n+1}+q_n)}<\left|\alpha-\frac{p_n}{q_n}\right|<\frac{1}{q_nq_{n+1}}$$
5. $$\left|\alpha-\frac{p_n}{q_n}\right|<\frac{1}{q_n^2}$$
6. $$\alpha=\lim\frac{p_n}{q_n}=[a_0,a_1,a_2,\ldots]$$

Beweis:

1. Es ist $q_0 = 1$, $q_1 = a_1 \geq 1$ und für $n \geq 2$
$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} > q_{n-1}.$$
2. Klar!
3. Wir haben die Darstellung
$$\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$$
und damit
$$\alpha = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}.$$
Daraus folgt
$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\alpha_{n+1} q_n + q_{n-1}}$$
Daraus folgt die Eigenschaft 3. Nun ist
$$\alpha_{n+1} q_n + q_{n-1} > a_{n+1} q_n + q_{n-1} = q_{n+1}$$
und
$$\alpha_{n+1} q_n + q_{n-1} < (a_{n+1} + 1) q_n + q_{n-1} = q_{n+1} + q_n$$
Daraus folgt die Eigenschaft 4. Der Rest ist klar. ■

Mit dem Kettenbruchalgorithmus erhält man also gute Approximationen an Irrationalzahlen.

FOLGERUNG 2. *Ist α irrational reell, so gibt es unendlich viele Brüche $\frac{p}{q}$ mit*
$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}.$$

Bemerkung: Ist α reell und q eine natürliche Zahl, so gibt es eine ganze Zahl m mit
$$\frac{m}{q} \leq \alpha < \frac{m+1}{q}.$$
Setzt man dann $p = m$ bzw. $p = m + 1$, so erhält man
$$|\alpha - \frac{p}{q}| < \frac{1}{2q}.$$
Ist q eine 10-er Potenz, so hat man die Approximation durch Dezimalbrüche. Die Kettenbruchapproximation ist aber wesentlich besser.

Bemerkung: Ist $\alpha = \frac{a}{b}$ rational, so folgt aus
$$0 < |\alpha - \frac{p}{q}| < \frac{1}{q^2}$$
sofort $q < b$, d.h. obige Folgerung gilt nicht: rationale Zahlen lassen sich nicht besonders gut approximieren.

Beispiel: $\pi = [3, 7, 15, 1, 292, \ldots]$ hat die Näherungsbrüche
$$\begin{aligned}
\frac{p_0}{q_0} = 3 &= 3.0000000000\ldots \\
\frac{p_1}{q_1} = \frac{22}{7} &= 3.1428571428\ldots \\
\frac{p_2}{q_2} = \frac{333}{106} &= 3.1415094339\ldots \\
\frac{p_3}{q_3} = \frac{355}{113} &= 3.1415929203\ldots \\
\frac{p_4}{q_4} = \frac{103993}{33102} &= 3.1415926530\ldots \\
\pi &= 3.1415926535\ldots
\end{aligned}$$

SATZ 4. *Von zwei aufeinanderfolgenden Näherungsbrüchen an die irrationale reelle Zahl α genügt zumindest eine der Ungleichung*

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}.$$

Beweis: Wir nehmen an, $|\alpha - \frac{p_{n-1}}{q_{n-1}}| \geq \frac{1}{2q_{n-1}^2}$ und $|\alpha - \frac{p_n}{q_n}| \geq \frac{1}{q_n^2}$. Dann gilt:

$$\frac{1}{q_{n-1}q_n} = |\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}| \geq \frac{1}{2q_{n-1}^2} + \frac{1}{2q_n^2},$$

was sofort $q_{n-1} = q_n$ impliziert, also notwendig $n = 1$ und $q_0 = q_1 = a_1 = 1$, also $q_2 = 2$ und damit

$$|\alpha - \frac{p_1}{q_1}| < \frac{1}{q_1 q_2} = \frac{1}{2q_1},$$

ein Widerspruch zu unserer Annahme. ■

Der folgende Satz gibt eine Umkehrung dieser Aussage:

SATZ 5. *Ist α irrational mit $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$, so gibt es ein n mit*

$$\frac{a}{b} = \frac{p_n}{q_n},$$

d.h. $\frac{a}{b}$ ist ein Näherungsbruch.

Beweis: Wir nehmen an, $\frac{a}{b}$ liegt zwischen $\frac{p_{n-1}}{q_{n-1}}$ und $\frac{p_{n+1}}{q_{n+1}}$ und ist von beiden Zahlen verschieden. Dann gilt zunächst:

$$\frac{1}{bq_{n-1}} \leq |\frac{a}{b} - \frac{p_{n-1}}{q_{n-1}}| < |\alpha - \frac{p_{n-1}}{q_{n-1}}| < \frac{1}{q_{n-1}q_n},$$

also $q_n < b$. Andererseits ist

$$\frac{1}{bq_{n+1}} \leq |\frac{a}{b} - \frac{p_{n+1}}{q_{n+1}}| < |\alpha - \frac{a}{b}| < \frac{1}{2b^2},$$

also $\frac{1}{q_{n+1}} < \frac{1}{2b}$. Damit gilt:

$$\frac{1}{bq_n} \leq |\frac{p_n}{q_n} - \frac{a}{b}| \leq |\alpha - \frac{p_n}{q_n}| + |\alpha - \frac{a}{b}| < \frac{1}{q_n q_{n+1}} + \frac{1}{2b^2} < \frac{1}{2bq_n} + \frac{1}{2b^2},$$

woraus sofort $b < q_n$ folgt, ein Widerspruch zu oben hergeleiteter Aussage.
Zwei Fälle haben wir noch nicht behandelt: $\frac{a}{b} < \frac{p_0}{q_0}$ und $\frac{p_1}{q_1} < \frac{a}{b}$.

- Der Fall $\frac{a}{b} < \frac{p_0}{q_0} = a_0$. Der Abstand von $\frac{a}{b}$ zu $\frac{p_0}{q_0}$ ist mindestens $\frac{1}{b}$, aber

  $$|\frac{a}{b} - \frac{p_0}{q_0}| < |\alpha - \frac{a}{b}| < \frac{1}{2b^2},$$

  was einen Widerspruch gibt.
- $\alpha < \frac{p_1}{q_1} < \frac{a}{b}$. Also ist

  $$\frac{1}{bq_1} < \frac{1}{2b^2},$$

  d.h. $\frac{1}{q_1} < \frac{1}{2b}$. Damit erhält man

  $$\frac{1}{b} \leq |\frac{p_0}{q_0} - \frac{a}{b}| < \frac{1}{q_0 q_1} + \frac{1}{2b^2} < \frac{1}{2b} + \frac{1}{2b^2},$$

  was sofort $b < 1$, also einen Widerspruch liefert.

■

SATZ 6. *Ist α irrational reell, so erfüllt mindestens einer von drei aufeinanderfolgenden Näherungsbrüchen $\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ die Ungleichung*

$$|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}.$$

Beweis: Angenommen, dies wäre nicht der Fall. Dann gilt:

$$\frac{1}{q_n q_{n+1}} = |\alpha - \frac{p_n}{q_n}| + |\alpha - \frac{p_{n+1}}{q_{n+1}}| \geq \frac{1}{\sqrt{5}q_n^2} + \frac{1}{\sqrt{5}q_{n+1}^2},$$

da die beiden Näherungsbrüche auf verschiedenen Seiten von α liegen, und dies liefert sofort

$$|q_{n+1} - \frac{\sqrt{5}}{2}q_n| \leq \frac{1}{2}q_n,$$

also

$$\frac{q_{n+1}}{q_n} \leq \frac{1+\sqrt{5}}{2}.$$

Genauso findet man

$$\frac{q_n}{q_{n-1}} \leq \frac{1+\sqrt{5}}{2}.$$

Nun ist

$$1 + \frac{q_{n-1}}{q_n} = \frac{q_n + q_{n-1}}{q_n} \leq \frac{a_{n+1}q_n + q_{n-1}}{q_n} = \frac{q_{n+1}}{q_n} \leq \frac{1+\sqrt{5}}{2},$$

also

$$\frac{q_{n-1}}{q_n} \leq \frac{\sqrt{5}-1}{2}.$$

Natürlich hat man hier ein striktes Ungleichheitszeichen, also

$$1 = \frac{q_n}{q_{n-1}} \cdot \frac{q_{n-1}}{q_n} < \frac{\sqrt{5}+1}{2}\frac{\sqrt{5}-1}{2} = 1,$$

ein Widerspruch. Also ist die Annahme falsch und die Behauptung folgt. ■

Wir wollen jetzt an einem Beispiel zeigen, daß obiger Satz optimal ist, wenn man alle irrationalen reellen Zahlen betrachtet.

Beispiel: Sei $\alpha = \frac{\sqrt{5}-1}{2}$. α genügt der Gleichung $f = x^2 + x - 1 = 0$. Sei $\frac{b_n}{c_n}$ eine Folge rationaler Zahlen mit

$$|\alpha - \frac{b_n}{c_n}| < \frac{1}{Ac_n^2}$$

für alle n. Nach dem Mittelwertsatz der Differentialrechnung gibt es ein ξ_n zwischen α und $\frac{b_n}{c_n}$ mit

$$\frac{f(\alpha) - f(\frac{b_n}{c_n})}{\alpha - \frac{b_n}{c_n}} = f'(\xi_n),$$

also

$$\frac{1}{c_n^2} \leq |\alpha - \frac{b_n}{c_n}||2\xi_n + 1| \leq \frac{1}{Ac_n^2}|2\xi_n + 1|,$$

d.h.

$$A \leq |2\xi_n + 1|.$$

Wegen $\lim \xi_n = \alpha$ folgt

$$A \leq \sqrt{5},$$

d.h. die Zahl $\sqrt{5}$ in obigem Satz ist wirklich optimal.

Beispiele: In den folgenden Beispielen vergleichen wir numerisch für die ersten Näherungsbrüche $\frac{p_n}{q_n}$ die Zahlen $q_n^2|\alpha - \frac{p_n}{q_n}|$ mit $\frac{1}{\sqrt{5}} = 0.447....$

- $\alpha = \pi$

$\frac{p_n}{q_n}$	$q_n^2 \lvert \pi - \frac{p_n}{q_n} \rvert$
3	$0.141...$
$\frac{22}{7}$	$0.061...$
$\frac{333}{106}$	$0.935...$
$\frac{355}{113}$	$0.003...$
$\frac{103993}{33102}$	$0.633...$
$\frac{104348}{33215}$	$0.365...$
$\frac{208341}{66317}$	$0.538...$
$\frac{312689}{99532}$	$0.288...$
$\frac{833719}{265381}$	$0.613...$

- Die Folge der entsprechenden Zahlen für $\alpha = e$:

$$0.718, 0.282, 0.465, 0.507, 0.196, 0.479, 0.507,$$
$$0.141, 0.488, 0.504, 0.110, 0.493, 0.502, 0.091, 0.495$$

KAPITEL 2

Die Pellsche Gleichung und quadratische Irrationalitäten

Zur Motivation betrachten wir folgendes

Beispiel: Bestimme die ganzzahligen Lösungen $x, y \in \mathbf{Z}$ der Pellschen Gleichung

$$x^2 - 13y^2 = 1.$$

- Auf den ersten Blick sieht man die trivialen Lösungen $\pm(1,0)$. Wir beschränken uns im folgenden also auf den Fall $y \neq 0$.
- Geometrisch hat man eine Hyperbel vor sich. Die Frage ist, wo diese das Gitter $\mathbf{Z}^2$ schneidet. Es gibt zwei Asymptoten:
$$x = \pm\sqrt{13}y.$$
- Eine Lösung (x,y) mit $y \neq 0$ liefert also eine Näherung $\frac{x}{y}$ für $\sqrt{13}$. Hat das etwas mit Kettenbrüchen zu tun?
- Sei (x,y) eine Lösung und o.E. $x, y > 0$. Dann gilt:
$$|\sqrt{13} - \frac{x}{y}| = \frac{1}{y(x+\sqrt{13}y)} < \frac{1}{\sqrt{13}y^2} < \frac{1}{2y^2},$$
also ist $\frac{x}{y}$ ein Näherungsbruch für $\sqrt{13}$.
- Wir berechnen numerisch die Kettenbruchentwicklung von $\sqrt{13}$ und dazu $p_n^2 - 13q_n^2$:

a_n	p_n	q_n	$p_n^2 - 13q_n^2$
3	3	1	-4
1	4	1	3
1	7	2	-3
1	11	3	4
1	18	5	-1
6	119	33	4
1	137	38	-3
1	256	71	3
1	393	109	-4
1	649	180	1
6	4287	1189	-4

- Also haben wir zumindest eine nichttriviale Lösung gefunden: $(649, 180)$.
- Wie findet man nun die weiteren Lösungen der Pellschen Gleichung. Kann man von vorneherein etwas über die Kettenbruchentwicklung von $\sqrt{13}$ sagen? Ist sie periodisch?

Im folgenden verstehen wir unter einer *reellquadratischen Zahl* α eine reelle Zahl α, die einer quadratischen Gleichung

$$A\alpha^2 + B\alpha + C = 0$$

genügt mit $A, B, C \in \mathbf{Z}$, nicht alle gleich 0.

SATZ 7. *Ist*

$$\alpha = [a_0, a_1, \ldots, a_{r-1}, \overline{a_r, \ldots, a_{r+k-1}}],$$

so ist α reellquadratisch.

Beweis:

- Wir betrachten zunächst den Fall, daß die Kettenbruchentwicklung rein periodisch ist:

$$\alpha = [\overline{a_0, \ldots, a_{k-1}}].$$

Dann ist

$$\alpha = \frac{\alpha p_{k-1} + p_{k-2}}{\alpha q_{k-1} + q_{k-2}},$$

also

$$q_{k-1}\alpha^2 + (q_{k-2} - p_{k-1})\alpha - p_{k-2} = 0,$$

woraus sofort die Behauptung folgt.

- Im allgemeinen ist

$$\alpha = [a_0, a_1, \ldots, a_{r-1}, \overline{a_r, \ldots, a_{r+k-1}}],$$

also ist

$$\beta = [\overline{a_r, \ldots, a_{r+k-1}}]$$

reellquadratisch und wegen

$$\alpha = \frac{\beta p_{r-1} + p_{r-2}}{\beta q_{r-1} + q_{r-2}}$$

ist $\alpha \in \mathbf{Q}(\beta)$, also auch reellquadratisch, da es nicht rational sein kann. ■

Beispiel: Der einfachste Fall einer periodischen Kettenbruchentwicklung ist der Fall

$$\alpha = [m, m, m, \ldots]$$

mit einer natürlichen Zahl m. Dann ist also $\alpha = m + \frac{1}{\alpha}$. Aufgelöst also

$$\alpha = \frac{m + \sqrt{m^2 + 4}}{2}.$$

Für $m = 1, 2, 3, 4, 5, 6$ erhält man explizit

$$\frac{1+\sqrt{5}}{2}, 1+\sqrt{2}, \frac{3+\sqrt{13}}{2}, 2+\sqrt{5}, \frac{5+\sqrt{29}}{2}, 3+\sqrt{10}.$$

Wir wollen uns jetzt mit der Umkehrung des Satzes beschäftigen.

LEMMA 1. *Jede reelle quadratische Zahl α läßt sich schreiben in der Form*

$$\frac{b + \sqrt{d}}{c} \text{ mit } c | b^2 - d.$$

Beweis: α genügt einer Gleichung $A\alpha^2 + B\alpha + C = 0$ mit $A, B, C \in \mathbf{Z}$. Dann ist

$$\alpha = \frac{-B + \sqrt{B^2 - 4AC}}{2A} \text{ oder } \alpha = \frac{B + \sqrt{B^2 - 4AC}}{-2A}$$

und offensichtlich teilt $\pm 2A$ die Zahl $(\pm B)^2 - (B^2 - 4AC)$. ■

LEMMA 2. *Ist $\alpha = \frac{b+\sqrt{d}}{c}$ eine reellquadratische Zahl mit $c | b^2 - d$, so ergibt sich die Kettenbruchentwicklung rekursiv aus*

$$a_n = \lfloor \alpha_n \rfloor, \quad b_{n+1} = a_n c_n - b_n, \quad c_{n+1} = \frac{d - b_{n+1}^2}{c_n}, \quad \alpha_{n+1} = \frac{b_{n+1} + \sqrt{d}}{c_{n+1}}$$

und man hat wieder $c_{n+1} | b_{n+1}^2 - d$.

Beweis: Natürlich muß man setzen $a_n = \lfloor \alpha_n \rfloor$. Da nun $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$, folgt

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{c_n}{(b_n - a_n c_n) + \sqrt{d}} = \frac{c_n(b_{n+1} + \sqrt{d})}{d - b_{n+1}^2} = \frac{b_{n+1} + \sqrt{d}}{\frac{d - b_{n+1}^2}{c_n}}.$$

Nun ist nach Voraussetzung $\frac{d - b_{n+1}^2}{c_n}$ eine ganze Zahl, die wir c_{n+1} setzen; natürlich gilt $c_{n+1} | b_{n+1}^2 - d$. ■

Wir wissen nun

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}.$$

Lösen wir dies nach α_n auf, so erhalten wir

$$\alpha_n = -\frac{q_{n-2}}{q_{n-1}} \frac{\alpha - \frac{p_{n-2}}{q_{n-2}}}{\alpha - \frac{p_{n-1}}{q_{n-1}}}.$$

Übergang zu den Konjugierten ergibt

$$\alpha_n' = -\frac{q_{n-2}}{q_{n-1}} \frac{\alpha' - \frac{p_{n-2}}{q_{n-2}}}{\alpha' - \frac{p_{n-1}}{q_{n-1}}}.$$

Für hinreichend großes n ist also

$$\alpha_n' < 0.$$

Weiter rechnet man nach

$$q_{n-1}(\alpha_n' + 1) - (q_{n-1} - q_{n-2}) = \frac{(-1)^n}{\alpha' q_{n-1} - p_{n-1}},$$

also

$$\alpha_n' + 1 = \frac{1}{q_n - 1}[(q_{n-1} - q_{n-2}) + \frac{(-1)^n}{q_{n-1}(\alpha' - \frac{p_{n-1}}{q_{n-1}})}].$$

Daraus sieht man, daß fUr große n gilt: $\alpha_n' > -1$, also haben wir insgesamt für große n:

$$-1 < \alpha_n' < 0 < 1 < \alpha_n.$$

DEFINITION 1. *Ein reellquadratisches α heißt reduziert, falls gilt*

$$-1 < \alpha' < 0 \text{ und } \alpha > 1.$$

LEMMA 3. *Sei $\alpha = \frac{b+\sqrt{d}}{c}$ mit $c|b^2 - d$. Dann ist α genau dann reduziert, wenn gilt:*

$$1 \leq b < \sqrt{d} \text{ und } \sqrt{d} - b < c < \sqrt{d} + b.$$

Insbesonder ist $1 \leq c < 2\sqrt{d}$.

Beweis: Wir nehmen an, daß α reduziert ist, d.h.

$$-1 < \alpha' < 0 < 1 < \alpha.$$

Aus $\alpha' < \alpha$ folgt zunächst $c \geq 1$. Aus $1 < \alpha - \alpha' = \frac{2\sqrt{d}}{c}$ folgt $c < 2\sqrt{d}$. Aus $0 < \alpha + \alpha' = \frac{2b}{c}$ folgt $b \geq 1$ und aus $0 > \alpha' = \frac{b-\sqrt{d}}{c}$ dann $b < \sqrt{d}$. Unter diesen Bedingungen sieht man nun sofort das Kriterium für Reduziertheit. ■

Ist

$$\mathcal{R}(d) = \{\alpha = \frac{b + \sqrt{d}}{c} : c|b^2 - d \text{ und } \alpha \text{ reduziert}\},$$

so haben wir gerade gesehen:

FOLGERUNG 3. *$\mathcal{R}(d)$ ist endlich.*

LEMMA 4.
1. *Der Nachfolger einer reduzierten Zahl in der Kettenbruchentwicklung ist wieder reduziert.*
2. *Es gibt nur einen möglichen reduzierten Vorgänger in der Kettenbruchentwicklung einer reduzierten Zahl.*

Beweis:

1. Wir haben $\alpha = a + \frac{1}{\beta}$ mit $\beta > 1$. Außerdem $\beta = \frac{1}{\alpha - a}$ und daher $\beta' = \frac{1}{\alpha' - a}$. Daraus ersieht man sofort $-1 < \beta' < 0$, also ist β reduziert.

2. Sei α reduziert und γ ein Vorgänger in der Kettenbruchentwicklung, d.h. $\gamma = c + \frac{1}{\alpha}$. γ ist genau dann reduziert, wenn $c \geq 1$ und c so, daß
$$-1 < c + \frac{1}{\alpha'} < 0,$$
d.h.
$$c = -\lfloor \frac{1}{\alpha'} \rfloor - 1.$$
Also ist γ eindeutig bestimmt. ■

SATZ 8. *Genau die reduzierten α haben eine rein periodische Kettenbruchentwicklung.*

Beweis:

- Ist die Kettenbruchentwicklung von α rein periodisch, so ist für große n α_n reduziert. Da auch α dabei vorkommt, folgt die Behauptung.
- Sei α reduziert. Da die Menge $\mathcal{R}(d)$ endlich ist, muß die Kettenbruchentwicklung irgendwann rein periodisch werden. Sei l die minimale Periode und m minimal mit $\alpha_m = \alpha_{m+l}$. Wir sind fertig, falls $m = 0$ ist. Angenommen, dies wäre nicht der Fall: Dann hätte α_m die zwei verschiedenen reduzierten Vorgänger α_{m-1} und α_{m+l-1}, was aber nicht sein kann. Daher folgt die Behauptung. ■

Ist α reellquadratisch, so haben wir gesehen, daß für große n die Zahl α_n reduziert ist, also hat α_n eine rein periodische Kettenbruchentwicklung. Damit folgt insgesamt:

FOLGERUNG 4. *Genau die reellquadratischen Zahlen haben eine periodische Kettenbruchentwicklung.*

Beispiel: $d = 79$. Dann besteht $\mathcal{R}(79)$ aus den 16 Zahlen
$$(3,7),(3,10),(4,7),(4,9),(5,6),(5,9),(7,2),(7,3),$$
$$(7,5),(7,6),(7,10),(7,15),(8,1),(8,3),(8,5),(8,15),$$
wobei (b,c) für die Zahl $\frac{b+\sqrt{79}}{c}$ steht. Betrachtet man die Kettenbruchentwicklung entstehen 3 Zykel:
$$(3,7) \to (4,9) \to (5,6) \to (7,5) \to (8,3) \to (7,10) \to (3,7) \ldots,$$
$$(3,10) \to (7,3) \to (8,5) \to (7,6) \to (5,9) \to (4,7) \to (3,10) \ldots,$$
$$(7,2) \to (7,15) \to (8,1) \to (8,15) \to (7,2) \ldots.$$
Nun ein einfaches Beispiel: Fangen wir mit $\alpha = \frac{-47+\sqrt{79}}{71}$ an, so erhalten wir
$$(-47,71) \to (-24,-7) \to (10,3) \to (8,5),$$
und die letzte Zahl ist bereits reduziert.

Fragen:

- Wie groß ist $\mathcal{R}(d)$?
- In wieviele Zykel zerfällt $\mathcal{R}(d)$?
- Wie lang ist die Kettenbruchentwicklung?
- Zeige, daß gilt
$$\sqrt{d} = [a_0, \overline{a_1, \ldots, 2a_0}]$$
mit $a_i = a_{k-i}$ für $i = 1, \ldots, k-1$.

Bemerkung: Wir wollen nun nochmals die Pellsche Gleichung betrachten. Sei d eine natürliche Zahl, aber kein Quadrat. Sind x, y natürliche Zahlen mit $x^2 - dy^2 = 1$, so gilt:
$$|\sqrt{d} - \frac{a}{y}| = \frac{1}{y(x+\sqrt{d}y)} < \frac{1}{y \cdot 2\sqrt{d}y} < \frac{1}{2y^2},$$
also ist $\frac{x}{y}$ ein Näherungsbruch, d.h. es gibt ein n mit $\frac{x}{y} = \frac{p_n}{q_n}$. Dies motiviert das Folgende:

Wir wollen nun die Kettenbruchentwicklung von $\sqrt{d}$ näher untersuchen. Ist $\alpha = \alpha_0 = \sqrt{d}$, so ist $a_0 = \lfloor\sqrt{d}\rfloor$ und $\alpha_1 = \frac{1}{\sqrt{d}-\lfloor\sqrt{d}\rfloor}$. Man sieht sofort, daß α_1 reduziert ist. Der reduzierte Vorgänger von α_1 ist dann $\tilde{\alpha}_0 = \lfloor\sqrt{d}\rfloor + \sqrt{d}$.

Wir wollen nun die Gleichung $p_n^2 - dq_n^2 =?$ untersuchen. Es ist

$$\sqrt{d} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}.$$

Setzt man hier $\alpha_{n+1} = \frac{b_{n+1}+\sqrt{d}}{c_{n+1}}$ ein und macht dann Koeffizientenvergleich, so erhält man:

$$p_n = b_{n+1}q_n + c_{n+1}q_{n-1} \text{ und } dq_n = b_{n+1}p_n + c_{n+1}p_{n-1},$$

also

$$p_n^2 - dq_n^2 = c_{n+1}(p_nq_{n-1} - p_{n-1}q_n) = c_{n+1}(-1)^{n+1}$$

Nun ist α_{n+1} reduziert, also ist die Frage, wann $c_{n+1} = 1$ gilt. Die Reduziertheitsbedingung liefert $0 < \sqrt{d} - b_{n+1} < c_{n+1} = 1$, also ist $b_{n+1} = \lfloor\sqrt{d}\rfloor$ und damit $\alpha_{n+1} = \tilde{\alpha}_0$. Die Umkehrung ist klar. $n+1$ ist also ein Vielfaches der Periode k. Dann haben wir:

$$p_n^2 - dq_n^2 = (-1)^{n+1} \iff n+1 = \ell k \text{ mit } \ell \geq 1.$$

Ergebnis: Sie Lösungen $x, y \in \mathbf{N}$ der Pellschen Gleichung sind die Paare

- $(p_{\ell k-1}, q_{\ell k-1})$, $\ell = 1, 2, \ldots$, falls die Periode k gerade ist,
- $(p_{2\ell k-1}, q_{2\ell k-1})$, $\ell = 1, 2, \ldots$, falls die Periode k ungerade ist.

Ein theoretisches Verständnis der Lösungen liefert der Satz:

SATZ 9. *Sei $d > 1$ kein Quadrat. Dann ist*

$$P(d) = \{x + \sqrt{d}y : x^2 - dy^2 = 1, x, y \in \mathbf{Z}\}$$

eine Gruppe bezüglich der Multiplikation, und zwar

$$P(d) = \{\pm(x_1 + y_1\sqrt{d})^n : n \in \mathbf{Z}\},$$

wo (x_1, y_1) die kleinste Lösung der Pellschen Gleichung in natürlichen Zahlen ist. ($P(d)$ ist eine Untergruppe der Einheitengruppe von $\mathbf{Z}[\sqrt{d}]$.)

