PELL GLEICHUNG UND EINHEITEN IN QUADRATISCHEN ZAHLKÖRPERN

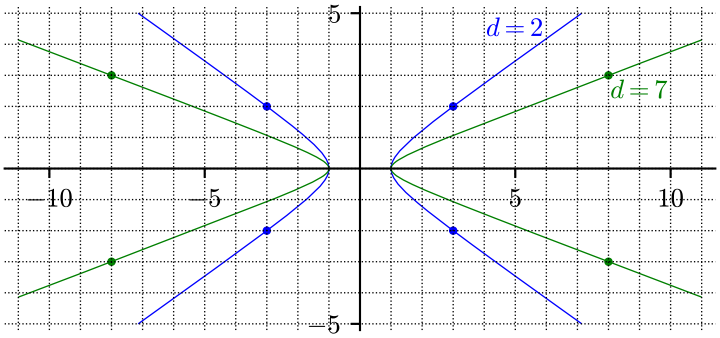
JOHANN BIRNICK

1. Die Pell Gleichung

Die Gleichung

$$x^2 - dy^2 = 1,$$

wobei $d > 0$ ganzzahlig, heißt *Pell Gleichung*. Die Lösungen $(x, y) \in \mathbb{R}^2$ bilden eine Hyperbel:



Wir suchen die ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$. Wie wir bald sehen werden, stehen diese in Zusammenhang mit der Struktur von Einheiten in bestimmten Ringen. Dem liegt die Identität $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$ zu Grunde, die uns bereits in diesem Kapitel helfen wird.

Wir haben immer die trivialen Lösungen $(x, y) = (\pm 1, 0)$. Falls $d = n^2$ eine Quadratzahl ist, so erfüllt jede Lösung $(x + ny)(x - ny) = 1$, also $x + ny = x - ny\ (= \pm 1)$, also $y = 0$, und wir haben nur die trivialen Lösungen. Für dieses Kapitel fixieren wir also ein d, dass keine Quadratzahl ist.

Es gibt verschiedenste Methoden, die Pell Gleichung zu lösen. Eine wichtige Beobachtung ist, dass große Lösungen (x, y) gute rationale Approximationen von $\sqrt{d}$ liefern, denn $x/y \approx \sqrt{d}$. Tatsächlich kann man $\sqrt{d}$ in Kettenbrüche entwickeln, und alle (positiven) Lösungen der Pellgleichung treten als solcher Kettenbruch auf. Wir verfolgen eine etwas andere Methode, die aber auch auf rationalen Approximationen beruht:

Satz 1 (Dirichlet Lemma)**.** *Sei $x \in \mathbb{R}$ und $N \in \mathbb{N}^+$. Dann gibt es $p, q \in \mathbb{Z}$ teilerfremd mit*

$$\left| x - \frac{p}{q} \right| \leqslant \frac{1}{q(N+1)} \quad \text{und} \quad 1 \leqslant q \leqslant N.$$

Beweis. Wir schreiben $[\xi]$ für $\xi - \lfloor \xi \rfloor$ und betrachten die $N+1$ Zahlen $0, [x], [2x], ..., [Nx] \in [0, 1)$. Wir teilen $[0, 1)$ in die $N + 1$ disjunkten Intervalle $[\frac{j}{N+1}, \frac{j+1}{N+1})$, $j = 0, ..., N$, auf.

Wenn im letzten Intervall eine Zahl liegt, gibt es also $1 \leqslant q \leqslant N$ ganz mit $\frac{N}{N+1} \leqslant [qx] < 1$. Mit $p \coloneqq \lfloor qx \rfloor$ folgt $|qx - p| \leqslant \frac{1}{N+1}$, also die Behauptung.

Sonst gibt es nach dem Schubfachprinzip ein Intervall, in dem zwei Zahlen liegen. Also $0 \leqslant r < s \leqslant N$ ganz mit $|[rx] - [sx]| < \frac{1}{N+1}$. Mit $q \coloneqq s - r$ und $p \coloneqq \lfloor sx \rfloor - \lfloor rx \rfloor$ folgt $|qx - p| = |sx - rx - \lfloor sx \rfloor + \lfloor rx \rfloor| = |[sx] - [rx]| < \frac{1}{N+1}$.

