Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Hhu
K. Halupczok

Z19: Pellsche Gleichung

Stichworte: Grundeinheiten quadratischer Zk, Pellsche Gleichung

19.1. Einleitung: Die Existenz von Grundeinheiten in $\mathbb{Q}(\sqrt{m})$ ist im reellquadratischen Fall (für $m>1$ quadratfrei) gesichert aufgrund des Dirichletschen Einheitensatzes. Die Grundeinheiten $u=a+b\sqrt{m}>1$ können dabei z.T. sehr große $a,b\in\frac{1}{2}\mathbb{Z}$ haben. Die bisher in dieser Vorlesung entwickelte algebraische Theorie liefert nur deren Existenz und gibt kaum Aufschluss für eine effiziente Konstruktion dieser Grundeinheiten: Es muss die Normgleichung $a^2-mb^2=\pm 1$ bzw. $=\pm 4$ gelöst werden, die auch Pellsche Gleichung genannt wird. Wir entwickeln in Z20–Z25 die Theorie der unendlichen Kettenbrüche, mit der die explizite und effiziente Lösung dieser Gleichung überhaupt erst möglich wird.

19.2. Bsp.: (1) Die Einheitengruppen der imaginärquadratischen Zk sind endlich.
[Imaginärquadratische Zk haben $s=0$ und $t=1$, also $s+t-1=0$, nun 18.5.]
(2) Sei $\mathbb{Q}=\sqrt{m}$ mit $m>1$ quadratfrei. Dann ist also $A^\times=\{\pm 1\}$ mal einer unendlichen zyklischen Gruppe vom Rang $2+0-1=1$, also $A^\times=\{\pm u^k;\ k\in\mathbb{Z}\}$, wo $u\in A^\times$ Grundeinheit. Nun ist jede der Zahlen $u,\frac{1}{u},-u,-\frac{1}{u}$ Grundeinheit, genau eine davon ist >1.

Bsp.:

m	$u>1$
2	$1+\sqrt{2}$
3	$2+\sqrt{3}$
94	$2\,143\,295+221\,064\sqrt{94}$
95	$39+4\sqrt{95}$

Die Grundeinheiten $u>1$ mit $u=a+b\sqrt{m}$ können gelegentlich mit sehr großen $a,b\in\frac{1}{2}\cdot\mathbb{Z}$ auftreten. Es gibt manchmal auch große Unterschiede bei aufeinanderfolgenden m.

19.3. **Bestimmung von $\nu > 1$:**

Für $\nu = a + b\sqrt{m} \in A^\times$, $\nu \neq \pm 1$, gilt:

$N(\nu) = (a+b\sqrt{m})(a-b\sqrt{m}) = \pm 1$, d.h. $\nu \cdot (\pm \nu^{-1}) = \pm 1$.

Die vier reellen Zahlen $\nu, -\nu, \nu^{-1}, -\nu^{-1}$ sind also $\pm a \pm b\sqrt{m}$.

Unter diesen vier Zahlen ist genau eine > 1, und es folgt:

$\nu > 1 \iff a, b > 0$.

- **Fall 1:** Sei $m \equiv 2, 3 \pmod 4$.

Dann ist $A = \mathbb{Z}[\sqrt{m}]$. Für $\nu = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ gilt:

$$\left\{ \begin{matrix} \nu \in A^\times \\ \nu > 1 \end{matrix} \right\} \iff \left\{ \begin{matrix} a^2 - b^2 m = \pm 1 \\ a, b > 0 \end{matrix} \right\} \quad \text{(Pellsche Gleichung)}$$

Suchen somit das kleinste $b \geq 1$ so, dass $b^2 m \pm 1$ ein Quadrat ($= a^2$) ist.

- **Fall 2:** Sei $m \equiv 1 \pmod 4$. Dann ist $A = \left\{ \frac{a + b\sqrt{m}}{2};\ a, b \in \mathbb{Z},\ a \equiv b \ (2) \right\}$ nach 4.4. Für $\nu = \frac{a+b\sqrt{m}}{2} \in A$ gilt:

$$\left\{ \begin{matrix} \nu \in A^\times \\ \nu > 1 \end{matrix} \right\} \iff \left\{ \begin{matrix} a^2 - b^2 m = \pm 4 \\ a, b > 0 \end{matrix} \right\}$$

Suchen somit das kleinste $b \geq 1$ so, dass $b^2 m \pm 4$ ein Quadrat ($= a^2$) ist.

Bem.: Die Lösungen mit $a \equiv b \equiv 0 \ (2)$ lösen die Pellsche Gl. mit: $\left(\frac{a}{2}\right)^2 - \left(\frac{b}{2}\right)^2 m = \pm 1$.

19.4. Das hier beschriebene Verfahren zur Bestimmung der Grundeinheit ist nur für recht kleine m nützlich und ist für größere m zu langsam bzw. zu aufwändig. Falls a, b sehr groß ausfällt, ist die Methode praktisch nicht brauchbar.

Die algorithmische Auffindung von Grundeinheiten behandeln wir in Z25, nachdem wir die Theorie der unendlichen Kettenbrüche ausreichend entwickelt haben.