Elementare Zahlentheorie
Sommersemester 2006

Prof. Dr. Annette Huber-Klawitter

Fassung vom 7. Juli 2006

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Augustusplatz 10/11
04109 Leipzig

0341-97 32 185
huber@mathematik.uni-leipzig.de

Kapitel 1

Einleitung

Gegenstand der Zahlentheorie sind die ganzen Zahlen und ihre Eigenschaften:

- Primzahlen und ihre Verteilung
- Lösbarkeit von Gleichungen in $\mathbb{Z}$
- ...

Damit ist sie eines der ältesten wissenschaftlichen Gebiete überhaupt. *Elementare Zahlentheorie* verwendet keine höheren Methoden, d.h. keine Analysis oder nichtlineare Algebra. Andersherum: nur die Methoden der Mittelstufe. Historisch reicht der Stoff bis ca. 1800. Übrigens: Elementar bedeutet nicht einfach! Wir beginnen mit einem Beispiel:

Definition 1.1. *Die ganzzahligen Lösungen der Gleichung*

$$x^2 + y^2 = z^2$$

heißen phythagoreische Tripel.

Beispiel.

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$
$$5^2 + 12^2 = 25 + 144 = 169 = 13^2$$

Dies wird z.B. zur Konstruktion von rechten Winkeln benutzt: Man teilt auf einer Schnur 12 Abschnitte ab und formt diese zum Dreieck.
Gibt es weitere Lösungen? Gibt es eine Formel? Hat die Menge der Lösungen eine Struktur? Die Lösungsformel war schon vor 3500 Jahren in Babylon bekannt.
1. Beobachtung: Gleichung $x^2 + y^2 = z^2$ ist homogen vom Grad 2. Ist (x, y, z) eine Lösung, dann auch $(\lambda x, \lambda y, \lambda z)$ für alle $\lambda \in \mathbb{Z}$:

$$(\lambda x)^2 + (\lambda y)^2 = \lambda^2(x^2 + y^2) = (\lambda z)^2$$

Es gibt also unendlich viele Lösungen. Wir studieren ab jetzt nur noch primitive Lösungen, d.h. $\mathrm{ggT}(x, y, z) = 1$.
2. Beobachtung: Teilt $\lambda | x, y$, so folgt $\lambda^2 | x^2 + y^2 = z^2$, also $\lambda | z$. Allgemeiner: teilt λ zwei der Zahlen x, y, z eines phytagoreischen Tripels, so auch die dritte. Also: bei primitiven Tripeln sind je zwei Zahlen teilerfremd:

$$\mathrm{ggT}(x, y) = \mathrm{ggT}(y, z) = \mathrm{ggT}(x, z) = 1$$

3. Beobachtung: Kann man etwas über Teilbarkeit der Lösungen durch ganze Zahlen sagen? Zunächst $p = 2$, also gerade/ungerade. Höchstens eine der Zahlen x, y, z ist gerade. Können alle drei ungerade sein?

$$x, y \text{ ungerade} \Rightarrow x^2, y^2 \text{ ungerade} \Rightarrow x^2 + y^2 = z^2 \text{ gerade} \Rightarrow z \text{ gerade}$$
$$x, z \text{ ungerade} \Rightarrow x^2, z^2 \text{ ungerade} \Rightarrow y^2 = z^2 - x^2 \text{ gerade} \Rightarrow y \text{ gerade}$$

Also ist mindestens eine der drei Zahlen gerade. Genaueres hinsehen: Angenommen, x, y sind ungerade. Dann gilt $x = 2x_0 + 1$, $y = 2y_0 + 1$, also

$$x^2 + y^2 = 4x_0^2 + 4x_0 + 1 + 4y_0^2 + 4y_0 + 1 = 4m + 2 = z^2$$

Dies ist unmöglich, den Quadratzahlen sind entweder 0 oder 1 modulo 4. Also: entweder x oder y ist gerade. Ab jetzt: x, z ungerade, $y = 2y_0$.

$$x^2 + 4y_0^2 = z^2 \Leftrightarrow 4y_0^2 = z^2 - x^2 = (z - x)(z + x)$$

Da x, z ungerade, sind $z \pm x$ gerade. Also

$$z - x = 2w, z + x = 2v$$
$$4y_0^2 = 4vw \Leftrightarrow y_0^2 = vy$$

Behauptung. *w, v sind teilerfremd.*

Angenommen, $\lambda | v, w$. Dann $\lambda | w + v = x$ und $\lambda | w - v = -x$, Widerspruch zu $\mathrm{ggT}(x, z) = 1$.
Primfaktorzerlegung von y_0^2 impliziert: w, v sind beides Quadratzahlen:

$$w = q^2, v = p^2 \Rightarrow y_0^2 = p^2 q^2 \Leftrightarrow y_0 = pq$$

Wir fassen zusammen, was wir wissen:

$$y = 2y_0 = 2pq$$
$$x = w + v = p^2 + q^2$$
$$z = v - x = p^2 - q^2$$

Gibt es weitere Bedingungen? Nein!

$$(p^2 - q^2)^2 + (2pq)^2 = p^4 - 2p^2q^2 + q^4 + 2p^2q^2 = p^4 + 2p^2q^2 + q^4 = (p^2 + q^2)^2$$

Satz 1.2. *Seien $p, q \in \mathbb{Z}$. Dann sind $x = p^2 - q^2$, $y = 2pq$ und $z = p^2 + q^2$ ein pythagoreisches Tripel. Jedes primitive Tripel ist von dieser Form.*

Aufgabe 1.1. Erstellen Sie eine Tabelle mit ca. 10 pythagoreischen Tripeln. Zu welchen p, q gehören die Tripel $(3, 4, 5), (5, 12, 13)$?

Aufgabe 1.2. Haben alle pythagoreischen Tripel die Form aus Satz 1.2?

Aufgabe 1.3. Bestimmen Sie alle Lösungen von $x^4 + y^4 = z^4$.

Oft betrachet man statt der phythagoreischen Gleichung

$$a^2 + b^2 = 1$$

und sucht Lösungen in $\mathbb{Q}$. Mit $a = x/z$, $b = y/z$ haben wir dies bereits gelöst:

Korollar 1.3. *Jede Lösung von $a^2 + b^2 = 1$ in $\mathbb{Q}$ hat die Form*

$$a = \frac{p^2 - q^2}{p^2 + q^2} \qquad b = \frac{2pq}{p^2 + q^2}$$

(oder umgekehrt) mit $p, q \in \mathbb{Z}$ (nicht beide gleichzeitig 0).

Aufgabe 1.4. Schreiben Sie einen sauberen Beweis aus Satz 1.2 auf.

Theorem 1.4 (Faltings 1983). *Sei $P \in \mathbb{Q}[X, Y]$ ein allgemeines Polynom vom Grad größer 3. Dann hat $P(X, Y) = 0$ nur endlich viele rationale Lösungen.*

Bereits vorher schon bekannt:

- $\deg P = 2$: entweder keine oder unendliche viele Lösungen.
- $\deg P = 3$: elliptische Kurven. keine, endlich oder unendlich viele Lösungen.

Weiterer Spezialfall:

Satz 1.5 (Fermat, vermutlich 1638). *Die Gleichung $x^4 + y^4 = z^2$ hat keine nicht-triviale ganzzahlige Lösung, d.h. keine mit $x, y, z > 0$.*

Was haben wir bisher benutzt?

- Teilbarkeitseigenschaften/Eindeutigkeit der Primfaktorzerlegung
- Rechnen mit Restklassen.

Dies soll systematisiert werden. Weitere Ziele der Vorlesung:

- Kettenbrüche und Pellsche Gleichung
- quadratisches Reziprozitätsgesetz
- Zwei-, Drei- und Vierquadratesatz
- $x^3 + y^3 = z^3$

Literatur:
Scharlau, Opolka: Von Fermat bis Minkowski
Serre: A course in arithmetic
Frey: Elementare Zahlentheorie

Kapitel 2

Primfaktorzerlegung

Sei R ein kommutativer Ring mit 1, ohne Nullteiler (d.h. $ab = 0$ nur wenn $a = 0$ oder $b = 0$). Unsere Beispiele: $\mathbb{Z}$, $\mathbb{Z}[i]$ Gaußsche ganze Zahlen, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\varrho]$ mit $\varrho = \mathrm{e}^{2\pi i/3}$.
Beachte: $(\varrho^3 - 1)/(\varrho - 1) = \varrho^2 + \varrho + 1 = 0$.

Aufgabe 2.1. Bestimmen Sie das von $1, \varrho$ in der Ebene aufgepannte Gitter.

Wesentliches Hilfsmittel ist die *Norm* $N : R \to \mathbb{N}_0$.

Definition 2.1. *Wir setzen* $N : \mathbb{Z} \to \mathbb{N}_0, x \mapsto |x|$. *Für* $R = \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\varrho]$ *setzen wir* $N(x) = |x|^2$

Konkret:

$$N(a + bi) = a^2 + b^2, N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

$$N(a + b\varrho) = (a + b\varrho)(a + b\overline{rho}) = (a + b\varrho)(a + b\varrho^2) = a^2 + ab(\varrho + \varrho^2) + b^2\varrho^3 = a^2 - ab + b^2$$

Die Norm ist in jedem dieser Fälle *multiplikativ*: $N(\alpha)N(\beta) = N(\alpha\beta)$.

Definition 2.2. $\alpha \in R$ *heißt* Einheit, *falls es* α^{-1} *in* R *gibt. Sei* R^* *die Gruppe der Einheiten.*
Ein Element $\alpha \in R$ *heißt* irreduzibel, *falls* $\alpha \neq 0$, $\alpha \notin R^*$ *und es gilt: falls* $\alpha = \beta\gamma$, *so ist* β *eine Einheit oder* γ *eine Einheit.*

Beispiel. $\mathbb{Z}^* = \{\pm 1\}$

Aufgabe 2.2. Überprüfen Sie die Gruppenaxiome für R^*.

Aufgabe 2.3. Bestimmen Sie die Einheiten des Polynomrings $k[T]$ und des Potenzreihenrings $k[[T]]$ für einen Körper k. Was passiert, wenn man k durch einen Ring ersetzt?

Lemma 2.3. *Sei* $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\varrho]$. *Ein Element* $\alpha \in R$ *ist eine Einheit genau dann, wenn* $N(\alpha) = 1$. *Ist* β *ein echter Teiler von* α, *dann folgt* $N(\alpha)$ *ein echter Teiler von* β.

Beweis: Sei α Einheit. Dann gilt $N(\alpha)N(\alpha^{-1} = N(1) = 1$. Umgekehrt $1 = N(\alpha) = \alpha\overline{\alpha}$, d.h. $\alpha^{-1} = \overline{\alpha}$ zunächst in $\mathbb{C}$. Aber offensichtlich gilt $\overline{\alpha} \in R$. Die Aussage für Teiler folgt hieraus direkt. □

Aufgabe 2.4. Gilt auch die Implikation $N(\beta)|N(\alpha) \Rightarrow \beta|\alpha$?

Beispiel. Sei $\alpha \in \mathbb{Z}[i]^*$, also $N(\alpha) = 1$.

$$\alpha = a + bi \Rightarrow a^2 + b^2 = 1 \Rightarrow (a, b) = (\pm 1, 0), (0, \pm 1)$$

Also $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Aufgabe 2.5. Zeigen Sie: $\mathbb{Z}[\varrho]^* = \{\pm 1, \varrho, \varrho^2, \varrho + 1, \varrho^2 + 1\}$

Beispiel. Die irreduziblen Zahlen in $\mathbb{Z}$ sind $\pm$ die Primzahlen.

Beispiel. $2 = (1 + i)(1 - i)$ ist nicht irreduzibel in $\mathbb{Z}[i]$, wohl aber in $\mathbb{Z}[\sqrt{-5}]$: $N(2) = 4$ hat als echte Teiler nur 2. Gesucht ist also $\beta = a + b\sqrt{-5}$ mit $N(\beta) = a^2 + 5b^2 = 2$. Dies ist unlösbar.

Aufgabe 2.6. Ist 2 irreduzibel in $\mathbb{Z}[\varrho]$? Wie steht es mit 3, 5, 7, 11, ...? Erkennen Sie ein Muster?

Definition 2.4. *R heißt* faktoriell, *wenn jedes $\alpha \in R \setminus \{0\}$ in der Form*

$$\alpha = up_1^{n_1} \dots p_k^{n_k}$$

geschrieben werden kann mit $u \in R^*$, p_i irreduzibel und verschieden, $n_i > 0$ und dabei die p_i eindeutig sind bis auf Einheit und die n_i eindeutig.

Wir wollen natürlich zeigen, dass $\mathbb{Z}$ faktoriell ist.

Beispiel. In $\mathbb{Z}[\sqrt{-5}]$ gilt

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Wir haben bereits gesehen, dass 2 irreduzibel ist. Aber 2 ist kein Teiler von $1 \pm \sqrt{-5}$, denn beide Elemente haben Norm 6.