Für p, q teilerfremd, teile einfach durch $\mathrm{ggT}(p, q)$; unsere Abschätzung wird nur strikter. □

Korollar 2. *Sei $x \in \mathbb{R} \backslash \mathbb{Q}$. Dann gibt es unendlich viele $p, q \in \mathbb{Z}$ teilerfremd mit $|qx - p| < \frac{1}{q}$.*

Beweis. Das Dirichlet Lemma mit N beliebig liefert ein solches Paar, da $|qx - p| \leqslant \frac{1}{N+1} < \frac{1}{q}$. Wenn es nur endlich viele solcher Paare (p_i, q_i) gibt, ist $\varepsilon \coloneqq \min_i |q_i x - p_i| > 0$ da $x \notin \mathbb{Q}$. Anwendung des Lemmas mit $N \geqslant 1/\varepsilon$ liefert dann wegen $|qx - p| < 1/N \leqslant \varepsilon$ aber ein verschiedenes Paar. ↯ □

Theorem 3. *Die Pell Gleichung $x^2-dy^2=1$, $0<d\neq n^2$, hat eine nichttriviale Lösung $(x,y)\in\mathbb{Z}^2$.*

Beweis. Nach Korollar 2 gibt es unendlich viele $x,y\in\mathbb{N}$ teilerfremd mit $|x-y\sqrt{d}|\leqslant\frac{1}{y}\leqslant 1$. ($\mathbb{N}$ statt $\mathbb{Z}$ da $\sqrt{d}>1$) Insbesondere gilt für diese auch $x\leqslant 1+y\sqrt{d}$, und somit

$$|x^2-dy^2|=|x+y\sqrt{d}||x-y\sqrt{d}|\leqslant\frac{x+y\sqrt{d}}{y}\leqslant\frac{1+2y\sqrt{d}}{y}\leqslant 1+2\sqrt{d}.$$

Da $|x^2-dy^2|$ ganz ist, gibt es nach dem Schubfachprinzip ein $M\in[-1-2\sqrt{d},1+2\sqrt{d}]$ ganzzahlig, sodass die Gleichung $x^2-dy^2=M$ unendlich viele Lösungen $(x,y)\in\mathbb{N}^2$ mit x,y teilerfremd hat.

$M\neq 0$ da $\sqrt{d}\notin\mathbb{Q}$. Da $(\mathbb{Z}/M\mathbb{Z})^2$ endlich ist, gibt es nach dem Schubfachprinzip zwei verschiedene Lösungen (x_1,y_1), $(x_2,y_2)\in\mathbb{N}^2$ mit $x_1\equiv x_2 \bmod M$ und $y_1\equiv y_2 \bmod M$. Wir definieren nun

$$\begin{aligned}A&\coloneqq x_1x_2-dy_1y_2\\ B&\coloneqq x_2y_1-x_1y_2\end{aligned}\quad\text{, sodass}\quad (x_1+y_1\sqrt{d})(x_2-y_2\sqrt{d})=A+B\sqrt{d}.$$

Es folgt $A\equiv x_1^2-dy_1^2\equiv 0 \bmod M$ und $B\equiv 0 \bmod M$, also $A=M\widetilde{A}$, $B=M\widetilde{B}$. Außerdem

$$A^2-dB^2=(A+B\sqrt{d})(A-B\sqrt{d})=(x_1^2-dy_1^2)(x_2^2-dy_2^2)=M^2,$$

also $\widetilde{A}^2-d\widetilde{B}^2=1$. Die Lösung ist nicht trivial, da $\widetilde{B}=0\implies x_2y_1=x_1y_2\implies\frac{x_1}{y_1}=\frac{x_2}{y_2}$ ↯. □

Um die Einheiten in besagten Ringen zu klassifizieren, genügt uns dieses Resultat bereits. Nichtsdestoweniger möchten wir noch zeigen, dass es sogar unendlich viele Lösungen der Pell Gleichung gibt! Wir rechnen hier explizit aus, was wir gleich implizit machen werden, indem wir Elemente in Ringen potenzieren.