Beweis:

- Die Gruppeneigenschaft ist sofort zu sehen.
- Die logarithmische Abbildung $\phi : P(d) \to \mathbf{R}^2$, die durch

  $$\phi(\alpha) = (\ln|\alpha|, \ln|\alpha'|)$$

  gegeben ist, hat als Bild eine diskrete Untergruppe von $\{(x, y) \in \mathbf{R}^2 : x + y = 0\}$ und als Kern $\{\pm 1\}$, wie man leicht sieht. Daraus folgt dann auch die zweite Behauptung. ■

Was passiert, wenn man nach rationalen Lösungen fragt?

Beispiel: Die kleinste nichttriviale ganzzahlige Lösung von

$$x^2 - 109y^2 = 1$$

war

$$(158070671986249, 15140424455100).$$

Wir suchen jetzt nach Lösungen $(\frac{a}{c}, \frac{b}{c})$ mit $|a|, |b|, |c| \leq 100$ und finden

$$(1,0), (\frac{55}{54}, \frac{1}{54}), (\frac{59}{50}, \frac{3}{50}), (\frac{67}{42}, \frac{5}{42}), (\frac{79}{30}, \frac{7}{30}), (\frac{95}{14}, \frac{9}{14}).$$

Es scheint also auch einfache Lösungen zu geben.
Geometrische Idee: Lege Gerade durch $(1,0)$ mit Steigung t und berechne den anderen Schnittpunkt mit der Hyperbel. Wir machen also den Ansatz $y = t(x-1)$ und setzen ein:

$$0 = x^2 - 109y^2 - 1 = x^2 - 109t^2(x-1)^2 - 1 = (1-109t^2)x^2 + 218t^2x + (-1-109t^2) = (x-1)(x - 109t^2x + 109t^2 + 1)$$

Neben der Lösung $(x, y) = (1, 0)$ gibt es also noch die Lösung

$$(x, y) = (\frac{109t^2 + 1}{109t^2 - 1}, \frac{2t}{109t^2 - 1}).$$

Man erhält so fast eine Bijektion zwischen den Punkten der Kurve und den Punkten der affinen Geraden der der Koordinate t.

Bemerkung: Man kann jetzt versuchen, die $t \in \mathbf{Q}$ herauszufinden, die zu einer ganzzahligen Lösung der Pellschen Gleichung führen. Dabei stellt man aber fest, daß man wieder Gleichungen vom Pellschen Typ zu lösen hat. Wir machen den Ansatz $t = \frac{u}{v}$. Dann ist

$$x = \frac{109u^2 + v^2}{109u^2 - v^2}, \quad y = \frac{2uv}{109u^2 - v^2},$$

die Bedingung lautet also $109u^2 - v^2 | 109u^2 + v^2$ und $109u^2 - v^2 | 2uv$.

- Falls ein p existiert mit $p | 109u^2 - v^2$: Man sieht sofort, daß dann $p | 2 \cdot 109u^2$ gilt. Da aber p die Zahl u nicht teilen kann, gilt $p = 2$ oder $p = 109$.
  - Falls $p = 2$ ist, so ist $u \equiv v \equiv 1 \bmod 2$. Wegen $109u^2 - v^2 \equiv 0 \bmod 4$ und $2uv \equiv 2 \bmod 4$ wäre dann aber y nicht ganz, ein Widerspruch.
  - Falls $p = 109$, so gilt $109 | v$, d.h. $v = 109w$. Also $109u^2 - v^2 = 109(u^2 - 109w^2)$. Da nun 109 die Zahl $u^2 - 109w^2$ nicht mehr teilen kann, muß gelten $u^2 - 109w^2 = \pm 1$, was wieder eine Pellsche Gleichung ist.

Die Kettenbruchentwicklung von $\sqrt{d}$ und die kleinste Lösung der Pellschen Gleichung $x^2 - dy^2 = 1$.

d	Kettenbruchentwicklung von $\sqrt{d}$	x	y
2	$[1, \overline{2}]$	3	2
3	$[1, \overline{1, 2}]$	2	1
5	$[2, \overline{4}]$	9	4
6	$[2, \overline{2, 4}]$	5	2
7	$[2, \overline{1, 1, 1, 4}]$	8	3
8	$[2, \overline{1, 4}]$	3	1
10	$[3, \overline{6}]$	19	6
11	$[3, \overline{3, 6}]$	10	3
12	$[3, \overline{2, 6}]$	7	2
13	$[3, \overline{1, 1, 1, 1, 6}]$	649	180
14	$[3, \overline{1, 2, 1, 6}]$	15	4
15	$[3, \overline{1, 6}]$	4	1
17	$[4, \overline{8}]$	33	8
18	$[4, \overline{4, 8}]$	17	4
19	$[4, \overline{2, 1, 3, 1, 2, 8}]$	170	39
20	$[4, \overline{2, 8}]$	9	2
21	$[4, \overline{1, 1, 2, 1, 1, 8}]$	55	12
22	$[4, \overline{1, 2, 4, 2, 1, 8}]$	197	42
23	$[4, \overline{1, 3, 1, 8}]$	24	5
24	$[4, \overline{1, 8}]$	5	1
26	$[5, \overline{10}]$	51	10
27	$[5, \overline{5, 10}]$	26	5
28	$[5, \overline{3, 2, 3, 10}]$	127	24
29	$[5, \overline{2, 1, 1, 2, 10}]$	9801	1820
30	$[5, \overline{2, 10}]$	11	2
31	$[5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$	1520	273
32	$[5, \overline{1, 1, 1, 10}]$	17	3
33	$[5, \overline{1, 2, 1, 10}]$	23	4
34	$[5, \overline{1, 4, 1, 10}]$	35	6
35	$[5, \overline{1, 10}]$	6	1
37	$[6, \overline{12}]$	73	12
38	$[6, \overline{6, 12}]$	37	6
39	$[6, \overline{4, 12}]$	25	4
40	$[6, \overline{3, 12}]$	19	3
41	$[6, \overline{2, 2, 12}]$	2049	320
42	$[6, \overline{2, 12}]$	13	2
43	$[6, 1, 1, 3, 1, 5, 1, 3, 1, 1, 12]$	3482	531
44	$[6, \overline{1, 1, 1, 2, 1, 1, 1, 12}]$	199	30
45	$[6, \overline{1, 2, 2, 2, 1, 12}]$	161	24
46	$[6, \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}]$	24335	3588
47	$[6, \overline{1, 5, 1, 12}]$	48	7
48	$[6, \overline{1, 12}]$	7	1
50	$[7, \overline{14}]$	99	14
51	$[7, \overline{7, 14}]$	50	7
52	$[7, \overline{4, 1, 2, 1, 4, 14}]$	649	90
53	$[7, \overline{3, 1, 1, 3, 14}]$	66249	9100
54	$[7, \overline{2, 1, 6, 1, 2, 14}]$	485	66
55	$[7, \overline{2, 2, 2, 14}]$	89	12

56	$[7,\overline{2,14}]$	15	2
57	$[7,\overline{1,1,4,1,1,14}]$	151	20
58	$[7,\overline{1,1,1,1,1,1,14}]$	19603	2574
59	$[7,\overline{1,2,7,2,1,14}]$	530	69
60	$[7,\overline{1,2,1,14}]$	31	4
61	$[7,\overline{1,4,3,1,2,2,1,3,4,1,14}]$	1766319049	226153980
62	$[7,\overline{1,6,1,14}]$	63	8
63	$[7,\overline{1,14}]$	8	1
65	$[8,\overline{16}]$	129	16
66	$[8,\overline{8,16}]$	65	8
67	$[8,\overline{5,2,1,1,7,1,1,2,5,16}]$	48842	5967
68	$[8,\overline{4,16}]$	33	4
69	$[8,\overline{3,3,1,4,1,3,3,16}]$	7775	936
70	$[8,\overline{2,1,2,1,2,16}]$	251	30
71	$[8,\overline{2,2,1,7,1,2,2,16}]$	3480	413
72	$[8,\overline{2,16}]$	17	2
73	$[8,\overline{1,1,5,5,1,1,16}]$	2281249	267000
74	$[8,\overline{1,1,1,1,16}]$	3699	430
75	$[8,\overline{1,1,1,16}]$	26	3
76	$[8,\overline{1,2,1,1,5,4,5,1,1,2,1,16}]$	57799	6630
77	$[8,\overline{1,3,2,3,1,16}]$	351	40
78	$[8,\overline{1,4,1,16}]$	53	6
79	$[8,\overline{1,7,1,16}]$	80	9
80	$[8,\overline{1,16}]$	9	1
82	$[9,\overline{18}]$	163	18
83	$[9,\overline{9,18}]$	82	9
84	$[9,\overline{6,18}]$	55	6
85	$[9,\overline{4,1,1,4,18}]$	285769	30996
86	$[9,\overline{3,1,1,1,8,1,1,1,3,18}]$	10405	1122
87	$[9,\overline{3,18}]$	28	3
88	$[9,\overline{2,1,1,1,2,18}]$	197	21
89	$[9,\overline{2,3,3,2,18}]$	500001	53000
90	$[9,\overline{2,18}]$	19	2
91	$[9,\overline{1,1,5,1,5,1,1,18}]$	1574	165
92	$[9,\overline{1,1,2,4,2,1,1,18}]$	1151	120
93	$[9,\overline{1,1,1,4,6,4,1,1,1,18}]$	12151	1260
94	$[9,\overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18}]$	2143295	221064
95	$[9,\overline{1,2,1,18}]$	39	4
96	$[9,\overline{1,3,1,18}]$	49	5
97	$[9,\overline{1,5,1,1,1,1,1,1,5,1,18}]$	62809633	6377352
98	$[9,\overline{1,8,1,18}]$	99	10
99	$[9,\overline{1,18}]$	10	1
101	$[10,\overline{20}]$	201	20
102	$[10,\overline{10,20}]$	101	10
103	$[10,\overline{6,1,2,1,1,9,1,1,2,1,6,20}]$	227528	22419
104	$[10,\overline{5,20}]$	51	5
105	$[10,\overline{4,20}]$	41	4
106	$[10,\overline{3,2,1,1,1,1,2,3,20}]$	32080051	3115890
107	$[10,\overline{2,1,9,1,2,20}]$	962	93
108	$[10,\overline{2,1,1,4,1,1,2,20}]$	1351	130
109	$[10,\overline{2,3,1,2,4,1,6,6,1,4,2,1,3,2,20}]$	158070671986249	15140424455100
110	$[10,\overline{2,20}]$	21	2

KAPITEL 3

Approximation algebraischer Zahlen

Beispiel: Suche alle ganzzahligen Lösungen der Gleichung

$$x^3 - 2y^3 = 1.$$

Auf den ersten Blick sieht man die Lösungen $(1,0)$ und $(-1,1)$. Gibt es weitere? Wie sieht die Kurve geometrisch aus? Sie hat die Asymptote $x = \alpha y$, wo $\alpha^3 = 2$ ist. Wir können o.E. $x, y \geq 1$ annehmen, wenn wir die Gleichung $x^3 - 2y^3 = \pm 1$ betrachten. Dann gilt:

$$|\alpha - \frac{x}{y}| = \frac{1}{y(x^2 + \alpha xy + \alpha^2 y^2)} < \frac{1}{\alpha^2 y^3}$$

Es gilt sicher für $y \geq 2$: $\frac{1}{\alpha^2 y^3} < \frac{1}{2y^2}$, weshalb $\frac{x}{y}$ als Näherungbruch in der Kettenbruchentwicklung von α auftaucht.
Als betrachten wir die Kettenbruchentwicklung von α. In nachfolgender Tabelle steht

$$n, \quad a_n, \quad p_n, \quad q_n, \quad p_n^3 - 2q_n^3$$

$$0, 1, 1, 1, -1$$

$$1, 3, 4, 3, 10$$

$$2, 1, 5, 4, -3$$

$$3, 5, 29, 23, 55$$

$$4, 1, 34, 27, -62$$

$$5, 1, 63, 50, 47$$

$$6, 4, 286, 227, -510$$

$$7, 1, 349, 277, 683$$

$$8, 1, 635, 504, -253$$

$$9, 8, 5429, 4309, 17331$$

$$10, 1, 6064, 4813, -1450$$

$$11, 14, 90325, 71691, 293383$$

$$12, 1, 96389, 76504, -32259$$

$$13, 10, 1054215, 836731, 1376593$$

$$14, 2, 2204819, 1749966, -4836133$$

$$15, 1, 3259034, 2586697, 2589558$$

$$16, 4, 15240955, 12096754, -4554253$$

$$17, 12, 186150494, 147747745, 295716534$$

$$18, 2, 387541943, 307592244, -381236761$$

$$19, 3, 1348776323, 1070524477, 1671371601$$

$$20, 2, 3085094589, 2448641198, -6671050315$$

Vermutungen:

- Es gibt keine weitere Lösung für $x^3 - 2y^3 = 1$.
- Die Gleichung $x^3 - 2y^3 = m$ für festes m mit $1 \leq m \leq 100$ hat nur für
$$m \in \{1, 3, 10, 47, 55, 62\}$$
eine Lösung, und zwar die oben sichtbaren.

Die Zahl α läßt sich also anscheinend nicht zu gut durch rationale Zahlen approximieren.

Eine algebraische Zahl α ist eine komplexe Zahl, die einer polynomialen Gleichung über $\mathbf{Q}$ genügt, d.h. es gibt $a_0, \ldots, a_d \in \mathbf{Z}$ mit
$$a_0\alpha^d + \cdots + a_{d-1}\alpha + a_d = 0.$$
Das minimale d mit dieser Eigenschaft nennt man den Grad d der algebraischen Zahl α. Also $d = [\mathbf{Q}(\alpha) : \mathbf{Q}]$.

Algebraische Zahlen lassen sich nicht zu gut durch rationale Zahlen approximieren. Es gilt folgender Satz von Liouville.

SATZ 10. *Ist α eine algebraische Zahl vom Grad $d > 1$, so gibt es eine Konstante $c(\alpha) > 0$ mit der Eigenschaft, daß für jeden rationalen Bruch $\frac{p}{q}$ gilt:*
$$|\alpha - \frac{p}{q}| \geq \frac{c(\alpha)}{q^d}.$$
Ist $f \in \mathbf{Z}[x]$ ein Minimalpolynom von α, so kann man wählen
$$c(\alpha) = \frac{1}{\sum_{i=1}^{d} \frac{|f^{(i)}|}{i!}}.$$

Beweis: Sei $f(x) \in \mathbf{Z}[x]$ ein Minimalpolynom von α. Dann hat man die Taylorreihenentwicklung
$$f(x) = \sum_{i=1}^{d} \frac{f^{(i)}(\alpha)}{i!}(x - \alpha)^i.$$
Sei nun $\frac{p}{q}$ eine rationale Zahl und $|\alpha - \frac{p}{q}| \leq 1$. Dann ist
$$\frac{1}{q^d} \leq |f(\frac{p}{q})| \leq |\alpha - \frac{p}{q}|\frac{1}{c(\alpha)},$$
woraus die Behauptung folgt. Im Falle $|\alpha - \frac{p}{q}| > 1$ folgt damit die Behauptung trivialerweise. ■

Den Satz von Liouville kann man nun umgekehrt zur Konstruktion transzendenter Zahlen benutzen. Wir nennen eine reelle Zahl α eine Liouvillesche Zahl, wenn für jedes $N \in \mathbf{N}$ die Ungleichung
$$|\alpha - \frac{p}{q}| < \frac{1}{q^N}$$

unendlich viele Lösungen besitzt.

SATZ 11. *Eine Liouvillesche Zahl α ist transzendent.*

Beweis: Angenommen, α wäre algebraisch vom Grad d. Dann hätten wir eine Ungleichung

$$\frac{c(\alpha}{q^d} < \frac{1}{q^N}$$

für unendlich viele q. Das kann aber nicht sein, wenn $N > d$ ist. Also ist α nicht algebraisch. ■

Beispiel: Die reelle Zahl

$$\alpha = \sum_{i=1}^{\infty} \frac{1}{10^{i!}}$$

ist eine Liouville-Zahl, also transzendent.
Beweis: Sei $n \geq N$ und $q = 10^{n!}$ und $\frac{p}{q} = \sum_{i=1}^{n} \frac{1}{10^{i!}}$. Dann ist

$$0 < \alpha - \sum_{i=1}^{n} \frac{1}{10^{i!}} = \sum_{i=n+1}^{\infty} \frac{1}{10^{i!}} < \sum_{k \geq (n+1)!} \frac{1}{10^k} = \frac{10}{9} \frac{1}{q^{n+1}} < \frac{1}{q^N}.$$

Da dies für alle $n \geq N$ gilt, ist α Liouvillesch. ■

Wie ist nun das Verhältnis zwischen algebraischen und transzendenten Zahlen?

SATZ 12. *Die Menge der algebraischen Zahlen ist abzählbar.*

Beweis: Sei für $N \in \mathbf{N}$

$$A_N = \{\alpha \in \mathbf{C} : a_0\alpha^d + \cdots + a_d = 0, (a_0, \ldots, a_d) \in \mathbf{Z}^{d+1} - \{0\}, \sum |a_i| \leq N\}.$$

Dann ist A_N eine endliche Menge. Also ist $\cup A_N$ abzählbar. $\cup A_N$ ist aber genau die Menge der algebraischen Zahlen. ■

Bemerkungen:

- Da $\mathbf{R}$ und $\mathbf{C}$ überabzählbar sind, gibt es also transzendente Zahlen.
- Ein sehr einfaches Beispiel einer transzendenten Zahl erhält man mit dem Satz von Liouville.
- Eine abzählbare Menge hat Lebesgue-Maß 0. Im Sinne des Lebesgueschen Maßes sind also fast alle Zahlen transzendent.

Wie gut läßt sich nun eine *allgemeine Zahl* approximieren? Wir definieren für $\delta > 0$:

$$S(\delta) = \{\alpha \in [0,1] : |\alpha - \frac{p}{q}| < \frac{1}{q^\delta} \text{ hat unendlich viele Lösungen}\}$$

Wir wissen bereits $S(2) = [0,1]$. Sei also jetzt $\delta > 2$ vorausgesetzt. Sei weiter

$$S(\delta, q) = \{\alpha \in [0,1] : |\alpha - \frac{p}{q}| < \frac{1}{q^\delta} \text{ für ein } p \in \mathbf{Z}\}.$$

$S(\delta, q)$ ist enthalten in der Vereinigung von Intervallen und

$$\lambda(S(\delta, q)) \geq \frac{2}{q^{\delta-1}}.$$

Nun ist

$$S(\delta) = \cap_{Q=1}^{\infty} \cup_{q=Q}^{\infty} S(\delta, q).$$

Wegen

$$\lambda(\cup_{q=Q}^{\infty} S(\delta, q)) \leq \sum_{q=Q}^{\infty} \frac{2}{q^{\delta-1}} < \infty$$

ist klar, daß $\lim_{Q\to\infty} \lambda(\cup_{q\geq Q} S(\delta, q)) = 0$ ist, also $\lambda(S(\delta)) = 0$. Also ist $S(\delta)$ eine Nullmenge.

Damit haben wir folgendes Ergebnis von Khintchine bewiesen:

SATZ 13. *Sei $\delta > 2$. Für fast alle reellen α hat die Ungleichung*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^\delta}$$

nur endlich viele Lösungen.

FOLGERUNG 5. *Die Liouville-Zahlen bilden eine Nullmenge.*

Frage: Welche Zahlen gehören zu *fast allen* aus obigem Satz?

Bemerkung: Erfüllt π die Bedingung im Satz? Mahler (1953) konnte zeigen: Die Ungleichung

$$|\pi - \frac{p}{q}| < \frac{1}{q^{42}}$$

hat nur endlich viele Lösungen.

Was kann man über algebraische Zahlen sagen, die uns eigentlich interessieren?

Vorausschau - Ergebnisse: Sei α algebraisch vom Grad d. Dann hat die Ungleichung

$$|\alpha - \frac{p}{q}| < \frac{1}{q^\mu}$$

nur endlich viele Lösungen für

- $\mu > d$ (Liouville 1844)
- $\mu > \frac{d}{2} + 1$ (Thue 1908/1909)
- $\mu > 2\sqrt{d}$ (Siegel 1921)
- $\mu > \sqrt{2d}$ (Dyson 1947)
- $\mu > 2$ (Roth 1955). Für dieses Ergebnis erhielt Roth die Fields Medal.

Der Wichtigkeit halber nochmals:

SATZ 14. *(Thue-Siegel-Roth) Für algebraisches α und $\mu > 2$ hat die Ungleichung*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^\mu}$$

nur endlich viele Lösungen in rationalen Zahlen $\frac{p}{q}$.

Anders formuliert:

SATZ 15. *Zu einer irrationalen algebraischen Zahl α und jedem $\epsilon > 0$ gibt es eine Konstante $C(\alpha, \epsilon)$ mit der Eigenschaft: Für jede rationale Zahl $\frac{p}{q}$ gilt:*

$$|\alpha - \frac{p}{q}| \geq \frac{C(\alpha, \epsilon)}{q^\mu}.$$

Leider ist der Satz nicht effektiv, d.h. man kann nicht einfach $C(\alpha, \epsilon)$ anschreiben. Für spezielle Zahlen und spezielle Werte von ϵ gibt es allerdings konkrete Ergebnisse.

Beispiel: Baker konnte zeigen, daß gilt

$$|\sqrt[3]{2} - \frac{p}{q}| > \frac{1}{10^6} \frac{1}{q^{2.955}}.$$

Verbesserungen gibt es von Chudnovsky, Baker, Stewart.

KAPITEL 4

Zwischenspiel: Die abc-Vermutung

Vorbemerkung: Ganze Zahlen und Polynome haben manches gemeinsam. So lassen sich auch Fragestellungen oder Einsichten oft transportieren und können helfen, das Verständnis zu vertiefen.

- Sowohl $\mathbf{Z}$ als auch $\mathbf{C}[t]$ sind faktorielle Ringe, d.h. haben eindeutige Primfaktorzerlegung.
- In $\mathbf{Z}$ hat man die Primzahlen, in $\mathbf{C}[t]$ sind die Polynome $t-\alpha$ die Primelemente.
- In $\mathbf{Z}$ sind die Einheiten ± 1, in $\mathbf{C}[t]$ alle Konstanten $\neq 0$.
- Die eindeutige Primfaktorzerlegung lautet dann jeweils
$$\pm \prod_i p_i^{n_i} \quad \text{und} \quad c\prod_i (t-\alpha_i)^{n_i}.$$
- Die Größe einer ganzen Zahl kann man durch den Absolutbetrag messen, die Größe eines Polynoms durch seinen Grad.

Für ein Polynom f bezeichne $n_0(f)$ die Anzahl der verschiedenen Nullstellen von f. Dann hat Mason den folgenden Satz gezeigt:

SATZ 16. *Sind a, b, c teilerfremde Polynome, nicht alle konstant, mit $a+b+c=0$, so ist*
$$\max(\text{grad}(a), \text{grad}(b), \text{grad}(c)) \leq n_0(abc) - 1.$$

Bevor wir den Beweis anschauen, wollen wir ein Beispiel betrachten, das die Nützlichkeit des Satzes zeigt:

Beispiel: Für $n \geq 3$ gibt es keine Polynome $x(t), y(t), z(t)$ mit $x(t)^n + y(t)^n = z(t)^n$ außer sie sind konstant.
Beweis: Wir nehmen an, es gäbe solche Polynome. O.E. sind die Polynome teilerfremd. Sei d der maximale Grad. Dann sagt unsere Ungleichung
$$nd \leq 3d - 1,$$
was nicht sein kann. ■

Wir $n = 2$ gibt es bekanntlich solche Polynome, wie die Identität
$$(t^2-1)^2 + (2t)^2 = (t^2+1)^2$$
zeigt.

Beweis des Satzes: O.E. sind a und b nicht konstant. Wir müssen dann nur die Grade von a und b abschätzen. Sei
$$a = \prod (t-\alpha_i)^{m_i}, \quad b = \prod (t-\beta_j)^{n_j}, \quad c = \prod (t-\gamma_k)^{r_k}.$$
Das Polynom $N = \prod(t-\alpha_i)\prod(t-\beta_j)\prod(t-\gamma_k)$ hat dann Grad $n_0(abc)$. Sei $f = \frac{a}{c}$ und $g = \frac{b}{c}$. Dann ist $f + g = 1$ und $f' = -g'$. Weiter gilt:
$$\frac{f'}{f} = \sum \frac{m_i}{t-\alpha_i} - \sum \frac{r_k}{t-\gamma_k}, \quad \frac{g'}{g} = \sum \frac{n_j}{t-\beta_j} - \sum \frac{r_k}{t-\gamma_k}.$$
Dann ist der Grad von $\frac{Nf'}{f}$ und $\frac{Ng'}{g}$ sicher $\leq \text{grad}(N) - 1$. Nun haben wir $ag = bf$, woraus sofort
$$a \cdot \frac{Nf'}{f} = -b \cdot \frac{Ng'}{g}$$
folgt und daraus wegen der Teilerfremdheit von a und b, daß
$$a \mid \frac{Ng'}{g} \text{ und } b \mid \frac{Nf'}{f},$$

woraus für die Grade sofort $\text{grad}(a) \leq n_0(abc) - 1$ folgt und das gleiche für b. Daraus ergibt sich die Behauptung. ■

Wie übersetzt sich nun der Satz von Mason in die Zahlentheorie? — Inspiriert durch Arbeiten von Mason, Frey, Szpiro entstand folgende auf Masser und Oesterlé zurückgehende Vermutung:

abc-Vermutung: *Zu jedem $\epsilon > 0$ gibt es eine Konstante $C(\epsilon) > 0$ mit der Eigenschaft: Sind a, b, c ganze Zahlen mit*

$$a + b + c = 0 \text{ und } \gcd(a, b, c) = 1,$$

so gilt

$$\max(|a|, |b|, |c|) \leq C(\epsilon) \cdot (\prod_{p|abc} p)^{1+\epsilon}.$$

Auf der rechten Seite steht also nur das Produkt der auftretenden Primzahlen, höhere Potenzen werden nicht berücksichtigt. Wir schreiben auch $P(a) = \prod_{p|a} p$. Daß in der Vermutung auf das ϵ im Exponenten nicht verzichtet werden kann, werden wir weiter unten sehen.

Beispiel: Wir betrachten $2^n + 1 = k$ als Testfall.

Gleichung	Maximum	$P(2k)$
$2^3 + 1 = 3^2$	9	6
$2^9 + 1 = 3^3 \cdot 19$	513	114
$2^{10} + 1 = 5^2 \cdot 41$	1025	410
$2^{27} + 1 = 3^4 \cdot 19 \cdot 87211$	134217729	9942054

Die Mächtigkeit der abc-Vermutung soll nun an einigen Beispielen erläutert werden.

Die Fermatsche Vermutung. Sie besagt, daß für $n \geq 3$ die Gleichung

$$x^n + y^n = z^n$$

keine Lösungen in natürlichen Zahlen x, y, z besitzt. Sie ist bewiesen für $n \leq 125000$ (?). Ein von Faltings bewiesener Satz impliziert, daß obige Gleichung für $n \geq 4$ nur endlich viele teilerfremde Lösungen besitzt. Was läßt sich nun mit der abc-Vermutung machen? Wir wenden sie für $\epsilon = 0.1$ an und schreiben einfach $C = C(0.1)$. Dann ist

$$z^n \leq C \cdot (xyz)^{1.1} \leq C \cdot z^{3.3}.$$

Sei o.E. $n \geq 4$. Dann ist also

$$z^{n-3.3} \leq C.$$

Wegen $z \geq 2$ sind dann nur endlich viele n's möglich, damit auch nur endlich viele z's etc. D.h. die Fermatsche Vermutung gilt für große n. Man kann Genaueres sagen, wenn man C kennt.