Satz 2.5. *$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\varrho]$ sind faktorielle Ringe.*

Existenz: Induktion nach $N(\alpha)$: Induktionsanfang: $N(\alpha) = 0 \Rightarrow \alpha = 0$, $N(\alpha) = 1 \Rightarrow \alpha = u \in R^*$. Sein nun $N(\alpha) > 1$. Entweder α ist irreduzibel, dann sind wir fertig. Oder es gibt eine echte Zerlegung $\alpha = \beta\gamma$. Dann gilt $N(\beta), N(\gamma) < N(\alpha)$. Nach Induktionsannahme haben wir Zerlegungen für $\beta, gamma$. Durch Zusammenfassen erhalten wir eine Produktdarstellung für α. **Eindeutigkeit:** z.z. ist: Sei $\pi \in R$ irreduzibel, dann ist π *prim*, d.h. $\pi|\alpha\beta$ impliziert $\pi|\alpha$ oder $\pi|\beta$.

Satz 2.6 (Euklidischer Algorithmus). *Sei $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\varrho]$. Seien $\alpha, \beta \in R$, $\beta \neq 0$. Dann gibt es $\gamma, \delta \in R$ mit*

$$\alpha = \beta\gamma + \delta$$

mit $N(\delta) < N(\beta)$.

Beweis: Die Aussage ist klar in $\mathbb{Z}$ (Sauberer Beweis in $\mathbb{N}$ mit vollständiger Induktion).
In den beiden anderen Fällen: Wir betrachten $\alpha\beta^{-1} \in \mathbb{C}$ und wählen das nächstgelegene γ, das im jeweiligen Gitter liegt. Man überlegt sich leicht, dass

$$|\alpha\beta^{-1} - \gamma| < 1$$

Setze $\delta = \alpha - \gamma\beta = (\alpha\beta^{-1} - \gamma)\beta \in R$. Es folgt $N(\delta) = |\delta|^2 < |\beta|^2 = N(\beta)$. □

Aufgabe 2.7. Zeigen Sie den euklidischen Algorithmus für $k[T]$ (k Körper), wobei N die Gradabbildung ist.

Korollar 2.7. *Sei $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\varrho]$. Seien $\alpha, \beta \in R \setminus \{0\}$. Dann gibt es einen größten gemeinsamen Teiler $\tau = \mathrm{ggT}(\alpha, \beta)$ bezüglich der Teilbarkeitsrelation, d.h. jeder andere gemeinsame Teiler teilt diesen. τ ist eindeutig bis auf Einheit und von der Form $n\alpha + m\beta$ für $n, m \in R$.*

Beweis: Sei τ ein minimales Element (bezüglich N) ungleich 0 in $\{n\alpha+m\beta|n, m \in R\}$.

Behauptung. $\tau|\alpha$.

Nach dem Euklidischen Algorithmus gilt

$$\alpha = \chi\tau + \delta$$

mit $N(\delta) < N(tau)$. Das Element δ liegt ebenfalls in unserer Menge. Nach Wahl von τ muss dann $\delta = 0$ sein.
Ebenso folgt $\tau|\beta$, dies ist also ein gemeinsamer Teiler. Aus der Darstellung von τ als Linearkombination folgt, dass jeder gemeinsame Teiler α und β auch τ teilt. Damit ist τ ein ggT. Seien τ, τ' beide ggTs. Dann folgt $\tau = u\tau'$ und $\tau' = u'\tau$. Also ist $\tau = u\tau' = uu'\tau$. Es folgt $N(uu') = 1$, also sind u und u' Einheiten. □

Satz 2.8. *Sei π irreduzibel in $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\varrho]$. Dann ist π prim, d.h. $\pi|\alpha\beta$ impliziert $\pi|\alpha$ oder $\pi|\beta$.*

Beweis: Sei $\pi|\alpha\beta$, aber $\pi \nmid \alpha, \pi \nmid \beta$. Das ggT von π und α ist ein Teiler von π. Es kann nicht gleich π sein, also ist es eine Einheit, ohne Einschränkung gleich 1. Nach Korollar 2.7 gilt

$$1 = \mathrm{ggT}(\pi, \alpha) = n_1\pi + m_1\alpha$$

Ebenso

$$1 = \mathrm{ggT}(\pi, \beta) = n_2\pi + m_2\beta$$

Produkt der Gleichungen ergibt

$$1 = (n_1\pi + m_1\alpha)(n_2\pi + m_2\beta) = x\pi + m_1n_2\alpha\beta$$

Da $\pi|\alpha\beta$ haben wir $\pi|1$. Dies ist ein Widerspruch. □

Eindeutigkeit: Seien

$$\alpha = up_1^{n_1} \dots p_k^{n_k} = u' q_1^{n_1'} \dots q_{k'}^{n_{k'}'}$$

zwei Primfaktorzerlegungen. Wir argumentieren mit vollständiger Induktion über $\sum n_i$.
Sei $\sum n_i = 0$, also $\alpha = u$ eine Einheit. Die p_i' sind dann invertierbar, bzw. sie tauchen gar nicht erst auf.
Allgemein teilt das Primelement p_1 die rechte Seite, also einen der Faktoren. $p_1 | u'$ ist nicht möglich, also folgt $p_1 | q_j$ für ein j. Da q_j irreduzibel ist und p_1 keine Einheit, folgt $p_1 = u_1 q_j$ für eine Einheit u_1. Ohne Einschränkung ist $j = 1$. Wir teilen beide Seiten der Gleichung durch p_1 und erhalten

$$up_1^{n_1 - 1} \dots p_k^{n_k} = vq_1^{n_1' - 1} \dots q_2^{n_2'} \dots q_{k'}^{n_{k'}'}$$

mit einer neuen Einheit v. Nach Induktionsvoraussetzung gilt $k = k'$, $p_i = u_i p_{\sigma(i)}$, $n_i = n_{\sigma(i)}$ für eine Permutation σ der Menge $\{1, \dots, k\}$. Damit folgt die Eindeutigkeit auch für α selbst.

Bemerkung. Es ist klar, warum 1 keine Primzahl ist - der Satz von der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ würde falsch! 1 ist - wie -1 eine *Einheit*.
Euklidischer Algorithmus Im Beweis haben wir den euklidischen Algorithmus verwendet. Er ist die beste Möglichkeit zur Bestimmung des ggT.

Beispiel. Wir bestimmen $\mathrm{ggT}(12345, 6789)$:

$$\begin{aligned} 12345 : 6789 &= 1 \text{ Rest } 5556 \\ 6789 : 5556 &= 1 \text{ Rest } 1233 \\ 5556 : 1233 &= 4 \text{ Rest } 624 \\ 1233 : 624 &= 2 \text{ Rest } -15 \\ 624 : 15 &= 41 \text{ Rest } 9 \\ 15 : 9 &= 2 \text{ Rest } -3 \end{aligned}$$

Also $\mathrm{ggT}(12345, 6789) = 3$.

Aufgabe 2.8. Nehmen Sie sich Pärchen von großen Zahlen (z.B. 10 Stellen? Wie wäre es mit mehr als Ihr Taschenrechner kann?) und berechnen Sie das ggT mit dem euklidischen Algorithmus. Können Sie abschätzen, wieviele Rechenschritte Sie benötigen?

Aufgabe 2.9. Berechnen Sie $\mathrm{ggT}(-47 + 72i, 21 + 22i)$ in $\mathbb{Z}[i]$.

Kapitel 3

Restklassenringe

Definition 3.1. *Sei $n \in \mathbb{N}$. Dann ist*

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$$

die Menge der Restklassen von ganzen Zahlen modulo n. Wir schreiben

$$a \mod n$$

für die Restklasse $a + n\mathbb{Z}$

Es gilt

$$a = b \mod n \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \subset \mathbb{Z} \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow n|a - b$$

Lemma 3.2. *Mit der Addition und Muliplikation induziert von $\mathbb{Z}$ ist $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring mit 1. Der Ring hat n Elemente.*

Beispiel.

$$3 + 2 = 5 \mod 7 \qquad 3 + 5 = 8 = 1 \mod 7 \qquad 3 \cdot 4 = 12 = 5 \mod 7$$

Beweis: Die Ringaxiome folgen direkt aus den Ringaxiomen für $\mathbb{Z}$. Interessanter ist ein anderes Problem: warum sind Addition und Muliplikation wohldefiniert? Sei $a = a' \mod n$, $b \in \mathbb{Z}$. Nach Vorausetzung gibt es $m \in \mathbb{Z}$ mit $a - a' = mn$. Dann ist

$$\begin{aligned}(a + n\mathbb{Z}) + (b + n\mathbb{Z}) &= (a + b) + n\mathbb{Z} = (a' + mn + b) + n\mathbb{Z} \\ &= (a' + b) + mn + n\mathbb{Z} = (a' + b) + n\mathbb{Z} = (a' + n\mathbb{Z}) + (b + n\mathbb{Z})\end{aligned}$$

denn $n\mathbb{Z} = mn + n\mathbb{Z}$ als Teilmengen von $\mathbb{Z}$. Ebenso sieht man:

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} = (a' + mn)b + n\mathbb{Z} = a'b + mnb + n\mathbb{Z} = a'b + n\mathbb{Z}$$

Die Restklassen von $0, 1, 2, \ldots, n - 1$ sind alle verschieden. Dies sind die n Elemente von $\mathbb{Z}/n\mathbb{Z}$. □

Beachte: In $\mathbb{Z}/n\mathbb{Z}$ kann es Nullteiler geben!

Beispiel.

$$2 \cdot 3 = 6 = 0 \mod 6$$

obwohl $2, 3 \neq 0 \mod 6$.

Aufgabe 3.1. Erstellen Sie ein Additions- und Multiplikationstabelle für $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$. Handelt es sich um Körper?

Satz 3.3 (Chinesicher Restsatz). *Seien $n, m \in \mathbb{N}$ teilerfremd. Dann ist die Abbildung*

$$\pi : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \qquad a + nm\mathbb{Z} \mapsto (a + n\mathbb{Z}, a + m\mathbb{Z})$$

ein Ringisomorphismus.

Beweis: Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sind komponentenweise erklärt. π ist offensichtlich verträglich mit Addition und Multiplikation. Interessant ist also die Bijektivität.
Der Kern von π ist

$$\{a + nm\mathbb{Z} \mid a = 0 \mod n, a = 0 \mod m\}$$

Dies bedeutetet $n|a$ und $m|a$. Da n und m teilerfremd sind, folgt $nm|a$. D.h. es gilt $a = 0 \mod nm$. Damit ist der Kern von π trivial, die Abbildung ist *injektiv*. Beide Seiten haben nm Elemente. Eine injektive Abbildung ist automatisch surjektiv. □

Der chinesische Restsatz sagt also: Eine Restklasse modulo nm ist eindeutig bestimmt durch ihre Reste modulo n und m. Zu einem Paaren von Resten modulo n und m gibt es ein gemeinsames $a \in \mathbb{Z}$, das beide Reste induziert (und a ist eindeutig modulo nm). Das Lösen von Gleichungen modulo nm wird so reduziert auf das Lösen von Gleichungen modulo n und modulo m.
Konvention: Wir unterscheiden meist nicht zwischen $a \in \mathbb{Z}$ und der Restklasse von a modulo n, d.h. $a + n\mathbb{Z}$.

Beispiel. Betrachte $x^3 + 2x = 3 \mod 6$. Wir lösen zunächst:

$$\begin{aligned} x^3 + 0x = 3 = 1 \mod 2 &\Leftrightarrow x = 1 \mod 2 \\ x^3 + 2x = 0 \mod 3 &\Leftrightarrow x(x^2 - 1) = x(x-1)(x+1) \mod 3 \\ &\Rightarrow x_1 = 0, x_2 = 1, x_3 = 2 \mod 3 \end{aligned}$$

Die Lösungen modulo 6 sind hierdurch eindeutig bestimmt:

$$x_1 = 3, x_2 = 1, x_3 = 5 \mod 6$$

Aufgabe 3.2. Lösen Sie die Gleichungen:

(i) $x^2 + x + 1 = 0 \mod 6$

(ii) $x^4 + x + 5 = 0 \mod 4$

(iii) $x^4 + x + 8 = 0 \mod 12$

(iv) ...

Aufgabe 3.3. Zeigen Sie die folgende allgemeinere Fassung des chinesischen Restsatzes: Seien $a_1, \ldots, a_n \in \mathbb{N}$ mit $\mathrm{ggT}(a_1, \ldots, a_n) = 1$. Dann ist

$$\mathbb{Z}/a_1 \ldots a_n\mathbb{Z} \cong \mathbb{Z}/a_!\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

Wir wollen die Struktur des Rings $\mathbb{Z}/n\mathbb{Z}$ besser verstehen. Dafür benutzen wir ein wenig Gruppentheorie.

Exkurs in die Gruppentheorie

Sei G eine endliche kommutative Gruppe. Für $a \in G$ sei

$$< a >= \{e, a, a^{-1}, a^2, a^{-2}, \ldots\}$$

die von a erzeugte Untergruppe in G. In einer additiven Gruppe ist entsprechend $< a >= \{0, \pm a, \pm 2a, \pm 3a, \ldots\}$. Da G endlich ist, ist es auch $< a >$.

Definition 3.4. *Die* Ordnung *von a ist $| < a > |$. Eine Gruppe heißt* zyklisch, *wenn $G =< a >$ für ein $a \in G$.*

Beispiel. $\mathbb{Z}/n\mathbb{Z}$ als abelsche Gruppe ist zyklisch mit dem Erzeuger 1.

Lemma 3.5. *Die Ordnung ist die kleinste natürliche Zahl mit $a^d = e$. Es gilt*

$$< a >= \{e, a, a^2, \ldots, a^{d-1}\}$$

Die Gruppe ist isomorph zu $\mathbb{Z}/d\mathbb{Z}$ via $a \mapsto 1$.