Korollar 4. *Die Pell Gleichung $x^2-dy^2=1$, $0<d\neq n^2$, hat unendlich viele Lösungen $(x,y)\in\mathbb{Z}^2$.*

Beweis. Sei (x,y) eine nichttriviale Lösung. Für $n\in\mathbb{N}^+$ definiere:

$$x_n\coloneqq\frac{(x+y\sqrt{d})^n+(x-y\sqrt{d})^n}{2}\qquad y_n\coloneqq\frac{(x+y\sqrt{d})^n-(x-y\sqrt{d})^n}{2\sqrt{d}}$$

Anhand der Binomialentwicklung sieht man, dass $x_n,y_n\in\mathbb{Z}$ ganzzahlig sind. Es gilt

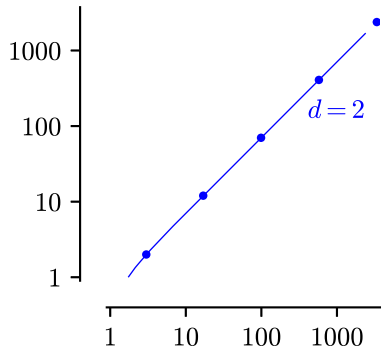
$$x_n+y_n\sqrt{d}=(x+y\sqrt{d})^n\quad\text{und}\quad x_n-y_n\sqrt{d}=(x-y\sqrt{d})^n,$$

also folgt $x_n^2-dy_n^2=(x_n+y_n\sqrt{d})(x_n-y_n\sqrt{d})=(x^2-dy^2)^n=1$.

Die Lösungen sind alle verschieden, da $|x_n+y_n\sqrt{d}|=|x+y\sqrt{d}|^n$ und $|x+y\sqrt{d}|\neq 1$ da sonst wegen $1=(x+y\sqrt{d})(x-y\sqrt{d})$ folgt $x+y\sqrt{d}=x-y\sqrt{d}$ $(=\pm 1)$, also $y=0$ ↯. □

Tatsächlich sind sogar alle Lösungen von solcher Form, in dem Sinne, dass es eine *Fundamentallösung* $(x,y)\in\mathbb{Z}^2$ gibt, und jede andere Lösung ist von der Form $(\pm x_n,\pm y_n)$ mit x_n,y_n wie im letzten Beweis. Wir werden das im nächsten Kapitel sehen. (Streng genommen nur für spezielle d, aber der Beweis funktioniert genauso für alle d, die wir hier betrachten.)

Die Lösungen von $x^2-2y^2=1$ sind generiert von $(\pm 3,\pm 2)$, und lauten weiter $(\pm 17,\pm 12)$, $(\pm 99,\pm 70)$, $(\pm 577,\pm 408)$, $(\pm 3363,\pm 2378)$, ... Nachfolgend sind sie auf einem log-log Plot dargestellt. Warum sind die Abstände (nahezu) linear?



2. Quadratische Zahlkörper und Zahlringe

Als *Zahlkörper* bezeichnen wir alle endlichen Körpererweiterungen von $\mathbb{Q}$. Für $\xi \in \mathbb{C}$ bezeichnet $\mathbb{Q}(\xi)$ den kleinsten Unterkörper von $\mathbb{C}$, der sowohl $\mathbb{Q}$ als auch ξ enthält. Im Folgenden möchten wir die *quadratischen Zahlkörper* $\mathbb{Q}(\sqrt{d})$ betrachten, wobei $d \in \mathbb{Z}$ eine ganze Zahl ist.

