Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Hhu
K. Halupczok

Z25: Pellsche Gleichung und KBE

Stichworte: Pellsche Gleichung, Grundeinheiten in $\mathbb{Q}(\sqrt{m})$, Schnelles Potenzieren, KBE von $\sqrt{m}$ und Pell-Lösungen, Berechnung der Minimallösungen

---

25.1. **Einleitung:** Wir betrachten die Pellsche Glg. (*) $\boxed{x^2 - my^2 = \pm 1}$, $m \in \mathbb{N}$.
Die Glg. ist seit dem Altertum bekannt, ihr Name kommt daher, dass Euler sie (irrtümlicherweise) dem engl. Mathematiker John Pell zugeschrieben hat.
Aus zahlentheoretischer Sicht ist diese interessant, da sie ein Beispiel für eine diophantische Glg. (= Glg., deren Lösungen in $\mathbb{Z}$ gesucht werden) abgibt, die unendlich viele ganzzahlige Lösungen besitzt. (Eine andere solche ist etwa die pythagoräische Glg. $x^2+y^2=z^2$, vgl. dazu Z1.7.) Ihre Lösungen hängen genau mit den Einheiten von $\mathbb{Q}(\sqrt{m})$ zusammen und können zur Berechnung der GE herangezogen werden.

25.2. **Def.:** Man nennt $x^2-my^2=1$ die (Pellsche) Plus-Gleichung (+), und entsprechend $x^2-my^2=-1$ die (Pellsche) Minus-Gleichung (−).

25.3. **Triviale Spezialfälle der Pellschen Glg.:**
- Ist $m = s^2$, $s \in \mathbb{N}$, eine Quadratzahl, ist die l.S. der Glg. $= x^2 - s^2y^2 = (x - sy)(x+sy)$, so dass für (*) die beiden Faktoren ± 1 sein müssen. Ihre Summe ist dann $2x = \pm 2$ oder $= 0$, das zugehörige y dann $= 0$ (oder $= \pm 1$ falls $s=1$), d.h. $\mathbb{L}_{(+)} = \{(\pm 1, 0)\}$, $\mathbb{L}_{(-)} = \emptyset$ für $m = s^2 > 1$ und $\mathbb{L}_{(+)} = \{(\pm 1, 0)\}$, $\mathbb{L}_{(-)} = \{(0, \pm 1)\}$ für $m = s^2 = 1$.
- Ist m keine Quadratzahl, aber nicht quadratfrei, so schreibe $m = s^2 \cdot n$ mit n quadratfrei (auch: quadratfreier Kern von m). Mit $x^2 - my^2 = x^2 - n(sy)^2$ können erst die Lösungen von $x^2 - nz^2 = \pm 1$ bestimmt werden. Die (x,z) mit $z = sy$ ergeben dann die Lösungspaare (x,y) der ursprünglichen Pellschen Glg. $\Rightarrow$ Kann also m quadratfrei angenommen werden. Wir werden die Lösungsmenge aber generell im Fall, dass m keine Quadratzahl ist, nämlich wenn $\sqrt{m} \notin \mathbb{Q}$ ist, komplett beschreiben können, vgl. Satz 25.9 für (+) und Satz 25.12 für (−).
- Weiter genügt es, Lösungspaare $(x,y) \in \mathbb{N}^2$ zu betrachten.

25.4. Sei $m \in \mathbb{N}$ quadratfrei.

Ganzzahlige Lösungen (x,y) entsprechen laut Z19.3 (gewissen) Einheiten im Zahlring A_m des reellquadratischen Zahlkörpers $\mathbb{Q}(\sqrt{m})$. Hatten:

- Im Falle $m \equiv 2,3\ (4)$ ist $A_m = \mathbb{Z}[\sqrt{m}]$, $N(x+\sqrt{m}y) = x^2 - my^2$.
- Im Falle $m \equiv 1\ (4)$ ist $A_m = \mathbb{Z}[\frac{\sqrt{m}+1}{2}]$, $N(\frac{x}{2} + \frac{y}{2}\sqrt{m}) = \frac{x^2}{4} - m\frac{y^2}{4}$.

Die Beschreibung der Lösungen von (*):

Laut Dirichletschem Einheitensatz Z18.5 werden alle Einheiten in A_m von genau einer Grundeinheit (GE) $u > 1$ erzeugt, d.h. $A_m^\times = \{\pm u^k;\ k \in \mathbb{Z}\}$. Somit:

25.5. **Satz:** Die Lösungsmenge von (*), m quadratfrei, ist $\mathbb{L} = \{(x,y);\ \exists k \in \mathbb{Z}: \pm u^k = x + \sqrt{m}y\}$.