Die Catalansche Vermutung. Wir betrachten die Gleichung

$$x^n - y^m = 1$$

in natürlichen Zahlen $x, y, m, n \geq 2$. Durch Probieren findet man, daß $3^2 - 2^3 = 1$ eine Lösung ist. Die Catalansche Vermutung ist, daß dies die einzige Lösung ist.
1976 bewies Tijdeman mit Methoden von Baker (Linearformen in Logarithmen), daß es nur endlich viele Lösungen der Catalanschen Gleichung gibt.

Was sagt die abc-Vermutung? Sicher gilt:

$$y^m < x^n \leq C(xy)^{1.1}$$

Wir unterscheiden der Einfachkeit halber ein paar Fälle:

- $n \geq 3$. Dann ist $y^2 \leq y^m \leq x^n$, also $y \leq x^{n/2}$, womit man erhält:
$$x^n \leq C x^{(1+n/2)\cdot 1.1},$$
oder umgeformt:
$$x^{0.45n-1.1} \leq C.$$
Wegen $n \geq 3$ ist damit x beschränkt und natürlich auch n. Damit sind auch y und m beschränkt.
- $m \geq 3$. Man hat $x^2 \leq x^n \leq 2y^m \leq 4y^m$, also $x \leq 2y^{m/2}$. Damit:
$$y^m \leq 4C y^{(1+m/2)\cdot 1.1}.$$
Analog wie vorher erhält man
$$y^{0.45m-1.1} \leq 4C.$$
Damit folgt sofort wieder die Beschränktheit von x, y, m, n.
- $m = n = 2$. Aus $(x-y)(x+y) = 1$ sieht man sofort, daß keine Lösungen $x, y \geq 1$ existieren.

Am Beispiel der Fermatschen und der Catalanschen Vermutung sieht man, wie mächtig die abc-Vermutung ist.

Das folgende Beispiel zeigt, daß man auf das ϵ im Exponenten nicht verzichten kann.

Beispiel: Wir zeigen zunächst, daß für $n \geq 1$ gilt
$$3^{2^n} - 1 = 2^{n+2} \cdot a_n$$
mit einer ungeraden natürlichen Zahl a_n.
Beweis durch Induktion: Für $n = 1$ hat man $3^2 - 1 = 2^3 \cdot 1$. Sei die Behauptung bereits für n bewiesen. Dann ist
$$3^{2^{n+1}} - 1 = (3^{2^n} - 1)(3^{2^n} + 1) = 2^n a_n \cdot 2 \cdot b_n,$$
wobei b_n ungerade sein muß. Damit folgt die Behauptung. ■

Wir betrachten nun
$$\frac{3^{2^n}}{P(3 \cdot 2 \cdot a_n)} \geq \frac{3^{2^n}}{3 \cdot 2 \cdot \frac{3^{2^n}}{2^{n+2}}} = \frac{2^{n+1}}{3}$$
und sehen sofort, daß der Quotient mit $n \to \infty$ gegen ∞ konvergiert, also kann man auf das ϵ im Exponenten der abc-Vermutung nicht verzichten.

Aufgabe: Untersuche dieses Beispiel, um eine Abschätzung für $C(\epsilon)$ zu erhalten.

Beispiele:

1. Es ist $5^4 \cdot 7 = 2 \cdot 3^7 + 1$, also muß gelten
$$5^4 \cdot 7 \leq C(\epsilon) \cdot (2 \cdot 3 \cdot 5 \cdot 7)^{1+\epsilon}, \text{ also } 4375 \leq C(\epsilon) \cdot 210^{1+\epsilon}.$$
Also erhält man
$$C(\epsilon) \geq \frac{4375}{210^{1+\epsilon}}.$$
2. Es ist
$$2^{21} \cdot 23 = 3^2 \cdot 5^6 \cdot 7^3 + 11^2$$
und damit hat man
$$2^{21} \cdot 23 \leq C(\epsilon) \cdot (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23)^{1+\epsilon} \text{ oder } 48234496 \leq C(\epsilon) \cdot 53130^{1+\epsilon}.$$
Also
$$C(\epsilon) \geq \frac{48234496}{53130^{1+\epsilon}}.$$
Damit erhält man durch Einsetzen:
$$C(0) > 907, \quad C(0.1) > 305, \quad C(0.2) > 103, \quad C(0.3) > 34.$$
3. Aufgabe: Finde weitere solcher Gleichungen.

Beispiel: Bei Betrachtung der Gleichung $x^3 - 2y^3 = 1$ hatten wir die Näherungsbrüche $\frac{p_n}{q_n}$ aus der Kettenbruchentwicklung zu $\sqrt[3]{2}$ genommen und $p_n^3 - 2q_n^3 = \pm t_n$ angeschaut ($t_n > 0$). Durch Einsetzen hatten wir den Eindruck, daß t_n groß wird. Kann man das mit der abc-Vermutung sehen?
Wir nehmen der Einfachkeit halber an, daß 2 das p_n nicht teilt. Da $\frac{p_n}{q_n} \sim \sqrt[3]{2}$ ist $q_n \leq p_n$, also folgt mit abc und $\epsilon \leq 1$:

$$p_n^3 \leq C(\epsilon)(p_n \cdot 2q_n \cdot t_n)^{1+\epsilon} \leq 2^{1+\epsilon} C(\epsilon) p_n^{2+2\epsilon} t_n^{1+\epsilon},$$

und damit

$$t_n \geq \frac{1}{2\sqrt[1+\epsilon]{C(\epsilon)}} p_n^{\frac{1-2\epsilon}{1+\epsilon}}.$$

Das zeigt, daß t_n mindestens so wie p_n wächst, was gut mit der Beobachtung übereinstimmt. (Aufgabe: Leite eine analoge Aussage mit dem Satz von Thue-Siegel-Roth her.)

Zum Schluß wollen wir noch die Frage streifen, wie groß die Lösungen der Mordell-Gleichung $y^2 = x^3 + k$ in Abhängigkeit von k sein können.

Beispiel: Wir nehmen teilerfremde Polynome f und g und wollen sie so konstruieren, daß $f^3 - g^2$ möglichst kleinen Grad hat. Also $f^3 - g^2 = h$. Was ist möglich? Damit sich der höchste Koeffizient herausheben kann, wählen wir $3\text{grad}(f) = 2\text{grad}(g)$. Dann sagt uns der Satz:

$$3\text{grad}(f) \leq \text{grad}(f) + \text{grad}(g) + \text{grad}(k) - 1 = \frac{5}{2}\text{grad}(f) + \text{grad}(h) - 1,$$

also

$$\text{grad}(h) \geq \frac{1}{2}\text{grad}(f) + 1.$$

Gibt es dazu Beispiele? Eines erhält man mit

$$f = t^6 + 4t^4 + 10t^2 + 6, \quad g = t^9 + 6t^7 + 21t^5 + 35t^3 + \frac{63}{2}t, \quad h = 27t^4 + \frac{351}{4}t^2 + 216.$$

KAPITEL 5

Der Satz von Thue-Siegel-Roth

Der Satz von Thue-Siegel-Roth, für dessen Beweis Roth 1958 die Fields medal erhielt, lautet:

SATZ 17. *Ist α eine algebraische Zahl und $\mu > 2$, so gibt es nur endlich viele rationale Zahlen $\frac{p}{q}$ mit*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^\mu}.$$

Bemerkung: Wir haben den Satz bereits gezeigt für $\mu = d$, wenn d der Grad der algebraischen Zahl ist. (Satz von Liouville.)

1. Beweisversuch:
   1. Wähle $f \in \mathbf{Z}[x]$ vom Grad r mit Multiplizität m in α, d.h. $f(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$.
   2. Erfüllt $\frac{p}{q}$ obige Ungleichung für μ, so ist entweder $f(\frac{p}{q}) = 0$ oder $f(\frac{p}{q}) \neq 0$ und damit
   $$\frac{1}{q^r} \leq |f(\frac{p}{q})| = |\sum_{i \geq m} \frac{f^{(i)}(\alpha)}{i!}(\frac{p}{q} - \alpha)i^i \leq c|\alpha - \frac{p}{q}|^m < \frac{c}{q^{m\mu}}.$$
   3. Ist $\mu > \frac{r}{m}$, so kann es also nur endlich viele Lösungen geben.
   4. Die Frage ist also: Wie klein kann $\frac{r}{m}$ gemacht werden? Ist $g(x)$ das Minimalpolynom von α vom Grad d, so gilt
   $$f(x) = g(x)^m h(x)$$
   mit einem weiteren Polynom $h(x) \in \mathbf{Q}[x]$. Gradvergleich liefert
   $$r = md + grad(h),$$
   also
   $$\frac{r}{m} = d + \ldots,$$
   also können wir so nur $\mu > d$ erhalten, was wir aber bereits bewiesen haben.
   5. Ein Polynom in einer Veränderlichen reicht also nicht aus.

2. Beweisversuch:

1. Wähle ein Polynom in zwei Veränderlichen $f(x, y) \in \mathbf{Z}[x, y]$ mit $f(\alpha, \alpha) = 0$, d.h. eine ebene Kurve $f(x, y) = 0$, die den Punkt (α, α) enthält.
2. Ist $\frac{p}{q}$ eine gute Approximation an α, so kann man versuchen $f(\frac{p}{q}, \frac{p}{q})$ anzuschauen. Aber es wird sofort klar, daß das nicht weiterführt, da die eigentlich nur Eigenschaften des Polynoms $f(x, x)$ in einer Veränderlichen ausnutzt, was wir bereits vorher abgehandelt haben.
3. Wir können nun zwei verschiedene Approximationen betrachten:
$$|\alpha - \frac{p_1}{q_1}| < \frac{1}{q_1^\mu} \text{ und } |\alpha - \frac{p_2}{q_2}| < \frac{1}{q_2^\mu}.$$
4. Ist $f(\frac{p_1}{q_1}, \frac{p_2}{q_2}) = 0$, so können wir nichts sagen. 1. Schwierigkeit.
5. Falls $f(\frac{p_1}{q_1}, \frac{p_2}{q_2}) \neq 0$, so gilt:
$$\frac{1}{q_1^{r_1} q_2^{r_2}} \leq \sum_{i+j \geq m} |c_{ij}| \frac{1}{q_1^{i\mu} q_2^{j\mu}} \leq c \frac{1}{q_1^{m\mu}},$$
falls $q_2 > q_1$ ist. Aber hieraus kann man auch nichts ableiten, wenn man nicht die Beziehung zwischen q_1 und q_2 im Griff hat.

Folgendes Beispiel soll einen Eindruck geben, daß man bei Polynomen in mehreren Veränderlichen mehr Freiheiten hat, als bei Polynomen in einer Veränderlichen.

Beispiel: Wir wollen die Polynome $f(x,y) \in \mathbf{Z}[x,y]$ vom Totalgrad ≤ 3 bestimmen, die in (α,α) verschwinden. Dabei $\alpha^3 = 2$. Wir machen den Ansatz

$$f = a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2 + a_6x^3 + a_7x^2y + a_8xy^2 + a_9y^3.$$

Nun setzen wir ein

$$f(\alpha,\alpha) = (a_0 + 2a_6 + 2a_7 + 2a_8 + 2a_9) + (a_1 + a_2)\alpha + (a_3 + a_4 + a_5)\alpha^2$$

und erhalten also drei lineare Gleichungen. Lösen wir diese, so erhalten wir

$$f = a_1(x-y) + a_3(x^2-y^2) + a_4(xy-y^2) + a_6(x^3-2) + a_7(x^2y-2) + a_8(xy^2-2) + a_9(y^3-2),$$

wobei die Koeffizienten beliebig in $\mathbf{Z}$ gewählt werden können. Will man haben, daß f in (α,α) mit Vielfachheit 2 verschwindet, so muß man noch die Bedingungen $f_x(\alpha,\alpha) = f_y(\alpha,\alpha) = 0$ erfüllen. Tut man das, so erhält man

$$f = (x-y)^2(a_3 + a_6x + (2a_6 + a_7)y),$$

was nicht mehr sehr interessant ist.

Wir werden im weiteren Polynome in mehreren Veränderlichen konstruieren, ähnlich wie im Beispiel. Dabei muß auch die Größe der Koeffizienten abgeschätzt werden. Wie wir sahen, führt dies auf ein lineares Gleichungssystem.

Es gilt folgendes Lemma von Siegel:

LEMMA 5. *Sei $A = (a_{ij})$ eine ganzzahlige Matrix mit m Zeilen und n Spalten und $n > m$. Sei weiter $H = \max(|a_{ij}|)$. Dann gibt es ein $x \in \mathbf{Z}^n, x \neq 0$ mit $Ax = 0$, d.h.*

$$\sum_{j=1}^{n} a_{ij}x_j = 0 \quad \text{für } i = 1,\ldots,m,$$

und

$$|x|_\infty = \max(|x_1|,\ldots,|x_n|) \leq (nH)^{\frac{m}{n-m}}.$$

Beweis: Sei

$$b_i = -\sum_{a_{ij}<0} a_{ij} \text{ und } c_i = \sum_{a_{ij}>0} a_{ij}.$$

Wählt man eine natürliche Zahl M und als Definitionsbereich

$$D = \{(x_1,\ldots,x_n) \in \mathbf{Z}^n : 0 \leq x_j \leq M\},$$

so bildet die Matrix A die Menge D ab in die Menge

$$W = \{(y_1,\ldots,y_m) \in \mathbf{Z}^m : -b_iM \leq y_i \leq c_iM\}.$$

Für die Größen von D und W gilt:

$$\#D = (M+1)^n, \quad \#W = \prod_i (b_iM + c_iM + 1) \leq (nHM+1)^m.$$

Sei nun

$$M = \lfloor (nH)^{\frac{m}{n-m}} \rfloor.$$

Dann ist

$$M + 1 > (nH)^{\frac{m}{n-m}}, \text{also } (M+1)^n > (nH)^m(M+1)^m = (nHM + nH)^m \geq (nHM+1)^m,$$

insbesondere $\#D > \#W$. Also werden zwei verschiedene Punkte x', x'' durch A auf den gleichen Punkt in W abgebildet. Setzt man jetzt $x = x' - x''$, so erfüllt x die Bedingungen des Lemmas. ■

Bemerkungen:

1. Da es mehr Unbekannte als Gleichungen gibt, ist klar, daß es nichttriviale Lösungen in $\mathbf{Q}^n$ und damit in $\mathbf{Z}^n$ gibt. Das Lemma behandelt die Frage nach der Existenz von kleinen Lösungen.

2. Der Exponent $\frac{m}{n-m}$ fällt monoton in n. Für $n = m+1$ hat man den Wert m, für $n = 2m$ den Wert 1, etc.

Wir nennen eine algebraische Zahl α *ganzalgebraisch*, wenn α einem ganzzahligen Polynom $f(x)$ genügt, wo der höchste Koeffizient ganz ist. Dies ist damit äquivalent, daß das normierte Minimalpolynom von α Koeffizienten in $\mathbf{Z}$ hat. (Beispiele: $\sqrt{2}$, $\sqrt[3]{2}$, $\frac{1+\sqrt{-3}}{2}$, nicht jedoch $\frac{1+\sqrt{3}}{2}$.)

Bemerkungen:

1. Sei α eine algebraische Zahl mit Minimalpolynom $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$. Ist $N \in \mathbf{N}$, so gilt:
$$(N\alpha)^d + (Na_1)(N\alpha)^{d-1} + \cdots + (N^d a_d) = 0.$$
Wählt man N so, daß $N^i a_i \in \mathbf{Z}$ ist, für alle i, so ist $\beta := N\alpha$ ganzalgebraisch, d.h. jede algebraische Zahl α hat die Form $\frac{\beta}{N}$ mit einer ganzalgebraischen Zahl β und einer natürlichen Zahl N.
2. Ist der Satz von Thue-Siegel-Roth für alle ganzalgebraischen Zahlen gezeigt, so gilt er auch für alle algebraischen Zahlen. Denn: Sei $\alpha = \frac{\beta}{N}$ wie eben gegeben. Sei $\mu > 2$. Wähle $\epsilon > 0$ mit $\mu - \epsilon > 2$. Sei nun $|\alpha - \frac{p}{q}| < \frac{1}{q^\mu}$. Ist $q \geq N^{\frac{1}{\epsilon}}$, so gilt
$$|\beta - \frac{Np}{q}| < \frac{N}{q^\mu} \leq \frac{1}{q^{\mu-\epsilon}}.$$
Für diese Ungleichung gibt es nun aber nach Voraussetzung nur endlich viele Möglichkeiten. Also folgt auch die Aussage für α.

Wie wir schon bei obigem Beispiel sahen, führt die Verschwindungsbedingung in (α, α) auf ein lineares Gleichungssystem. Um die Koeffizienten dabei abschätzen zu können, beweisen wir folgendes Lemma:

LEMMA 6. *Sei α eine ganzalgebraische Zahl vom Grad d mit Minimalpolynom f. Dann gibt es für jedes $n \in \mathbf{N}$ Zahlen $a_{ni} \in \mathbf{Z}$ mit*
$$\alpha^n = \sum_{i=0}^{d-1} a_{ni}\alpha^i,$$
wobei wir abschätzen können
$$|a_{ni}| \leq (|f|+1)^n.$$

Beweis: Wir schreiben f in der Form $f = x^d - a_{d-1}x^{d-1} - \cdots - a_0$. Dann gilt
$$\alpha^d = \sum_{i=0}^{d-1} a_i \alpha^i.$$
Die Behauptung gilt dann sicher für alle $n \leq d$. Wir beweisen sie insgesamt durch Induktion:
$$\alpha^{n+1} = (\sum_{i=0}^{d-1} a_{ni}\alpha^i)\cdot\alpha = a_0 a_{n,d-1} + \sum_{i=1}^{d-1}(a_i a_{n,d-1} + a_{n,i-1})\alpha^i.$$
Das liefert sofort
$$a_{n+1,0} = a_0 a_{n,d-1}, \quad a_{n+1,i} = a_i a_{n,d-1} + a_{n,i-1},$$
also sicher
$$|a_{n+1,i}| \leq (|f|+1)\cdot \max_j |a_{n,j}|,$$
woraus die Behauptung folgt. ■

Für ein Polynom $f(x_1, \ldots, x_m)$ bezeichne $|f|$ das Maximum der Koeffizienten von f. Außerdem betrachten wir die modifizierten Ableitungen
$$f_{i_1 \ldots i_m} = \frac{1}{i_1! \ldots i_m!} \frac{\delta^{i_1+\cdots+i_m}}{\delta x_1^{i_1} \ldots} f.$$
Dann ist die Taylorreihenentwicklung im Punkt $(\alpha_1, \ldots, \alpha_m)$:
$$f = \sum f_{i_1 \ldots i_m}(\alpha_1, \ldots, \alpha_m)(x_1 - \alpha_1)^{i_1} \ldots (x_m - \alpha_m)^{i_m}.$$

LEMMA 7. *Sei $f \in \mathbf{Z}[x_1, \ldots, x_m]$ vom Grad $\leq r_i$ in x_i. Dann ist auch $f_{i_1 \ldots i_m} \in \mathbf{Z}[x_1, \ldots, x_m]$ und*

$$|f_{i_1 \ldots i_m}| \leq 2^{r_1 + \cdots + r_m} |P|.$$

Beweis: Sei

$$f = \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} a_{j_1 \ldots j_m} x_1^{j_1} \ldots x_m^{j_m}.$$

Dann ist

$$f_{i_1 \ldots i_m} = \sum_{j_1=i_1}^{r_1} \cdots \sum_{j_m=i_m}^{r_m} \binom{j_1}{i_1} \ldots \binom{j_m}{i_m} a_{j_1 \ldots j_m} x_1^{j_1 - i_1} \ldots x_m^{j_m - i_m}.$$

Nun ist

$$\binom{j}{i} \leq 2^j \leq 2^r,$$

woraus dann die Abschätzung folgt. ■

Wir brauchen nun noch einen Verschwindungsbegriff. Sei $f \in \mathbf{Z}[x_1, \ldots, x_m]$ ein Polynom, $(\alpha_1, \ldots, \alpha_m) \in \mathbf{R}^m$ und $(r_1, \ldots, r_m) \in \mathbf{N}^m$. Dann wird der Index $index(f)$ von f bezüglich $(r_1, \ldots, r_m)$ in $(\alpha_1, \ldots, \alpha_m)$ definiert durch

$$index(f) = \min\{\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m} : f_{i_1 \ldots i_m}(\alpha_1, \ldots, \alpha_m) \neq 0\}.$$

Ist $r_1 = \cdots = r_m = 1$, so spricht man auch von der Verschwindungsordnung von f im Punkt $(\alpha_1, \ldots, \alpha_m)$.

Beispiel: $f = y^2 - x^3$. Dann ist

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

Die einzigen in $(0,0)$ nichtverschwindenden Ableitungen sind also $f_{3,0}(0,0) = -1$ und $f_{0,2}(0,0) = 1$. Damit ist der Index von f in $(0,0)$ bezüglich (r,s):

$$index(f) = \min\{\frac{3}{r}, \frac{2}{s}\}.$$

Bemerkung: Mit $c_{i_1 \ldots i_m} = f_{i_1 \ldots i_m}(\alpha_1, \ldots, \alpha_m)$ lautet die Taylorreihenentwicklung von f:

$$f = \sum c_{i_1 \ldots i_m} (x_1 - \alpha_1)^{i_1} \ldots (x_m - \alpha_m)^{i_m}.$$

Substituiert man nun $x_i = \alpha_i + y_i t^{\frac{1}{r_i}}$, so erhält man:

$$f = \sum c_{i_1 \ldots i_m} y_1^{i_1} \ldots y_m^{i_m} t^{\frac{i_1}{r_1} + \ldots \frac{i_m}{r_m}},$$

also ist der Exponent des ersten nichtverschwindenden Terms der Index von f.

LEMMA 8. *Für den Index in $(\alpha_1, \ldots, \alpha_m)$ bezüglich $(r_1, \ldots, r_m)$ gilt:*

- $index(f_{i_1 \ldots i_m}) \geq index(f) - \sum \frac{i_h}{r_h}$.
- $index(f + g) \geq \min(index(f), index(g))$.
- $index(fg) = index(f) + index(g)$.
- $index(f) = 0$ *genau dann, wenn* $f(\alpha_1, \ldots, \alpha_m) \neq 0$.

Beweis:

- Sei $g = f_{i_1 \ldots i_m}$ und $index(g) = \frac{j_1}{r_1} + \ldots \frac{j_m}{r_m}$ mit $g_{j_1 \ldots j_m}(\alpha_1, \ldots, \alpha_m) \neq 0$. Dann ist auch $f_{i_1 + j_1, \ldots, i_m + j_m}(\alpha_1, \ldots, \alpha_m) \neq 0$, also
$$index(f) \leq \sum \frac{i_h + j_h}{r_h} = index(g) + \sum \frac{i_h}{r_h},$$
woraus die erste Behauptung folgt.
- Die zweite und dritte Behauptung folgen leicht mit obiger Bemerkung. Die vierte Behauptung ist trivial. ■

SATZ 18 (A). *Sei α eine ganze algebraische Zahl vom Grad $d \geq 2$. Sei $\epsilon > 0$ beliebig und $m \in \mathbf{N}$ so, daß*

$$m > \frac{16 \log 4d}{\epsilon^2}.$$

Seien weiter $r_1, \ldots, r_m$ natürliche Zahlen. Dann gibt es ein Polynom $f(x_1, \ldots, x_m) \in \mathbf{Z}[x_1, \ldots, x_m]$, $f \neq 0$ mit den Eigenschaften:

- *$grad_{x_h} f \leq r_h$ für $h = 1, \ldots, m$.*
- *$index(f) \geq \frac{m}{2}(1-\epsilon)$ in $(\alpha, \ldots, \alpha)$ bezüglich $(r_1, \ldots, r_m)$.*
- *$|f| \leq B^{r_1 + \cdots + r_m}$, wo $B = B(\alpha) = 4(|Q|+1)$ gewählt werden kann mit Q dem Minimalpolynom von α.*

Beweis: Wir machen den Ansatz

$$f = \sum_{j_1=0}^{r_1} \cdots \sum_{i_m=0}^{r_m} c_{j_1 \ldots j_m} x_1^{j_1} \ldots x_m^{j_m},$$

und wollen $c_{j_1 \ldots j_m} \in \mathbf{Z}$ so bestimmen, daß die Aussagen des Satzes erfüllt sind. Von den c's gibt es

$$N = (r_1 + 1) \ldots (r_m + 1)$$

Stück, d.h. soviele unbekannte Größen haben wir. Die zweite Bedingung lautet nun

$$f_{i_1 \ldots i_m}(\alpha, \ldots, \alpha) = 0 \quad \text{für} \quad \frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m} < \frac{m}{2}(1-\epsilon).$$

Um die Anzahl dieser Bedingungen abzuschätzen, benutzen wir folgendes kombinatorische Lemma:

LEMMA 9.

$$\#\{(i_1, \ldots, i_m) : 0 \leq i_h \leq r_h, |\sum \frac{i_h}{r_h} - \frac{m}{2}| \geq \epsilon \frac{m}{2}\} \leq (r_1 + 1) \ldots (r_m + 1) \cdots 2e^{-\frac{\epsilon^2 m}{16}}.$$

Den Beweis des Lemmas stellen wir zurück. (Siehe W. M. Schmidt, Diophantine Approximation, LN 785, S. 121.)

Fortsetzung des Beweises: Ist $\sum \frac{i_h}{r_h} < \frac{m}{2}(1-\epsilon)$, so läßt sich dies auch schreiben $\epsilon \frac{m}{2} < \frac{m}{2} - \sum \frac{i_h}{r_h}$, so daß man das Lemma anwenden kann. Also sind höchstens

$$(r_1 + 1) \ldots (r_m + 1) \cdot 2e^{-\frac{\epsilon^2 m}{16}} < \frac{N}{2d}$$

Ausdrücke $f_{i_1 \ldots i_m}(\alpha, \ldots, \alpha) = 0$ zu betrachten. Wir betrachten eine Gleichung:

$$f_{i_1 \ldots i_m}(\alpha, \ldots, \alpha) = \sum \binom{j_1}{i_1} \ldots \binom{j_m}{i_m} c_{j_1 \ldots j_m} \alpha^{j_1 - i_1 + \cdots + j_m - i_m} = 0.$$

Hier hat man jetzt nach $1, \alpha, \ldots, \alpha^{d-1}$ zu entwickeln. Nach einem früheren Lemma ist der Koeffizient bei $c_{j_1 \ldots j_m}$ in dieser Gleichung nach oben durch

$$\binom{j_1}{i_1} \ldots \binom{j_m}{i_m} (|Q|+1)^{j_1 - i_1 + \cdots + j_m - i_m} \leq (2|Q|+2)^{r_1 + \cdots + r_m}$$

beschränkt. Also gibt es $\leq \frac{N}{2}$ Gleichungen. Nach dem Lemma von Siegel gibt es also eine nichttriviale Lösung mit

$$|f| = \max(|c_{j_1 \ldots j_m}|) \leq (N \cdot (2|Q|+2)^{r_1 + \cdots + r_m})^{\frac{M}{N-M}} \leq N \cdot (2|Q|+2)^{r_1 + \cdots + r_m} \leq (4(|Q|+1)^{r_1 + \cdots + r_m},$$

womit alles gezeigt wäre. ■

Wir wollen nun zeigen, daß solch ein Polynom f auch in $(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m})$ entsprechend verschwinden muß, wenn die $\frac{p_i}{q_i}$ gute Approximationen an α sind. Dies geht ganz in Analogie zum Satz von Liouville.