Beweis: Wegen $a^d = e$ folgt $a^n = a^m$ für $n = m \mod d$. Also hat die Gruppe die angegebene Form. Wir bestimmen die Anzahl der Elemente: Angenommen, es gilt $a^n = a^m$ für $0 \leq n < m < d$. Dann folgt $e = a^0 = a^{m-n}$. Dies ist ein Widerspruch zur Minimalität von d. Damit hat $< a >$ wirklich d verschiedene Elemente. Die Abbildung $< a > \to \mathbb{Z}/d$ ist wohldefiniert, da $a^d = e \mapsto d = 0 \mod d$. Sie ist offensichtlich bijektiv. □

Satz 3.6. *Sei G eine endliche abelsche Gruppe $a \in G$.*

(i) Es gilt $a^{|G|} = e$ für alle $a \in G$.

(ii) Die Ordnung von $a \in G$ teilt die Ordnung von G.

Beweis: Sei $G = \{a_1, \ldots, a_n$. Wir betrachten $g = a_1 \ldots a_n$. Die Abbildung

$$G \to G \qquad x \mapsto ax$$

ist bijektiv, daher kommt auch in dem Produkt

$$g' = (aa_1)(aa_2)\dots(aa_n)$$

jedes Gruppenelement genau einmal vor. Da es auf die Reihenfolge nicht ankommt, gilt $g' = g$. Anderseits ist

$$g' = a^n g \Rightarrow e = a^n$$

Sei d die Ordnung von a, $d' = \mathrm{ggT}(d, n)$. Dann gibt es $\alpha, \beta \in \mathbb{Z}$ mit

$$d' = \alpha d + \beta n \Rightarrow a^{d'} = (a^d)^\alpha (a^n)^\beta = ee = e$$

Nach Wahl von d als kleinster Exponent mit $a^d = e$ muss nun $d = d'$ sein, d.h. $d|n$. □

Bemerkung. Der Satz gilt natürlich auch für nicht-abelsche Gruppen. Er folgt sofort aus dem Satz von Lagrange. Dies ist der bessere Beweis!

Satz 3.7 (Elementarteilersatz). *Jede endliche abelsche Gruppe ist isomorph zu*

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_n$$

für gewisse $d_i \in \mathbb{N}$. Die d_i können teilerfremd gewählt werden. Sie können auch gewählt werden, so dass $d_{i+1}|d_i$. In dieser letzten Form sind sie eindeutig.

Beweis: Ohne Beweis. □

Die multiplikative Gruppe von $\mathbb{Z}/n\mathbb{Z}$.

Lemma 3.8. *Die Einheiten von $\mathbb{Z}/n\mathbb{Z}$ sind*

$$\{(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a, n) = 1\} = \{a \in \mathbb{Z}/n\mathbb{Z} \mid < a >= \mathbb{Z}/n\mathbb{Z}\}$$

Beweis: Sei a Einheit, d.h. es gibt b mit $ab = 1 \mod n$, d.h. es gibt $m \in \mathbb{Z}$ mit

$$ab + mn = 1$$

Dann gilt $\mathrm{ggT}(a, n)|1$. Sei umgekehrt $\mathrm{ggT}(a, n) = 1$. Mit Hilfe des euklidischen Algorithmus 2.7 schreiben wir

$$1 = \mathrm{ggT}(a, n) = a\alpha + n\beta$$

Mit $\alpha, \beta \in \mathbb{Z}$. Die Restklasse von α ist dann invers zu a bezüglich der Multiplikation.
Sei wieder a Einheit, $b \in \mathbb{Z}$ mit $ab = 1 \mod n$. Dann ist $1 = ba \in < a >$. Wegen $c = c \cdot 1 \in \mathbb{Z}/n\mathbb{Z}$ enhält $< a >$ dann alle Elemente des Rings. Umgekehrt sei $< a >= \mathbb{Z}/n\mathbb{Z}$. Dann gibt es $b \in \mathbb{Z}$ mit $ba = 1 \mod n$ und a ist Einheit. □

Aufgabe 3.4. Bestimmen Sie die Inversen aller Elemente von $\mathbb{Z}/5$ ungleich Null. Bestimmen Sie die Einheiten von $\mathbb{Z}/6$ und $\mathbb{Z}/12$.

Definition 3.9.

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

heißt Eulersche φ-Funktion.

Es gilt also $\varphi(n)$ ist die Anzahl der Zahlen echt kleiner als n, die teilerfremd sind zu n.

Lemma 3.10. *(i) Seien n, m teilerfremd. Dann gilt $\varphi(nm) = \varphi(n)\varphi(m)$.*

(ii) Sei p Primzahl. Dann gilt $\varphi(p^n) = (p-1)p^{n-1}$.

Beweis: Nach dem chinesischen Restsatz gilt

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Insbesondere ist eine Restklasse genau dann invertierbar, wenn sie invertierbar modulo n und modulo m ist, d.h.

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n)^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Dann stimmen auch die Anzahlen der beiden Mengen überein. Dies ist die Behauptung.
Sei nun p eine Primzahl. Dann ist $\varphi(p^n)$ die Anzahl der Zahlen in $0, 1, \ldots, p^n - 1$, die teilerfremd zu p^n sind (äquivalent: die teilerfremd zu p sind). Dies ist p^n weniger die Anzahl der Zahlen, die durch p teilbar sind. Also

$$\varphi(p^n) = p^n - p^{n-1}$$

□

Beispiel.

$$\varphi(12) = \varphi(3)\varphi(4) = (3-1)2(2-1) = 4$$

Aufgabe 3.5. Berechnen Sie $\varphi(n)$ für $n = 1, 2, 3, \ldots, 20, 81, 155$.

Korollar 3.11. *Sei p eine Primzahl. Dann ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.*

Beweis: Wir haben gezeigt, dass $(\mathbb{Z}/p\mathbb{Z})^*$ genau $p-1$ Elemente hat, nämlich alle Restklassen ungleich 0. Dass heißt gerade dass alle Elemente ungleich 0 inertierbar bezüglich der Multiplikation sind. □

Aufgabe 3.6. Ist $\mathbb{Z}/4\mathbb{Z}$ ein Körper? Gibt es einen Körper mit 4 Elementen?

Korollar 3.12 (Kleiner Satz von Fermat). *Sei p eine Primzahl, $x \in \mathbb{Z}$. Dann gilt*

$$x^p = x \mod p$$

Beweis: Die Aussage ist wahr für $x = 0 \mod p$. Andernfalls ist $x \mod p$ ein Elemente der Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ mit $p-1$ Elementen. Dann folgt nach Satz 3.6

$$x^{p-1} = 1 \mod p$$

Multiplikation mit p gibt die Behauptung. □

Bemerkung. Dies ist ein Primzahltest: Um zu überprüfen, ob eine gegeben Zahl eine Primzahl ist, berechnet man testhalber x^p für viele x. Das Rechnen mit Restklassen ist schnell, daher ist dies eine gute Methode.

Aufgabe 3.7. Betrachten Sie die Zahlen $1377, 11111, 559$ Handelt es sich um Primzahlen?

Hier eine Variante des kleinen Satzes von Fermat für zwei Primzahlen.

Korollar 3.13. *Seien $p \neq q$ Primzahlen, $n = pq$. Sei $m = 1 \mod \varphi(n)$ Dann gilt für alle $x \in \mathbb{Z}/n\mathbb{Z}$*

$$x^m = x \mod n$$

Beweis: Nach dem chinesischen Restsatz genügt es, die Aussage $\mod p$ und $\mod q$ zu zeigen. Wegen $\varphi(n) = (p-1)(q-1)$ gilt $m = 1 + a(p-1)(q-1)$, also $m = 1 \mod p-1$. Genau wie im Beweis des kleinen Satzes von Fermat (Fallunterscheidung nach x teilerfremd zu p oder nicht), gilt $x^m = x \mod p$. Genauso argumentiert man für q. □

Dieser Fall ist interessant, da er in der Kryptografie verwendet wird.

Public Key Kryptografie

Alice will Bob eine geheime Botschaft senden. Sie gehen wie folgt vor:

- Bob wählt zwei (große) Primzahlen p, q und berechnet $pq = n$. Er wählt einen geheimen Schlüssel $e \in \mathbb{Z}/n\mathbb{Z}$, der teilerfremd zu $\varphi(n)$ ist. Dies überprüft er mittels des euklidischen Algorithmus. Dieser liefert ihm auch eine Darstellung
  $$1 = de + s\varphi(n)$$
  Er veröffentlich d und n. (Tageszeitung, Internet...)
- Alice wandelt ihre Botschaft in eine Zahl x in $\mathbb{Z}/n\mathbb{Z}$ um. Sie berechnet $y = x^d \mod n$. Das kann sie, denn d und n kennt ja jeder.
- Alice schickt y an Bob (Tagesezeitung, Internet...)
- Bob berechnet y^e. Er kann das, schließlich hat er sich e gemerkt. Er erhält
  $$y^e = (x^d)^e = x^1 \mod n$$
  denn $de = 1 \mod \varphi(n)$.

Es geht noch besser:

- Auch Alice wählt einen geheimen Schlüssel e' und den zugehörigen öffentlichen Schlüssel d'.
- Sie verschickt $z = x^{e'd} \mod n$.
- Bob berechnet $z^{ed'} = x^{e'd'ed} = x \mod n$.

Diesmal kann niemand die Nachricht mitlesen und Bob ist sicher, dass sie von Alice kam.
Wie sicher ist das Verfahren? Es ist leicht, d aus e und $\varphi(n)$ zu berechnen (so machen es Alice und Bob). Aber es ist schwer, $\varphi(n)$ aus n zu berechnen - man muss die Zahl als Produkt von Primfaktoren schreiben. In der Praxis werden 100-200-stellige Primzahlen verwendet. Man muss noch ein paar "offensichtliche" Probleme vermeiden (z.B. p und q nahe beieinander), dann ist das Verfahren nach derzeitigem Stand der Technik sicher.

Aufgabe 3.8. Suchen Sie einen Partner und senden Sie sich gegenseitig geheime Nachrichten. Mit der Hand reichen 2-stellige Primzahlen, aber vielleicht finden Sie ja auch ein Programm (oder schreiben es selbst).

Satz 3.14. *Sei $n \in \mathbb{N}$. Dann gilt $\sum_{d|n} \varphi(d) = n$.*

Beweis: Die Summationsformel benutzt ein wenig Gruppentheorie. Sei $d|n$. Wir setzen $C_d =< \frac{n}{d} > \subset \mathbb{Z}/n\mathbb{Z}$. Es gilt $C_d \cong \mathbb{Z}/d\mathbb{Z}$ via $n/d \mapsto 1$ als abelsche Gruppen. Sei

$$\Phi_d \subset C_d$$

die Teilmenge der Erzeuger, d.h. diejenigen Elemente, die genau die Ordnung d haben. Wegen $C_d \cong \mathbb{Z}/d\mathbb{Z}$ folgt aus 3.3 $\Phi_d \cong (\mathbb{Z}/d\mathbb{Z})^*$, also ist

$$\varphi(d) = |\Phi_d|$$

Jedes Element von $\mathbb{Z}/n$ gehört zu genau einem Φ_d. Es gilt also

$$\mathbb{Z}/n\mathbb{Z} = \dot{\bigcup} \Phi_d$$

Durch Abzählen erhält man die Formel. □

Beispiel.

$$\begin{aligned}\varphi(12) &= 12 - \varphi(6) - -\varphi(4) - \varphi(3) - \varphi(2) - \varphi(1)\\ &= 12 - (6 - \varphi(3) - \varphi(2) - \varphi(1)) - \varphi(4) - \varphi(3) - \varphi(2) - \varphi(1)\\ &= 6 - \varphi(4) = 6 - (4 - \varphi(2) - \varphi(1)) = 6 - (4 - 2) = 2\end{aligned}$$

Struktur von $(\mathbb{Z}/p^n)^*$

Satz 3.15. *Sei p Primzahl. Dann ist $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch, d.h. alle Elemente sind Potenzen eines Erzeugers α. Die Erzeuger heißen* primitive Einheiten

Bemerkung. Allgemeiner gilt: jede endliche Untergruppe der Gruppe K^* eines Körpers ist zyklisch. Der Beweis ist praktisch der gleiche, wie der in unserem Fall.

Beweis: Der Beweis argumentiert für $(\mathbb{Z}/p\mathbb{Z})^*$ wie wir in Satz 3.14 für $\mathbb{Z}/n$ argumentiert haben.

Sei $d|p-1$. Seien $E_d \subset H_d \subset (\mathbb{Z}/p\mathbb{Z})^*$ Untermengen, nämlich E_d die Menge der Elemente der Ordnung d (bezüglich der Multiplikation),

$$H_d = \{a \in (\mathbb{Z}/p\mathbb{Z})^* \mid a^d = 1\}$$

Wir betrachten das Polynom $X^d - 1$. Es hat höchstens d Nullstellen, also gilt

$$|H_d| \leq d$$

Es gibt zwei Fälle, nämlich E_d leer oder nicht leer. Im ersten Fall gilt offensichtlich $|E_d| = 0$. Im zweiten sei $\alpha \in E_d$. Dann gilt

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\} \subset H_d$$

und die linke Menge hat genau d Elemente. In diesem Fall ist also $< \alpha >= H_d$. Damit ist $H_d \cong \mathbb{Z}/d\mathbb{Z}$. Darin gibt es genau $\varphi(d)$ Elemente der Ordnung d, $|E_d| = \varphi(d)$.
Jedes Element von $(\mathbb{Z}/p\mathbb{Z})^*$ hat irgendeine Ordnung, also

$$(\mathbb{Z}/p\mathbb{Z})^* = \dot{\bigcup} E_d \Rightarrow p-1 = \sum_{d|p-1} |E_d| \leq \sum_{d|p-1} \varphi(d) = p-1$$

Also haben wir Gleichheit, alle E_d sind nicht-leer. Dies gilt insbesondere für E_{p-1}, d.h. die Gruppe hat Elemente der Ordnung $p-1$. □

Aufgabe 3.9. Bestimmen Sie primitive Einheiten von $\mathbb{Z}/3$, $\mathbb{Z}/7$, $\mathbb{Z}/19$.