- Im Falle $m \equiv 2,3\ (4)$ sind dies genau die Potenzen $\pm u^k$, $k \in \mathbb{Z}$, ebenso falls $m \equiv 1\ (4)$ und $A^\times = B^\times$ für $B = \mathbb{Z}[\sqrt{m}]$.
- Im Falle $m \equiv 1\ (4)$ und $A^\times \neq B^\times$, sind dies genau die Potenzen $\pm(u^3)^k$, $k \in \mathbb{Z}$.

Bew.: Klar für $m \equiv 2,3\ (4)$, sei also $m \equiv 1\ (4)$ und $A = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, setze $B := \mathbb{Z}[\sqrt{m}]$.

- Falls $u \in B$, folgt $A^\times = \{\pm u^k;\ k \in \mathbb{Z}\} \subseteq B^\times$, und da $B \subseteq A$ folgt $A^\times = B^\times$.
- Falls $u \notin B$, ist $u^2 \notin B$, da $u = \frac{1}{2}(a + b\sqrt{m})$ mit $a \equiv b \equiv 1\ (2)$
  und $u^2 = \frac{1}{4}(a^2 + b^2 m + 2ab\sqrt{m}) \notin B$ da $4 \nmid 2ab$.

Es gilt aber $u^3 \in B$, da

$u^3 = \frac{1}{8}(a^3 + 3a^2 b\sqrt{m} + 3ab^2 m + b^3 m\sqrt{m})$, haben $a^2 = mb^2 \pm 4$,
da u Einheit, also

$$u^3 = \frac{1}{8}\left(a^3 + 3a(a^2 \mp 4) + (3a^2 b + (a^2 \mp 4)b)\sqrt{m}\right)$$

$$= \frac{1}{8}\Big(\underbrace{a(4a^2 \mp 12)}_{\text{durch 8 teilbar: } a^2 \mp 3 \equiv 0\ (2)} + \underbrace{b(4a^2 \mp 4)\sqrt{m}}_{\text{durch 8 teilbar: } a^2 \mp 1 \equiv 0\ (2)}\Big) \in B.$$

Somit: $A^\times / B^\times = \{e, u, u^2\}$,
d.h. $\#(A^\times/B^\times) = 3$.

- Lösungen der Pellschen Gl.: $a^2 - b^2 m = \pm 1$ für $m \equiv 1\ (4)$:
  Falls $\frac{1}{2}(v + w\sqrt{m})$ eine Einheit im ZR A ist, wo $2 \nmid v, 2 \nmid w$, so ist $v^2 = mw^2 + 4$, also $(\frac{v}{2}, \frac{w}{2})$ Lsg.

Somit: Falls $A^\times = B^\times$, sind die Komponenten von $\{\pm u^k;\ k \in \mathbb{Z}\}$ Lsg.,
für $\#(A^\times/B^\times) = 3$ " von $B^\times = \{\pm u^{3k};\ k \in \mathbb{Z}\}$ Lsgn. □

Bsp.: $m = 5$: $u = \frac{1}{2}(1+\sqrt{5}) \notin \mathbb{Z}[\sqrt{5}]$, also $\#(A^\times/B^\times) = 3$, $m = 17$: $u = 4 + \sqrt{17} \in \mathbb{Z}[\sqrt{17}] \rightsquigarrow A^\times = B^\times$.

25.6. **Bem.:** • Im letzten Fall in Satz 25.5 ist notwendig $m \equiv 5 \ (8)$, denn ist $u^2 - mv^2 = \pm 4$ mit $u, v \in \mathbb{Z}$, $2 \nmid u, 2 \nmid v$, lösbar, folgt $1 - m \equiv \pm 4 \ (8)$ $(=)$ $m \equiv 1 \mp 4 \equiv 5 \ (8)$ weil $u^2 \equiv 1 \ (8)$ für jede ungerade Zahl u gilt.

• Ist die GE $n > 1$ bekannt, können die Potenzen u^q (bzw. u^{34}) effektiv und schnell berechnet werden mit der Methode des schnellen Potenzierens.

25.7. **Methode des schnellen Potenzierens** ["square and multiply" / "binäre Exponentiation"], ["Double-and-add-Algorithmus" für eine additiv geschriebene Gruppe]:

Geg. sei eine Gruppe $(G, \cdot)$, zu berechnen ist für $k \in \mathbb{N}$, $u \in G$, die Potenz $u^k := \underbrace{u \cdots u}_{k\text{-mal}}$ in der Gruppe G.