SATZ 19 (B). *Sei f wie im vorigen Satz gegeben und $0 < \delta < 1$ und $0 < \epsilon < \frac{\delta}{23}$. Sind $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ rationale Approximationen an α mit*

$$|\alpha - \frac{p_h}{q_h}| < \frac{1}{q_h^{2+\delta}} \quad \text{und} \quad q_h^{\delta} > D$$

für alle $h = 1, \ldots, m$, wo $D = D(\alpha) = (16B(\alpha)\max(1, |\alpha|))^4$. Wir nehmen weiter an, daß

$$r_1 \ln q_1 \leq r_h \ln q_h \leq (1+\epsilon) r_1 \ln q_1$$

für alle $h = 1, \ldots, m$. Dann gilt für den Index von f in $(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m})$ bezüglich $(r_1, \ldots, r_m)$:

$$index(f) \geq \epsilon m.$$

Beweis: Zu zeigen ist: Ist

$$\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} < \epsilon m \quad \text{und} \quad g = f_{j_1 \ldots j_m},$$

so gilt

$$g(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}) = 0.$$

Nun ist $|f| \leq B^{r_1 + \cdots + r_m}$, und damit nacheinander durch Anwendung eines Lemmas:

$$|g| \leq (2B)^{r_1 + \cdots + r_m}, \quad |g_{i_1 \ldots i_m}| \leq (4B)^{r_1 + \cdots + r_m}.$$

Daher ist

$$\begin{aligned} |g_{i_1 \ldots i_m}(\alpha, \ldots, \alpha)| &\leq (r_1 + 1) \ldots (r_m + 1) \cdot (4B)^{r_1 + \cdots + r_m} (\max(1, |\alpha|))^{r_1 + \cdots + r_m} \\ &\leq (8B \max(1, |\alpha|)^{r_1 + \cdots + r_m} = C^{r_1 + \cdots + r_m}, \end{aligned}$$

wenn wir $C = C(\alpha) = 8B \max(1, |\alpha|)$ setzen. Der Index von g in $(\alpha, \ldots, \alpha)$ ist nun nach Lemma

$$index(g) \geq \frac{m}{2}(1-\epsilon) - \sum \frac{j_h}{r_h} \geq \frac{m}{2}(1-\epsilon) - \epsilon m = \frac{m}{2}(1 - 3\epsilon).$$

Wir betrachten nun die Taylorreihenentwicklung von g in Punkt $(\alpha, \ldots, \alpha)$:

$$g = \sum_{\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m} \geq \frac{m}{2}(1-3\epsilon)} g_{i_1 \ldots i_m}(\alpha, \ldots, \alpha)(x_1 - \alpha)^{i_1} \ldots (x_m - \alpha)^{i_m},$$

und daher

$$\begin{aligned} |g(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m})| &< \sum_{\sum \frac{i_h}{r_h} \geq \frac{m}{2}(1-3\epsilon)} C^{r_1 + \cdots + r_m} (q_1^{i_1} \ldots q_m^{i_m})^{-2-\delta} = \\ &= \sum_{\sum \frac{i_h}{r_h} \geq \frac{m}{2}(1-3\epsilon)} C^{r_1 + \cdots + r_m} (q_1^{r_1 \frac{i_1}{r_1}} \ldots q_m^{r_m \frac{i_m}{r_m}})^{-2-\delta} \leq \\ &\leq \sum_{\sum \frac{i_h}{r_h} \geq \frac{m}{2}(1-3\epsilon)} C^{r_1 + \cdots + r_m} \frac{1}{q_1^{r_1(2+\delta)(\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m})}} \leq \\ &\leq (2C)^{r_1 + \cdots + r_m} \frac{1}{q_1^{r_1(2+\delta)(\frac{m}{2}(1-3\epsilon))}} = \\ &= \prod_{h=1}^{m} \frac{(2C)^{r_h}}{q_1^{r_1(1+\epsilon)\frac{(2+\delta)(1-3\epsilon)}{2(1+\epsilon)}}} \leq \\ &\leq \prod_{h=1}^{m} \left(\frac{2C}{q_h^{\frac{(2+\delta)(1-3\epsilon)}{2(1+\epsilon)}}} \right)^{r_h} \end{aligned}$$

Nun ist $\frac{(2+\delta)(1-3\epsilon)}{2(1+\epsilon)} \geq 1 + \frac{\delta}{4}$ äquivalent zu $\epsilon \leq \frac{\delta}{16+7\delta}$. Wir hatten aber $\delta < 1$ und $\epsilon < \frac{\delta}{23}$ vorausgesetzt, also gilt

$$\epsilon < \frac{\delta}{16+7} < \frac{\delta}{16+7\delta},$$

und damit

$$|g(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m})| < \prod_{h=1}^{m}\left(\frac{2C}{q_h^{1+\delta/4}}\right)^{r_h} \le \prod_{h=1}^{m}\frac{1}{q_h^{r_h}},$$

da nach Voraussetzung $(2C)^4 \le q_h$ gilt.
Nun ist aber nach altbekanntem Schluß

$$g(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}) \in \prod_{h=1}^{m}\frac{1}{q_h^{r_h}}\cdot\mathbf{Z},$$

woraus mit obiger Abschätzung aber sofort $g(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}) = 0$ folgt. Damit ist der Beweis beendet. ■

Der wichtige Schritt kommt nun: f kann in $(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m})$ doch nicht zu stark verschwinden. Diese Aussage liefert das sogenannte Rothsche Lemma:

Satz 20 (C). *Sei $0 < \epsilon < \frac{1}{12}$ und $m \in \mathbf{N}$. Setze $\omega = \omega(m,\epsilon) = \frac{24}{2^m}(\frac{\epsilon}{12})^{2^{m-1}}$. Seien $r_1,\ldots,r_m$ natürliche Zahlen mit $\omega r_h \ge r_{h+1}$. Seien weiter $\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}$ rationale Zahlen (gekürzt, $q_h > 0$) mit*

$$q_h^{r_h} \ge q_1^{r_1} \text{ und } q_h^{\omega} \ge 2^{3m}.$$

Ist $f \in \mathbf{Z}[x_1,\ldots,x_m]$, $f \ne 0$, vom Grad $\le r_h$ in x_h mit $|f| \le q_1^{\omega r_1}$, dann ist der Index von f in $(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m})$ bezüglich $(r_1,\ldots,r_m)$

$$index(f) \le \epsilon.$$

Bemerkungen zum Beweis stellen wir zunächst zurück. Wir wollen nun erst den Satz von Thue-Siegel-Roth beweisen. Sei α eine algebraische Zahl vom Grad $d \ge 2$ und $\delta > 0$. Wir nehmen an, die Ungleichung

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\delta}}$$

besitzt unendlich viele Lösungen.

1. O.E. sei $0 < \delta < 1$. Wir wählen ϵ mit $0 < \epsilon < \frac{\delta}{23}$. Dann ist auch $0 < \epsilon < \frac{1}{12}$.
2. Wähle $m \in \mathbf{N}$ mit $m > \frac{16\log 4d}{\epsilon^2}$ und definiere $\omega = \omega(m,\epsilon)$ wie zuvor.
3. Wähle eine Approximation $\frac{p_1}{q_1}$, die obige Ungleichung erfüllt und $q_1^{\omega} > B(\alpha)^m$, sowie $q_1^{\delta} > D(\alpha)$. Wegen $B \ge 8$ ist $q_1^{\omega} > 2^{3m}$.
4. Wähle sukzessiv $\frac{p_2}{q_2},\ldots,\frac{p_m}{q_m}$, die die Ungleichung erfüllen und mit $\omega\log q_{h+1} \ge 2\log q_h$.
5. Sei r_1 eine natürliche Zahl mit $\epsilon r_1 \log q_1 \ge \log q_m$.
6. Setze für $h = 2,\ldots,m$: $r_h = \lfloor \frac{r_1\log q_1}{\log q_h}\rfloor + 1$. Dann gilt für $h = 2,\ldots,m$:

$$r_1\log q_1 < r_h\log q_h \le r_1\log q_1 + \log q_h \le (1+\epsilon)r_1\log q_1.$$

Weiter folgt:

$$\begin{aligned}\frac{r_{h+1}}{r_h} &\le \frac{\frac{r_1\log q_1}{\log q_{h+1}}+1}{\frac{r_1\log q_1}{\log q_h}} = \\ &= \frac{\log q_h}{\log q_{h+1}}\frac{r_1\log q_1+\log q_{h+1}}{r_1\log q_1} \le \\ &\le \frac{\log q_h}{\log q_{h+1}}\frac{r_1\log q_1(1+\epsilon)}{r_1\log q_1} \le \\ &\le \frac{\omega}{2}(1+\epsilon) < \omega.\end{aligned}$$

7. Die Voraussetzungen von Satz A sind nun erfüllt und es gibt dazu ein Polynom $f \in \mathbf{Z}[x_1,\ldots,x_m]$ mit den entsprechenden Eigenschaften.
8. Nach Satz B ist der Index von f in $(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m})$ bezüglich $(r_1,\ldots,r_m) \ge \epsilon m$.
9. Die Voraussetzungen von Satz C sind erfüllt, denn es gilt die Abschätzung

$$|f| \le B^{r_1+\cdots+r_m} \le B^{mr_1} \le q_1^{\omega r_1},$$

also gilt der Satz und liefert für den Index: $index(f) \le \epsilon$. Dies ist aber ein Widerspruch zur vorhergehenden Aussage über den Index. Also ist die Annahme falsch, daß man beliebig gute Approximationen an α finden kann, d.h. der Satz von Thue-Siegel-Roth ist bewiesen. ■

Bemerkung:

1. Sei $\delta > 0$ und α algebraisch vom Grad $d \geq 2$. Dann gibt es eine natürliche Zahl $Q(\alpha, \delta)$ mit der Eigenschaft:
$$|\alpha - \frac{p}{q}| \geq \frac{1}{q^{2+\delta}} \quad \text{für} \quad q \geq Q(\alpha, \delta).$$
Der Beweis beruht auf Annahme und Widerspruch. Er liefert leider keine Möglichkeit $Q(\alpha, \delta)$ zu berechnen.
2. Für $d = 2$ ist natürlich der Satz von Liouville schärfer und außerdem konstruktiv. D.h. der Satz von Thue-Siegel-Roth ist erst für algebraische Zahlen vom Grad ≥ 3 interessant.
3. Ist $\alpha \in \mathbf{C} \notin \mathbf{R}$, so gilt natürlich
$$|\alpha - \frac{p}{q}| \geq |im\alpha|,$$
und damit kann es nur endlich viele $\frac{p}{q}$ geben mit
$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\delta}},$$
d.h. in diesem Fall ist der Satz von Thue-Siegel-Roth trivialerweise erfüllt.

Beweis von Satz C für $m = 1$: In diesem Fall ist $\omega = \epsilon$. Sei also $f \in \mathbf{Z}[x]$ gegeben vom Grad $\leq r$. Wir wollen den Index von f in $\frac{p}{q}$ abschätzen. Sei i die Nullstellenordnung von f in $\frac{p}{q}$. Dann gibt es ein $g \in \mathbf{Z}[x]$ mit
$$f = (qx - p)^i \cdot g.$$
Da g ganze Koeffizienten hat, teilt q^i den höchsten Koeffizienten von f, also
$$q^i \leq |f|.$$
Damit gilt für den Index von f in $\frac{p}{q}$ bezüglich r:
$$index(f) = \frac{i}{r} \leq \frac{\log |f|}{\log q}.$$
Wird nun $|f| \leq q^{\omega r}$ vorausgesetzt, so folgt sofort $index(f) \leq \epsilon$, was wir zeigen wollten. ■

Der Beweis des Lemmas von Roth im Fall $m \geq 2$ ist deutlich aufwendiger. Er soll hier nicht behandelt werden. Vielleicht kommen wir beim Produktsatz von Faltings darauf zurück.

KAPITEL 6

Thue-Gleichungen

Thue hat 1908 Gleichungen untersucht, die jetzt nach ihm benannt werden:

$$f(x,y) = m,$$

wo $f(x,y) = \sum_{i=0}^{d} a_i x^{d-i} y^i$ ein homogenes Polynom vom Grad d mit ganzen Koeffizienten ist.

Bemerkung: Wir haben bereits gesehen, daß für eine quadratfreie natürliche Zahl $n >$ die Pellsche Gleichung $x^2 - ny^2 = 1$ unendlich viele ganzzahlige Lösungen hat.

Überlegung:

- Sei $f(x,y) = \sum_{i=0}^{d} a_i x^{d-i} y^i$ ein irreduzibles homogenes Polynom in $\mathbf{Z}[x,y]$ vom Grad $d \geq 3$.
- Ist
$$f(x,1) = a_0 \prod (x - \alpha_i),$$
so sind die α_i konjugierte algebraische Zahlen vom Grad d. Es gilt
$$f(x,y) = a_0 \prod (x - \alpha_i y) = a_d \prod (\frac{1}{\alpha_i} x - y).$$
- Sei
$$2r = \min(\min_{i \neq j} |\alpha_i - \alpha_j|, \min_{i \neq j} |\frac{1}{\alpha_i} - \frac{1}{\alpha_j}|).$$
- Sei weiter $c = c(\epsilon) > 0$ so, daß
$$|\alpha_i - \frac{p}{q}| \geq \frac{c}{q^{2+\epsilon}}, \quad |\beta - \frac{p}{q}| \geq \frac{c}{q^{2+\epsilon}}.$$
- Wir wollen jetzt $f(x,y)$ abschätzen für $(x,y) \in \mathbf{Z}^2$. Wir betrachten zunächst den Fall $y \neq 0$. Die Zahl $\frac{x}{y}$ kann nicht von zwei verschiedenen α_i einen Abstand $< r$ haben, o.E. $|\alpha_i - \frac{x}{y}| \geq r$ für $i \neq i_0$. Damit können wir abschätzen:
$$\begin{aligned} |f(x,y)| &= |y|^d |a_0| \prod_{i \neq i_0} |\alpha_i - \frac{x}{y}| \cdot |\alpha_{i_0} - \frac{x}{y}| \geq \\ &\geq |y|^d |a_0| r^{d-1} \frac{c}{|y|^{2+\epsilon}} = \\ &= |a_0| c r^{d-1} \cdot |y|^{d-2-\epsilon}. \end{aligned}$$
- Ist $x \neq 0$, so studiert man die Approximation von $\frac{y}{x}$ an $\frac{1}{\alpha_i}$ und erhält analog:
$$|f(x,y)| \geq |a_d| c r^{d-1} \cdot |x|^{d-2-\epsilon}.$$
- Damit haben wir folgenden Satz bewiesen:

SATZ 21. *Ist $f(x,y) \in \mathbf{Z}[x,y]$ homogen und irreduzibel vom Grad $d \geq 3$, so gibt es für jedes $\epsilon > 0$ ein $C(\epsilon) > 0$ mit der Eigenschaft, daß für alle $(x,y) \in \mathbf{Z}^2$ gilt:*

$$|f(x,y)| \geq C(\epsilon) \max(|x|, |y|)^{d-2-\epsilon}.$$

Bemerkungen: Sei $f(x,y) \in \mathbf{Z}[x,y]$ wie im Satz.

1. Trivalerweise haben wir die Abschätzung
$$|f(x,y)| \leq (d+1)|f| \cdot \max(|x|, |y|)^d.$$

2. Wie gut ist die Abschätzung in obigem Satz? Wir nehmen an, daß $\alpha = \alpha_1$ reell ist. Ist dann $\frac{p}{q}$ ein Näherungsbruch an α, so gilt
$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}$$
und
$$|\alpha_i - \frac{p}{q}| \leq |\alpha_i - \alpha| + |\alpha - \frac{p}{q}| \leq |\alpha_i - \alpha| + 1.$$
Ist $k = |a_0| \prod_{i=2}^{d} (|\alpha_i - \alpha| + 1)$, so gilt
$$|f(p,q)| < k \cdot q^{d-2} \leq k \max(|p|, q)^{d-2}.$$

Daraus erfolgt sich als Folgerung unmittelbar der auf Thue zurückgehende Satz:

SATZ 22. *Sei $f(x,y)$ ein irreduzibles homogenes Polynom vom Grad $d \geq 3$ mit ganzen Koeffizienten und $m \in \mathbf{N}$. Dann besitzt die Gleichung*
$$f(x,y) = m$$
nur endlich viele ganzzahlige Lösungen.

Zur Übung beweise man folgenden Satz:

SATZ 23. *Ist $f(x,y) \in \mathbf{Z}[x,y]$ ein irreduzibles homogenes Polynom vom Grad $d \geq 3$ und $g(x,y) \in \mathbf{Z}[x,y]$ mit Totalgrad $\leq d-3$, so hat die Gleichung*
$$f(x,y) = g(x,y)$$
nur endlich viele Lösungen $(x,y) \in \mathbf{Z}^2$.

Bemerkung: Da Thue-Siegel-Roth nicht in einer effektiven Version vorhanden ist, liefert der Beweis leider auch nur eine Endlichkeitsaussage.

Beispiel: Der Satz liefert, daß $x^3 - 2y^3 = 1$ nur endlich viele Lösungen hat. Zwei davon sieht man sofort, nämlich $(1,0)$ und $(-1,-1)$. Gibt es weitere? Wie bereits erwähnt, hat Baker die Abschätzung
$$|\sqrt[3]{2} - \frac{p}{q}| \geq \frac{1}{10^6 \cdot q^{2.955}}$$
bewiesen. Sei $\alpha = \sqrt[3]{2}$. Dann ist
$$|\frac{x}{y} - \zeta_3 \alpha| \geq |im(\zeta_3 \alpha)| = \frac{1}{2}\sqrt{3}\sqrt[3]{2},$$
und das gleiche gilt für das komplex Konjugierte. Also haben wir
$$\begin{aligned} \frac{1}{|y|^3} &= |\alpha - \frac{x}{y}| \cdot |\zeta_3 \alpha - \frac{x}{y}| \cdot |\zeta_3^2 \alpha - \frac{x}{y}| > \\ \frac{1}{10^6 \cdot |y|^{2.955}} \cdot (\frac{1}{2}\sqrt{3}\sqrt[3]{2})^2 &= \\ &= \frac{3\sqrt[3]{4}}{4 \cdot 10^6 |y|^{2.955}} \end{aligned}$$
Damit
$$|y| < \left(\frac{4 \cdot 10^6}{3\sqrt[3]{4}}\right)^{\frac{1}{0.045}} < 4.5 \cdot 10^{131}.$$
Leider ist dies auch noch eine sehr große Zahl, aber im Prinzip kann man durchprobieren, ob es weitere Lösungen gibt.

Mit den Methoden der diophantischen Approximation lassen sich aber Abschätzungen für die Anzahl der Lösungen einer Thue-Gleichung herleiten. Dafür wollen wir ohne Beweis ein Beispiel geben. Folgender Satz findet sich bei W. M. Schmidt, LN 1467, S. 75:

SATZ 24. *Es gibt eine absolute Konstante c mit der Eigenschaft: Ist $f \in \mathbf{Z}[x,y]$ irreduzibel homogen vom Grad $d \geq 3$, so gilt:*
$$\#\{(x,y) \in \mathbf{Z}^2 : |f(x,y)| \leq m\} \leq c \cdot d \cdot m^{\frac{2}{d}} \cdot (1 + \log m^{\frac{1}{d}}).$$

Bemerkung: Für $m = 1$ sagt der Satz:

$$\#\{(x, y) \in \mathbf{Z}^2 : f(x, y) = 1\} \leq c \cdot d.$$

Betrachte nun

$$f = x^d + \lambda(x - y)(2x - y) \dots (dx - y) = 1.$$

Diese Gleichung hat mindestens d Lösungen, nämlich

$$(1, 1), \quad (1, 2), \dots, (1, d).$$

Ist d gerade, so gibt es außerdem noch die Lösungen

$$(-1, -1), \quad (-1, -2), \quad \dots, (-1, -d),$$

dann hat man insgesamt also mindestens $2d$ Lösungen. Mit diesem Beispiel sieht man, daß die Abschätzung für $m = 1$ bis auf die Konstante gut ist.

KAPITEL 7

Die Gleichung $x^3 - dy^3 = 1$

In diesem Abschnitt wollen wir versuchen, etwas mehr über die ganzzahligen Lösungen der Gleichung $x^3 - dy^3 = 1$ auszusagen. O.E. können wir $d \geq 0$ annehmen. Ist die Form $x^3 - dy^3 \in \mathbf{Z}[x, y]$ irreduzibel, so gibt es nach dem Satz von Thue nur endlich viele ganzzahlige Lösungen.
Andererseits ist für $d = 0$ die Bedingung einfach $x = 1$, es gibt also unendlich viele ganzzahlige Lösungen.
Im folgenden können wir also $d > 0$ annehmen.
Eine ganzzahlige Lösung hat man immer, nämlich $(1, 0)$.

Geometrie: Wie sehen die Kurven aus? Es ist mit $\alpha = \sqrt[3]{d}$

$$y = \sqrt[3]{\frac{x^3 - 1}{d}} = \frac{1}{\alpha}\sqrt[3]{x^3 - 1} = \frac{x}{\alpha}\sqrt[3]{1 - \frac{1}{x^3}}.$$

Weiter:

$$\frac{dy}{dx} = \frac{1}{\alpha}\left(\frac{x}{\sqrt[3]{x^3 - 1}}\right)^2,$$

$y(x)$ ist also monoton, die Steigung in $x = 1$ ist unendlich, die Steigung in $x = 0$ ist 0. Damit kann man ein Bild zeichnen.

Der Fall $d = m^3 > 0$**:** O.E.$y \neq 0$. In diesem Fall faktorisiert die Gleichung:

$$(x - my)(x^2 + mxy + m^2y^2) = 1.$$

Also muß gelten

$$x - my = x^2 + mxy + m^2y^2 = \pm 1.$$

$m \geq 2$**:** Nun ist

$$x^2 + mxy + m^2y^2 = (x + \frac{m}{2}y)^2 + \frac{3m^2}{4}y^2 \geq 3,$$

es gibt also keine Lösungen mit $y \neq 0$.

$m = 1$**:** Es ist

$$x^2 + xy + y^2 = (x + \frac{y}{2})^2 + \frac{3}{4}y^2.$$

Für $|y| \geq 2$ gilt daher

$$x^2 + xy + y^2 \geq 3,$$

d.h. wir erhalten keine Lösung. Bleibt also nur noch der Fall $y = \pm 1$ zu behandeln. Wir setzen einfach ein: $y = 1$ geht nicht, $y = -1$ liefert $x = 0$.

Zusammenfassung: Die Lösungsmenge der Gleichung $x^3 - m^3y^3 = 1$ sieht wie folgt aus: $\{(1, y) : y \in \mathbf{Z}\}$ für $m = 0$, $\{(1, 0), (0, -1)\}$ für $m = 1$ und $\{(1, 0)\}$ für $m \geq 2$.

Wir können uns jetzt also auf den Fall, daß d kubikfrei ist beschränken. Was kann man mit diophantischer Approximation erreichen? Sei $\alpha = \sqrt[3]{d}$. Wir nehmen an, (x, y) ist eine Lösung von $x^3 - dy^3 = 1$ mit $y \neq 0$. Dann gilt:

$$|\alpha - \frac{x}{y} = \frac{1}{((\frac{x}{y})^2 + \alpha(\frac{x}{y}) + \alpha^2)|y| \cdot |y|^2}.$$

- Für $|y| \geq 2$ gilt:

$$((\frac{x}{y})^2 + \alpha(\frac{x}{y}) + \alpha^2)|y| \geq \frac{3}{4}\alpha^2|y| \geq \frac{3}{4}\sqrt[3]{4} \cdot 2 \geq 2.38,$$

  also

$$|\alpha - \frac{x}{y}| \leq \frac{2.38y^2}{.}$$

- Für $y = 1$ ist $x = \sqrt[3]{d+1}$, für $y = -1$ ist $x = -\sqrt[3]{d-1}$, wir müssen also abschätzen

$$|\sqrt[3]{d} - \sqrt[3]{d+1}| \text{ bzw. } |\sqrt[3]{d} - \sqrt[3]{d-1}.$$

  Für $z = x^{1/3}$ ist $z' = \frac{1}{3x^{2/3}}$, nach dem Mittelwertsatz der Differentialrechnung sind also obige Ausdrücke für $d \geq 2$ sicher $\leq \frac{1}{3}$.

Wir haben also sicher die Approximation

$$|\alpha - \frac{x}{y}| < \frac{1}{2y^2},$$

falls (x, y) eine ganzzahlige Lösung mit $y \neq 0$ ist. Daher erhalten wir:

Ergebnis: Für kubikfreies $d > 0$ kommt $\pm\frac{x}{y}$ als Näherungsbruch in der Kettenbruchentwicklung von $\sqrt[3]{d}$ vor. (Vom trivialen Fall $(1, 0)$ abgesehen.)

Beispiele: Berechne die Kettenbruchentwicklung von $\alpha = \sqrt[3]{d}$ und betrachte für die Näherungsbrüche $\frac{p_n}{q_n}$, ob $p_n^3 - dq_n^3 = \pm 1$ ist.

1. $d = 3$: Dann ist

$$\sqrt[3]{3} = [1, 2, 3, 1, 4, 1, 5, 1, 1, 6, 2, \ldots]$$

   und damit

$$p_n^3 - 3q_n^3 = -2, 3, -29, 10, -193, 51, -928, 1103, -587, 11435, -10351, \ldots,$$

   die Gleichung $x^3 - 3y^3 = 1$ scheint also keine weitere Lösung zu besitzen.
2. $d = 20$: Man findet

$$\sqrt[3]{20} = [2, 1, 2, 1, 1, 154, 6, 1, 1, 1, 6, \ldots]$$

   und damit

$$p_n^3 - 20q_n^3 = -12, 7, -28, 51, -1, 3593, -84259, 61732, \ldots;$$

   der zu -1 gehörige Näherungsbruch ist $\frac{19}{7}$, also gibt es noch die Lösung $(-19, -7)$.
3. Betrachtet man für die kubikfreien Zahlen $2 \geq d \geq 100$ die Kettenbruchentwicklungen auf 10 Stellen genau, so findet man für die nachfolgenden d noch als zusätzliche Lösung:

d	weitere Lösung
2	$(-1, -1)$
7	$(2, 1)$
9	$(-2, -1)$
17	$(18, 7)$
19	$(-8, -3)$
20	$(-19, -7)$
26	$(3, 1)$
28	$(-3, -1)$
37	$(10, 3)$
43	$(-7, -2)$
63	$(4, 1)$
65	$(-4, -1)$
91	$(9, 2)$

Wir wollen jetzt versuchen, auf algebraischem Weg etwas über die Gleichung $x^3 - dy^3 = 1$ auszusagen. Dazu bemerken wir, daß mit $\alpha = \sqrt[3]{d}$ gilt:

$$x^3 - dy^3 = (x - y\alpha)(x^2 + xy\alpha + y^2\alpha^2),$$

d.h. $x - y\alpha$ ist eine Einheit im Ring $\mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2$. Als Endergebnis wollen wir zeigen:

SATZ 25. *Sei d eine kubenfreie natürliche Zahl $d > 1$. Dann besitzt die Gleichung $x^3 - dy^3 = 1$ außer $(x, y) = (1, 0)$ höchstens noch eine weitere Lösung in ganzen Zahlen. In diesem Fall ist $x - y\alpha$ eine Grundeinheit in $\mathbf{Z}[\alpha]$.*

Der Beweis wird etwas Raum beanspruchen. Deshalb zunächst einige Vorüberlegungen zu den Einheiten von $\mathbf{Z}[\alpha]$.