Die Fälle $d \in \{0, 1\}$ sind schnell abgehandelt. Und wenn $n^2|d$ für ein $n \in \mathbb{N}$, so ist $\sqrt{d} = n\sqrt{d/n^2}$, also $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d/n^2})$. Deshalb können wir voraussetzen, dass $d \notin \{0, 1\}$ und d *quadratfrei*, das heißt d besitzt nur einfache Primfaktoren. Wir fixieren ab nun ein solches $d \in \mathbb{Z}$.

$\sqrt{d}$ ist (per Definition) Nullstelle des Polynoms $X^2 - d \in \mathbb{Q}[X]$, also algebraisch über $\mathbb{Q}$. Da d quadratfrei ist, ist auch $\sqrt{d} \notin \mathbb{Q}$, also ist dies das Minimalpolynom und es folgt:

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

Dem Leser ist sicher bereits aufgefallen, dass in unserer bisher einheitlichen Betrachtung sich doch zwei durchaus verschiedene Fälle ergeben. Ist nämlich $d < 0$, so ist $\sqrt{d}$ rein imaginär und wir erhalten bildlich gesehen ein gleichmäßiges Gitter in $\mathbb{C}$. In diesem Fall heißt der Körper *imaginär-quadratisch*. Wenn hingegen $d > 0$, so ist $\mathbb{Q}(d)$ ein Unterkörper von $\mathbb{R}$, und er heißt *reell-quadratisch*. Trotzdem möchten wir eine – zu der im komplexen Fall bereits bekannten analoge – allgemeine Konjugation definieren:

$$\begin{aligned} \overline{\square}: \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \\ & z = a + b\sqrt{d} \mapsto \overline{z} \coloneqq a - b\sqrt{d} \end{aligned}$$

Dies ist ein Körperautomorphismus. So sieht man auch, dass die Konjugation gleichermaßen für den Fall $d > 0$ Sinn ergibt und wichtig ist, denn $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \overline{\square}\}$.

Dass $\mathbb{Q}(\sqrt{d})$ ein endlichdimensionaler $\mathbb{Q}$-Vektorraum ist, kann man noch anderweitig nutzen. Die Multiplikation $L_{a+b\sqrt{d}}$ mit $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ ist wegen dem Distributiv- und Assoziativgesetz nämlich eine lineare Abbildung auf $\mathbb{Q}(\sqrt{d})$. Wählen wir zum Beispiel die Basis $(1, \sqrt{d})$, besitzt sie die Matrixdarstellung

$$L_{a+b\sqrt{d}} \simeq \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Über Determinante und Spur – beides unabhängig von der Wahl der Basis – können wir also $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ weitere Eigenschaften zuordnen, die *Norm* und die *Spur*:

$$\begin{aligned} N: \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q} & \qquad \mathrm{tr}: \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q} \\ & z = a + b\sqrt{d} \mapsto a^2 - db^2 = z \cdot \overline{z} & & z = a + b\sqrt{d} \mapsto 2a = z + \overline{z} \end{aligned}$$

Man verifiziert, unter Verwendung der Multiplikativität der Determinante, dass:

$$N(z \cdot w) = N(z) \cdot N(w) \qquad \mathrm{tr}(z + w) = \mathrm{tr}(z) + \mathrm{tr}(w)$$

Analog zu den ganzen Zahlen $\mathbb{Z}$ in den rationalen, möchten wir nun einen Unterring $\mathcal{O}_d \subseteq \mathbb{Q}(\sqrt{d})$ von $\mathbb{Q}(\sqrt{d})$ als die "ganzen" Zahlen identifizieren. Eine sinnvolle Forderung scheint $\mathcal{O}_d \cap \mathbb{Q} = \mathbb{Z}$. Die erste Idee ist $\mathbb{Z} + \mathbb{Z}\sqrt{d}$. Doch wir wollen stattdessden das normierte Minimalpolynom von $z \in \mathbb{Q}(\sqrt{d})$ betrachten, $(X - z)(X - \overline{z}) = X^2 - \mathrm{tr}(z)X + N(z) \in \mathbb{Q}[X]$ bzw. $X - z$, und fordern, dass es ganzzahlige Koeffizienten hat.