1. Schritt: Mit höchstens $r := \left\lfloor \frac{\log k}{\log 2} \right\rfloor$ vielen Verknüpfungen in G berechne durch sukzessives Quadrieren: u^2, $u^{2^2} = u^4 = (u^2) \cdot (u^2)$, $u^{2^3} = (u^{2^2}) \cdot (u^{2^2})$, $u^{2^4} = (u^{2^3}) \cdot (u^{2^3})$, $\ldots$, u^{2^r}

2. Schritt: Schreiben k als Binärzahl: $k = \sum_{i=0}^{r} c_i 2^i$ mit $c_i \in \{0, 1\}$.

3. Schritt: Berechnen $u^k = u^{c_0} \cdot u^{2c_1} \cdot u^{2^2 c_2} \cdots u^{2^r c_r} = (u^{c_0}) \cdot (u^2)^{c_1} \cdot (u^{2^2})^{c_2} \cdots (u^{2^r})^{c_r}$ mit maximal r weiteren Verknüpfungen in G.

Somit reichen höchstens $2r = O(\log k)$ viele Anwendungen der Gruppenverknüpfung "$\cdot$".

Bsp.: $5^{12} = 5^{2^2 + 2^3} = 5^{2^2} \cdot 5^{2^3}$, modulo 11 rechnen wir: $5^2 \equiv 3 \ (11)$, $5^{2^2} \equiv 3^2 \equiv -2 \ (11)$, $5^{2^3} \equiv (-2)^2 \equiv 4 \ (11)$, also $5^{12} \equiv (-2) \cdot 4 \equiv 3 \ (11)$; geht schneller als $5^{12} = 244140625$ von Hand durch 11 zu teilen (bzw. das $\mathfrak{I}$ auszurechnen...

25.8. **Bem.:** Es genügt nun, die GE $u > 1$ in A_m zu bestimmen (bzw. u^3). Das explizite Auffinden der Lösungen von ⊛ erledigen wir mit der KBE von $\sqrt{m}$. Denn: ist $x^2 - my^2 = \pm 1$, d.h. $(x - y\sqrt{m})(x + y\sqrt{m}) = \pm 1$, so ist mit $x, y > 0$, $m > 4$, also $\left| \sqrt{m} - \frac{x}{y} \right| = \frac{1}{y^2 (\sqrt{m} + \frac{x}{y})} < \frac{1}{2y^2}$. Nach Satz 22.6(ii) von Lagrange ist $\frac{x}{y}$ also ein NB in der KBE von $\sqrt{m}$. Diese NBe halten somit alle Lösungen bereit. Fragt sich nur, welche NBe Lösungen von ⊛ sind.

Wir behandeln zunächst die Plus-Glg. (+):

25.9. **Satz:** Sei $\sqrt{m} \notin \mathbb{Q}$. Dann hat die Pellsche Plus-Glg. $x^2 - my^2 = 1$ unendlich viele Lösungen $(x_n, y_n) \in \mathbb{N}^2$, gg. durch $(x_n, y_n) = \begin{cases} (c_{kl-1}, d_{kl-1}), & 2 \nmid l, \\ (c_{2kl-1}, d_{2kl-1}), & 2 \mid l, \end{cases}$

dabei sind $\frac{c_n}{d_n}$ die NBe in der KBE von $\sqrt{m}$, und l die Periodenlänge darin, d.h. $\sqrt{m} = [\lfloor\sqrt{m}\rfloor; \overline{q_1, \dots, q_{l-1}, 2\lfloor\sqrt{m}\rfloor}]$ nach Satz 24.16.

Bew.: Schreibe in der KBE von $\sqrt{m}$:

$\sqrt{m} = [\lfloor\sqrt{m}\rfloor; q_1, \dots, q_{n-1}, s_n]$.

1.) **Beh.:** Für $n \geq 0$ ex. $u_n, v_n \in \mathbb{Z}$: $s_n = \frac{u_n + \sqrt{m}}{v_n}$, wo $m - u_n^2 \equiv 0 \ (v_n)$.

Bew.: • Für $n = 0$ ist $s_0 = \sqrt{m}$, also $v_0 = 1$, $u_0 = 0$.

• Für $n = 1$ ist $s_1 = \frac{1}{\sqrt{m} - \lfloor\sqrt{m}\rfloor} = \frac{\sqrt{m} + \lfloor\sqrt{m}\rfloor}{m - \lfloor\sqrt{m}\rfloor^2}$, also $v_1 = m - \lfloor\sqrt{m}\rfloor^2$ und $u_1 = \lfloor\sqrt{m}\rfloor$.