- Die Konjugierten von $x + y\alpha + z\alpha^2$ sind $x + y\zeta\alpha + z\zeta^2\alpha^2$ und $x + y\zeta^2\alpha + z\zeta\alpha^2$, ihr Produkt ist die Norm:
$$N(x + y\alpha + z\alpha^2) = x^3 + dy^3 + d^2z^3 - 3dxyz,$$
die multiplikativ ist.
- Sei U die Gruppe der Einheiten von $\mathbf{Z}[\alpha]$. Wegen der Multiplikativität der Norm gilt:
$$x + y\alpha + z\alpha^2 \in U \iff x^3 + dy^3 + d^2z^3 - 3dxyz = \pm 1.$$
In diesem Fall gilt:
$$(x + y\alpha + z\alpha^2)^{-1} = \pm(x^2 - dyz) + (dz^2 - xy)\alpha + (y^2 - xz)\alpha^2).$$
- Ähnlich wie bei der Pellschen Gleichung für die Einheiten von $\mathbf{Z}[\sqrt{d}]$ kann man auch hier folgende logarithmische Abbildung betrachten:
$$\phi : U \to \mathbf{R}^2, x + y\alpha + z\alpha^2 \mapsto (\log|x + y\alpha + z\alpha^2|, \log|x + y\zeta\alpha + z\zeta^2\alpha^2|).$$
Wegen der Normbedingung ist $\phi(U) \subseteq \{x + 2y = 0\}$ und man überzeigt sich, daß $\phi(U)$ eine diskrete Untergruppe ist. Also hat U die Form
$$U = \{\pm\mu^n : n \in \mathbf{Z}\}$$
oder $U = \{\pm 1\}$. Der letzte Fall kann aber nicht eintreten. μ heißt dann eine Grundeinheit.
- Die Frage, die wir untersuchen müssen, lautet also: Für welche $n \in \mathbf{Z}$ ist der Koeffizient von μ^n bei α^2 identisch 0? Der Einfachkeit halber nennen wir eine solche Einheit eine binomiale Einheit.

LEMMA 10. 1. *Eine binomiale Einheit hat Betrag < 1.*

2. *Keine Einheit der Form*
$$(x + y\alpha)^n, n = \pm 2, \pm 3, dots, (x + z\alpha^2)^n, n = \pm 1, \pm 2, \ldots$$
ist binomial.
3. *Das Quadrat einer Einheit ist nicht binomial.*
4. *Die dritte Potenz einer Einheit ist nicht binomial.*
5. *Ist $\mu = x + y\alpha + z\alpha^2$ eine Einheit mit $xyz \neq 0$, so ist für $n \in \mathbf{N}$ und $n \equiv 1 \bmod 2$, $n \equiv 1 \bmod 3$ die Potenz μ^n nicht binomial.*
6. *Ist $\mu = x + y\alpha + z\alpha^2$ eine Einheit mit $xyz \neq 0$, so ist für $n \in \mathbf{N}$ und $n \equiv 1 \bmod 2$, $n \equiv 2 \bmod 3$ die Potenz μ^n nicht binomial.*

Ist das Lemma bewiesen, so folgt daraus sofort der Satz. Es gibt dann also zwei Möglichkeiten: Sei $\mu = x + y\alpha + z\alpha^2$ Grundeinheit mit $|\mu| < 1$. Ist $z = 0$, so ist $x^3 + dy^3 = \pm 1$, wir haben also eine weitere Lösung unserer Gleichung, wenn nicht, gibt es keine weitere Lösung. Um wirkliche Konstruktivität zu erreichen, müßte jetzt noch ein Algorithmus angegeben werden, der die Grundeinheit μ bestimmt. Darauf wollen wir aber verzichten.

Wir wollen hier den Beweis des Lemmas nicht ganz vorführen. Der Beweis findet sich bei Mordell, S. 220-225. Hier nur ein paar triviale Anmerkungen:

Zu 1.: Ist $x - y\alpha$ eine Einheit mit $y \neq 0$ und $x^3 - dy^3 = 1$, so haben wir gesehen, daß $|\alpha - \frac{x}{y}| < \frac{1}{2y^2}$ ist, also

$$|x - y\alpha| = |y||\alpha - \frac{x}{y}| < \frac{1}{2|y|} < 1,$$

was in 1. behauptet war.

Zu 3.: Sei $\mu = x + y\alpha + z\alpha^2$ eine Einheit mit $xyz \neq 0$ und Norm 1. Dann ist

$$\mu^2 = (x^2 + 2dyz) + (2xy + dz^2)\alpha + (2xz + y^2)\alpha^2.$$

μ^2 ist binomial, wenn $2xz + y^2 = 0$ ist. Wir müssen also das Gleichungssystem

$$x^3 + dy^3 + d^2z^3 - 3dxyz = 1 \text{ und } 2xz + y^2 = 0$$

ganzen Zahlen lösen. Dies ist zunächst nicht trivial. Man kann zeigen, daß nur die Lösungen $(1, 0, 0)$ und für $d = 1$ außerdem $(0, 0, 1)$ existieren. Diese sind aber in unserem Fall uninteressant.

Zu 6.: Wir schreiben $\mu = x + y\alpha + z\alpha^2$ und nehmen an, daß gilt:

$$\mu^n = u + v\alpha.$$

Sind μ_1 und μ_2 die Konjugierten von μ, so gilt:

$$\mu^n + \zeta\mu_1^n + \zeta^2\mu_2^n = \cdots = 0.$$

Wegen $n \equiv 2 \bmod 3$ läßt sich dies aber auch so schreiben:

$$\mu^n + (\zeta^2\mu_1)^n + (\zeta\mu_2)^n = 0.$$

Da n ungerade ist, teilt $\zeta^2\mu_1 + \zeta\mu_2$ die Zahl μ^n, muß also selbst Einheit sein. Nun ist

$$\zeta^2\mu_1 + \zeta\mu_2 = -x + 2y\alpha - z\alpha^2.$$

Die Normbedingungen liefern daher:

$$x^3 + dy^3 + d^2z^3 - 3dxyz = 1 \text{ und } -x^3 + 8dy^3 - d^2z^3 - 6dxyz = 1$$

oder

$$x^3 + dy^3 + d^2z^3 - 3dxyz = 1 \text{ und } -x^3 + 8dy^3 - d^2z^3 - 6dxyz = -1.$$

Das erste Gleichungssytem führt auf $9dy^3 - 9dxzy = 2$, was nicht geht. Also bleibt das zweite. Hier erhält man durch Addition

$$y(y^2 - xz) = 0.$$

Da $y \neq 0$ vorausgesetzt war, bleibt $y^2 = xz$. Dann ist aber nach unseren Vorüberlegungen

$$\mu^{-1} = (x^2 - dyz) + (dz^2 - xy)\alpha$$

eine binomiale Einheit, also müßte nach 1. $|\mu| > 1$ gelten. Andererseits gilt aber wieder nach 1. $|\mu^n| < 1$, was einen Widerspruch ergibt. Also ist damit 6. gezeigt.

Ähnliche Methoden kann man natürlich auch für Gleichungen höheren Grades verwenden. Wir wollen zum Abschluß nur noch kurz die Gleichung $x^4 - dy^4 = 1$ streifen. O.E. sei $d \in \mathbf{N}$ kein Quadrat. Dann ist natürlich

$$1 = (x^2 + y^2\sqrt{d})(x^2 - y^2\sqrt{d}),$$

d.h. $x^2 + y^2\sqrt{d}$ ist Einheit in $\mathbf{Z}[\sqrt{d}]$. Es gilt der Satz (Mordell, S. 275):

SATZ 26. *Die Gleichung $x^4 - dy^4 = 1$ hat höchstens eine Lösung $x, y \in \mathbf{N}$. Ist dies der Fall und $d \neq 7140$, so ist $x^2 + y^2\sqrt{d}$ Grundeinheit in $\mathbf{Z}[\sqrt{d}]$, die sich ja mit dem Kettenbruchalgorithmus leicht bestimmen läßt. (Also kann man sehen, ob die Gleichung lösbar ist). Für $d = 7140$ ist $(239, 26)$ eine Lösung, aber*

$$239^2 + 26^2\sqrt{7140} = (169 + 2\sqrt{7140})^2$$

ist Quadrat der Grundeinheit.

Beispiele: In folgender Tabelle sind die d mit $2 \leq d \leq 10000$, d kein Quadrat, d ohne vierte Potenz, aufgelistet, für die wir durch einfaches Suchen eine nichttriviale Lösung gefunden haben. Ob es mehr Lösungen gibt, folgt damit noch nicht.

5	3	2
15	2	1
39	5	2
150	7	2
255	4	1
410	9	2
915	11	2
1295	6	1
1785	13	2
3164	25	2
4095	8	1
5220	17	2
7140	239	26
8145	19	2
9999	10	1

KAPITEL 8

$f(\mathbf{Q}) \cap \mathbf{Z}$

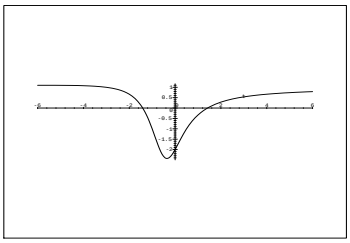
Sei $f \in \mathbf{Q}(t)$, d.h. $f(t) = \frac{g(t)}{h(t)}$, wo g und h Polynome mit ganzen Koeffizienten sind. Ist $t_0 \in \mathbf{Q}$, so ist t_0 eine Polstelle von f oder $f(t_0) \in \mathbf{Q}$. Uns interessiert:

$$\{t_0 \in \mathbf{Q} : f(t_0) \in \mathbf{Z}\},$$

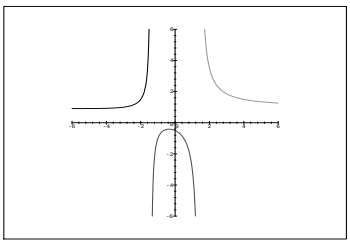
d.h. die Frage, für welche rationalen Zahlen die rationale Funktion f ganzzahlige Werte annimmt.

Beispiel:

- $f = 5t - 7$: Das ist trivial!
- $f = \frac{t^2-2}{t^2+t+1}$. Wie sieht die rationale Funktion f aus? Kurvendiskussion liefert, daß es nur endlich viele Möglichkeiten für t gibt. Die Ableitung ist $f' = \frac{t^2+6t+2}{(t^2+t+1)^2}$.



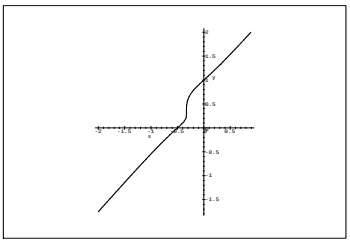
- $f = \frac{t^2+t+1}{t^2-2}$. Die rationale Funktion f hat jetzt Polstellen in $\pm\sqrt{2}$, es könnte also viele $t \in \mathbf{Q}$ mit $f(t) \in \mathbf{Z}$ geben. Wie weiter?

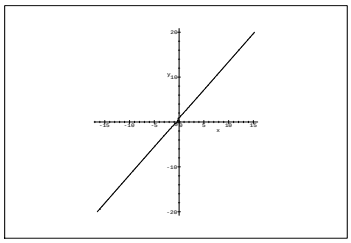


Motivierendes Beispiel: Bestimme die ganzzahligen Lösungen der Gleichung

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

(Gibt es unendlich viele Lösungen?)





- Eine Lösung sieht man sofort: $(x,y) = (0,0)$. Sei jetzt $x \neq 0$. Mit $\alpha = \sqrt[3]{2}$ gilt:
$$\frac{y}{x} - \alpha = \frac{x^2 + xy + y^2}{x(y^2 + \alpha xy + \alpha^2 x^2)}.$$
- Nun gibt es $c_1, c_2 > 0$ mit
$$c_1 \leq \frac{x^2 + xy + y^2}{y^2 + \alpha xy + \alpha^2 x^2} \leq c_2,$$
also
$$\frac{c_1}{|x|} \leq |\alpha - \frac{y}{x}| \leq \frac{c_2}{|x|}.$$
(Man kann wählen $c_1 = 0.6$, $c_2 = 1.1$.) Damit ist zwar $y = \alpha x$ die Asymptote unserer Kurve, aber $\frac{y}{x}$ ist keine besonders gute Approximation an α. Ist unsere bisherige Theorie in diesem Fall also sinnlos?
- Betrachte die Skizze! Beachte, daß es einen isolierten Punkt gibt.
- Wir machen einen neuen Ansatz: $y = tx$, dann hat man die Formeln:
$$x = \frac{t^2 + t + 1}{t^3 - 2}, y = \frac{t(t^2 + t + 1)}{t^3 - 2}, t = \frac{x}{y}.$$
Die rationalen Kurvenpunkte stehen also fast in Bijektion zu den $t \in \mathbf{Q}$. Unsere Aufgabe reduziert sich also darauf, zu bestimmen, für welche $t \in \mathbf{Q}$ die Zahlen $x(t)$ und $y(t)$ wieder in $\mathbf{Z}$ sind. Das aber ist genau das Grundproblem dieses Paragraphen.

Bemerkung: Sei
$$f(t) = \frac{\sum a_i t^i}{\sum b_i t^i}$$
und n das Maximum von Zählergrad und Nennergrad. Setzt man jetzt $t = \frac{u}{v}$, so erhält man
$$f(\frac{u}{v}) = \frac{\sum a_i u^i v^{n-i}}{\sum b_i u^u} v^{n-i} = \frac{G(u,v)}{H(u,v)},$$
wo $G(u,v)$ und $H(u,v)$ homogene teilerfremde Polynome gleichen Grades sind.

Beispiele:

1. $f = \frac{t}{3t-2}$. Dann ist
$$f(\frac{u}{v}) = \frac{u}{3u - 2v}.$$
Setzt man ein $u = 1 + 2\lambda$, $v = 1 + 3\lambda$, so erhält man
$$f(\frac{1+2\lambda}{1+3\lambda}) = 1 + 2\lambda,$$
und man erhält für $\lambda \in \mathbf{Z}$ unendlich viele Lösungen.
2. $f = \frac{3t}{t^2-2}$. Dann ist
$$f(\frac{u}{v}) = \frac{3uv}{u^2 - 2v^2}.$$
Es gibt unendlich viele $u, v \in \mathbf{Z}$ mit $u^2 - 2v^2 = 1$, also erfüllen diese $f(\frac{u}{v}) \in \mathbf{Z}$.

LEMMA 11. *Seien $G(u,v), H(u,v)$ teilerfremde homogene Polynome gleichen Grades mit ganzen Koeffizienten. Dann gibt es homogene Polynome $A, B, C, D \in \mathbf{Z}[u,v]$, $M, m \in \mathbf{N}$ mit*
$$AG + BH = Mu^m, \quad CG + DH = Mv^m.$$

Beweis: Sei $G = \sum g_i u^i v^{n-i}$ und $H = \sum h_i i^i v^{n-1}$. Dann sind auch die Polynome $G(t,1)$ und $H(t,1)$ teilerfremd in $\mathbf{Q}[t]$, (denn wäre $T(t)$ ein gemeinsamer Teiler vom Grad d, so wäre $v^d T(\frac{u}{v})$ ein gemeinsamer Teiler von G und H). Also gibt es $a_i, b_i \in \mathbf{Z}$, $M \in \mathbf{N}$ mit:
$$\frac{\sum a_i t^i}{M} G(t,1) + \frac{\sum b_i t^i}{M} H(t,1) = 1.$$
Setzt man $t = \frac{u}{v}$ ein und multipliziert die ganze Gleichung mit Mv^{k+n}, so erhält man:
$$\sum a_i u^i v^{k-i} G(u,v) + \sum b_i u^i v^{k-i} H(u,v) = Mv^{k+n}.$$

Aus Symmetriegründen erhält man eine analoge Gleichung auch für u statt v und damit folgt die Behauptung. ■

SATZ 27. *Sei* $f(t) \in \mathbf{Q}(t)$ *und*

$$f(\frac{u}{v}) = \frac{G(u,v)}{H(u,v)},$$

mit teilerfremden homogenen G *und* H. *Dann gibt es ein* $M \in \mathbf{N}$ *mit der Eigenschaft: Ist* $\frac{p}{q} \in \mathbf{Q}$ *(teilerfremd dargestellt) und* $f(\frac{p}{q}) \in \mathbf{Z}$, *so gilt*

$$H(p.q)|M.$$

Beweis: Nach dem Lemma haben wir zwei Darstellungen

$$A(u,v)G(u,v) + B(u,v)H(u,v) = Mu^m \text{ und } C(u,v)G(u,v) + D(u,v)H(u,v) = Mv^m.$$

Sei jetzt $f(\frac{p}{q}) \in \mathbf{Z}$. Dann folgt mit

$$A(p,q)f(\frac{p}{q}) + B(p,q) = \frac{Mp^m}{H(p,q)} \text{ und } C(p,q)f(\frac{p}{q}) + D(p,q) = \frac{Mq^m}{H(p,q)},$$

daß auch $\frac{Mp^m}{H(p,q)}$ und $\frac{Mq^m}{H(p,q)} \in \mathbf{Z}$ sind, also

$$\frac{M}{H(p,q)} \in \mathbf{Z},$$

woraus sofort die Behauptung folgt. ■

Beispiele:

1. Für welche $t \in \mathbf{Q}$ ist $f(t) = \frac{t^2+t+1}{t^3-2} \in \mathbf{Z}$? Wir haben

   $$f(\frac{u}{v}) = \frac{(u^2+uv+v^2)v}{u^3-2v^3}.$$

   Nun ist

   $$resultant(G,H,u) = v^9 \text{ und } resultant(G,H,v) = u^9,$$

   also kann man hier $M = 1$ wählen. Unsere Lösungen erfüllen also $u^3-2v^3 = \pm 1$, o.E. $u^3-2v^3 = 1$. Es gibt also nach dem letzten Paragraphen nur zwei Lösungen $(u,v) = (1,0)$ und $(u,v) = (-1,-1)$. Die erste geht nicht, die zweite liefert $t = 1$.
2. Nun zu $f(t) = \frac{t^4+t+1}{t^2-2}$. Es ist

   $$f(\frac{u}{v}) = \frac{u^4+uv^3+v^4}{v^2(u^2-2v^2)}.$$

   Die Resultantenbildung liefert 23, d.h. $v^2(u^2-2v^2)$ muß 23 teilen. Da v o.E. positiv ist, bleibt nur der Fall $v = 1$. Dann bleibt als Bedingung $u^2 - 2|23$. Dies wird von $u = \pm 1$ und $u = \pm 5$ erfüllt. Man findet nun $f(1) = 3$, $f(-1) = -1$, $f(5) = \frac{631}{23}$ und $f(-5) = 27$. Man sieht also auch, daß die Bedingung des Satzes zwar notwendig, nicht jedoch hinreichend ist.

Bemerkung: Unsere Fragestellung führt uns also wieder auf eine Thue-Gleichung: $H(u,v) = m$, mit $m \in \mathbf{Z}$, $m|M$. Damit sollte es möglich sein eine Endlichkeitsaussage zu erhalten.

Wir wollen jetzt nochmals die Thue-Gleichung betrachten und auch reduzible Formen $f(x,y)$ zulassen.

SATZ 28. *Sei* $f(x,y) \in \mathbf{Z}[x,y]$ *homogen* $m \in \mathbf{Z}, m \neq 0$. *Sei*

$$f(x,y) = kf_1(x,y)^{n_1} \dots f_r(x,y)^{n_r}$$

die Zerlegung von f *in irreduzible Faktoren in* $\mathbf{Z}[x,y]$. *Besitzt die Gleichung*

$$f(x,y) = m$$

unendlich viele ganzzahlige Lösungen, so ist $r = 1$ *und* f_1 *linear oder quadratisch (mit zwei reellen Nullstellen). Explizit:*

$$f(x,y) = k(ax+by)^n,$$

oder

$$f(x,y) = k(ax^2 + bxy + cy^2)^n$$

mit $b^2 - 4ac > 0$ *und kein Quadrat.*

Beweis:

- Ist eines der f_i vom Grad ≥ 3, so liefert unser früherer Satz von Thue, daß es nur endlich viele ganze Zahlen x, y gibt mit $|f_i(x,y)| \leq m$.
- Falls
$$f(x,y) = kf_1(x,y)^{n_1} f_2(x,y)^{n_2}$$
ist, mit f_1 linear und f_2 quadratisch und mit unendlich vielen ganzzahligen Lösungen, so gibt es unendlich viele x, y mit
$$f_1(x,y) = m_1 \text{ und } f_2(x,y) = m_2.$$
Man überlegt sich aber sofort, daß es höchstens zwei gemeinsame Lösungen gibt. Also kann auch dieser Fall nicht vorkommen.
- Wir haben noch den Fall
$$f(x,y) = k(ax^2 + bxy + cy^2)^n$$
auszuschließen, falls $b^2 - 4ac < 0$ ist. Das geht aber wie früher.
- Damit ist alles gezeigt. ■

Wir wollen dies noch etwas umformulieren:

Folgerung 6. *Sei $f(t)$ eine rationale Funktion mit rationalen Koeffizienten, die für unendlich viele rationale Zahlen ganze Werte annimmt. Dann liegt einer der folgenden Fälle vor:*

- *$f(t)$ ist ein Polynom.*
- *Es gibt ein Polynom $g(t) \in \mathbf{Q}[t]$ vom Grad $\leq n$ und ein $t_0 \in \mathbf{Q}$ mit*
$$F(t) = \frac{g(t)}{(t - t_0)^n}.$$
- *Es gibt ein Polynom $g(t) \in \mathbf{Q}[t]$ vom Grad $\leq 2n$ und ein irreduzibles Polynom $t^2 + rt + s \in \mathbf{Q}[t]$ mit zwei reellen Nullstellen, so daß gilt*
$$f(t) = \frac{g(t)}{(t^2 + rt + s)^n}.$$

Der Beweis ist klar.

Bemerkung: Wir haben Beispiele gesehen, in denen die Ausnahmefälle auch tatsächlich auftreten. Bei der Umkehrung des Satzes können allerdings Hindernisse auftreten. Wir betrachten zum Beispiel $f(t) = t^2 + \frac{1}{4}$. Für kein $t \in \mathbf{Q}$ ist hier $f(t) \in \mathbf{Z}$. (Übung!)

KAPITEL 9

Rationale Kurven

Zwei Grundprobleme bei den diophantischen Gleichungen lauten: Gegeben sei ein Polynom $f(x,y) \in \mathbf{Z}[x,y]$. Bestimme die *ganzzahligen* und *rationalen* Lösungen der Gleichung

$$f(x,y) = 0.$$

Davon haben wir bereits einige Beispiele gesehen. Wir wollen nun ein paar Vereinfachungen vornehmen.

- Wir zerlegen $f(x,y)$ in irreduzible Faktoren über $\mathbf{Z}$:

  $$f(x,y) = kf_1(x,y)^{n_1} \dots f_r(x,y)^{n_r}.$$

  Da dann

  $$\{f(x,y) = 0\} = \{f_1(x,y) = 0\} \cup \dots \cup \{f_r(x,y) = 0\}$$

  gilt, können wir uns auf irreduzible Polynome beschränken.

  Beispiel: Die Gleichung $y^2 = x^4$ zerlegt sich in die zwei Gleichungen $y = x^2$ und $y = -x^2$.
- Es kann passieren, daß $f(x,y)$ über $\mathbf{Q}$ irreduzibel ist, nicht jedoch über $\overline{\mathbf{Q}}$ oder $\mathbf{C}$.

  Beispiel: Das Polynom

  $$f = 4x^4 - 4x^2y^2 + y^4 - 12x^2 - 6y^2 + 9$$

  zerfällt in vier konjugierte Faktoren:

  $$f = (y + sqrt2x + \sqrt{3})(y + sqrt2x - \sqrt{3})(y - sqrt2x + \sqrt{3})(y - sqrt2x - \sqrt{3}).$$

  Ist $F(x,y)$ also irreduzibel über $\mathbf{Q}$, aber reduzibel über $\overline{\mathbf{Q}}$, so zerfällt f in ein Produkt konjugierter Faktoren:

  $$f(x,y) = kg_1(x,y) \dots g_r(x,y),$$

  wo die $g_i(x,y)$ jetzt algebraische Koeffizienten haben. Ist (x_0, y_0) eine rationale Lösung von $f(x,y) = 0$, so ist (x_0, y_0) Nullstelle von allen $g_i(x,y) = 0$, d.h. die rationalen Lösungen und damit erst recht die ganzzahligen Lösungen von $f(x,y) = 0$ liegen im Durchschnitt

  $$\{(x,y) : g_1(x,y) = \dots = g_r(x,y) = 0\}.$$

  Diese Menge aber ist endlich und kann berechnet werden (Elimination, Resultante). Damit ist in diesem Fall unser Ausgangsproblem leicht zu lösen.
- Jetzt können wir uns also auf den Fall beschränken, daß $f(x,y)$ ganze Koeffizienten hat und über $\mathbf{C}$ irreduzibel ist. Solche Polynome nennt man absolut irreduzibel.

Sei $f \in \mathbf{Z}[x,y]$ absolut irreduzibel. Die Kurve $f(x,y) = 0$ heißt rational, wenn es rationale Funktionen $x(t), y(t) \in \mathbf{Q}(t)$ gibt, nicht beide konstant, mit

$$f(x(t), y(t)) = 0.$$

Mit anderen Worten: $f = 0$ besitzt eine Parametrisierung.

Beispiele:

1. Die Kurve $x^2 - dy^2 = 1$ besitzt die Parametrisierung

   $$x(t) = \frac{dt^2 + 1}{dt^2 - 1}, y(t) = \frac{2t}{dt^2 - 1}.$$

2. Jede absolut irreduzible Kurve $f(x,y)=0$ vom Grad ≤ 2 mit einem rationalen Punkt $(x_0,y_0)\in\mathbf{Q}^2$ ist eine rationale Kurve. (Betrachte die Geraden durch (x_0,y_0) mit Steigung t; sie werden durch die Gleichung $y=y_0+t(x-x_0)$ gegeben. Setzt man dies ein in $f(x,y)=0$, so erhält man ein quadratisches Polynom in x mit einer Nullstelle x_0. Löst man den Rest auf, so erhält man x als Funktion von t und dann schließlich auch y als Funktion von t.)
3. Die Neilsche Parabel $y^2=x^3$ hat die Parametrisierung
$$x=t^2, y=t^3,$$
ist also rational.
4. Die Kurve $y^3-2x^3=x^2+xy+y^2$ ist rational, da sie die Parametrisierung
$$x(t)=\frac{t^2+t+1}{t^3-2}, y(t)=\frac{t(t^2+t+1)}{t^3-2}$$
besitzt.