Wir verallgemeinern dies auf $\mathbb{Z}/p^n\mathbb{Z}$.

Satz 3.16. *Sei $p \neq 2$ Primzahl. Dann ist $(\mathbb{Z}/p^n)^*$ zyklisch.*

Aufgabe 3.10. Bestimmen Sie die primitiven Einheiten von $\mathbb{Z}/8$, $\mathbb{Z}/9$, $\mathbb{Z}/25$, $\mathbb{Z}/49$, $\mathbb{Z}/81$.

Bemerkung. Im allgemeinen ist $\mathbb{Z}/n$ nicht zyklisch. Sei etwa $n = pq$ für zwei Primzahlen p, q. Dann gilt

$$(\mathbb{Z}/pq)^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/p-1 \times \mathbb{Z}/q-1$$

Falls $p-1$ und $q-1$ teilerfremd sind, so erlaubt der chinesische Restsatz die Zusammenfassung zu $\mathbb{Z}/(p-1)(q-1)$. Aber meist haben sie Faktoren gemeinsam, etwa die 2

Aufgabe 3.11. Suchen Sie ein Beispiel für ein n, das keine Primzahlpotenz ist, aber $(\mathbb{Z}/p^n)$ ist zyklisch. Suchen Sie ein Gegenbeispiel.

Nun zum Beweis von Satz 3.16. Wir fixieren nun eine Primzahl p.

Definition 3.17. *Sei $U_1/p^n = \mathrm{Ker}(\pi : (\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*)$.*

Lemma 3.18. *U_1/p^n hat p^{n-1} Elemente.*

Beweis: Es gilt $|U_1/p^n| \cdot |\operatorname{Im}\pi| = |(\mathbb{Z}/p^n\mathbb{Z})^*| = (p-1)p^n$. Zu zeigen ist also, dass π surjektiv ist. Sei $a \in \mathbb{Z}$ Einheit in $\mathbb{Z}/p$, d.h. a teilerfremd zu p. Dann ist a auch teilerfremd zu p^n. Dies ist das gesuchte Urbild von $a \mod p$. □

Der wesentliche Beweisschritt ist die folgende Eigenschaft:

Satz 3.19. *Für $p \neq 2$ gilt*

$$U_1/p^n \cong \mathbb{Z}/p^{n-1}$$

Für $p = 2$ und $n \geq 2$ gilt

$$U_1/2^n \cong \{\pm 1\} \times \mathbb{Z}/2^{n-2}$$

Beispiel.

$$U_1/2^2 = \operatorname{Ker}(\mathbb{Z}/4^* \to \mathbb{Z}/2^*) = \mathbb{Z}/4^* = \{\pm 1 \mod 4\}$$
$$U_1/3 = \mathbb{Z}/8^* = \{1,3,5,7 \mod 8\} = \{1,7 \mod 8\} \times \{1,3 \mod 8\}$$

denn $3^2 = 9 = 1$ (zyklisch der Ordnung 2), $3 \cdot 7 = 21 = 5 \mod 8$.

$$U_1/27^* = \{1,4,7,10,13,16,19,22,25 \mod 27\}$$

(Beachte: $\varphi(3^3) = 3^2 \cdot 2 = 18$. Ist 4 ein Erzeuger? Ja!

$$4^2 = 16, 4^3 = 2^6 = 64 = 10, 4^4 = 40 = 13, 4^5 = 52 = -2, 4^6 = -8,$$
$$4^7 = -32 = -5, 4^8 = -20 = 7, 4^9 = 28 = 1$$

Beweis: (von Satz 3.16 aus Satz 3.19) Sei $p \neq 2$. Wir wählen einen Erzeuger von $\mathbb{Z}/p^*$. Sei $a \in (\mathbb{Z}/p^n)^*$ ein Urbild dieses Erzeugers. Die Ordnung von a ist dann ein Teiler von $(p-1)p^n$ und ein Vielfaches von $p-1$, also von der Form $(p-1)p^i$. Dann hat $b = a^{p^i}$ die Ordnung $p-1$. Sei c ein Erzeuger von U_1/p^n, also von der Ordnung p^{n-1}. Wir setzen $d = bc$. Was ist die Ordnung von d? Das Bild von d in $(\mathbb{Z}/p)^*$ is a^{p^i}. Da p^i und $p-1$ teilerfremd sind, hat es die Ordnung $p-1$. Also ist die Ordnung von d von der Form $(p-1)p^j$. Wir betrachten $d^{(p-1)} = 1 \cdot c^{p-1}$. Da c die Ordnung p^{n-1} hat und dieses teilerfremd zu $p-1$ ist, hat c^{p-1} ebenfalls die Ordnung p^{n-1}. Insgesamt hat d die maximale Ordnung $(p-1)p^{n-1}$. □

Beweis: Sei $p \neq 2$.

Behauptung. *$1+p$ erzeugt U_1/p^n, d.h. es hat Ordnung p^{n-1}.*

Sei $\alpha_n = (1+p)^{p^{n-2}}$. Zu zeigen ist $\alpha_n \neq 1 \mod p^n$. Da die Ordnung ein Teiler von p^{n-1} ist, muss sie dann auch gleich p^{n-1} sein. Klar ist $\alpha_n = 1 \mod p^{n-1}$, da U_1/p^{n-1} Ordnung p^{n-1} hat.
Wir argumentieren mit vollständiger Induktion nach n und zeigen

$$\alpha_n = 1 + p^{n-1} + lp^n$$

Für $n = 2$ gilt

$$(1+p)^{p^0} = 1 + p \mod p^2$$

Sei nun $n \geq 2$ und die Formel für n gezeigt. Wir berechnen α_{n+1}:

$$\alpha_{n+1} = \alpha_n^p = (1 + p^{n-1} + lp^n)^p = \sum_{i=0}^{p} \binom{p}{i} (1 + lp)^i p^{(n-1)i} \mod p^{n+1}$$

Wann ist $(n-1)i \geq n+1$? Für $i > 2$

$$(n-1)i \geq 2n - 2 \geq n - 1$$

da $n \geq 2$. Damit reduziert sich die Summe zu

$$\alpha_{n+1} = 1p^0 + p(1 + lp)p^{n-1} = 1 + p^n \mod p^{n+1}$$

abar wie zu zeigen war.
Sei nun $p = 2$, $n \geq 2$.

Behauptung. $1 + 4$ *erzeugt* $U_2/2^n = \{a \in \mathbb{Z}/2^n \mid a = 1 \mod 4\}$

Die Gruppe hat Ordnung 2^{n-2}. Zu zeigen ist

$$(1 + 4)^{2^{n-3}} = 1 + 2^{n-1} + l2^n$$

Der Induktionsanfang ist $n = 3$:

$$5^1 = 1 + 2^2 + 0$$

Die Aussage sei gezeigt für $n \geq 3$. Dann ist

$$\begin{aligned}(1 + 2^{n-1} + l2^n)^2 &= 1 + 2 \cdot 2^{n-1} + 2l2^n + 2l2^{2n-1} + 2^{4n-2} + l^2 2^{2n} \\ &= 1 + 2^n + l2^{n+1} + l2^{2n} + 2^{4n-2} + l^2 2^{2n} = 1 + 2^n \mod 2^{n+1}\end{aligned}$$

(beachte: $2n \geq n + 1 \Leftrightarrow n \geq 1$, $4n - 2 \geq n + 1 \Leftrightarrow 3n \geq 1$). Nun betrachten wir

$$\{\pm 1\} \times U_2/2^n \to U_1/2^n \cong (\mathbb{Z}/2^n)^*$$

Beide Seiten haben die Ordnung 2^{n-1}. Wir bestimmen den Kern, also

$$\{\pm 1\} \cap < 5 >$$

Wegen $-1 \neq 5^i \mod 4$ ist der Schnitt trivial. Die Abbildung ist eine Bijektion. □

Aufgabe 3.12. Schreiben Sie die folgenden Gruppen in Termen von Elementarteilern (vergleiche Satz 3.7 mit $d_{i+1}|d_i$: $\mathbb{Z}/12^*$, $\mathbb{Z}/14^*$, $\mathbb{Z}/18^*$

Kapitel 4

Quadratisches Reziprozitätsgesetz

Sei p eine Primzahl, $a \in \mathbb{Z}$. Wann ist a eine Quadratzahl modulo p?
Sei $a \in \mathbb{Z}$, p eine Primzahl. Dann heißt a quadratischer Rest modulo p (bzw. Nichtrest), wenn die Gleichung $x^2 = a$ modulo p lösbar ist (bzw. unlösbar).

Beispiel. $p = 7$. Wir berechnen alle Quadrate:

1	2	3	4	5	6
1	4	2	2	4	1

Wir beobachten: Nur die Hälfte der Zahlen kommt vor - kein Wunder, denn wenn a Quadrat ist einer Zahl, dann von zweien.

Aufgabe 4.1. Sei p ungerade Primzahl. Zeigen Sie, dass die Hälfte der Restklassen in $(\mathbb{Z}/p)^*$ Quadratzahlen sind modulo p. Tipp: $x \mapsto x^2$ ist ein Gruppenhomomorphismus.

Definition 4.1. *Sei $p \neq 2$ Primzahl. Das* Legendre-Symbol *ist*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ 1 & a \text{ ist Quadratzahl} \\ -1 & \text{sonst} \end{cases} \mod p$$

Beispiel. $\left(\frac{2}{7}\right) = 1$, $\left(\frac{3}{7}\right) = -1$

Bemerkung. Die Funktion $\left(\frac{\cdot}{p}\right)$ ist p-periodisch.

Lemma 4.2. *Die Funktion $\left(\frac{\cdot}{p}\right)$ ist multiplikativ, d.h.*

$$\left(\frac{n}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{nm}{p}\right)$$

Beweis: Falls $p|n \Rightarrow p|nm$, d.h. beide Seiten sind Null. Sei nun $p \nmid nm$, d.h. $n, m \mod p$ liegen in $(\mathbb{Z}/p)^*$. Wir schreiben $\mathbb{F}_p$ für den Körper $\mathbb{Z}/p$. Sei $\mathbb{F}_p^{*2}$ die Untergruppe der Quadratzahlen in $\mathbb{F}_p^*$. Sei $x \in \mathbb{F}_p^*$, $y \in \overline{F}_p$ mit $y^2 = x$. Dann gilt

$$(y^{p-1})^2 = x^{p-1} = 1 \Leftrightarrow y^{p-1} = \pm 1$$

Damit können wir umformulieren: x ist ein Quadrat genau dann, wenn $y \in \mathbb{F}_p$. Hieraus folgt $y^{p-1} = 1$. Sei umgekehrt $y^{p-1} = 1$. Dann ist y eine Nullstelle von $X^{p-1} - 1$. Das Polynom hat $p - 1$ Nullstellen in $\mathbb{F}_p$, also liegen alle Nullstellen (insbesondere y) in $\mathbb{F}_p$. Also $y \in \mathbb{F}_p$ genau dann, wenn $y^{p-1} = 1$. Es gilt also

$$\left(\frac{x}{p}\right) = y^{p-1}$$

Wir verifizieren nun die Behauptung. Sei $y_1^2 = n$, $y_2^2 = m$. Dann gilt $(y_1 y_2)^2 = nm$. Es gilt daher

$$\left(\frac{nm}{p}\right) = (y_1 y_2)^{p-1} = y_1^{p-1} y_2^{p-1} = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$$

□

Aufgabe 4.2. Führen Sie einen alternativen Beweis mit Hilfe von Aufgabe 4.1: $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ ist eine Gruppe mit zwei Elementen. Das Legendre-Symbol identifiziert sie mit $\{\pm 1\}$.

Theorem 4.3 (Gauß). *Seien l, p Primzahlen ungleich 2. Dann gilt das* Quadratische Reziprozitätsgesetz

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2}q-12}$$

Bemerkung. $p-1$ ist gerade, also ist $(p-1)/2$ eine ganze Zahl. In der Formel kommt es nur auf ihre Parität an:

$$\frac{p-1}{2} = \begin{cases} 0 \mod 2 & p = 1 \mod 4 \\ 1 \mod 2 & p = 3 \mod 4 \end{cases}$$

Beispiel. Ist 77 eine Quadratzahl modulo 101?

$$\begin{aligned}\left(\frac{77}{101}\right) = \left(\frac{7}{101}\right)\left(\frac{11}{101}\right) &= \left(\frac{101}{7}\right)(-1)^{\frac{7-1}{2}\frac{101-1}{2}}\left(\frac{101}{11}\right)(-1)^{\frac{101-1}{2}\frac{11-1}{2}} \\ = \left(\frac{3}{7}\right)\left(\frac{2}{11}\right) = \left(\frac{7}{3}\right)(-1)^{\frac{3-1}{2}\frac{7-1}{2}}\left(\frac{2}{11}\right) &= -\left(\frac{1}{3}\right)\left(\frac{2}{11}\right) \\ &= -1 \cdot 1 \cdot \left(\frac{2}{11}\right)\end{aligned}$$

Quadrate modulo 11 sind $1, 4, 9, 5, 3$. Es gilt $\left(\frac{2}{11}\right) = -1$, also ist das Endergebnis 1, d.h. 77 ist Quadratzahl.