• Induktiv:

$$s_{n+1} = \frac{1}{s_n - q_n} = \frac{v_n}{u_n - q_n v_n + \sqrt{m}} = \frac{v_n(u_n - q_n v_n - \sqrt{m})}{(u_n - q_n v_n)^2 - m} =: \frac{u_{n+1} + \sqrt{m}}{v_{n+1}},$$

wo $u_{n+1} = q_n v_n - u_n$

und $v_{n+1} = \frac{m - (u_n - v_n q_n)^2}{v_n} = \underbrace{\frac{m - u_n^2}{v_n}}_{\in \mathbb{Z} \text{ nach I.V.}} + 2q_n u_n - q_n^2 v_n$,

also $u_{n+1}, v_{n+1} \in \mathbb{Z}$.

Wegen $v_n = \frac{m - (u_n - q_n v_n)^2}{v_{n+1}} = \frac{m - u_{n+1}^2}{v_{n+1}}$ folgt $v_{n+1} \mid m - u_{n+1}^2$.

Dies zeigt 1.).

2.) Aus $s_n = \frac{u_n + \sqrt{m}}{v_n}$ folgt $\sqrt{m} = \frac{s_n c_{n-1} + c_{n-2}}{s_n d_{n-1} + d_{n-2}} = \frac{(u_n + \sqrt{m})c_{n-1} + c_{n-2} v_n}{(u_n + \sqrt{m})d_{n-1} + d_{n-2} v_n}$

bzw. $\sqrt{m} \cdot \big((u_n + \sqrt{m}) d_{n-1} + d_{n-2} v_n \big) = (u_n + \sqrt{m}) c_{n-1} + c_{n-2} v_n$.

Da $\sqrt{m} \notin \mathbb{Q}$, kann dieser Ausdruck in den rationalen und irrationalen Bestandteil aufgeteilt werden, so dass $m d_{n-1} = u_n c_{n-1} + c_{n-2} v_n$

und $c_{n-1} = u_n d_{n-1} + d_{n-2} v_n$.

Multiplikation der ersten Glg. mit d_{n-1}, der zweiten mit c_{n-1} und Subtraktion zeigt, dass $c_{n-1}^2 - m d_{n-1}^2 = v_n (c_{n-1} d_{n-2} - d_{n-1} c_{n-2}) = (-1)^n v_n$ nach 20.18(iii).

Ist n nun ein Vielfaches der Periodenlänge, d.h. $n = kl$, $k \in \mathbb{N}$, so folgt

$\frac{u_{kl} + \sqrt{m}}{v_{kl}} = s_{kl} = [0; \overline{q_1, \dots, q_{l-1}}] = \sqrt{m} - \lfloor\sqrt{m}\rfloor$. Somit ist $v_{kl} = 1$.

Also ist $c_{kl-1}^2 - m d_{kl-1}^2 = (-1)^{kl}$. ☒

Dies zeigt die Beh. □

25.10. **Def.:** Die Lösung $(x,y)\in\mathbb{N}$ der Pellschen Glg. (*) mit minimalem x heißt Minimallösung. (Und entspricht nach 25.5 also u bzw. u^3.)

25.11. **Satz:** In der Notation von Satz 25.9 ist $v_n\neq -1$ für alle $n\in\mathbb{N}$ und $v_n=1$ genau wenn $\ell\mid n$. Insb. ist die Minimallösung der Pellschen Plus-Glg. (+) geg. durch $(x,y)=\begin{cases}(c_{\ell-1},d_{\ell-1}), & 2\nmid\ell,\\ (c_{2\ell-1},d_{2\ell-1}), & 2\mid\ell.\end{cases}$

Bew.: Für die s_n in Satz 25.9 gilt: $s_0,s_1,\dots,s_\ell$ sind alle verschieden, sonst wäre ℓ nicht Periodenlänge. Also ist $s_n=s_{n+1}\ (\Leftrightarrow)\ \ell\mid n$.
Die u_n,v_n im Bew. von Satz 25.9 sind $\in\mathbb{Z}$, speziell ist $v_{k\ell}=1$.
Darin entsprechen Lösungspaare (x,y) von (+) den (c_{n-1},d_{n-1}) mit $v_n=1$ oder $=-1$.
Also gen. z.Z., dass $v_n\neq\pm1$ für $1\le n<\ell$ gilt.