Unmittelbar aus der Definition folgt die Bemerkung:

Bemerkung: Eine rationale Kurve hat unendlich viele rationale Punkte.

Bevor wir uns den ganzzahligen Punkten zuwenden, noch ein Beispiel darür, daß nicht jede Kurve rational sein muß.

Beispiele:

1. Für $n\geq 3$ und $d\neq 0$ ist die Kurve $x^n-dy^n=1$ nicht rational.
Beweis: Wir nehmen an, die Kurve wäre rational. Dann gäbe es $X,Y,Z\in\mathbf{Q}[t]$, nicht alle konstant, teilerfremd, mit
$$X^n-dY^n=Z^n.$$
Die *abc*-Vermutung für Polynome war bewiesen und liefert hier:
$$\max(grad(X^n),grad(dY^n),grad(Z^n))\leq \#(\text{verschiedene Nullstellen von } X^ndY^nZ^n)-1,$$
also
$$n\max(grad(X),grad(Y),grad(Z))\leq grad(X)+grad(Y)+grad(Z)-1,$$
was aber offensichtlich nicht geht. Also ist unsere Kurve nicht rational. ■

2. Die Kurve $x^2+y^2=3$ ist nicht rational.
Beweis: Durch Betrachtung modulo 4 findet man, daß $x^2+y^2=3$ keinen rationalen Punkt besitzt, die Kurve kann also nicht rational sein. ■

Manchmal hat man auch eine Parametrisierung vorgegeben und such dazu eine Kurvengleichung:

LEMMA 12. *Seien $u(t)=\frac{X(t)}{Z(t)}$ und $v(t)=\frac{Y(t)}{Z(t)}$ rationale Funktionen mit $X,Y,Z\in\mathbf{Z}[t]$, so daß $u(t)$ und $v(t)$ nicht beide konstant sind. Dann gibt es ein absolut irreduzibles $f(x,y)\in\mathbf{Z}[x,y]$ mit*
$$f(\frac{X(t)}{Z(t)},\frac{Y(t)}{Z(t)})=0.$$

Praktisch ist $f(x,y)$ bis auf eine Konstante:
$$f(x,y)=Resultante_t(X(t)-Z(t)x,Y(t)-Z(t)y).$$

Idee: Mit $x=X/Y, y=Y/Z$ hat man zwei Gleichungen und drei Unbestimmte x,y,t, man kann also t eliminieren.

Erinnerung an die Resultante:

- Sei A ein Integritätsring und
$$f = a_0 t^n + \cdots + a_n, g = b_0 t^m + \cdots + b_m \in A[t].$$
Die Resultante von f und g bezüglich t ist dann
$$R_t(f,g) = resultant_t(f,g) = \ldots.$$
- Es gibt Polynome $\phi, \psi \in A[t]$ mit
$$\phi(t)f(t) + \psi(t)g(t) = R_t(f,g).$$
- Ist
$$f(t) = a_0(t-\alpha_1)\ldots(t-\alpha_n) \text{ und } g(t) = b_0(t-\beta_1)\ldots(t-\beta_m),$$
so gilt
$$R_t(f,g) = a_0^m b_0^n \prod_{i,j}(\alpha_i - \beta_j).$$
- Die Resultante $R_t(f,g)$ ist genau dann 0, wenn $a_0 = 0$ oder $b_0 = 0$ oder f und g in $Quot(R)[t]$ einen gemeinsamen Faktor haben.
- Außerdem haben wir für die Diskriminante von f:
$$R_t(f,f') = (-1)^{\frac{n(n-1)}{2}} a_0 D(f).$$

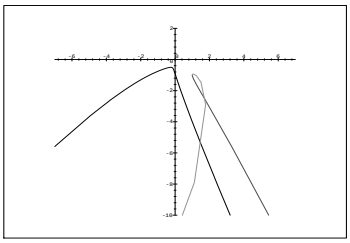
Beweis des Lemmas: Als Ring wählen wir $A = \mathbf{Z}[x,y]$, weiter
$$f(t) = X(t) - Z(t)x, g(t) = Y(t) - yZ(t).$$
Die Resultante R ist dann $\in \mathbf{Z}[x,y]$ und es gibt $\phi, \psi \in \mathbf{Z}[x,y,t]$ mit
$$\phi(x,y,t)(X(t) - Z(t)x) + \psi(x,y,t)(Y(t) - Z(t)y) = R(x,y).$$
Setzt man jetzt $x = X(t)/Z(t), y = Y(t)/Z(t)$ ein, so erhält man $R(X/Z, Y/Z) = 0$. Wieso ist $R(x,y)$ absolut irreduzibel? Dies ergibt sich leicht mit nachfolgenden Bemerkungen. ■

Bemerkungen:

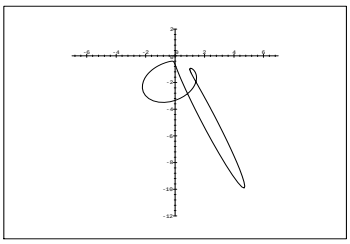
1. Sei $f(x,y) \in \mathbf{Z}[x,y]$ ein irreduzibles Polynom vom Grad n. Schneidet man $f = 0$ mit einer Geraden $y = \alpha x + \beta$, so erhält man durch Einsetzen die Gleichung in x:
$$f(x, \alpha x + \beta) = 0.$$
Von endlich vielen Werten von x abgesehen ist dies eine Gleichung n-ten Grades für x. Man wird also im allgemeinen n Schnittpunkte erhalten (eventuell Schnittpunkte in $\mathbf{C}^2$).
2. Sei eine Kurve parametrisiert gegeben durch
$$x = \frac{X(t)}{Z(t)}, \quad y = \frac{Y(t)}{Z(t)}$$
mit möglichst gekürzter Darstellung. Sei
$$m = \max(grad(X), grad(Y), grad(Z)).$$
Wie oft schneidet eine Gerade $ax+by+c = 0$ die Kurve? Wir setzen ein und erhalten die Gleichung
$$aX(t) + bY(t) + cZ(t) = 0.$$
Im allgemeinen gibt es dann m Lösungen, also auch Schnittpunkte.
3. Aus den vorigen Bemerkungen folgt: Wird die rationale Kurve $f(x,y) = 0$ durch Polynome $X(t), Y(t), Z(t)$ mit maximalem Grad n beschrieben, so hat auch f Grad n.

Beispiele:

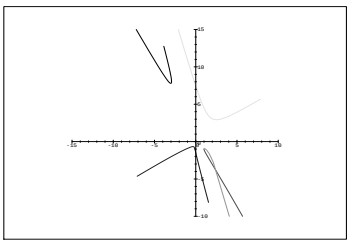
1. Wir wählen
$$X = t^4 - t^2 + 2t - 1, Y = -t^4 - t^3 - 2, Z = (t^2 - 2)^2$$
und erhalten
$$\begin{aligned} f &= 11 + 197 * x + 156 * y + 1292 * y * x + 709 * y^2 + 1456 * x^2 + 2580 * y^2 * x \\ &\quad +2680 * y * x^2 + 650 * y^3 - 800 * x^3 + 49 * y^4 + 784 * x^4 + 56 * y^3 * x \\ &\quad -376 * y^2 * x^2 - 224 * y * x^3 \end{aligned}$$



2.
$$X := t^4 - t^2 + 2 * t - 1; Y := -t^4 - t^3 - 2; Z := (t^2 - 2)^2 + 1;$$
und erhalten
$$\begin{aligned} f &= 11 + 243 * x + 174 * y + 1838 * y * x + 956 * y^2 + 1883 * x^2 + 4523 * y^2 * x \\ &\quad +4696 * y * x^2 + 1290 * y^3 - 415 * x^3 + 305 * y^4 + 890 * x^4 + 1112 * y^3 * x \\ &\quad +1022 * y^2 * x^2 + 308 * y * x^3; \end{aligned}$$



3.
$$X := t^4 - t^2 + 2 * t - 1; Y := -t^4 - t^3 - 2; Z := (t^2 - 2)^2 - 1;$$
$$\begin{aligned} f &= 11 + 151 * x + 138 * y + 858 * y * x + 500 * y^2 + 1141 * x^2 + 1303 * y^2 * x \\ &\quad +1356 * y * x^2 + 222 * y^3 - 1027 * x^3 - 39 * y^4 + 752 * x^4 - 352 * y^3 * x \\ &\quad -918 * y^2 * x^2 - 348 * y * x^3; \end{aligned}$$



Bemerkung: Für eine rationale Kurve $f(x, y) = 0$ läßt sich eine Parametrisierung $x(t), y(t)$ immer so finden, daß t wieder eine rationale Funktion in x und y ist. Das impliziert, daß die rationalen Punkte auf $f(x, y) = 0$ bis auf endlich viele Ausnahmen in Bijektion sehen zu den $t \in \mathbf{Q}$. Die Ausnahmen kommen durch die Polstellenn zustande. (Der Beweis ergibt sich mit dem Satz von Lüroth.)

Wir kommen nun zu den ganzzahligen Punkten auf rationalen Kurven. Es gilt folgender Satz:

SATZ 29. *Sei eine rationale Kurve $f(x,y)=0$ mit der Parametrisierung*

$$x=\frac{X(t)}{Z(t)}, y=\frac{Y(t)}{Z(t)}$$

gegeben, wo $X,Y,Z\in\mathbf{Q}[t]$ teilerfremd sind und $Z(t)$ höchsten Koeffizienten 1 hat. $f(x,y)=0$ habe unendlich viele ganzzahlige Punkte. Dann liegt einer der folgenden Fälle vor:

- $Z(t)=1$.
- $Z(t)=(t-r)^m$ *mit* $r\in\mathbf{Q}$ *und* $X(t)$ *und* $Y(t)$ *haben Grad* $\leq m$.
- $Z(t)=(t^2+rt+s)^n$ *mit* $r,s\in\mathbf{Q}$, t^2+rt+s *irreduzibel über* $\mathbf{Q}$ *mit zwei reellen Nullstellen und* $X(t)$ *und* $Y(t)$ *haben Grad* $\leq 2n$.

Beweis: Sind $\frac{X(t)}{Z(t)}$ und $\frac{Y(t)}{Z(t)}$ bereits gekürzte Darstellungen, so folgt die Aussage des Satzes bereits aus den Ergebnissen des letzten Paragraphen. Es bleibt der Fall, daß dies nicht so ist. Da $Z(t)$ nur endlich viele komplexe Nullstellen hat, gibt es sicher unendlich viele $l\in\mathbf{Z}$, so daß $\frac{X(t)+lY(t)}{Z(t)}$ schon gekürzt ist. Da auch für diese Funktion an unendlich vielen Stellen ganze Zahlen als Werte angenommen werden, folgt die Behauptung für $Z(t)$ und dann auch für $X(t)$ und $Y(t)$ wegen

$$Y(t)=\frac{(X+l_1Y)-(X+l_2Y)}{l_1-l_2} \text{ und } X(t)=\frac{l_2(X+l_1Y)-l_1(X+l_2Y)}{l_2-l_1}.$$

■

Ohne Beweis zitieren wir noch folgenden Satz von Siegel, der allerdings die Methoden der Vorlesung weit übersteigt:

SATZ 30. *Sei $f(x,y)\in\mathbf{Z}[x,y]$ absolut irreduzibel und $f(x,y)=0$ besitze unendlich viele ganzzahlige Lösungen. Dann ist die Kurve $f=0$ rational und*

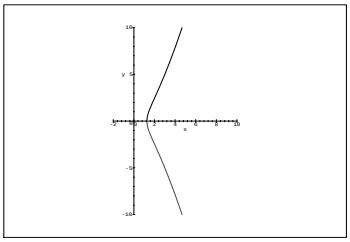
KAPITEL 10

Elliptische Kurven

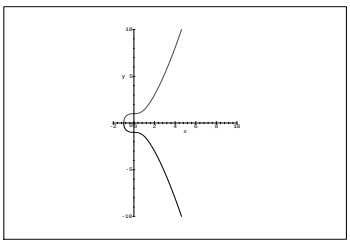
Wir werden rationale Punkte auf Kurven der Form $y^2 = x^3 + ax + b$ studieren.

Beispiele: (Konstruktion neuer rationaler Punkte aus vorgegebenen mit der Methode von Bachet)

1. Die Kurve $y^2 = x^3 - 2$ werde betrachtet. Durch etwas Probieren findet man, daß $(3, 5)$ ein Punkt auf der Kurve ist. Wir bestimmen die Tangente in diesem Punkt: Die Taylorreihenentwicklung lautet
$$f = 27(x-3) - 10(y-5) + 9(x-3)^2 - (y-5)^2 + (x-3)^3,$$
die Tangente ist also
$$y = \frac{27x - 31}{10}.$$
Man erhält
$$f(x, \frac{27x-31}{10}) = (x-3)^2(x - \frac{129}{100}).$$
Daraus errechnet man: die Tangente schneidet unsere Kurve in dem weiteren Punkt $(x_2, y_2) = (\frac{129}{100}, \frac{383}{1000})$. Nimmt man nun die Tangente in (x_2, y_2) und schneidet sie mit der Kurve, so erhält man den neuen Punkt $(x_3, y_3) = (\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000})$.



2. Bei der Kurve $y^2 = x^3 + 1$ sieht man schnell die Punkte $(0, \pm 1)$ und $(-1, 0)$. Die Verbindungsgerade zwischen den Punkten $(-1, 0)$ und $(1, 0)$ ist $y = x + 1$. Der dritte Schnittpunkt ist $(2, 3)$. Die Tangente in $(2, 3)$ ist $y = 2x - 1$. Dann ist der dritte Schnittpunkt $(0, -1)$. Welche Punkte gibt es?



Tangenten und singuläre Punkte:

- Was ist die Tangente einer ebenen Kurve $f(x, y) = 0$ im Kurvenpunkt (x_0, y_0)? Dies ist der lineare Anteil in der Taylorreihenentwicklung von f um den Punkt (x_0, y_0). Allgemein ist
$$f(x,y) = \sum_{i,j \geq 0} \frac{f^{(i,j)}(x_0, y_0)}{i!j!}(x - x_0)^i (y - y_0)^j = \frac{df}{dx}(x_0, y_0(x - x_0) + \frac{df}{dy}(x_0, y_0)(y - y_0) + \ldots$$

Die Tangente ist also .... Sind die beiden Ableitungen $= 0$, so existiert die Tangente nicht, wir nennen den Kurvenpunkt singulär.

- *Aussehen:* Wir wollen $f(x,y) = 0$ in einem Punkt (x_0, y_0) betrachten. Nach Koordinatenwechsel können wir $(x_0, y_0) = (0,0)$ annehmen. Wir betrachten die Taylorreihenentwicklung von f:

$$f(x,y) = \dots.$$

  - Falls $f = 0$ nicht singulär ist:

$$f(x,y) = ax + by + \dots, \quad (a,b) \neq 0.$$

    Dann kann man reell die Gleichung nach dem Satz über implizite Funktionen lokal nach x oder y auflösen.
  - Falls $f = 0$ singulär ist und

$$f = ax^2 + bxy + cy^2 + \dots \quad \text{mit } (a,b,c) \neq 0.$$

    Dann gibt es zwei Fälle:
    * $ax^2 + bxy + cy^2$ ist positiv oder negativ definit. Dann ist lokal um 0: $f(x,y) \neq 0$ für $(x,y) \neq (0,0)$, d.h. lokal hat $f = 0$ einen isolierten Punkt.
    * $ax^2 + bxy + cy^2$ ist indefinit mit zwei verschiedenen reellen Nullstellen: nach Koordinatenwechsel ist

$$f = xy + \dots,$$

      also schaut $f = 0$ lokal wie ein Achsenkreuz aus.
    * $ax^2 + bxy + cy^2$ ist indefinit mit zwei gleichen Nullstellen, o.E.

$$f = y^2 + \dots.$$

      Beispiele: $y^2 = x^3$ und $y^2 = x^4 + x^5$.
- Wann ist $f = x^3 + ax + b - y^2$ singulär? Die folgenden Gleichungen müssen gleichzeitig erfüllt sein:

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

  Dies ist gleichwertig mit

$$y = 0, x^2 = -\frac{a}{3}, \frac{2}{3}ax = -b.$$

  Dies kann man auflösen:

$$4a^3 + 27b^2 = 0, y = 0, x = -\frac{3b}{2a} \text{ bzw. } 0.$$

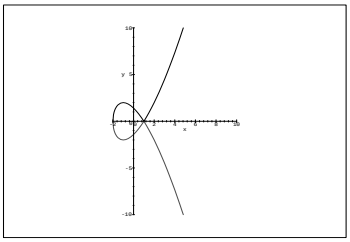
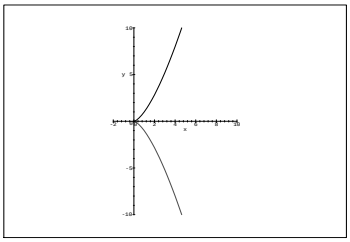
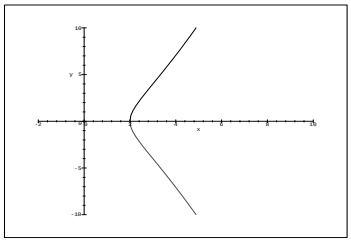
Der folgende Satz zeigt, daß singuläre Kurven vom Typ $y^2 = x^3 + ax + b$ nichts Neues ergeben:

SATZ 31. *Sei die Kurve $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Q}$ gegeben. Sie ist genau dann singulär, wenn $4a^3 + 27b^2 = 0$ ist. Ist dies der Fall, dann ist die Kurve rational. Genauer, es gibt ein $c \in \mathbf{Q}$ mit $a = -3c^2$ und $b = 2c^3$. Ein Parametrisierung wird gegeben durch*

$$x = t^2 - 2e, \quad y = t(t^2 - 3e).$$

Beweis: ■

Aufgabe: Betrachte $y^2 = (x - c)^2(x + 2c)$ bei variierendem $c \in \mathbf{R}$. Unterscheide die Fälle $c > 0$, $c = 0$, $c < 0$.

SATZ 32. *Ist $4a^3 + 27b^2 \neq 0$, so ist die Kurve $y^2 = x^3 + ax + b$ nicht rational.*

Beweisidee: Wir nehmen an, es gäbe ein Parametrisierung $x(t), y(t) \in \mathbf{Q}(t)$. Der Grad von Zähler und Nenner von $x(t)$ und $y(t)$ wäre dann ≤ 3. Sei

$$x(t) = \frac{\dots}{p_1(t)^{n_1} \dots} \text{ und } y(t) = \frac{\dots}{p_1(t)^{m_1} \dots}.$$

Dann gilt $2m_1 = 3n_1$, also $m_1 = 3k_1$, $n_1 = 2k_1$. Aus Gradgründen gibt es dann nur ein $p_i(t)$, dieses ist linear und $k_1 = 1$. Nach Koordinatenwechsel in t: o.E. $p_1(t) = t$. Also können wir ansetzen:

$$x(t) = \frac{a_0 + a_1 t + a_2 t^2}{t^2} \text{ und } y(t) = \frac{b_0 + b_1 t + b_2 t^2 + b_3 t^3}{t^3} \text{ mit } a_0, b_0 \neq 0.$$

Dies liefert ein großes Gleichungssystem. Nach Elimination findet man $4a^3 + 27b^2 = 0$, ein Widerspruch zur Voraussetzung. Also ist unsere Kurve nicht rational. ■

Kurvendiskussion: Über $\mathbf{R}$ gibt es nur zwei Möglichkeiten:

- $x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$ mit drei reellen Zahlen e_i.
- $x^3 + ax + b$ hat genau eine reelle Nullstelle e.

Schnitte mit Geraden: Sei die Kurve $y^2 = x^3 + ax + b$ gegeben. Wie oft schneidet eine Gerade die Kurve?

- $y = cx + d$. Einsetzen liefert ein kubisches Polynom in x. Man erhält also richtig gezählt immer drei Schnittpunkte.
- $x = c$. In diesem Fall gibt es nur zwei Schnittpunkte: $(x_0, \pm y_0)$.

Vermutung von Poincare(?): Für eine nichtsinguläre Kurve $y^2 = x^3 + ax = b$ gibt es endlich viele rationale Punkte, so daß sich alle anderen rationalen Punkte durch die Tangenten- und Sekantenmethode aus den vorgegebenen Punkten gewinnen lassen.

Hat man zwei Punkte, so kann man also im allgemeinen noch einen weiteren dritten dazu findet. Kann man also eine Verknüpfung auf der Kurve definieren? Ein Problem ist, daß die Geraden $x = c$ die Kurve nur zweimal schneiden. Doch das läßt sich beheben.

Der unendlich ferne Punkt O:

- Zunächst wollen wir versuchen zu verstehen, wie sich die Kurve verhält für $y \to \infty$. Dazu machen wir einen Koordinatenwechsel:

  $$x = \frac{u}{v}, \quad y = \frac{1}{v}.$$

  Umgekehrt ist dann $u = xy$ und $v = \frac{1}{y}$. Wir wollen also sehen, was passiert für $v \to 0$. Einsetzen liefert:

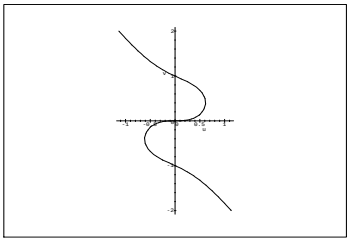
  $$v = u^3 + a\,uv^2 + bv^3.$$

  Für $v = 0$ erhalten wir sofort $u = 0$, d.h. einen Punkt. Diesen Punkt nennen wir O.
- Was passiert mit den Geraden $x = c$? Einsetzen liefert

  $$u = cv.$$

  Für $v = 0$ erhalten wir also $u = 0$, d.h. wieder den Punkt O.
- Für $v = 0$ gehen also die Kurven $y^2 = x^3 + ax + b$ und die Geraden $x = c$ durch einen gemeinsamen Punkt $u = 0, v = 0$.
- Wir betrachten spaßeshalber noch das Verhalten der Geraden $y = cx + d$. Man erhält $1 = cu + dv$: Diese Geraden gehen nie durch den Punkt O.
- Um die Kurve zu vervollständigen, nehmen wir noch einen unendlich fernen Punkt O hinzu.

- Bild im Unendlichen.



- All diese Probleme umgeht man, wenn man die Situation in der projektiven Ebene betrachtet.

Wir wollen jetzt eine Addition auf der Kurve $y^2 = x^3 + ax + b$ einführen. Für einen Körper K sei

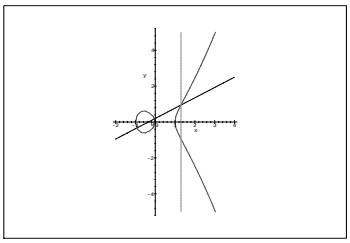
$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\} \cup \{O\}.$$

- Für $P, Q \in E(K)$ sei $g(P, Q)$ die Verbindungsgerade zwischen P und Q bzw. die Tangente, falls $P = Q$ ist. Neben P und Q liegt dann bei richtiger Zählung noch ein weiterer Punkt R auf der Geraden $g(P, Q)$. Dieser werde mit $h(P, Q)$ bezeichnet.
- Für $P, Q \in E(K)$ definieren wir jetzt:

$$P + Q := h(h(P, Q), O).$$

  Geometrisch: ...
- Wir erhalten die Eigenschaften:
  - $P + Q = Q + P$
  - $P + O = P$
  - $P + h(P, O) = O$
  - Mit einigem Aufwand kann man auch zeigen: $P + (Q + R) = (P + Q) + R$.

  Also ist $E(K)$ versehen mit $+$ eine abelsche Gruppe. Wir nennen die Kurve eine elliptische Kurve. Eine elliptische Kurve E ist für uns also eine Kurve $y^2 = x^3+ax+b$ zusammen mit einem unendlich fernen Punkt O und dem eben beschriebenen Additionsgesetz.



Da der Punkt O eine Sonderrolle spielt, können wir das Additionsgesetz auch noch etwas einfacher anschreiben: Seien $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ vorgegeben. (Also $\neq O$.) Dann lassen sich für die Addition folgende Fälle unterscheiden:

1. $x_1 \neq x_2$: Lege die Gerade durch P_1 und P_2. Der dritte Schnittpunkt mit E sei (x_3, y_3). Definiere dann
$$(x_1, y_1) + (x_2, y_2) = (x_3, -y_3).$$
2. $x_1 = x_2$ und $y_1 = -y_2$. Setze dann
$$(x_1, y_1) + (x_1, -y_1) = O.$$
3. $x_1 = x_2$ und $y_1 = y_2 \neq 0$. Ist (x_3, y_3) der dritte Schnittpunkt der Tangenten in (x_1, y_1) mit E, so setze
$$(x_1, y_1) + (x_2, y_2) = (x_3, -y_3).$$

Beispiel: Für $E : y^2 = x^3 + 1$ haben wir

$$E(\mathbf{Q}) \supseteq \{O, (-1,0), (0,1), (0,-1), (2,3), (2,-3)\}.$$

Wie sieht die Gruppenstruktur aus?

Indem man nun die Geradengleichungen explizit aufstellt, gewinnt man folgenden Satz:

SATZ 33. *Sei $E : y^2 = x^3 + ax + b$ gegeben mit $4a^3 + 27b^2 \neq 0$. Für $(x_1, y_1), (x_2, y_2) \in E(K)$ gilt dann*

- $-(x_1, y_1) = (x_1, -y_1)$.
- *Für $x_1 \neq x_2$ und $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ gilt:*

$$x_3 = -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \quad -y_3 = \frac{y_2 - y_1}{x_2 - x_1} x_3 + \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$$

- *Für $x_1 = x_2$ und $y_1 = y_2 \neq 0$ und $(x_3, y_3) = 2(x_1, y_1)$ gilt:*

$$x_3 = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4(x_1^3 + ax_1 + b)}, \quad -y_3 = \frac{3x_1^2 + a}{2y_1} x_3 + \frac{-x_1^3 + ax_1 + 2b}{2y_1}.$$

Beweisskizze: ■

Bemerkung: Mit obigen Formeln kann man auch versuchen, das Assoziativgesetz explizit nachzurechnen.

Obwohl die Bilder dann nicht mehr stimmen, kann man obige Konstruktionen auch über endlichen Körpern machen.

Beispiele:

1. Wir betrachten die Kurve $E : y^2 = x^3 + 3x + 2$ über dem Körper $K = \mathbf{F}_5$. Dann ist $4a^3 + 27b^2 = 1 \neq 0$. Es ist

x	0	1	2	3	4
$x^3 + 3x + 2$	2	1	1	3	3

   Quadrate in $\mathbf{F}_5$ sind die Zahlen 0, 1, 4, also ist

$$E(\mathbf{F}_5) = \{O, (1,1), (1,4), (2,1), (2,4)\}.$$

   Was ist $2(1,1)$? Die Tangente ind $(1,1)$ ist $y = 3x + 3$. Der andere Schnittpunkt ist dann $(2,4)$, also $2(1,1) = (2,1)$. Etc. Trivial ist die Bemerkung $E(\mathbf{F}_5) \simeq \mathbf{Z}/5\mathbf{Z}$.
2. Auch die Kurve $y^2 = x^3 + x + 2$ ist über $\mathbf{F}_5$ elliptisch wegen $4a^3 + 27b^2 = 2 \neq 0$.

x	0	1	2	3	4
$x^3 + x + 2$	2	4	2	2	0

   Quadrate in $\mathbf{F}_5$ sind die Zahlen 0, 1, 4, also ist

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

   Welche Gruppenstruktur liegt vor?