Definition 5. $\mathcal{O}_d \coloneqq \{z \in \mathbb{Q}(\sqrt{d}) \mid \mathrm{tr}(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{d})$ *heißt* quadratischer Zahlring.

Bemerkung 6. Auch für einen beliebigen Zahlkörper K betrachtet man die ganzen Zahlen $\mathcal{O}_K \subseteq K$ als die Elemente in K, deren normiertes Minimalpolynom in $\mathbb{Z}[X]$ liegt. Man nennt sie auch *ganz-algebraische* Zahlen. Eine Zahl ist im Übrigen ganz-algebraisch genau dann, wenn sie Nullstelle *irgendeines* normierten Polynoms in $\mathbb{Z}[X]$ ist. Das beweist man mit Hilfe des Gauss-Lemmas.

Lemma 7. *$\mathcal{O}_d$ ist tatsächlich ein Unterring, und es gilt:*

- $\mathcal{O}_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ *falls* $d \equiv 2, 3 \bmod 4$
- $\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}$ *und* $a \equiv b \bmod 2\} = \mathbb{Z} + \mathbb{Z}\omega$ *mit* $\omega = \frac{1+\sqrt{d}}{2}$ *falls* $d \equiv 1 \bmod 4$

Bemerkung 8. $(1, \sqrt{d})$ beziehungsweise $(1, \frac{1+\sqrt{d}}{2})$ nennt man auch *Ganzheitsbasis* von $\mathcal{O}_d$.

Beweis. Durch Berechnen von Norm und Spur prüft man nach, dass die beschriebenen Mengen tatsächlich in $\mathcal{O}_d$ liegen. Sei nun $\frac{A+B\sqrt{d}}{2} \in \mathcal{O}_d$ mit $A, B \in \mathbb{Q}$. Also $A \in \mathbb{Z}$ und $\frac{A^2-dB^2}{4} \in \mathbb{Z}$. Insbesondere $A^2 - dB^2 \in \mathbb{Z}$, also wegen $A^2 \in \mathbb{Z}$ auch $dB^2 \in \mathbb{Z}$. Da d quadratfrei, folgt somit $B \in \mathbb{Z}$.

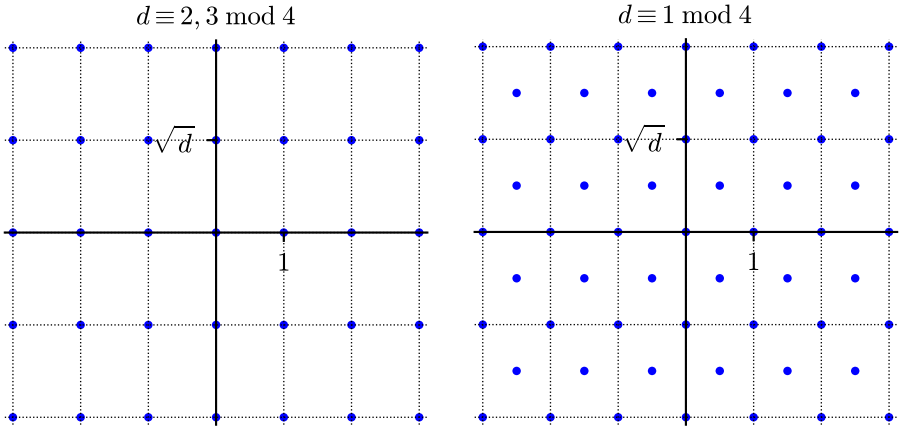
Wir haben also $A, B \in \mathbb{Z}$ und $A^2 \equiv dB^2 \bmod 4$. Die einzigen Quadrate in $\mathbb{Z}/4\mathbb{Z}$ sind 0 und 1.

$\rightsquigarrow$ $d \equiv 2, 3 \bmod 4 \implies A^2 \equiv B^2 \equiv 0 \bmod 4 \implies A \equiv B \equiv 0 \bmod 2$.