Aufgabe 4.3. Finden Sie die Restklasse mit Quadrat 77.

Noch mächtiger wird das Reziprozitätsgesetz durch den Ergänzungssatz.

Theorem 4.4. *Sei p ungerade Primzahl. Dann gilt*

$$\left(\frac{1}{p}\right) = 1 \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p = \pm 1 \mod 8 \\ -1 & p = \pm 5 \mod 8 \end{cases}$$

Beweis: 1 ist eine Quadratzahl. Für -1 benutzen wir die Formel aus dem Beweis von Lemma 4.2: Sei $y^2 = -1$ in $\overline{F}_p$. Dann ist

$$\left(\frac{-1}{p}\right) = y^{p-1} = (y^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

Der Fall 2 is schwieriger. Wir bestimmen z mit $z^2 = 2$ wie folgt. Sei α eine primitive 8-te Einheitswurzel in $\overline{F}_p$, also Nullstelle von

$$X^8 - 1 = (X^4 - 1)(X^4 + 1) = (X - 1)(X + 1)(X^2 + 1)(X^4 + 1)$$

α primitiv heißt, α ist Nullstelle von $X^4 + 1$, also

$$\alpha^4 = -1 \Leftrightarrow \alpha^2 = -\alpha^{-2}$$

Wir setzen

$$z = \alpha + \alpha^{-1} \Rightarrow y^2 = (\alpha + \alpha^{-2}) = \alpha^2 + 2 + \alpha^{-2} = 2$$

Wie im Beweis von Lemma 4.2 gilt

$$\left(\frac{2}{p}\right) = z^{p-1}$$

1. Fall: $p = \pm 1 \mod 8$.

$$z^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = z$$

da $\alpha^8 = 1$ und $p = \pm 1 \mod 8$. In diesem Fall folgt also $z^{p-1} = 1$. Wir überprüfen noch die angegebene Formel: $p = \pm 1 + 8k \Rightarrow p^2 = 1 \pm 2 \cdot 8k + 8^2k^2$, d.h. $(p^2 - 1)/8$ ist gerade.

2. Fall: $p = \pm 5 \mod 8$.

$$z^p = \alpha^p + \alpha^{-p} = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -z$$

da $\alpha^4 = -1$. In diesem Fall folgt $z^{p-1} = -1$. Sei $p = \pm 5 + 8k$. Dann ist $p^2 = 25 \pm 2 \cdot 5 \cdot 8k + 8^2k^2$. Dann ist

$$\frac{p^2 - 1}{8} = 3 \pm 10k + 8k^2$$

ungerade. □

Aufgabe 4.4. Quadratischer Rest oder Nichtrest? $7 \mod 13$, $7 \mod 19$, $7 \mod 89$, $7 \mod 571$, $2003 \mod 1091$.

Aufgabe 4.5. Zeigen Sie: Seien n, m teilerfremd. Dann ist a eine Quadratzahl modulo nm genau dann, wenn es eine Quadratzahl modulo n und modulo m ist.

Aufgabe 4.6. Sei p ungerade Primzahl, a eine Quadratzahl modulo p. Was kann man modulo p^2 sagen?

Zum Beweis des Reziprozitätsgesetzes müssen wir noch etwas Vorarbeit leisten. Der Beweis folgt der Darstellung von Serre in 'A course in arithmetic'.

Definition 4.5. *Seien p, l ungerade Primzahlen, $\omega \in \overline{F}_p$ eine primitive Lösung von $X^l - 1$ (d.h. $\omega \neq 1$). Wir setzen*

$$y = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{l}\right) \omega^x$$

Bemerkung. ω^x ist wohldefiniert wegen $\omega^l = 1$.

Lemma 4.6. $y^2 = (-1)^{\frac{l-1}{2}} l$.

Beweis: Es gilt

$$y^2 = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) \omega^x \sum_{z \in \mathbb{F}_l} \left(\frac{z}{l}\right) \omega^z = \sum_{x,z \in \mathbb{F}_l} \left(\frac{xz}{l}\right) \omega^{x+z}$$

Wir setzen nun $u = x + z$:

$$y^2 = \sum_{u \in \mathbb{F}_l} \omega^u \sum_{x \in \mathbb{F}_l} \left(\frac{x(u-x)}{l}\right)$$

Das Legendre-Symbol ist 0 für $x = 0$. Für $x \neq 0$ gilt

$$\left(\frac{x(u-x)}{l}\right) = \left(\frac{-x^2}{l}\right)\left(\frac{1-ux^{-1}}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{1-ux^{-1}}{l}\right) = (-1)^{\frac{l-1}{2}}\left(\frac{1-ux^{-1}}{l}\right)$$

Nun unterscheiden wir zwei Fälle:
1. Fall: $u = 0$

$$\sum_{x \in \mathbb{F}_l^*} \left(\frac{1-ux^{-1}}{l}\right) = \sum_{x \in \mathbb{F}_l^*} \left(\frac{1}{l}\right) = l - 1$$

2. Fall: $u \neq 0$. Dann durchläuft mit x auch ux^{-1} die gesamte Gruppe $\mathbb{F}_l^*$. Der Ausdruck $1 - ux^{-1}$ durchläuft dann $\mathbb{F}_l \setminus \{1\}$. Also

$$\sum_{x \in \mathbb{F}_l^*} \left(\frac{1-ux^{-1}}{l}\right) = \sum_{s \in \mathbb{F}_l} \left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) = 0 - 1$$

denn $\mathbb{F}_l$ hat genauso viele Quadrate wie nicht-Quadrate.

Wir fassen zusammen:

$$y^2 = (-1)^{\frac{l-1}{2}} \left[\omega^0 (l-1) + \sum_{u \in \mathbb{F}_l^*} \omega^u (-1) \right] = (-1)^{\frac{l-1}{2}} \left[l - \sum_{u \in \mathbb{F}_l} \omega^u \right] == (-1)^{\frac{l-1}{2}} l$$

wegen $\omega^l = 1 \Rightarrow 1 + \omega + \omega^2 + \ldots \omega^{l-1} = 0$ □

Lemma 4.7. $y^{p-1} = \left(\frac{p}{l}\right)$.

Beweis: Wir benutzen die Rechenregel $(a+b)^p = a^p + b^p$ in $\overline{\mathbb{F}}_p$:

$$y^p = \sum_{x \in \mathbb{F}_l^*} \left(\frac{x}{p}\right)^p \omega^{xp} = \sum_{x \in \mathbb{F}_l^*} \left(\frac{x}{p}\right) \omega^{xp}$$

da p ungerade. Wir setzen $z = xp$ in $\mathbb{F}_l^*$, also $x = zp^{-1}$ für die Restklasse p^{-1} invers zu p modulo l. (Da $p \neq l$ ist es invertierbar!)

$$y^p = \sum_{z \in \mathbb{F}_l^*} \left(\frac{zp^{-1}}{l}\right) \omega^z) = \left(\frac{p^{-1}}{l}\right) \sum_{z \in \mathbb{F}_l} \left(\frac{z}{l}\right) \omega^z = \left(\frac{p}{l}\right) y$$

Wegen des letzten Lemmas ist $y \neq 0$, also folgt die Behauptung. □

Beweis: (von Theorem 4.3) Nach Lemma 4.7

$$\left(\frac{p}{l}\right) = y^{p-1} = \left(\frac{(-1)^{l-1} 2l}{p}\right)$$

denn nach Lemma 4.6 erfüllt y die Gleichung $y^2 = (-1)^{\frac{l-1}{2}} l$. Weiter folgt aus der Multiplikativität des Restsymboles

$$= \left(\frac{-1}{p}\right)^{\frac{l-1}{2}} \left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}} \left(\frac{l}{p}\right)$$

mit Hilfe des Ergänzungssatzes. □

Bemerkung. Im Prinzip sind diese Beweise konstruktiv.

Kapitel 5

Der Zweiquadratesatz

Theorem 5.1 (Fermat). *Sei p eine Primzahl mit Rest* $1 \mod 4$. *Dann ist p eindeutig als Summe von zwei Quadraten zu schreiben:*

$$p = x^2 + y^2$$

Bemerkung. (i) Für $p = 2$ gilt $2 = 1 + 1$.

(ii) Ist $p = 3 \mod 4$, dann ist die Gleichung unlösbar, denn sie unlösbar mod 4.

Beispiel. $5 = 4 + 1, 13 = 9 + 4, 17 = 16 + 1, \ldots$

Aufgabe 5.1. Lässt sich jede Zahl $n = 1 \mod 4$ als Summe von zwei Quadraten schreiben?

Lemma 5.2. *Die Gleichung $p = x^2 + y^2$ ist nicht-trivial lösbar* $\mod p$, *falls die Primzahl p den Rest* $1 \mod 4$ *hat, nicht-trivial unlösbar falls* $p = 3 \mod 4$.

Beweis: Sei nun $p = 1 \mod 4$. Setze $x = 1$. Wir betrachten die Gleichung

$$0 = 1 + y^2 \mod p$$

Sie ist lösbar genau dann, wenn

$$1 = \left(\frac{-1}{p}\right) \overset{4.4}{=} (-1)^{\frac{p-1}{2}}$$

Dies ist für $p = 1 \mod 4$ der Fall. Ist (x, y) eine Lösung, so gilt $x^2 = -y^2$, also ist -1 ein Quadrat modulo p. Dann ist nach derselben Formel $p = 1 \mod 4$. □

Elementarer Beweis der Existenz in Theorem 5.1. Angenommen, die Behauptung ist falsch. Sei $p = 4k + 1$ die kleinste Primzahl, die *nicht* Summe von zwei Quadratzahlen ist. Nach Lemma 5.2 ist ein Vielfaches von p als Summe von zwei Quadraten zu schreiben. Sein n minimal, so dass es $x, y \in \mathbb{Z}$ gibt mit

$$np = x^2 + y^2$$

Ohne Einschränkung sind $x, y \geq 0$.

Behauptung. $x, y < p/2$

Sei $x' = x - ap$, $y' = y - bp$, so dass $|x'|, |y'| < p/2$. Dann ist $(x')^2 + (y')^2$ ein Vielfaches von p mit

$$(x')^2 + (y')^2 \leq x^2 + y^2$$

Da n minimal war, ist $|x| = |x'$ und $|y| = |y'|$.
Nun folgt $np = x^2 + y^2 < 2\frac{p^2}{2^2} = \frac{p}{2}p$, also $n < p$.

Behauptung. *Die Zahlen x, y sind teilerfremd.*

Ein gemeinsamer Primteiler q teilt np (tasächlich sogar $q^2|np$. Die Zahl q ist als Teiler von x kleiner als $p/2$, also nur ein Teiler von n. Damit kann der Faktor aus der Gleichung gekürzt werden. Da n minimal war, gibt es diese Primteiler nicht. Insbesondere sind nicht x, y beide gerade.

Behauptung. *x und y sind nicht beide ungerade.*

Sonst ist 2 ein Teiler von n und $x \pm y$. Es gilt

$$\frac{(x+y)^2}{4} + \frac{(x-y)^2}{4} = \frac{x^2 + 2xy + y^2 + x^2 - 2xy + y^2}{4} = \frac{x^2 + y^2}{2} = \frac{n}{2}p$$

Dies ist wieder ein Widerspruch zur Minimalität. Sei l ein Primfaktor von n. Dann gilt

$$0 = x^2 + y^2 \mod l$$

Nach Lemma 5.2 ist dann $l = 1 \mod 4$. Wegen $l \leq n < p$ und der Wahl von p ist dann l als Summe von zwei Quadratzahlen zu schreiben.

$$l = u^2 + v^2$$

Dann gilt

$$\frac{n}{l}p = \frac{x^2 + y^2}{u^2 + v^2} = \left(\frac{uy + vx}{u^2 + v^2}\right)^2 + \left(\frac{ux - vy}{u^2 + v^2}\right)^2 \qquad (*)$$

Behauptung. $l|ux - vy$

Wir rechnen modulo l. Es gilt

$$0 = u^2 + v^2 = x^2 + y^2 \Rightarrow \frac{v^2}{u^2} = -1 = \frac{x^2}{y^2} \Rightarrow \frac{v}{u} = \pm\frac{x}{y}$$

Ohne Beschränkung der Allgemeinheit (ersetze x durch $-x$) gilt das Plusvorzeichen. Dann gilt

$$vy = ux \mod l$$

In der Gleichung (*) sind dann zwei Summanden ganz, also auch der dritte. Damit haben wir eine kleinere Darstellung eines Vielfachen von p als Summe von zwei Quadraten gefunden. Dies ist ein Widerspruch zur Wahl von n. Damit kann es den Primteiler l nicht geben, es gilt $n = 1$. □

Prinzipiell ist dies ein konstruktiver Beweis: man löst das Problem modulo p, liftet nach $\mathbb{Z}$. Dann muss man den Vorfaktor n verkleinern. Zuerst durch minimale Wahl von x, y in der Restklasse - dann indem man die Frage für die Primfaktoren von n löst.
Was haben die geschickten Formeln für Quadrate zu bedeuten? Wie kommt man auf den Beweis?