Bemerkung: Elliptische Kurven über endlichen Körpern spielen auch in der Kryptographie eine Rolle.

Wir wollen der Vollständigkeit halber noch eine Tatsache erwähnen:

Bemerkungen:

- Sei nun $a, b \in \mathbf{R}$ vorausgesetzt. Ist $4a^3 + 27b^2 \neq 0$, so ist $E(\mathbf{R})$ eine Gruppe und eine reelle kompakte Kurve. Was kann die Gruppenstruktur sein? An kompakten Gruppen gibt es den Kreis S^1. Für $4a^3 + 27b^2 <> 0$ ist

$$E(\mathbf{R}) \simeq \mathbf{R}/\mathbf{Z} \text{ bzw. } \mathbf{R}/\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

- Sind $a, b \in \mathbf{C}$ mit $4a^3 + 27b^2 \neq 0$ und $E : y^2 = x^3 + ax + b$. Was ist dann $E(\mathbf{C})$? Es gilt: Es gibt ein Gitter $\Gamma \subseteq \mathbf{C}$ mit
$$E(\mathbf{C}) \simeq \mathbf{C}/\Gamma.$$
Der Isomorphismus kann durch sogenannte elliptische oder doppeltperiodische Funktionen beschrieben werden.

Aufgabe: Untersuche das geometrische Additionsgesetz für die singulären Kurven $y^2 = x^3 + ax + b$ mit $4a^3 + 27b^2 = 0$.

Isomorphie: Wir wollen ein paar Bemerkungen zum Isomorphiebegriff elliptischer Kurven machen. Wir nennen zwei elliptische Kurven $E : y^2 = x^3 + ax + b$ und $E' : y'^2 = x'^3 + a'x' + b'$ isomorph über einem Körper K, wenn es eine Koordinatentransformation
$$x' = \alpha x, y' = \beta y$$
gibt, so daß dadurch E' in E übergeht und $\alpha, \beta \in K$.

- Das liefert sofort $\beta^2 = \alpha^3$, also ein $\gamma \in K$ mit
$$\alpha = \gamma^2, \beta = \gamma^3.$$
- Damit erhalten wir
$$x' = \gamma^2 x, y' = \gamma^3 y$$
und damit nach einigen Umformungen:
$$a' = \gamma^4 a, b' = \gamma^6 b.$$
- Was passiert mit der Diskriminante?
$$4a'^3 + 27b'^2 = \gamma^{12}(4a^3 + 27b^2).$$
- Der Ausdruck
$$j = 1728\frac{4a^3}{4a^3 + 27b^2}$$
hängt nicht von der Basiswahl ab: isomorphe elliptische Kurven haben gleiche j-Invariante.
- Umgekehrt kann man (leicht) zeigen: Haben E und E' gleiche j-Invariante, so sind sie über dem algebraischen Abschluß isomorph.
- *Beispiel:* Die Kurven $E : y^2 = x^3 - x$ und $E' : y^2 = x^3 - 2x$ haben beide die j-Invariante 1728. Man muß ein γ finden mit $2 = \gamma^4$. Also sind E und E' isomorph über K, sofern $\sqrt[4]{2} \in K$ ist.

Wir interessieren uns aber zunächst für die rationalen Punkte auf elliptischen Kurven, die über $\mathbf{Q}$ definiert sind.

LEMMA 13. *Sei E die elliptische Kurve $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$. Ein Punkt $P \in E(\mathbf{Q})$ mit $P \neq O$ hat dann die Form*
$$P = (\frac{r}{u^2}, \frac{s}{u^3},$$
mit $u \in \mathbf{N}$, $r, s \in \mathbf{Z}$ und $ggT(r, u) = ggT(s, u) = 1$.

Beweis: Zur Übung. ■

Beispiel: Wir wollen für $E : y^2 = x^3 - x + 4$ die rationalen Lösungen bestimmen. Setzt man ein $-10 \leq r \leq 10, 1 \leq u \leq 10$, so findet man die Punkte
$$(-1, \pm 2), (0, \pm 2), (1, \pm 2), (4, \pm 8), (-\frac{7}{4}, \pm\frac{5}{8}), (\frac{9}{4}, \pm\frac{29}{8}), (\frac{1}{16}, \pm\frac{127}{64}).$$
Nutzt man jetzt die Gruppenstruktur aus, so findet man mit $P_1 = (-1, 2)$ und $P_2 = (0, 2)$:
$$(1, 2) = -P_1 - P_2, (4, 8) = 2P_1 + P_2, (-\frac{7}{4}, \frac{5}{8}) = 2P_1 + 2P_2, (\frac{9}{4}, \frac{29}{8}) = -2P_1, (\frac{1}{16}, \frac{127}{64}) = -2P_2.$$
Die angegebenen Punkte sind also Linearkombinationen von P_1 und P_2. Ein weiteres Beispiel ist
$$3P_1 - 2P_2 = (-\frac{3682249}{2301289}, -\frac{4280578234}{3491055413}).$$

Die Frage stellt sich: Ist

$$E(\mathbf{Q}) = \mathbf{Z}P_1 + \mathbf{Z}P_2?$$

Ist die Summe sogar direkt?

Wir wollen später folgenden Satz von Mordell skizzieren:

SATZ 34. *Sei E eine elliptische Kurve über $\mathbf{Q}$. Dann ist die Gruppe $E(\mathbf{Q})$ eine endlich erzeugte abelsche Gruppe. D.h. die Torsionsuntergruppe $E(\mathbf{Q})_{tor}$ der Elemente endlicher Ordnung ist endlich und es gibt $P_1, \ldots, P_r$ mit*

$$E(\mathbf{Q}) = E(\mathbf{Q})_{tor} \oplus \mathbf{Z}P_1 \oplus \cdots \oplus \mathbf{Z}P_r.$$

r heißt dabei der Rang der elliptischen Kurve.

KAPITEL 11

Torsionspunkte auf elliptischen Kurven

Sei E eine elliptische Kurve über einem Körper K gegeben durch eine Gleichung $y^2 = x^3 + ax + b$, mit $a, b \in K$ und $4a^3 + 27b^2 \neq 0$. (Außerdem haben wir irgendwann $char(K) \neq 2, 3$ benutzt.) Uns interessiert

$$E_{tors}(K) = \{P \in E(K) : \text{ es gibt ein } n \in \mathbf{N} \text{ mit } nP = O\}.$$

$$E_n(K) = \ldots$$

Punkte der Ordnung 2: Sei $P = (x, y)$. Wann ist $2P = 0$? Es gilt:

$$2P = 0 \iff P = -P \iff (x, y) = -(x, y) = (x, -y) \iff y = 0.$$

Die Punkte der Ordnung 2 sind also die Schnittpunkte der Kurve mit der x-Achse und O.

Beispiele über Q:

1. $y^2 = x^3 - x$. Wegen $x^3 - x = x(x-1)(x+1)$ gibt es vier 2-Teilungspunkte:
$$\{O, (-1, 0), (0, 0), (1, 0)\}.$$
2. $y^2 = x^3 - 1$. Wegen $x^3 - 1 = (x-1)(x^2 + x + 1)$ gibt es zwei 2-Teilungspunkte:
$$\{O, (1, 0)\} \simeq \mathbf{Z}/2.$$
3. $y^2 = x^3 - x - 1$. Das Polynom $x^3 - x - 1$ ist irreduzibel über $\mathbf{Q}$, also gibt es nur den trivialen 2-Teilungspunkt O.
4. Da alle drei kubischen Polynome drei Nullstellen in $\mathbf{C}$ haben, ist klar, daß in diesem Fall $E_2(\mathbf{C}) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$ gilt.

3-Teilungspunkte: Sei $P = (x, y)$. Wann gilt $3P = 0$? Dies ist gleichwertig mit $2P = -P$. Nun ist

$$2P = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \ldots\right),$$

die Bedingung lautet also

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} = x,$$

denn $2P = P$ kommt hier nicht vor. Umgeformt gibt dies die Bedingung

$$3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

Da mit $P = (x, y)$ auch $-P = (x, -y)$ ein 3-Teilungspunkt ist, kann es also maximal 8 nichttriviale 3-Teilungspunkte geben, d.h.

$$E_3(K) = \{O\} \text{ oder } \mathbf{Z}/3 \text{ oder } \mathbf{Z}/3 \times \mathbf{Z}/3.$$

Beispiele über Q:

1. $y^2 = x^3 + x + 1$. Das obige Polynom ist irreduzibel über $\mathbf{Q}$, also ist $E_3(\mathbf{Q}) = \{O\}$.
2. $y^2 = x^3 + 1$. Dann ist das obige Polynom $3x(x^3 + 4)$, also ist
$$E_3(\mathbf{Q}) = \{O, (0, \pm 1)\}.$$
3. Kann der Fall $E_3(\mathbf{Q}) = \mathbf{Z}/3 \times \mathbf{Z}/3$ vorkommen? Dazu muß das Polynom
$$3x^4 + 6ax^2 + 12bx - a^2$$
über $\mathbf{Q}$ in Linearfaktoren zerfallen.

Wir wollen uns jetzt allgemein $E_{tors}(\mathbf{Q})$ zuwenden. Dazu noch ein Beispiel:

Beispiel: Auf der elliptischen Kurve $y^2 = x^3 + 4x - 1$ liegt der Punkt $P = (\frac{1}{4}, \frac{1}{8})$. Dann ist

$$2P = (\frac{4481}{16}, -\frac{299967}{64}, 3P = (\frac{22443265}{2^2 \cdot 11^4 \cdot 37^2}, \frac{270195523967}{2^3 \cdot 11^6 \cdot 37^3}.$$

Die Vermutung liegt also nahe, daß die Nenner immer größer werden, und daß P also kein Torsionspunkt ist.

Sei E eine vorgegebene elliptische Kurve über $\mathbf{Q}$ und p eine Primzahl. Wir betrachten die Menge

$$E(p^{e_0}) = \{(\frac{r}{m^2 p^{2e}}, \frac{s}{m^3 p^{3e}}) \in E(\mathbf{Q}) : e \geq e_0, ggT(p, rsm) = 1\} \cup \{O\},$$

d.h. p^{2e_0} bzw. p^{3e_0} kommt tatsächlich im Nenner vor.

Es ist klar, daß wir folgende Inklusionen haben:

$$E(p) \supseteq E(p^2) \supseteq E(p^3) \supseteq \cdots \supseteq \{O\}.$$

(p-adische Umgebungen der O.)

Wir hatten früher schon zur Einführung von O ein anderes Koordinatensystem benutzt. Ist $P = (x, y)$, so war $u(P) = \frac{x}{y}$. In unserem Fall ist also

$$u(\frac{r}{m^2 p^{2e}}, \frac{s}{m^3 p^{3e}}) = \frac{ms}{r} \cdot p^e.$$

Es gilt dann das folgende Lemma:

LEMMA 14. *$E(p^{e_0})$ ist eine Untergruppe von $E(\mathbf{Q})$ und für $P_1, P_2 \in E(p^{e_0})$ gilt:*

$$u(P_1 + P_2) \equiv u(P_1) + u(P_2) \bmod p^{5e_0}.$$

Das Beweis ist nicht schwierig, benutzt aber geschickte Umformungen. Wir verzichten hier darauf.

Wir nutzen aber das Lemma sofort aus:

LEMMA 15. *$E(p)$ enthält keinen Teilungspunkt $\neq 0$.*

Beweis: Angenommen, es gäbe einen Teilungspunkt $P \neq O$ mit $P \in E(p)$. Indem wir zu einem vielfachen von P übergehen. können wir annehmen, daß P ein q-Teilungspunkt ist für eine Primzahl q. Sei $P \in E(p^e)$, aber $P \notin E(p^{e+1})$. Dann ist nach dem vorausgegangenen Lemma modulo p^{5e}:

$$0 = u(O) = u(q \cdot P) \equiv qu(P) \bmod p^{5e},$$

also auf jeden Fall

$$u(P) \equiv 0 \bmod p^{5e-1},$$

aber nach Voraussetzung war $u(P) \not\equiv 0 \bmod p^{e+1}$. Dies ist ein Widerspruch, also war die Annahme falsch. ■

FOLGERUNG 7. *Ist $P = (x, y)$ ein Torsionspunkt der elliptischen Kurve $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$, so gilt $x, y \in \mathbf{Z}$.*

Beweis: Angenommen, x oder y wären nicht ganze Zahlen. Dann gibt es eine Primzahl p, die im Nenner vorkommt, also $P \in E(p)$. Das geht aber nach dem eben gezeigten Lemma nicht. ■

Wir können nun den folgenden Satz von Lutz-Nagell zeigen:

SATZ 35. *Ist $P = (x, y) \neq O$ ein Teilungspunkt der elliptischen Kurve $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$, so gilt:*

- *$x, y \in \mathbf{Z}$,*
- *$y = 0$ oder $y | 4a^3 + 27b^2$.*

Beweis: Den ersten Teil haben wir bereits gesehen. Ist nun P Torsionspunkt, so auch $2P$. Ist $2P = 0$, so ist $y = 0$ und wir sind fertig. Andernfalls ist

$$2P = (\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \ldots),$$

also muß auch

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} \in \mathbf{Z}$$

gelten. Weiter findet man mit der Resultante

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} \cdot 4(3x^2 + 4a) - 3x^4 + 5ax + 27b = \frac{4a^3 + 27b^2}{y^2}.$$

Da die linke Seite der Gleichung in $\mathbf{Z}$ ist, muß es auch die rechte sein, woraus dann sofort die Behauptung folgt. ■

Bemerkung: Der Satz von Lutz-Nagell liefert für eine konkret gegebene elliptische Kurve eine effektive Methode, die rationalen Teilungspunkte zu bestimmen.

Beispiele:

1. $y^2 = x^3 - 43x + 166$. Dann ist $4a^4 + 27b^2 = 2^{15} \cdot 13$. Ist $(x, y) \in E_{tors}(\mathbf{Q})$ und $y \neq 0$, so gilt also $y^2 | 2^{15} \cdot 13$, also $y | 2^7$. Durch Ausprobieren findet man:
$$E_{tors}(\mathbf{Q}) = \{O, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\} \simeq \mathbf{Z}/7.$$
2. $y^2 = x^3 - 432x + 8208$. Dann ist
$$4a^3 + 27b^2 = 2^8 \cdot 3^{12} \cdot 11.$$
Für $(x, y) \in E_{tors}(\mathbf{Q})$ mit $y \neq 0$ muß also gelten $y | 2^4 \cdot 3^6$. Durch Ausprobieren findet man
$$E_{tors}(\mathbf{Q}) = \{O, (-12, \pm 108), (24, \pm 108)\} \simeq \mathbf{Z}/5.$$

Nun kann man sich fragen, welche endliche Gruppen überhaupt auftreten als $E_{tors}(\mathbf{Q})$. Wir haben oben bereits gesehen, daß wir auf einfache Weise keine Untergruppe $\mathbf{Z}/3 \times \mathbf{Z}/3$ konstruieren konnten. Das schwierige Problem wurde von Mazur gelöst. Das Ergebnis ist der folgende Satz, dessen Beweis die Vorlesung weit übersteigt.

SATZ 36. *Ist E eine elliptische Kurve über $\mathbf{Q}$, dann ist $E_{tors}(\mathbf{Q})$ eine der folgenden Gruppen:*

- $\mathbf{Z}/m$ *für* $1 \leq m \leq 10$ *oder* $m = 12$,
- $\mathbf{Z}/2 \times \mathbf{Z}/n$ *für* $n = 2, 4, 6, 8$.

Reduktion modulo p Sei E eine elliptische Kurve über $\mathbf{Q}$ gegeben durch die Gleichung $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$. Ist p eine Primzahl mit $2(4a^3 + 27b^2) \not\equiv 0 \bmod p$, so erhält man durch Betrachtung der Gleichung modulo p eine elliptische Kurve über $\mathbf{F}_p$. Wir erhalten dann eine Abbildung

$$\rho : E_{tors}(\mathbf{Q}) \to E(\mathbf{F}_p).$$

ρ ist ein Gruppenhomomorphismus, da die Addition geometrisch definiert war. Natürlich ist ρ dann auch injektiv, da ein Punkt $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ modulo p betrachtet in $\mathbf{F}_p \times \mathbf{F}_p$ liegt, also von O verschieden ist. Also ist

$$E_{tors}(\mathbf{Q}) \hookrightarrow E(\mathbf{F}_p),$$

Ergebnis: Sei $2(4a^3 + 27b^2) \not\equiv 0 \bmod p$.

- $E_{tors}(\mathbf{Q})$ ist eine Untergruppe von $E(\mathbf{F}_p)$.
- Speziell gilt deshalb
$$\#E_{tors}(\mathbf{Q}) | \#E(\mathbf{F}_p).$$

Dies kann praktisch sehr hilfreich sein, um $E_{tors}(\mathbf{Q})$ zu bestimmen.

Beispiele:

1. $y^2 = x^3 - 43x + 166$ hatten wir bereits betrachtet.

p	3	5	7	11	17	19
$\#E(\mathbf{F}_p)$	7	7	7	14	21	14

   Also gilt: $E_{tors}(\mathbf{Q}) \in \{1, 7\}$.
2. $y^2 = x^3 - 432x + 8202$ haben wir auch schon betrachtet.

p	5	7	13	17	19	23	29
$\#E(\mathbf{F}_p)$	5	10	10	20	20	25	30

   Also gilt: $E_{tors}(\mathbf{Q}) \in \{1, 5\}$.

KAPITEL 12

Elliptischen Kurven über Q

1. Rationale Punkte — Der Satz von Mordell-Weil

Wir betrachten elliptische Kurven E über $\mathbf{Q}$ gegeben durch eine Gleichung $y^2 = x^3 + ax + b$ mit $a, b \in \mathbf{Z}$. Wir wissen bereits, daß die rationalen Punkte zusammen mit dem unendlich fernen Punkt O eine abelsche Gruppe bilden. Es gilt der Satz von Mordell:

SATZ 37 (Mordell-Weil). *$E(\mathbf{Q})$ ist eine endlich erzeugte abelsche Gruppe, d.h.*

$$E(\mathbf{Q}) \simeq E_{tors}(\mathbf{Q}) \times \mathbf{Z}^r,$$

mit einer ganzen Zahl $r \geq 0$. (r heißt der Rang der elliptischen Kurve E.)

Der Beweis erfolgt in zwei Schritten.

- Zuerst zeigen wir, daß $E(\mathbf{Q})/[2]E(\mathbf{Q})$ endlich ist. (Das reicht aber für die Endlicherzeugtheit noch nicht aus, wie $\mathbf{Q}/2\mathbf{Q} = 0$ zeigt.)
- Dann werden wir versuchen mit der Methode des Abstiegs - Descente 'große' Lösungen auf kleinere zurückzuführen, um so ein endliches Erzeugendensystem zu erhalten. Dazu ist es wichtig, die Größe - Höhe - von Punkten zu messen.

Dieser Satz soll im folgenden Fall bewiesen werden für den Spezialfall, daß die 2-Teilungspunkte bereits über $\mathbf{Q}$ definiert sind, d.h. $x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$ mit $e_i \in \mathbf{Q}$.

Der Beweis erfolgt in zwei Schritten.

- Zuerst zeigen wir, daß $E(\mathbf{Q})/[2]E(\mathbf{Q})$ endlich ist. (Das reicht aber für die Endlicherzeugtheit noch nicht aus, wie $\mathbf{Q}/2\mathbf{Q} = 0$ zeigt.)
- Dann werden wir versuchen mit der Methode des Abstiegs - Descente 'große' Lösungen auf kleinere zurückzuführen, um so ein endliches Erzeugendensystem zu erhalten. Dazu ist es wichtig, die Größe - Höhe - von Punkten zu messen.

1.1. Der schwache Satz von Mordell-Weil. Sei K ein Körper der Charakteristik $\neq 2, 3$. Wir betrachten elliptische Kurven E, gegeben durch

$$y^2 = x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3),$$

wo alle e_i in K liegen.
Sind $x, y \in K$ mit $y^2 = (x - e_1)(x - e_2)(x - e_3)$, so läßt sich fragen, wieweit sich $x - e_i$ von einem Quadrat unterscheidet.
Wir definieren daher:

Definition: $\phi : E(K) \to K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ werde wie folgt definiert:

$$\phi(x,y) = \begin{cases} (x - e_1, x - e_2) & (x,y) \neq (e_1,0), (e_2,0), O \\ ((e_1 - e_2)(e_1 - e_3), e_1 - e_2) & (x,y) = (e_1,0) \\ (e_2 - e_1, (e_2 - e_1)(e_2 - e_3)) & (x,y) = (e_2,0) \\ 1 & O \end{cases}$$

wobei jeweils die Klassen in $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ zu nehmen sind.

Bemerkung: Da i.a.

$$x - e_3 = \frac{y^2}{(x - e_1)(x - e_2)} = (x - e_1)(x - e_2) \cdot \left(\frac{y}{(x - e_1)(x - e_2)}\right)^2$$

gilt, kann man auf die Betrachtung von $x - e_3$ verzichten.

Gilt auf E: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, dann rechnet man nach, daß gilt:

$$(x_1 - e_i)(x_2 - e_i)(x_3 - e_i) = \left(\frac{e_i(y_1 - y_2) + x_1 y_2 - x_2 y_1}{x_1 - x_2}\right)^2.$$

Eine unmittelbare Folgerung ist:

LEMMA 16. *ϕ ist ein Gruppenhomomorphismus.*

Beispiel: Wir nehmen $E : y^2 = x^3 - 25x$. Wir haben bereits vier nichttriviale Punkte. Wir definieren: $\phi((x, y)) =$ Klasse von $(x, x - 5)$.

$$\begin{aligned}
\phi((0,0)) &= ((0-5)(0+5), 0-5) \sim (-1,-5)\\
\phi((5,0)) &= (5-0, (5-0)(5+5)) \sim (5,2)\\
\phi((-5,0)) &= (-5-0, -5-5) \sim (-5,-10)\\
\phi((-4,6)) &= (-4-0, -4-5) \sim (-1,-1)
\end{aligned}$$

Beispiele:

1. Alle Elemente in $\mathbf{C}$ sind Quadrate, also $\mathbf{C}^\times/(\mathbf{C}^\times)^2 = 1$
2. In $\mathbf{R}$ sind genau die positiven Elemente Quadrate, also $\mathbf{R}^\times/(\mathbf{R}^\times)^2 = \{\pm 1\}$
3. Wegen der eindeutigen Primfaktorzerlegung in $\mathbf{Z}$ ist jedes $x \in \mathbf{Q}$, $x \neq 0$ modulo Quadraten von der Form $x \sim \pm p_1 \ldots p_r$, wo die p_i Primzahlen sind.

Da $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ Exponent 2 hat, sollte $[2]E(K)$ im Kern von ϕ liegen, und in der Tat gilt: Ist $(x_2, y_2) = [2](x, y)$, so folgt:

$$x_2 = \frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}$$

und man rechnet aus:

$$\begin{aligned}
x_2 - e_1 &= \left(\frac{x^2 - 2e_1 x - e_1^2 + e_1 e_2 + e_2^2}{2y}\right)^2\\
x_2 - e_2 &= \left(\frac{x^2 - 2e_2 x + e_1^2 + e_1 e_2 - e_2^2}{2y}\right)^2
\end{aligned}$$

woraus unmittelbar die Bemerkung folgt.

Was ist der Kern von ϕ? (x, y) ein Element daraus, also

$$x - e_i = a_i^2, \quad y = a_1 a_2 a_3$$

Dann hat man natürlich $e_1 + a_1^2 = e_2 + a_2^2 = e_3 + a_3^2$. Da außerdem $e_3 = -e_1 - e_2$ erhält man schnell:

$$\begin{aligned}
e_1 &= \frac{1}{3}(-2a_1^2 + a_2^2 + a_3^2)\\
e_2 &= \frac{1}{3}(a_1^2 - 2a_2^2 + a_3^2)\\
e_3 &= \frac{1}{3}(a_1^2 + a_2^2 - 2a_3^2)
\end{aligned}$$

Wir betrachten nun die Geraden durch $(x, -y) = (\frac{1}{3}(a_1^2 + a_2^2 + a_3^2), -a_1 a_2 a_3)$:

$$y_g = (x_g - \frac{1}{3}(a_1^2 + a_2^2 + a_3^2)) - a_1 a_2 a_3$$

und untersuchen wann sie auch Tangente sind. Wir setzen in $f = x_g^3 + a x_g + b - y_g^2$ ein und erhalten nach Abspaltung des trivialen Faktors ein quadratisches Polynom in x_g, dessen Diskriminante

$$81(a_1 + a_2 + a_3 - t)(a_1 - a_2 - a_3 - t)(-a_1 - a_2 + a_3 - t)(-a_1 + a_2 - a_3 - t)$$

ist. Wir erhalten also 4 Tangenten. Eine davon erhält man für $t = a_1 + a_2 + a_3$. Man rechnet dann sofort nach:

$$[2](\frac{1}{3}(a_1^2 + a_2^2 + a_3^2) + a_1a_2 + a_1a_3 + a_2a_3, (a_1 + a_2)(a_1 + a_3)(a_2 + a_3)) = (\frac{1}{3}(a_1^2 + a_2^2 + a_3^2), a_1a_2a_3).$$

Also erhält man schließlich den Satz:

SATZ 38. *ϕ induziert eine Einbettung*

$$E(K)/[2]E(K) \hookrightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Wir betrachten nun den Fall $K = \mathbf{Q}$ genauer. Sei $(x, y) = (\frac{r}{u^2}, \frac{s}{u^3}) \in E(\mathbf{Q})$. Dann gilt:

$$s^2 = (r - u^2e_1)(r - u^2e_2)(r - u^2e_3).$$

Wir schreiben

$$r - u^2e_1 = \pm p_1 \dots p_r \cdot v^2$$

mit verschiedenen Primteilern p_i. Da links ein Quadrat steht, muß p_1 noch in einem weiteren $r - u^2e_i$ vorkommen, o.E. in $r - u^2e_2$. Dann teilt p_1 auch die Differenz $u^2(e_1 - e^2)$, ist aber fremd zu u, weil p_1 sonst auch r teilen würde. Also: $p_1|e_1 - e_2$. Analoges gilt für die anderen p_i, d.h. alle p_i treten als Teiler von $(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$ auf. Das gleiche gilt für $r - u^2e_2$ und $r - u^2e_3$. Und wegen $x - e_i = (r - u^2e_i) \cdot \frac{1}{u^2}$ gilt für die Quadratklassen:

SATZ 39. *Seien p_i die Primteiler von $(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. Dann ist das Bild von ϕ enthalten in der von*

$$(\pm p_i, \pm p_j)$$

erzeugten Untergruppe von $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$.

Also liegt $\phi(E(\mathbf{Q}))$ in einer endlichen Untergruppe von $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$, woraus unmittelbar der schwache Satz von Mordell-Weil folgt:

SATZ 40. *$E(\mathbf{Q})/[2]E(\mathbf{Q})$ ist endlich.*

1.2. Höhen. Wir wollen nun die Größe von Zahlen messen. Dazu definieren wir:

Definition: Sei $x = (r_0 : \cdots : r_n) \in \P^n(\mathbf{Q})$ dargestellt mit $r_i \in \mathbf{Z}$ und $\mathrm{ggT}(r_0, \dots, r_n) = 1$. Dann heißt $H(x) = \max(|r_i|)$ die *Höhe* von x. Desweiteren heißt $h(x) = \log H(x)$ die logarithmische Höhe von x.