$\rightsquigarrow$ $d \equiv 1 \bmod 4 \implies A^2 \equiv B^2 \bmod 2 \implies A \equiv B \bmod 2$.

Also folgen die behaupteten Gleichungen. Dass diese Mengen tatsächlich einen Unterring bilden, prüft man durch eine kurze Rechnung nach. □

Nachfolgend sind die Elemente von $\mathcal{O}_d$ als Vektoren bezüglich der Basis $(1, \sqrt{d})$ dargestellt. Man beachte, dass das nur im Fall $d < 0$ auch der komplexen Zahlenebene entspricht!



3. Einheiten in quadratischen Zahlringen

Welche Elemente in $\mathcal{O}_d$ sind invertierbar? Über die Norm finden wir dafür ein klares Kriterium. Und durch die Darstellung in Lemma 7 können wir dieses in diophantische Gleichungen umwandeln.

Lemma 9. *Für $z \in \mathcal{O}_d$ ist* $z \in \mathcal{O}_d^\times \iff N(z) = \pm 1$.

Beweis. $\boxed{\Rightarrow}$ $zw = 1 \implies 1 = N(1) = N(z)N(w) \implies N(z) = \pm 1$

$\boxed{\Leftarrow}$ $\pm 1 = N(z) = z\overline{z} \implies z$ hat Inverses $\pm\overline{z}$ □

Korollar 10. *Für $a, b \in \mathbb{Z}$ gilt:*

- $a + b\sqrt{d} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 1$ *falls* $d \equiv 2, 3 \bmod 4$
- $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 4$ *falls* $d \equiv 1 \bmod 4$

Beweis. Im Fall $d \equiv 2, 3 \bmod 4$ ist das genau Lemma 9. Für $d \equiv 1 \bmod 4$ haben wir auch $\pm 1 = N(\frac{a+b\sqrt{d}}{2}) = \left(\frac{a}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 \iff \pm 4 = a^2 - db^2$, aber wir müssen zeigen, dass für jede Lösung der rechten Gleichung auch $a \equiv b \bmod 2$ gilt. Wir haben aber $d \equiv 1 \bmod 2$, also folgt wegen $a^2 - db^2 \equiv 0 \bmod 2$, dass $a^2 \equiv b^2 \bmod 2$, also $a \equiv b \bmod 2$. □

Im Fall $d > 0$ entspricht die Norm dem Absolutbetrag. Dann sieht man schnell an obigem Bildchen, dass wir nur endlich viele Einheiten haben können.

Satz 11. *Im imaginär-quadratischen Fall $d < 0$ sind alle Einheiten Einheitswurzeln. Konkret:*

$$\mathcal{O}_{-1}^\times = \langle \xi_4 \rangle \qquad \mathcal{O}_{-3}^\times = \langle \xi_6 \rangle \qquad \mathcal{O}_d^\times = \langle \xi_2 \rangle = \pm 1 \quad \textit{für } d \leqslant -5 \textit{ oder } d = -2$$

Beweis. Sei $e \in \mathcal{O}_d$. Da $d < 0$ entspricht die Norm dem komplexen Absolutbetrag. Insbesondere ist $N(e) > 0$, also mit Lemma 9 $N(e) = 1$. $\mathcal{O}_d^\times$ kann aber nur endlich viele Elemente auf dem Einheitskreis haben. Für $e \in \mathcal{O}_d^\times$ folgt also $e^k = e^l$ mit $k > l \in \mathbb{N}$, also $e^{k-l} = 1$.