Moderner Beweis von Theorem 5.1. Wir rechnen in $\mathbb{Z}[i]$.

$$x^2 + y^2 = (x + iy)(x - iy) = N(x + iy)$$

Die Gleichung $p = x^2 + y^2$ ist genau dann lösbar, wenn p *kein* Primelement in $\mathbb{Z}[i]$ ist. In diesem Fall ist $x + iy$ ein Primelement.
Wir zeigen zunächst die Eindeutigkeit. Sei

$$p = x^2 + y^2 = (x + iy)(x - iy) = u^2 + v^2 = (u + iy)(u + iy)$$

Da in $\mathbb{Z}[i]$ die Eindeutigkeit der Primfaktorzerlegung gilt (Satz 2.5), sind die Faktoren eindeutig bis auf $\pm 1, \pm i$. Für ± 1 erhält man die selben Quadratzahlen. Es gilt

$$i(x + iy) = ix - y = -y + ix$$

Hier werden nur x und y vertauscht.
Nun zur Existenz. Sei $a \in \mathbb{Z}$ mit $a^2 = -1 \mod p$. (Dies gibt es, wie wir im Beweis von Lemma 5.2 nachgerechnet haben.) Sei λ der größte gemeinsame Teiler von p und $i + a$. Es gilt $N(p) = p^2$, also $N(\lambda) = 1, p, p^2$. Da p kein Teiler von $i + a$ ist, scheidet $N(\lambda) = p^2$ aus.
Ist $N(\lambda) = 1$, so ist λ eine Einheit, also ohne Einschränkung gleich 1. Nach dem Euklidischen Algorithmus lässt sich 1 als Linearkombination von p und $i + a$ schreiben:

$$1 = \alpha p + \beta(i + a)$$

Wir betrachten diese Gleichung modulo p, also

$$1 = \beta(i + a) \mod p\mathbb{Z}[i]$$

Damit ist $(i + a) \mod p$ ein Einheit. Gleichzeitig gilt aber

$$(i + a)(i - a) = 0 \mod p$$

Wir multiplizieren mit dem Inversen von $i + a$ und erhalten $i - a = 0 \mod p$. Dies ist falsch. Damit gilt tatsächlich $N(\lambda) = p$. □

Bemerkung. Auch dieser Beweis ist im Prinzip konstruktiv. Man muss jedoch ggTs in $\mathbb{Z}[i]$ berechnen.

Aufgabe 5.2. Interpretieren Sie den ersten Beweis (insbesondere die Multiplikationsformeln) in Termen von $\mathbb{Z}[i]$.

Aufgabe 5.3. Schreiben Sie die Primzahlen bis 100 als Summe von zwei Quadraten (soweit möglich). Tipp: Wahrscheinlich geht es schneller, die Summen von Quadratzahlen auszurechnen.

Aufgabe 5.4. Gehen Sie beide Beweise explizit für den Fall $p = 101$ durch. Tipp: Es gilt $10^2 = -1 \mod 101$.

Kapitel 6

Der Vierquadratesatz

Theorem 6.1 (Lagrange, Euler). *Jede natürliche Zahl ist Summe von vier Quadraten.*

Bemerkung. Hierbei zählt auch 0 als Quadrat, bzw. man benötigt höchstens vier Quadratzahlen.

Beispiel. $7 = 4 + 1 + 1 + 1$. Drei Quadrate genügen im allemeinen nicht.

Aufgabe 6.1. Schreiben Sie die Zahlen $2, \ldots, 20, 50-59, 111, 12345$ als Summe von vier Quadraten.

Aufgabe 6.2. Ist die Darstellung eindeutig?

Die Darstellung als Summe von zwei Quadraten ließ sich in Termen von $\mathbb{Z}[i]$ ausdrücken. Für vier Quadrate übernehmen die *Quaternionen* diese Rolle.
Literatur: Ebbinghaus et. al.: Zahlen, Grundwissen Mathematik 1, Springer Verlag.

Definition 6.2. *Sei* $\mathbb{H} = (\mathbb{R}^4, +, \cdot)$ *mit der komponentenweisen Addition und der Multiplikation definiert durch*

$$1x = x, i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ik = -ki = j$$

mit

$$1 = (1,0,0,0), i = (0,1,0,0), j = (0,0,1,0), k = (0,0,0,1)$$

$\mathbb{H}$ *heißt Raum der* Hamiltonschen Quaternionen *Die Abbildung* $\alpha = a + bi + cj + dk \mapsto \overline{\alpha} = a - bi - cj - dk$ *heißt* Konjugation*. Die Abbildung* $\alpha \mapsto \alpha\overline{\alpha}$ *heißt* Norm*.*

Bemerkung. Es gilt

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 - (bi + cj + dk)^2$$
$$= a^2 + b^2 + c^2 + d^2 + bc(ij + ji) + bd(ik + ki) + cd(jk + kj) = a^2 + b^2 + c^2 + d^2$$

Satz 6.3. *$\mathbb{H}$ ist ein Schiefkörper, d.h. die Körperaxiome gelten mit einer nicht-kommutativen Multiplikation. Die Konjugationsabbildung ist ein Anti-Homomorphismus, d.h. es gilt*

$$\overline{\alpha}\overline{\beta} = \overline{(\alpha\beta)}$$

Die Norm $N : \mathbb{H} \to \mathbb{R}_{\geq 0}$ ist multiplikativ. Sie erfüllt $N(\alpha) = N(\overline{\alpha})$.

Beweis: $(\mathbb{R}^4, +)$ ist eine abelsche Gruppe. Die Multiplikation ist so definiert, dass die die Distributivgesetze automatisch gelten. Zu verifizieren ist jedoch das Assoziativgesetz für die Multiplikation, z.B.

$$(ij)k = k^2 = -1, i(jk) = i^2 = -1$$

Ebenso für die anderen Erzeuger. Damit ist $\mathbb{H}$ ein nicht-kommutativer Ring mit Eins.
Wir betrachten die Konjugationsabbildung. Sie ist $\mathbb{R}$-linear. Um zu zeigen, dass sie ein Anti-Homomorphismus ist, genügt es die Basiselemente zu betrachten.

$$\overline{ij} = \overline{k} = -k, \overline{ji} = (-j)(-i) = ji = -k$$

Ebenso für alle anderen Produkte. Nach der oben angegebenen Formel ist die Norm stets reell und positiv. Sie verschwindet nur für 0. Insbesondere vertauscht $N(\beta)$ mit allen Quaternionen. Dann gilt auch

$$N(\alpha\beta) = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = \alpha\overline{\alpha}N(\beta) = N(\alpha)N(\beta)$$

Die Gleichung $N(\alpha) = N(\overline{\alpha})$ folgt entweder hieraus oder aus der expliziten Formel. Wir setzen nun

$$\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}$$

Dann folgt

$$\alpha\alpha^{-1} = \frac{N(\alpha)}{N(\alpha)} = 1, \alpha^{-1}\alpha = \frac{N(\alpha)}{N(\alpha)} = 1$$

Damit ist $\mathbb{H}$ ein Schiefkörper. □

Eine alternative Beschreibung verkürzt die Rechnungen:

$$\mathcal{H} = \left\{ \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \in M_{2\times 2}(\mathbb{C}) \right\}$$

Die ist ein reell vierdimensionaler Vektorraum. Der Raum $\mathcal{H}$ ist abgeschlossen unter Produkten und komplexer Konjugation. Es gilt

$$\det \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} = |w|^2 + |z|^2$$

Dies ist ungleich Null für alle Elemente ungleich Null. Damit ist $\mathcal{H}$ ein Schiefkörper.

Satz 6.4. *Die Abbildung $F : \mathbb{H} \to \mathcal{H}$ mit*

$$a + bi + cj + dk \mapsto \begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix}$$

ist ein Isomorphismus.

Beweis: Die Abbildung ist $\mathbb{R}$-linear. Man rechnet explizit nach, dass die Multiplikationsregeln für $1, i, j, k$ erfüllt sind. Die Bilder der Basisvektoren sind Basisvektoren, also ist die Abbildung bijektiv. □

Bemerkung. Die einzigen Schiefkörper, die endlich dimensional über $\mathbb{R}$ sind, sind $\mathbb{C}$ und $\mathbb{H}$. Alle Schiefkörper, die endlich dimensional über $\mathbb{Z}/p\mathbb{Z}$ sind, sind kommutativ. Über anderen Körpern kann es aber mehr Beispiele geben. Dies ist die Theorie der zentraleinfachen Algebren.

Nun zurück zum Thema. Sei $H_\mathbb{Z} = \mathbb{H} \cap \mathbb{Z}^4$ die Menge der ganzen Quaternionen. Dies ist ein Unterring von $\mathbb{H}$. Eine natürliche Zahl ist Summe von vier Quadraten genau dann, wenn $n = N(\alpha)$ für ein $\alpha \in \mathbb{H}_\mathbb{Z}$.

Korollar 6.5. *Seien $n, m \in \mathbb{N}$ Summen von vier Quadraten. Dann ist auch nm Summe von vier Quadraten.*

Beweis: Sei $n = N(\alpha)$, $m = N(\beta)$. Dann ist $nm = N(\alpha\beta)$. □

Aufgabe 6.3. Beweisen Sie das Korollar direkt, ohne Quaternionen zu erwähnen.

Um Theorem 6.1 zu beweisen, genügt es also Primzahlen zu betrachten. Wegen des Zweiquadratesatzes genügt es sogar Primzahlen mit $p = 3 \mod 4$ zu behandeln.

Lemma 6.6. *Sei p ein Primzahl. Dann ist*

$$x^2 + y^2 + 1 = p$$

lösbar modulo p.

Beweis: $1+0+1 = 2$ ist eine Lösung für $p = 2$. Sei nun p ungerade. Wir zählen der möglichen Werte für $x^2 \mod p$ ab: Dies $(p-1)/2$ Werte für $x \neq 0$, sowie die $0^2 = 0$. Insgesamt also $(p+1)/2$. Wir zählen nun die möglichen Werte für $-1-y^2$ ab. Dies sind genauso viele wie die möglichen Werte für y^2, also ebenfalls $(p+1)/2$. Zusammen sind dies $(p+1)$ Werte $\mod p$, also haben beide Mengen ein Element gemeinsam. Es gibt x_0 und y_0 mit $x^2 = -1 - y_0^2 \mod p$. □

Aufgabe 6.4. Jede Primzahl $p = 1 \mod 6$ ist von der Form $x^2 + 3y^2$.

Lemma 6.7. *Sei p Primzahl, $1 < m < p$ und mp Summe von vier Quadraten. Dann gibt es $0 < r < m$ mit rp Summe von vier Quadraten.*

Beweis: Sei $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Sei zunächst m gerade. Dann können wir zwei Paare von x_i, x_j von gleicher Parität bilden, etwa (x_1, x_2) und (x_3, x_4). Dann ist

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{mp}{2}$$

Mit $r = m/2$ ist die Aussage gezeigt.
Sei nun m ungerade. Nach Voraussetzung gilt

$$mp = N(\alpha)$$

wobei $\alpha = x_1 + x_2 i + x_3 j + x_4 k \in \mathbb{H}_\mathbb{Z}$. Sei $\beta = y_1 + y_2 i + y_3 j + y_4 k$ mit $|y_i| \leq m/2$ und $\beta = \alpha \mod m$ (d.h. $x_i = y_i \mod m$). Da m ungerade ist, gilt tatsächlich $|y_i| < m/2$.
Dann gilt $N(y) = N(x) \mod m$, also auch $N(y) = 0 \mod m$. Dies bedeutet konkret

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\frac{m^2}{4} = m^2$$

Also gilt $0 \leq r < m$.

Behauptung. $r \neq 0$.

Falls $r = 0$, so war m ein Teiler aller x_i, also $m^2 | N(x) = mp$. Wegen $m < p$ muss dann $m = 1$ sein. Damit scheidet diese Möglichkeit aus.
Wegen $\alpha = \beta \mod m$ ist auch

$$\alpha\overline{\beta} = \alpha\overline{\alpha} = N(\alpha) = mp = 0 \mod m$$

Daher ist $\gamma = \frac{\alpha\overline{\beta}}{m} \in \mathbb{H}_\mathbb{Z}$. Dann gilt

$$N(\gamma) = \frac{N(\alpha)N(\overline{\beta})}{m^2} = \frac{mprm}{m^2} = rp$$

wie behauptet. □

Beweis von Theorem 6.1. Nach Lemma 6.5 genügt es, die Aussage für Primzahlen zu zeigen. Sei also p Primzahl. Nach Lemma 6.6 gibt es x, y, m mit

$$x^2 + y^2 + 1 = mp$$

Dabei kann $|x|, |y| < p/2$ gewählt werden. Dann folgt

$$x^2 + y^2 + 1 < 2\frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2$$

da $2 < p^2$. Also gilt $0 < m < p$. Falls $m = 1$, so sind wir fertig. Andernfalls können wir nach Lemma 6.7 m durch $r < m$ ersetzen. Nach endlich vielen Schritten endet das Verfahren. □

Bemerkung. Eigentlich braucht man die Quaternionen für den Beweis nicht - sie erleichtern aber das Hinschreiben der Formeln ganz erheblich!