Beispiel: Seien r, s ganze teilerfremde Zahlen mit $s \neq 0$. Dann entspricht $\frac{r}{s}$ dem Punkt $(1 : \frac{r}{s}) = (s : r)$, also

$$H(\frac{r}{s}) = \max(|r|, |s|).$$

Z.B. $H(\frac{5}{7}) = 7$.

Wir definieren nun auch analog eine Höhe auf $E(\mathbf{Q})$. Da die y-Koordinate im wesentlichen durch die x-Koordinate bis aufs Vorzeichen festgelegt ist, beschränken wir uns auf die x-Koordinate und definieren für $(x, y) = (\frac{r}{u^2}, \frac{s}{u^3}) \in E(\mathbf{Q})$:

$$H(P) = H(x) = \max(|r|, u^2).$$

Welche Eigenschaften hat nun die Höhe auf $E(\mathbf{Q})$?

SATZ 41. *Seien Q_i, $i = 1, \dots, s$ Punkte in $E(\mathbf{Q})$. Dann gibt es Konstanten $c_1 = c_1(a, b, Q_i)$ und $c_2 = c_2(a, b)$ mit der Eigenschaft:*

1. $h(P + Q_i) \leq 2h(P) + c_1$
2. $h([2]P) \geq 4h(P) - c_2$
3. *Für alle $c \in \mathbf{R}$ ist $\{P \in E(\mathbf{Q}) : h(P) \leq c\}$ endlich.*

Zum Beweis benützt man folgendes Lemma:

LEMMA 17. *Sei $E : y^2 + ax + b$. Dann gilt:*

1. *Ist* $(\frac{r_0}{u_0^2}, \frac{s_0}{u_0^3}) + (\frac{r}{u^2}, \frac{s}{u^3}) = (x_a, y_a)$, *so gilt:*

$$x_a = \frac{a\,r_0\,{u_0}^2 u^4 - 2\,s_0\,s{u_0}\,u + 2\,b{u_0}^4 u^4 + a\,r{u_0}^4 u^2 + {r_0}^2 r u^2 + r^2 r_0\,{u_0}^2}{\left(r{u_0}^2 - r_0\,u^2\right)^2}$$

2. *Ist* $[2](\frac{r}{u^2}, \frac{s}{u^3}) = (x_2, y_2)$, *so gilt:*

$$x_2 = \frac{r^4 - 2\,r^2 a u^4 + a^2 u^8 - 8\,rbu^6}{4\,u^2\,(r^3 + aru^4 + bu^6)}$$

Sei $x_2 = \frac{Z}{N}$ *mit*

$$Z = r^4 - 2ar^2u^4 - 8bru^6 + a^2u^8, \quad N = 4u^2(r^3 + aru^4 + bu^6).$$

Dann gilt:

$$Z(-12r^2u^2 - 16u^6a) + N(3r^3 - 5aru^4 - 27bu^6) = -4u^{14}(4a^3 + 27b^2)$$

und

$$Z \cdot N_1 + N \cdot Z_1 = -4r^7(4a^3 + 27b^2)$$

mit

$$N_1 = -12\,ru^4a^4 - 12\,a^3bu^6 - 16\,a^3r^3 + 4\,r^2ba^2u^2 - 88\,rb^2u^4a - 96\,b^3u^6 - 108\,r^3b^2$$

$$Z_1 = 3\,u^6a^5 - 5\,r^2u^2a^4 - 26\,rbu^4a^3 + 24\,a^2u^6b^2 - r^3ba^2 - 32\,r^2u^2b^2a - 192\,rb^3u^4$$

Das Lemma beweist man einfach durch Nachrechnen.

Beweisskizze für den Satz:

- Sei H_i die Höhe von Q_i etc. Nun gilt: $s^2 = |r^3 + aru^4 + bu^6| \le H^3 + |a|H^3 + |b|H^3$, also $(su)^2 \le (1 + |a| + b|)H^4$, also $|su| \le (1 + |a| + |b|)^{\frac{1}{2}}H^2$. Damit kann man abschätzen:

$$\begin{aligned} |\text{Zähler von } x_a| &\le 4H_i^2H^2 \\ |\text{Nenner von } x_a| &\le 4(1 + |a| + |b|)H_i^2H^2 \end{aligned}$$

  woraus sofort $H(x_a) \le 4(1 + |a| + |b|)H_i^2H^2$ folgt.
- Zunächst sieht man $\mathrm{ggT}(Z, N)|\Delta$, woraus folgt:

$$|Z| \le |\Delta|H_2, \quad |N| \le |\Delta|H_2$$

  Setzt man dies ein, so erhält man:

$$u^1 4|\Delta| \le H_2|\Delta|(15 + 21|a| + 27|b|)H^3.$$

  Aus der anderen Formel erhält man analog:

$$|r^7||\Delta| \le H_2|\Delta|c(a, b)H^3.$$

  Daraus folgt sofort:

$$H^4 \le H_2c_2(a, b)$$

Anwendung auf die Bestimmung von $E(\mathbf{Q})$**:** Seien $Q_1, \ldots Q_s$ Repräsentanten von $E(\mathbf{Q})/[2]E(\mathbf{Q})$. Sei $P = P_0$ gegeben. Wir konstruieren rekursiv Punkte P_i wie folgt:
Bestimme $Q_{f(i)}$ mit $\phi(P_i) = \phi(Q_{f(i)})$. Dann ist also

$$P_i = Q_{f(i)} + [2]P_{i+1}$$

mit einem neuen Punkt P_{i+1}. Wir können jetzt abschätzen:

$$\begin{aligned} h(P_{i+1}) &\le \frac{1}{4}[h([2]P_i) + c_2] \\ &= \frac{1}{4}h(p_i - Q_{f(i)}) + \frac{c_2}{4} \\ &\le \frac{1}{2}h(P_i) + \frac{c_1 + c_2}{4} \end{aligned}$$

Daraus erhält man:

$$h(P_i) \le \frac{1}{2^i}h(P) + \frac{c_1 + c_2}{2}$$

und als unmittelbare Folgerung:

Ergebnis: Die Menge

$$\{P \in E(\mathbf{Q}) : h(P) \leq c_1 + c_2\}$$

erzeugt $E(\mathbf{Q})$.

Damit ist der Satz von Mordell bewiesen.

Bemerkung: Wir können $E(\mathbf{Q})$ bestimmen, falls wir $E(\mathbf{Q})/[2]E(\mathbf{Q})$ kennen. Der Rest ist konstruktiv.

Bemerkungen:

1. Es gibt verschiedene Methoden, um die Bestimmung von $E(\mathbf{Q})$ anzugehen, es ist aber kein allgemeiner Algorithmus bekannt.
2. Wie groß kann r (der *Rang* der elliptischen Kurve) werden, wo
$$E(\mathbf{Q}) \simeq E_{tors}(\mathbf{Q}) \oplus \mathbf{Z}^r$$
3. Die Kurve
$$y^2 = x^3 - 1015969383 52x + 12361366202306320$$
hat Rang ≥ 12.
Die Kurve
$$y^2 + 357573631y = x^3 + 2597055x^2 - 549082x - 19608054$$
hat Rang ≥ 14.
4. Ist der Rang groß, so hat E also viele rationale Punkte, sollte also auch viele Punkte modulo p haben. Dies haben Birch und Swinnerton-Dyer untersucht. Eine ihrer Vermutungen läßt sich so formulieren:
Sei $f(P) = \Pi_{p \leq p} \frac{\#E(\mathbf{F}_p)}{p}$. Dann gilt asymptotisch für $P \to \infty$:
$$f(P) \sim C(\log P)^r$$
mit einer Konstanten r. Die Vermutungen von Birch und Swinnerton-Dyer erstrecken sich auch auf E zugeordnete L-Reihen und sind bis heute noch nicht allgemein bewiesen.
5. Sei p_i die Folge der Primzahlen. Betrachte dann die Folge
$$a_n = \frac{\sum_{i \leq n} \log \frac{\#E(\mathbf{F}_{p_i})}{p_i}}{\log \log p_n}$$
Frage: Was hat a_n mit dem Rang r zu tun?
6. Beispiele

Kurve	Rang	a_{100}	a_{200}
$y^2 = x^3 + 1$	0	0.75	0.70
$y^2 = x^3 - 25x$	1	1.58	1.44
$y^2 = x^3 - x + 4$	2	2.40	2.40

L-Reihen: Ist E über $\mathbf{F}_p$ nichtsingulär, so definieren wir

$$a_p = p + 1 - \#E(\mathbf{F}_p).$$

Damit

$$L_E(s) = \prod_{\text{gute } p} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{\text{schlechte } p} \ldots .$$

Birch und Swinnerton-Dyer haben dann unter anderem Folgendes vermutet:

- $L_E(s)$ hat eine analytische Fortsetzung auf ganz $\mathbf{C}$.
- Die Nullstellenordnung von $L_E(s)$ im Punkt $s = 1$ ist der Rang der elliptischen Kurve.

2. Ganzzahlige Punkte — Der Satz von Siegel

Es gilt der Satz

SATZ 42 (Siegel). *Auf der elliptischen Kurve* $y^2 = x^3 + ax + b$ *mit* $a, b \in \mathbf{Z}$ *gibt es nur endlich viele Punkte mit ganzen Koeffizienten.*

Genauer gilt: Ist P_n die Folge der rationalen Punkte mit $H(P_n) \leq H(P_{n+1})$ und $P_n = (\frac{a_n}{b_n}, \ldots)$, so gilt

$$\lim_{n\to\infty} \frac{\log |a_n|}{\log |b_n|} = 1.$$

D.h. die Anzahl der Dezimalstellen von Zähler und Nenner ist ungefähr gleich. (?)

Beispiel: $y^2 = x^3 - x$

KAPITEL 13

Übersicht über rationale und ganzzahlige Lösungen

Gegeben sei eine Kurve C durch ein absolut irreduzibles Polynom $f(x,y) \in \mathbf{Z}[x,y]$ vom Grad d. Wir fragen nach den rationalen und ganzzahligen Punkten auf C.

Wir wollen eine Invariante von C einführen, das Geschlecht.

Die Riemannsche Fläche von C: Zerlegt man

$$f(x_1 + ix_2, x_3 + ix_4) = g(x_1, x_2, x_3, x_4) + ih(x_1, x_2, x_3, x_4),$$

wo g und h Polynome mit ganzzahligen Koeffizienten sind, so lassen sich die komplexen Lösungen von $f(x,y) = 0$ reell wie folgt beschreiben:

$$\begin{aligned} \tilde{C}_0 &= \{(x_1, \ldots, x_4) \in \mathbf{R}^4 : f(x_1 + ix_2, x_3 + ix_4) = 0\} = \\ &= \{(x_1, \ldots, x_4) \in \mathbf{R}^4 : g(x_1, x_2, x_3, x_4) = h(x_1, x_2, x_3, x_4) = 0\}. \end{aligned}$$

$\tilde{C}_0$ ist dann eine reelle Fläche im $\mathbf{R}^4$. Nach Desingularisierung und Kompaktifizierung erhält man dann aus $\tilde{C}_0$ eine reelle glatte kompakte Fläche $\tilde{C}$, die automatische orientierbar ist. (Riemannsche Fläche von C)

Topologische Klassifikation der reellen kompakten orientierbaren Flächen: Jede reelle kompakte orientierbare Fläche ist topologisch isomorph zu einer Kugel mit g angehängten Henkeln. g heißt das Geschlecht der Fläche.
Skizze:

So kann man also $g(C)$ als das Geschlecht der zugeordneten Riemannschen Fläche $\tilde{C}$ definieren. Berechnen kann man so aber $g(C)$ nicht. Es gibt eine algebraische Berechnungsmethode. Der einfachste Fall davon ist:

SATZ 43. *Ist C vom Grad d und hat C keine Singularitäten, weder im Endlichen noch im Unendlichen, so gilt*

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

Nun können wir eine Übersicht geben. Sei R bzw. Z die Anzahl der rationalen bzw. ganzzahligen Punkte auf C. Dann gibt es folgende Fälle:

$g = 0$ Über dem Grundkörper $\mathbf{C}$ ist die Kurve rational, d.h. besitzt eine Parametrisierung.
  $R = \infty$ Dies ist genau dann der Fall, wenn C rational ist, d.h. es gibt eine Parametrisierung

$$x = \frac{X(t)}{Z(t)}, y = \frac{Y(t)}{Z(t)}.$$

    $Z = \infty$ Dann ist $Z(t)$ von spezieller Bauart.
    $Z < \infty$
  $R < \infty$ Dann ist bereits $R = 0$, also auch $Z = 0$. Beispiel: $x^2 + y^2 = 3$.
$g = 1$ Über dem Grundkörper C ist die Kurve elliptisch.
  $R > 0$ Dann ist C isomorph zu einer elliptischen Kurve über $\mathbf{Q}$. Der Satz von Siegel sagt, daß $Z < \infty$ gilt. Genau dann ist $R = \infty$, wenn der Rang r der elliptischen Kurve > 0 ist. Die rationalen Punkte bilden eine endlich erzeugte abelsche Gruppe.
  $R = 0$ Beispiel $3x^3 + 4y^3 = 5$.
$g > 1$ Nach dem Satz von Siegel ist $Z < \infty$, nach dem Satz von Mordell-Faltings ist $R < \infty$. Beispiel: Für $d \geq 4$ hat die Kurve $x^d + y^d = 1$ Geschlecht $\frac{(d-1)(d-2)}{2} > 1$.

ANHANG A

Vorlesungsankündigung

MATHEMATISCHES INSTITUT
UNIVERSITÄT ERLANGEN-NÜRNBERG
Priv.-Doz. Dr. W. Ruppert

Bismarckstraße 1 1/2, 15. Februar 1993
D-8520 Erlangen
Tel. (09131) 85 2466 (Durchwahl)

SS 1993

Ausgewählte Kapitel aus der Zahlentheorie:

Diophantische Approximationen und Diophantische Gleichungen

Ausgangspunkt der diophantischen Approximationen ist die Fragestellung: Wie gut läßt sich eine reelle Zahl α durch rationale Zahlen $\frac{p}{q}$ approximieren? Bei diophantischen Gleichungen sucht man nach ganzzahligen oder rationalen Lösungen polynomialer Gleichungen.

Beispiel: Hat man eine Lösung $x, y \in \mathbf{N}$ der Pellschen Gleichung $x^2 - dy^2 = 1$, so findet man $|\sqrt{d} - \frac{x}{y}| < \frac{1}{\sqrt{d}y^2}$, d.h. man hat $\sqrt{d}$ durch die rationale Zahl $\frac{x}{y}$ gut approximiert. Umgekehrt kann man mit dem Kettenbruchalgorithmus gute Approximationen an $\sqrt{d}$ gewinnen und damit die Pellsche Gleichung lösen.

In der Vorlesung soll es um das Wechselspiel zwischen beiden Themenbereichen gehen.

Ein paar Themen im Einzelnen:

- Kettenbrüche, quadratische Irrationalitäten und die Pellsche Gleichung
- Transzendente Zahlen
- Der Approximationssatz von Thue-Siegel-Roth
- Der Satz von Siegel über ganzzahlige Punkte auf ebenen Kurven
- Linearformen in Logarithmen
- Die abc-Vermutung

Die vierstündige Vorlesung richtet sich an Studenten des Hauptstudiums, gehört zum Gebiet Algebra, Zahlentheorie und kann im Anschluß an die Vorlesung Algebra und Zahlentheorie I gehört werden.

Zeit und Ort: Di, Do 10-12, Übungsraum 1
Beginn: 4. Mai 1993
Nummer im Vorlesungsverzeichnis:

gez. W. Ruppert

ANHANG B

Formeln für elliptische Kurven

1. Normalform

Wir betrachten elliptische Kurven E der Form

$$y^2 = x^3 + ax + b$$

über einem Körper K (mit Charakteristik $\neq 2, 3$). Die Diskriminante ist

$$\Delta = -16(4a^3 + 27b^2)$$

und die j-Invariante:

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

Die Isomorphismen zwischen E und $E' : y'^2 = x'^3 + a'x' + b'$ werden durch ein $u \in K^*$ gegeben mit:

$$x = u^2x', \quad y = u^3y', \quad a = u^4a', \quad b = u^6b'.$$

Ist $j \in K$ und $j \neq 0, 1728$, so liefert für jedes $u \in K^*$ und $c = \frac{j}{1728-j}$

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

eine elliptische Kurve mit j-Invariante j.

2. Addition

$$\begin{aligned}
-(x,y) &= (x,-y) \\
2\cdot(x,y) &= \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3+ax+b)}, \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8y(x^3+ax+b)}\right) \\
(x,y) + (u,v) &= \left(\frac{ux^2 + (u^2+a)x - 2vy + au + 2b}{(x-u)^2},\right. \\
&\qquad \left.\frac{vx^3 + 3uvx^2 - (3u^2+a)xy - 3avx - (u^3 + 3au + 4b)y + auv + 4bv}{(x-u)^3}\right)
\end{aligned}$$

3. q-Entwicklungen

Für $q = e^{2\pi i\tau}$ gilt:

$$g_2 = \frac{4}{3}\pi^4 + 320\pi^4\sum_{n=1}^{\infty}\sigma_3(n)q^n \qquad g_3 = \frac{8}{27}\pi^6 - \frac{448}{3}\pi^6\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

wobei $\sigma_k(n) = \sum_{d|n} d^k$ ist. Es ist

$$j = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

und man hat die q-Entwicklung:

$$
\begin{aligned}
j &= \frac{1}{q} + 196884\,q + 21493760\,q^2 + 864299970\,q^3 + 20245856256\,q^4 \\
&\quad + 333202640600\,q^5 + 4252023300096\,q^6 + 44656994071935\,q^7 \\
&\quad + 401490886656000\,q^8 + 3176440229784420\,q^9 + 22567393309593600\,q^{10} \\
&\quad + 146211911499519294\,q^{11} + 874313719685775360\,q^{12} \\
&\quad + 4872010111798142520\,q^{13} + 25497827389410525184\,q^{14} \\
&\quad + 126142916465781843075\,q^{15} + 593121772421445058560\,q^{16} \\
&\quad + 2662842413150775245160\,q^{17} + 11459912788444786513920\,q^{18} \\
&\quad + 47438786801234168813250\,q^{19} + 189449976248893390028800\,q^{20}
\end{aligned}
$$

4. n-Teilungspunkte

4.1. Rekursionsformeln.

$$
\begin{aligned}
\psi_{2n} &= \frac{\psi_n\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right)}{2\,y} \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3
\end{aligned}
$$

4.2. Einzelne ψ_n's.

$$
\begin{aligned}
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
\psi_5 &= 5x^{12} + 62ax^{10} + 380bx^9 - 105a^2x^8 + 240abx^7 - 300a^3x^6 - 240b^2x^6 - 696a^2bx^5 \\
&\quad - 1920ab^2x^4 - 125a^4x^4 - 80a^3bx^3 - 1600b^3x^3 - 50a^5x^2 - 240a^2b^2x^2 - 100a^4bx - 640ab^3x \\
&\quad + a^6 - 256b^4 - 32b^2a^3 \\
\psi_6 &= 2\left(3\,x^4 + 6\,ax^2 + 12\,bx - a^2\right)y(x^{12} + 22\,ax^{10} + 220\,bx^9 - 165\,a^2x^8 - 528\,abx^7 \\
&\quad - 92\,a^3x^6 - 1776\,b^2x^6 + 264\,ba^2x^5 - 960\,ab^2x^4 - 185\,a^4x^4 - 80\,a^3bx^3 - 320\,b^3x^3 \\
&\quad - 90\,a^5x^2 - 624\,b^2a^2x^2 - 132\,ba^4x - 896\,ab^3x - 3\,a^6 - 512\,b^4 - 96\,b^2a^3) \\
\psi_7 &= 7\,x^{24} + 308\,ax^{22} + 3944\,bx^{21} - 2954\,a^2x^{20} - 112\,abx^{19} - 19852\,a^3x^{18} - 42896\,b^2x^{18} \\
&\quad - 92568\,a^2bx^{17} - 571872\,ab^2x^{16} - 35231\,a^4x^{16} - 31808\,a^3bx^{15} - 829696\,b^3x^{15} \\
&\quad - 615360\,a^2b^2x^{14} - 82264\,a^5x^{14} - 2132480\,ab^3x^{13} - 161840\,a^4bx^{13} \\
&\quad - 928256\,b^4x^{12} - 297472\,a^3b^2x^{12} - 111916\,a^6x^{12} - 608160\,a^5bx^{11} - 2603776\,b^3a^2x^{11} \\
&\quad - 42168\,a^7x^{10} - 1192800\,b^2a^4x^{10} - 3293696\,b^4ax^{10} \\
&\quad - 42571\,2ba^6x^9 - 1555456\,b^5x^9 - 3727360\,a^3b^3x^9 \\
&\quad + 15673\,a^8x^8 - 831936\,a^5b^2x^8 - 7069440\,b^4a^2x^8 \\
&\quad - 1314560\,b^3a^4x^7 - 53824\,a^7bx^7 - 7127040\,ab^5x^7 \\
&\quad - 190400\,a^6b^2x^6 + 14756\,a^9x^6 - 2293760\,a^3b^4x^6 - 2809856\,b^6x^6 \\
&\quad - 168448\,a^5b^3x^5 - 3698688\,b^5a^2x^5 + 57288\,a^8bx^5 \\
&\quad + 134400\,a^7b^2x^4 + 394240\,b^4a^4x^4 - 3039232\,b^6ax^4 + 1302\,a^{10}x^4 \\
&\quad + 152320\,a^6b^3x^3 - 802816\,b^7x^3 + 1680\,a^9bx^3 + 831488\,b^5a^3x^3 \\
&\quad + 96768\,b^4a^5x^2 + 196\,a^{11}x^2 + 3696\,a^8b^2x^2 + 544768\,b^6a^2x^2 \\
&\quad + 392\,a^{10}bx + 64512\,b^5a^4x + 7168\,b^3a^7x + 229376\,b^7ax \\
&\quad + 160\,b^2a^9 - a^{12} + 65536\,b^8 + 24576\,a^3b^6 + 3328\,b^4a^6
\end{aligned}
$$

5. Isogenien I

6. Isogenien II

$$\begin{aligned}\phi_2 &= x^3+y^3-x^2y^2+1488\,(x^2y+xy^2)-162000\,(x^2+y^2)+40773375\,xy\\ &\quad +8748000000\,(x+y)-157464000000000\\ \phi_3 &= x^4+y^4-x^3y^3+2232(x^3y^2+x^2y^3)-1069956(x^3y+xy^3)+36864000(x^3+y^3)\\ &\quad +2587918086x^2y^2+8900222976000(x^2y+xy^2)+452984832000000(x^2+y^2)\\ &\quad -770845966336000000xy+18554258718720000000000(x+y)\end{aligned}$$

7. Komplexe Multiplikation

Tabelle der singulären rationalen j-Invarianten

Ring	j	Beispiel
$\mathbf{Z}[\sqrt{-1}]$	$2^6\cdot 3^3$	$y^2=x^3-x$
$\mathbf{Z}[2\sqrt{-1}]$	$2^3\cdot 3^3\cdot 11^3$	$y^2=x^3-11x-14$
$\mathbf{Z}[\sqrt{-2}]$	$2^6\cdot 5^3$	$y^2=x^3-30x-56$
$\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$	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}	$y^2=x^3-264x-1694$
$\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$	$-2^{15}\cdot 3^3$	$y^2=x^3-152x-722$
$\mathbf{Z}[\frac{1+\sqrt{-43}}{2}]$	$-2^{18}\cdot 3^3\cdot 5^3$	$y^2=x^3-3440x-77658$
$\mathbf{Z}[\frac{1+\sqrt{-67}}{2}]$	$-2^{15}\cdot 3^3\cdot 5^3\cdot 11^3$	$y^2=x^3-29480x-1948226$
$\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$	$-2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3$	$y^2=x^3-8697680x-9873093538$

ANHANG C

Approximation von $\sqrt[3]{2}$

Literatur

19??: Baker

1979: G. V. Chudnovsky, Formules d'Hermite pour les approximants de Padé de logarithmes et des fonctions binomes, et mesures d'irrationalité, C. R. Acad. Sci. Paris, Ser. A **288** (1979), 965-967.

1982: G. V. Chudnovsky, Approx..., C. R. Acad. Sci. Paris, Ser I **295** (1982), 219-221.

1988: *Baker, Stewart,* in: New Advances... 1986

Invertieren. Man findet leicht folgende Formel

$$\frac{1}{x_0+x_1\alpha+x_2\alpha^2}=\frac{x_0^2-2x_1x_2}{x_0^3-6x_0x_1x_2+2x_1^3+4x_2^3}+\frac{-x_0x_1+2x_2^2}{x_0^3-6x_0x_1x_2+2x_1^3+4x_2^3}\alpha+\frac{-x_0x_2+x_1^2}{x_0^3-6x_0x_1x_2+2x_1^3+4x_2^3}\alpha^2.$$

Die Kettenbruchentwicklung von $2^{\frac{1}{3}}$.

```
[1, 3, 1, 5, 1, 1, 4, 1, 1, 8, 1, 14, 1, 10, 2, 1, 4, 12, 2, 3, 2, 1, 3, 4, 1,

    1, 2, 14, 3, 12, 1, 15, 3, 1, 4, 534, 1, 1, 5, 1, 1, 121, 1, 2, 2, 4, 10,

    3, 2, 2, 41, 1, 1, 1, 3, 7, 2, 2, 9, 4, 1, 3, 7, 6, 1, 1, 2, 2, 9, 3, 1,

    1, 69, 4, 4, 5, 12, 1, 1, 5, 15, 1, 4, 1, 1, 1, 1, 1, 89, 1, 22, 186, 6,

    2, 3, 1, 3, 2, 1, 1, 5, 1, 3, 1, 8, 9, 1, 26, 1, 7, 1, 18, 6, 1, 372, 3,

    13, 1, 1, 14, 2, 2, 2, 1, 1, 4, 3, 2, 2, 1, 1, 9, 1, 6, 1, 38, 1, 2, 25,

    1, 4, 2, 44, 1, 22, 2, 12, 11, 1, 1, 49, 2, 6, 8, 2, 3, 2, 1, 3, 5, 1, 1,

    1, 3, 1, 2, 1, 2, 4, 1, 1, 3, 2, 1, 9, 4, 1, 4, 1, 2, 1, 27, 1, 1, 5, 5,

    1, 3, 2, 1, 2, 2, 3, 1, 4, 2, 2, 8, 4, 1, 6, ...]
```

Literaturverzeichnis

[HW] *G. H. Hardy, E. M. Wright,* An Introduction to the Theory of Numbers, Clarendon Press, Oxford

[La] *S. Lang,* Introduction to Diophantine Approximations, Addison-Wesley, Reading, MA, 1966

[Mo] *L. J. Mordell,* Diophantine Equations, Academic Press, London – New York, 1969

[Schm1] *W. M. Schmidt,* Diophantische Approximationen und Diophantische Gleichungen

[Schm] *W. M. Schmidt,* Diophantine Approximations and Diophantine Equations, Lecture Notes in Mathematics **1467**, Springer, 1991

[ST] *Stewart - Tijdeman,* Monatshefte Math. **102** (1986), 251-257