Die behaupteten Gleichungen scheinen grafisch plausibel. Man kann sie mit Hilfe konkreter Rechnungen und einer Abschätzung für $d \leqslant -5$ nachprüfen. (Es gibt nur endlich viele Elemente mit Norm $\leqslant 1$, z.B. da die quadratische Form $a^2 - db^2$ ist positiv definit ist. Für $d \leqslant -5$ gibt es eben gar keine.) □

Der Fall $d > 0$ ist nicht ganz so einfach. Wichtig zu beobachten ist, dass wir wieder im ersten Kapitel angekommen sind: Wir müssen die Gleichungen $x^2 - dy^2 = \pm 1, \pm 4$ mit $d \in \mathbb{N}^+$ lösen! Wir haben zwar nur die Gleichung ... = 1 gelöst, aber damit erhalten wir auch eine Lösung für ... = 4, also in jedem Fall eine nichttriviale Einheit. Aus dieser konstruieren wir dann alle:

Lemma 12. *Im reellquadratischen Fall $d > 0$ ist $\mathcal{O}_d^\times \cap (1, M)$ endlich für alle $M > 1$.*

Beweis. Für $e \in \mathcal{O}_d^\times \cap (1, M)$ folgt wegen $e\overline{e} = N(e) = \pm 1$, dass $\overline{e} \in (-1, 1)$. Also $\mathrm{tr}(e) = e + \overline{e} \in (0, M + 1)$. Es gibt also nur endlich viele Möglichkeiten für $N(e)$ und $\mathrm{tr}(e)$.

Da e Nullstelle von $(X - e)(X - \overline{e}) = X^2 - \mathrm{tr}(e)X + N(e)$ ist, ist e also eine der $4M$ Nullstellen von $\{X^2 - aX + b\}_{a \in \{1,\dots,M\}, b = \pm 1}$. □

Satz 13. *Im reellquadratischen Fall $d > 0$ gibt es $\varepsilon \in \mathcal{O}_d^\times, \varepsilon \neq \pm 1$, sodass $\mathcal{O}_d^\times = \{\pm \varepsilon^k \mid k \in \mathbb{Z}\}$.*

Beweis. Wir zeigen zunächst, dass es eine nichttriviale Einheit gibt. Wegen Korollar 10 genügt es, eine nichttriviale Lösung der entsprechenden Gleichung zu finden. Diese existiert nach Theorem 3 aus dem ersten Kapitel, wobei wir im Fall $d \equiv 1 \bmod 4$ die Lösung der einfachen Pell Gleichung mit 2 multiplizieren.

Da mit $e \in \mathcal{O}_d^\times$ auch $-e, e^{-1}, -e^{-1} \in \mathcal{O}_d^\times$, gibt es also $e \in \mathcal{O}_d^\times$ mit $e > 1$. Nach Lemma 12 gibt es dann eine kleinste Einheit $\varepsilon > 1$. $\{\pm \varepsilon^k\}_{k \in \mathbb{Z}} \subseteq \mathcal{O}_d^\times$ ist klar. Angenommen es gibt $e \in \mathcal{O}_d^\times, e \neq \varepsilon^k$. O.b.d.A. $e > 0$. Also $\varepsilon^k < e < \varepsilon^{k+1}$ mit $k \in \mathbb{Z}$. Dann ist aber $1 < e\varepsilon^{-k} < \varepsilon$ und $e\varepsilon^{-k} \in \mathcal{O}_d^\times$ ↯. □

Die Einheit ε in Satz 13 und ihre nahen Verwandten $-\varepsilon, \pm\varepsilon^{-1}$ heißen *Fundamentaleinheit*.

Insgesamt haben wir also folgendes Endresultat bewiesen:

Theorem 14. *Sei $d \in \mathbb{Z} \backslash \{0, 1\}$ quadratfrei und $U \subseteq \mathcal{O}_d$ die multiplikative Gruppe der Einheitswurzeln im Ganzzahlring $\mathcal{O}_d$ des Körpers $\mathbb{Q}(\sqrt{d})$. Dann gilt:*

$$\mathcal{O}_d^\times \cong \begin{cases} U & d < 0 \\ U \times \mathbb{Z} & d > 0 \end{cases}$$

References

[1] A. Schmidt, *Einführung in die algebraische Zahlentheorie*. Springer, Berlin, 2007

[2] U. Zannier, *Lecture notes on Diophantine analysis*. Edizioni della Normale, Pisa, 2009

Email address: jbirnick@student.ethz.ch