Kapitel 7

$x^3 + y^3 = z^3$

Theorem 7.1. *Die Gleichung $x^3+y^3 = z^3$ hat in $\mathbb{Z}$ nur die trivialen Lösungen mit $xy = 0$.*

1. Fall: Es gibt keine Lösungen 1. Art, d.h. mit $3 \nmid xyz$.

Beweis: Wir betrachten die Gleichung $\mod 3$ und $\mod 9$. Wenn $x = \pm 1 \mod 3$, dann gilt

$$x^3 = (\pm 1 + 3t)^3 = (\pm 1)^3 + 3 \cdot 3t + 3 \cdot +(\pm 1)^2 9t^2 + 27t^3 = 1 \mod 9$$

Damit ergibt sich

$$x^3 + y^3 = \pm 1 \pm 1 = \begin{cases} 2 \\ 0 \\ -2 \end{cases} \mod 9$$

Andererseits ist $z^3 = \pm 1 \mod 9$. Dies ist ein Widerspruch. □

Bemerkung. Auch für andere Primzahlen ist der Fall 1. Art einfacher als der allgemeine!

Aufgabe 7.1. Zeigen Sie, dass $x^5 + y^5 = z^5$ keine Lösungen 1. Art hat. (Vorsicht, schwer.)

2. Fall: $3 \mid xyz$. Da die Gleichung homogen ist, können wir ohne Einschränkung annehmen, dass x, y, z paarweise teilerfremd sind. Wegen

$$0 = x^3 + y^3 + (-z)^3$$

ist es egal, welche der drei Zahlen durch 3 teilbar ist. Ab jetzt:

$$3 \mid z$$

Sei wie früher $\varrho = \mathrm{e}^{2\pi/3}$. Wir rechnen in $\mathbb{Z}[\varrho]$. Hier gilt

$$x^3 + y^3 = (x + y)(x + \varrho y)(x + \varrho^2 y) = z^3$$

denn das Polynom $X^3 + y^3$ hat die Nullstellen $-y, -\varrho y, -\varrho^2 y$. Nach Satz 2.5 ist der Ring $\mathbb{Z}[\varrho]$ faktoriell. Wir können nun mit Teilbarkeitsargumenten in dem Produkt arbeiten. Wir erinnern uns:

$$\mathbb{Z}[\varrho]^* = \{\pm 1, \pm\varrho, \pm\varrho^2\}$$

Sei $\lambda = 1 - \varrho$. Dann gilt

$$N(\lambda) = (1 - \varrho)(1 - \overline{\varrho}) = (1 - \varrho)(1 - \varrho^2) = 1 - \varrho - \varrho^2 + \varrho^3 = 1 + 1 + 1 = 3$$

da $\varrho + \varrho^2 = -1$. Daher ist λ ein Primelement, ein Primteiler von 3. Es gilt

$$1 - \varrho^2 = \varrho^{-1}(\varrho - \varrho^3) = -\varrho 2(1 - \varrho) = -\varrho^2\lambda$$

Die Primfaktorzerlegung der 3 ist also

$$3 = -\varrho^2\lambda^2$$

Statt modulo 3 und 9 rechnen wir nun modulo λ und λ^2.

Lemma 7.2. *Sei $x \in \mathbb{Z}[\varrho]$ mit $\lambda \nmid x$. Dann gilt*

$$x^3 = \pm 1 \mod \lambda^4$$

Die 6 Einheiten von $\mathbb{Z}[\varrho]$ sind verschieden modulo λ^2.

Beweis: Es gilt $\lambda = 1 - \varrho$, also $1 = \varrho \mod \lambda$. Jede Restklasse modulo λ wird also von einer ganzen Zahlen vertreten. Wegen $3 = -\varrho^3\lambda^2$ gilt $3 = 0 \mod \lambda$. Damit gibt es nur drei Restklassen modulo λ, nämlich die Restklassen von 0 und ± 1. Diese sind auch tatsächlich verschieden, da λ weder 1 noch 2 teilt.
Nach Voraussetzung ist $x \neq 0 \mod \lambda$, also $x = \pm 1 \mod \lambda$. Sei also zunächst

$$x = 1 + \lambda t \text{ für ein } t \in \mathbb{Z}[\varrho]$$

Dann gilt

$$\begin{aligned} x^3 - 1 = (x - 1)(x - \varrho)(x - \varrho^2) &= \lambda t(1 - \varrho + \lambda t)(1 - \varrho^2 + \lambda t) \\ &= \lambda t(\lambda + \lambda t)(-\varrho^2\lambda + \lambda t) = \lambda^3 t(1 + t)(-\varrho^2 + t) \end{aligned}$$

Zu zeigen bleibt, dass einer der Faktoren durch λ teilbar ist. Wegen $\varrho = 1 \mod \lambda$ ist $-\varrho^2 = -1 \mod \lambda$. Damit sind die drei Faktoren modulo λ gleich $t, t + 1, -1 + t$. Einer von ihnen ist durch λ teilbar. Der Fall $x = -1 + \lambda t$ folgt genauso.
Wegen $\varrho = 1 - \lambda$ ist $\pm\varrho \neq \pm 1 \mod \lambda^2$. Wegen $\varrho^2 = (1-\lambda)^2 = 1 - 2\lambda \mod \lambda^2$ gilt auch $\pm\varrho^2 \neq \pm 1 \mod \lambda^2$. Keine zwei dieser Zahlen sind gleich modulo λ^2. □

Aufgabe 7.2. Bestimmen Sie die Restklassen von $2, 3, 4, 5, 6, 7, 8$ modulo $\lambda, \lambda^2, \lambda^3$.

Satz 7.3. *Sei $u \in \mathbb{Z}[\varrho]^*$. Dann ist die Gleichung*

$$u(\lambda z)^3 = x^3 + y^3 = (x + y)(x + \varrho y)(x + \varrho^2 y)$$

unlösbar in $\mathbb{Z}[\varrho]$.

Korollar 7.4. *Die Fermatsche Gleichung für $n = 3$ hat keine Lösung 3. Art.*

Beweis: Sei $x^3 + y^3 = z^3$ mit $3|z$. Dann ist λ ein Teiler von z in $\mathbb{Z}[\varrho]$. Das Tripel $x, y, z/\lambda$ ist eine Lösung der Gleichung des Satzes mit $u = 1$. Dies ist unmöglich. □

Beweis des Satzes. Sei x, y, z eine Lösung in $\mathbb{Z}[\varrho]$. Ohne Einschränkung sind die drei Zahlen paarweise teilerfremd. Sei π ein gemeinsamer Teiler von $x + y$ und $x + \varrho y$. Dann gilt

$$\pi \mid x + y - x - \varrho y = y(1 - \varrho) = y\lambda$$

Wäre π ein Teiler von y, dann auch von x. Dies ist ein Widerspruch. Also ist $\pi|\lambda$. Da λ ein Primelement ist, stimmen dann π und λ bis auf Einheit überein. Genauso argumentiert man für die anderen Paare von Faktoren: der einzige mögliche gemeinsame Teiler ist jeweils λ. Die Rechnung zeigt aber auch: Ist einer der Faktoren durch λ teilbar, dann alle drei.
Sei $\lambda^n|z$, aber $\lambda^{n+1} \nmid z$. Nach Voraussetzung gilt dann

$$\lambda^{3n+3} \mid x^3 + y^3 = (x + y)(x + \varrho y)(x + \varrho^2 y)$$

Also teilt λ einen der Faktoren - nach der Vorüberlegung dann alle drei. Nur höchstens einer der Faktoren wird jedoch von λ^2 geteilt. Also gilt (ohne Einschränkung) $\lambda^{3n+1}|x + y$. Alle anderen Primfaktoren von z können nur einen der Faktoren teilen, tauchen dort also in Dreierpotenzen auf. Damit können wir schreiben

$$x + y = u_1\lambda^{3n+1}\alpha^3, x + \varrho y = u_2\lambda\beta^3, x + \varrho^2 y = u_3\lambda\beta^3$$

mit Einheiten $u_i \in \mathbb{Z}[\varrho]^*$ und $\lambda \nmid \alpha, \beta, \gamma$.
Es folgt

$$\begin{aligned}(x + y) + \varrho(x + \varrho y) + \varrho^2(x + \varrho^2 y) = x + \varrho x + \varrho^2 x + y + \varrho y + \varrho^2 y = 0 \\ = u_1\lambda^{3n+1}\alpha^3 + \varrho u_2\lambda\beta^3 + \varrho^2 u_3\lambda\gamma^3\end{aligned}$$

Kürzen liefert dann

$$u_1\lambda^{3n}\alpha^3 + \varrho u_2\beta^3 + \varrho^2 u_3\gamma^3 = 0$$

bzw.

$$u'(\lambda\lambda^{n-1}\alpha)^3 = \varepsilon_1\beta^3 + \gamma^3$$

mit neuen Einheiten $u', \varepsilon \in \mathbb{Z}[\varrho]^*$. Dies fast eine Lösung unserer Gleichung, nur ε stört. Wir betrachten die Gleichung modulo λ^2. Wegen Lemma 7.2 lautet sie

$$0 = \varepsilon(\pm 1) \pm 1 \mod \Leftrightarrow \varepsilon = \pm 1 \lambda^2$$

Wegen $\varrho = 1 - \lambda$ ist $\pm\varrho \neq \pm 1 \mod \lambda^2$. Nach Lemma 7.2 gilt dann auch $\varepsilon = \pm 1$ in $\mathbb{Z}[\varrho]$. Dieses Vorzeichen kann in β aufgenommen worden und wir haben eine neue Lösung der Gleichung gefunden.

$$u'(\lambda z')^3 = (x')^3 + (y')^3$$

doch nun wird z' nur noch von λ^{n-1} geteilt. Wir iterieren das Verfahren, bis wir zu einer Lösung kommen mit $\lambda \nmid x, y, z$. Diese Gleichung betrachten wir modulo λ^4. Nach Lemma 7.2 gilt

$$u\lambda^3(\pm 1) = \pm 1 \pm 1 = \begin{cases} 0 \\ \pm 2 \end{cases} \mod \lambda^4$$

Der Fall 0 scheidet sofort aus. λ ist kein Teiler von 2, $N(\lambda) = 3 \nmid N(2) = 4$. Damit ist auch der zweite Fall unmöglich. Dies ist der gesuchte Widerspruch. □

Bemerkung. Für allgemeine Primzahlen scheitert dieser Beweis daran, dass $\mathbb{Z}[\zeta]$ ($\zeta^p = 1$) kein faktorieller Ring ist. Genaueres Hinsehen zeigt, dass man das nicht ganz braucht, und so liefert das Argument weitere Fälle. In den letzten dreihundert Jahren wurde es immer weiter verfeinert - zum vollständigen Beweis reicht es bis heute (auf diesem Weg) nicht.

Aufgabe 7.3. Bestimmen Sie alle Lösungen von $x^2 + y^2 = z^2$ in $\mathbb{Z}[i]$.

Literatur: G.H. Hardy, E.M. Wright: An Introduction to the Theory of Numbers, Oxford 1938.
E. Landau: Vorlesungen über Zahlentheorie, Leipzig 1927.

Kapitel 8

Die Pellsche Gleichung

Die Pellsche Gleichung lautet

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

Für $d < 0$ ist dies sehr übersichtlich:

- $d = -1$: $x^2 + y^2 = 1$ hat die Lösungen $(\pm 1, 0), (0, \pm 1)$.
- $d < -1$: Nur die Lösung $(\pm 1, 0)$.
- $d = 1$: $1 = x^2 - y^2 = (x - y)(x + y)$ hat die Lösungen $(\pm 1, 0)$.

Also ab jetzt: $d > 1$ (in $\mathbb{Z}$). Ist d Quadratzahl, so ist $(x, \sqrt{d}y)$ Lösung von $X^2 - Y^2 = 1$, also $X = x = \pm 1$, $y = 0$. Daher ab jetzt: d **keine Quadratzzahl**

Beispiel.

- $2^2 - 3 \cdot 1^2 = 1$ Lösung für $d = 3$.
- $19^2 - 10 \cdot 6^2 = 401 - 40 - 10 \cdot 36 = 1$ für $d = 10$.
- $10^2 - 11 \cdot 3^2 = 100 - 99 = 1$ für $d = 11$.
- $649^2 - 13 \cdot 180^2 = 421201 - 42200 = 1$ für $d = 13$.
- $15^2 - 14 \cdot 4^2 = 225 - 224 = 1$ für $d = 14$.
- ...

Aufgabe 8.1. Suchen Sie Lösungen für $d = 12$ und $d = 15$.

Tatsächlich ist die Gleichung immer lösbar! Aber das Lösungsverhalten ist erratisch. Wir faktorisieren:

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

gesucht sind also Einheiten in $\mathbb{Z}[\sqrt{d}]$. Sei wieder

$$N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}, x + \sqrt{d}y \mapsto (x + \sqrt{d}y)(x - \sqrt{d}y) = x^2 - dy^2$$

Diese Normabbildung ist multiplikativ, da auch die Konjugationsabbildung

$$\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}, x + \sqrt{d}y \mapsto x - \sqrt{d}y$$

multiplikativ ist.

Bemerkung. Dies ist nicht die komplexe Konjugation, sondern das nicht-triviale Element von $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Anders als im imaginärquadratischen Fall ($d < 0$) kann die Norm auch negative Werte annehmen.