- Ann. $v_n=1$. Dann ist $s_n=u_n+\sqrt{m}$. Für $n\ge1$ haben die s_n eine reinperiodische KBE, nämlich $s_n=[\overline{q_{n-1},\dots,q_\ell,q_1,\dots,q_{n-1}}]$. Nach dem Satz 24.14 von Galois sind die s_n demnach reduziert, d.h. $\sqrt{m}-1<u_n<\sqrt{m}$.
Also folgt $u_n=\lfloor\sqrt{m}\rfloor$, also $s_n=\lfloor\sqrt{m}\rfloor+\sqrt{m}$ und $s_{n+1}=s_1$, d.h. $\ell\mid n$.
- Ann. $v_n=-1$. Dann ist $s_n=-u_n-\sqrt{m}$. Nach dem Satz 24.14 von Galois folgt $-1<-u_n+\sqrt{m}<0$ und $1<-u_n-\sqrt{m}$, also $\sqrt{m}<u_n<-\sqrt{m}-1$, ↯. □

Nun noch zur Behandlung der Pellschen Minus-Glg. (−):

25.12. **Satz:** Die Pellsche Minus-Glg. (−) hat genau dann unendlich viele Lösungen, falls $2\nmid\ell$, wo ℓ wie oben die Periodenlänge in der KBE von $\sqrt{m}$ bezeichnet.
In diesem Fall sind alle Lösungen $\in\mathbb{N}^2$ geg. durch $(x_k,y_k)=(c_{(2k-1)\ell-1},d_{(2k-1)\ell-1})$, $k\in\mathbb{N}$.
Die Minimallösung ergibt sich als $(c_{\ell-1},d_{\ell-1})$.

Bew.: Glg. (*) zeigt $2\nmid\ell$. Die Paare zu ungeradem k darin ergeben die Lösungen. □

25.13. **Bem.:** Die Lösungen der Minus-G/g. bilden keine Gruppe (da $(1,0) \notin \mathbb{L}_{(-)}$).
Für $m \equiv 3 (4)$ ist $x^2 - my^2 \equiv 0$ oder $\equiv 1 (4)$, da $x^2, y^2 \equiv 0, 1 (4)$,
d.h. die Minus-G/g. ist dann unlösbar. Aus Satz 25.12 folgt dann, dass $2 | \ell$ sein muss,
die Periodenlänge der KBE von $\sqrt{m}$ ist in diesem Fall also notwendig gerade.

Nicht jeder NB von $\sqrt{m}$ ist Lösung der Pellschen G/g. ⊛, aber "nicht weit weg" davon:

25.14. **Satz:** Ist $\frac{c}{d}$ ein NB der KBE von $\sqrt{m}$, so bildet $(x,y) = (c,d)$ eine Lösung
der Gleichung $x^2 - my^2 = s$ mit $s \in \mathbb{Z}$, $|s| < 1 + 2\sqrt{m}$.

Bew.: Da $\frac{c}{d}$ NB, gilt $|\sqrt{m} - \frac{c}{d}| < \frac{\hat{1}}{d^2} \Leftrightarrow |c - d\sqrt{m}| < \frac{\hat{1}}{d}$ nach Satz 21.15(iii).
Wegen $d \geq 1$ folgt $|c + d\sqrt{m}| = |(c - d\sqrt{m}) + 2d\sqrt{m}| \leq |c - d\sqrt{m}| + 2d\sqrt{m}$
$< \frac{\hat{1}}{d} + 2d\sqrt{m} \leq (1 + 2\sqrt{m})\, d$,
also ist $|c^2 - md^2| = |c - d\sqrt{m}| \cdot |c + d\sqrt{m}| < \frac{\hat{1}}{d}(1 + 2\sqrt{m})\, d = 1 + 2\sqrt{m}$. □

25.15. **Bsp.:** $\sqrt{13} = [3; \overline{1,1,1,6}]$ hat $\ell = 5$. Berechnung der NBe $\frac{c_n}{d_n}$:

n		0	1	2	3	4	5	6	7	8	9
q_n		3	1	1	1	1	6	1	1	1	1
c_n	0	1	3	4	7	11	18	119	137	256	393	649
d_n	1	0	1	1	2	3	5	33	38	71	109	180

Nach Satz 25.9 ist $(c_9, d_9) = (649, 180)$ die Minimallösung von $x^2 - 13y^2 = 1$.

Haben: $\sqrt[3]{649 + 180\sqrt{13}} = \frac{11 + 3\sqrt{13}}{2} = u^2$, wobei in A_{13} von $\mathbb{Q}(\sqrt{13})$
$u = \frac{3 + \sqrt{13}}{2}$ die GE (der Norm -1) ist.

Die Minimallösung der Pellschen Minusg/g. $x^2 - 13y^2 = -1$ ist laut Satz 25.12
gleich $(c_4, d_4) = (18, 5)$.

Ende der Vorlesung ZT I