Korollar 8.1. *Lösungen von $x^2 - dy^2 = 1$ entsprechen Zahlen $x + \sqrt{d}y$ mit Norm 1.*

Dies sagt uns zwar nicht, warum es Lösung gibt, aber er verät uns Eigenschaften des Lösungsraumes:

Korollar 8.2. *Seien $\alpha = x + \sqrt{d}y$, $\alpha' = x' + \sqrt{d}y'$ Elemente mit Norm 1 in $\mathbb{Z}[\sqrt{d}]$. Dann hat auch*

$$\alpha\alpha' = (x + \sqrt{d}y)(x' + \sqrt{d}y') = xx' + dyy' + (xy' + x'y)\sqrt{d}$$

eine Norm 1, d.h. auch $(xx' + dyy', xy' + x'y)$ löst die Pellsche Gleichung.

Diese Einheiten bilden eine Gruppe.

Aufgabe 8.2. Bestimmen Sie die Einheiten von $\mathbb{Z}[\sqrt{d}]$ für $d < 0$ quadratfrei.

Korollar 8.3. *Sei $x^2 - dy^2 = 1$ lösbar mit $y \neq 0$. Dann gibt es unendlich viele Lösungen.*

Beweis: Ohne Einschränkung ist $x, y > 0$, also $x + \sqrt{d}y > 1$ in $\mathbb{R}$. Mit $x + \sqrt{d}y$ sind auch alle $(x + \sqrt{d}y)^n$ Einheiten. Wegen $(x + \sqrt{d}y)^{n+1} > (x + \sqrt{d}y)^n$ sind dies lauter verschiedene Lösungen. □

Definition 8.4. *Sei $\varphi = x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]^*$ mit $x > 0, y > 0$ mit minimalem Betrag (äquivalent: mit x minimal). Dann heißt (x, y)* Fundamentallösung.

Wenn die Pellsche Gleichung nicht-trivial lösbar ist (noch nicht gezeigt), dann gibt es auch eine Fundamentallösung.

Satz 8.5. *Sei (x, y) eine Fundamentallösung. Dann entsprechen die Lösungen der Pellschen Gleichung genau den Zahlen $\pm(x + \sqrt{d}y)^n$ mit $n \in \mathbb{Z}$.*

Beweis: Sei $\alpha = a + \sqrt{d}b$ eine Einheit, dann ist auch $-\alpha$ Einheit. Es ist

$$(a - \sqrt{d}b) = (a + \sqrt{d}b)^{-1}, -a + \sqrt{d}b = (-a - \sqrt{d}b)^{-1}$$

Alle Vorzeichenkombinationen kommen also vor. Der Fall $a = 0$ kommt nicht vor. Für $b = 0$ ist $a = \pm 1$, dies entspricht $n = 0$. Also genügt es $a, b > 0$ zu betrachten, also $\alpha \geq 1$.

Behauptung. $\alpha = (x + \sqrt{d}y)^n$ *mit* $n \in \mathbb{N}$.

Die Potenzen von φ werden beliebig groß. Daher gibt es eine natürliche Zahl n mit

$$\varphi^n \leq \alpha < \varphi^{n+1} \Rightarrow 1 \leq \frac{\alpha}{\varphi^n} < \varphi$$

φ^n ist eine Einheit in $\mathbb{Z}[\sqrt{d}]$, also ist $\alpha\varphi^{-n} \in \mathbb{Z}[\sqrt{d}]^*$. Da φ minimal war, folgt

$$1 = \frac{\alpha}{\varphi^n} \Rightarrow \alpha = \varphi^n$$

□

Damit bleibt die interessanteste Frage übrig:

Theorem 8.6. *$x^2 - dy^2$ hat eine Lösung ungleich $(\pm 1, 0)$.*

Zunächst:

Lemma 8.7. *Sei $\alpha \in \mathbb{R}$, $m \in \mathbb{N}$. Dann gibt es $x, y \in \mathbb{Z}$ mit $0 < y \leq m$, so dass*

$$|x - \alpha y| < \frac{1}{m}$$

Beweis: Für $v = 0, \ldots, m$ setzen wir jeweils $u = [\alpha v] + 1$. Hierbei ist $[\cdot]$ die Gauß-Klammer, d.h. es gilt

$$\alpha v - 1 < [\alpha v] \leq \alpha v \Rightarrow \alpha v < u \leq \alpha v + 1 \Rightarrow 0 < u - \alpha v \leq 1$$

Wir haben $m + 1$ Zahlen in $(0, 1]$ konstruiert. Daher liegen in einem der m Teilintervalle $(\frac{h}{m}, \frac{h+1}{m}$ zwei der Zahlen. Es gibt also $v_1 \neq v_2$ mit zugehörigen u_1, u_2, so dass

$$|(u_1 - \alpha v_1) - (u_2 - \alpha v_2)| \leq \frac{1}{m}$$

Wir setzen $x = u_1 - u_2, y = v_1 - v_2$. □

Lemma 8.8. *Die Ungleichung*

$$|x - y\sqrt{d}| < \frac{1}{y}$$

hat unendlich viele Lösungen.

Beweis: Wir setzen $\alpha = \sqrt{d}$, $m = 1$ im Lemma 8.7. Dann gibt es x, y mit $0 < y \leq 1$ (also $y = 1$) mit $|x - \sqrt{d}| < 1$ (nämlich $x = [\sqrt{d}]$). Die ist eine Lösung der Ungleichung.

Behauptung. *Zu jeder Lösung gibt es eine kleinere.*

Sei (x, y) eine Lösung. Wähle m mit

$$\frac{1}{m} < |x - y\sqrt{d}||$$

Dies ist möglich, da $\sqrt{d} \notin \mathbb{Q}$. Nach Lemma 8.7 gibt es x', y' mit

$$|x' - \sqrt{d}y'| < \frac{1}{m} < |x - y\sqrt{d}|$$

Hierbei ist $y' \leq m$, also $1/m \leq 1/y'$. □

Satz 8.9. *Zu gegebenen d gibt es $k \neq 0$, so dass $x^2 - dy^2 = k$ unendlich viele Lösungen x, y hat.*

Beweis: Wir betrachten $x \in \mathbb{Z}$, $y \in \mathbb{N}$ mit $|x + \sqrt{d}y| < 1/y$. Dann folgt

$$|x - \sqrt{d}y| = |x + \sqrt{d}y - 2\sqrt{d}y| < \frac{1}{y} + 2y\sqrt{d} \leq y + 2\sqrt{d}y = (1 + 2\sqrt{d})y$$

Hieraus folgt

$$0 < |x^2 - dy^2| = |(x + \sqrt{d}y)(x - \sqrt{d}y)| < \frac{(1 + 2\sqrt{d})y}{y} = 1 + 2\sqrt{d}$$

D.h. wir haben für jedes Paar (x, y) aus Lemma 8.8 gilt $x^2 - dy^2 = k$ mit $0 < k < 1 + 2\sqrt{d}$. Da es unendlich viele Paare gibt, kommt auch eines der k unendlich oft vor. □

Beweis des Theorems. Wir betrachten die unendlich vielen positiven Lösungen von $x^2 - dy^2 = k$. Die Paare (x, y) verteilen sich auf die verschiedenen Restklassen modulo k. In einer dieser Klassen liegen zwei Elemente, also $x = x' \mod k$, $y = y' \mod k$ und

$$x^2 - dy^2 = (x')^2 - d(y')^2 = k$$

Wir betrachten

$$\alpha = \frac{(x + \sqrt{d}y)(x' - \sqrt{d}y')}{k}$$

Dieses Element hat $N(\alpha) = \frac{kk}{k^2} = 1$.

Behauptung. $\alpha \in \mathbb{Z}[\sqrt{d}]$

Nach Voraussetzung $x + \sqrt{d}y = x' + \sqrt{d}y' + k(a + b\sqrt{d})$ mit $a, b \in \mathbb{Z}$. Daher ist

$$\alpha = \frac{(x' + \sqrt{d}y')(x' - \sqrt{d}y')}{k} + \frac{k(a + b\sqrt{d})(x' - \sqrt{d}y')}{k} = 1 + (a + b\sqrt{d})(x' - \sqrt{d}y')$$

Behauptung. $\alpha \neq \pm 1$

Wäre $\alpha = \pm 1$, so hätten wir $\pm k = (x + \sqrt{d}y)(x' - \sqrt{d}y')$. Andererseits gilt $k = (x + \sqrt{d}y)(x - \sqrt{d}y)$, daher folgt $x - \sqrt{d}y = \pm(x' - \sqrt{d}y')$. Dies bedeutet $x = \pm x'$, $y = \pm y'$. Wegen $x, x', y, y' \geq 0$ sind dann die Paare gleich. □

Aufgabe 8.3. (i) Sei $d \in \mathbb{Z}$ quadratfrei, $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $\overline{\alpha} = x - y\sqrt{d}$. Zeigen Sie: $P_\alpha(X)(X - \alpha)(X - \overline{\alpha})$ hat Koeffizienten in $\mathbb{Q}$.

(ii) Betrachten Sie

$$R_d = \{\alpha \in \mathbb{Q}(\sqrt{d}) \mid P_\alpha(X) \in \mathbb{Z}[X]\}$$

Zeigen Sie, dass R ein Ring ist, der $\mathbb{Z}[\sqrt{d}]$ enthält.

(iii) Sei wie vorher $\varrho = exp(2\pi i/3)$. Zeigen Sie $\varrho \in \mathbb{Q}(\sqrt{-2})$. Zeigen Sie dann $R_{-2} = \mathbb{Z}[\varrho] \neq \mathbb{Z}[\sqrt{-2}]$.

(iv) Für welche d gilt $R_d = \mathbb{Z}[\sqrt{d}]$?

(v) Bestimmen Sie die Einheiten von R_d.

Kapitel 9

Kettenbrüche

Definition 9.1. *Seien $\alpha_1, \alpha_2 \ldots, \alpha_n \in \mathbb{R}_{\geq 1}$. Wir setzen*

$$[\alpha_1, \ldots, \alpha_n] = \alpha_1 + \frac{1}{\alpha_2 + \frac{1}{\alpha_3 + \ldots \frac{1}{\alpha_{n-1} + \frac{1}{\alpha_n}}}}$$

Dies ist ein endlicher Kettenbruch. *Für eine Folge $\alpha_1, \alpha_2 \ldots$ steht $[\alpha_1, \alpha_2, \ldots]$ für die Folge der endlichen Kettenbrüche $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ bzw. deren Grenzwert. Für $x \in \mathbb{R}_{\geq 1}$ heißt $[a_1, a_2, \ldots]$* Kettenbruchentwicklung, *falls $a_i \in \mathbb{N}$ und $x = [a_1, a_2, \ldots]$. Dabei kann die Folge der a_i endlich oder unendlich sein.*

Bemerkung. Eigentlich interessieren uns nur $\alpha_i \in \mathbb{N}$, aber es hat technische Vorteile, auch $\alpha_i \in \mathbb{R}_{\geq 1}$ zu erlauben.

Rechenregeln:

(i) $[\alpha_1, \ldots, \alpha_n] = \alpha_1 + \frac{1}{[\alpha_2, \ldots, \alpha_n]}$ Insbesondere ist $[\alpha_1, \ldots, \alpha_n] > 1$ (einzige Ausnahme: $n = 1$, $\alpha_1 = 0$).

(ii) $[\alpha_1, \ldots, \alpha_n] = [\alpha_1, \ldots, \alpha_{n-1} + \frac{1}{\alpha_n}]$

Die Kettenbruchentwicklung wird durch den folgenden Algorithmus bestimmt:

(i) Sei $x \in \mathbb{R}_{\geq 1}$, $a_1 = [x_1]$ (Gauß-Klammer)

(ii) $x = [a_1, x_2] = a_1 + \frac{1}{x_2}$, d.h. $x_2 = (x - a_1)^{-1} > 1$ da $0 \leq x - a_1 < 1$. Sei $a_2 = [x_2]$.

(iii) $x = [a_1, a_2, x_3]$ mit $x_3 = (x_2 - a_2)^{-1} > 1$

(iv) etc.

Das Verfahren bricht ab, falls $x_i = a_i$ ganz.

Korollar 9.2. *$x \in \mathbb{R}_{\geq 1}$ wird genau dann durch eine endlichen Kettenbruch dargestellt, wenn $x \in \mathbb{Q}_{\geq 1}$.*

Beweis: Ist $x = [a_1, \ldots, a_n]$ mit $a_i \in \mathbb{N}$, so ist x rational.
Sei umgekehrt $x = \frac{y_0}{y_1} \in \mathbb{Q}_{\geq 1}$, $y_i \in \mathbb{N}$ teilerfremd. Wir wenden den Algorithmus auf x an. Es gilt

$$\frac{y_0}{y_1} = a_1 + \frac{y_2}{y_1} \Leftrightarrow y_0 = a_1 y_1 + y_2$$

mit $a_i \in \mathbb{N}$, $0 \leq y_2 < y_1$. Für $x_2 = \frac{y_2}{y_1}$ erhalten wir

$$\frac{y_2}{y_1} = a_2 + \frac{y_3}{y_2} \Leftrightarrow y_2 = a_2 y_2 + y_3$$

mit $a_2 \in \mathbb{N}$, $0 \leq y_3 < y_2$. D.h. der Kettenbruchalgorithmus ist der Euklidische Algorithmus. Er endet nach endlich vielen Schritten. □

Aufgabe 9.1. Bestimmen Sie die Kettenbruchentwicklung von $3/2, 5/4, 7777/123$.

Wie steht es mit der Eindeutigkeit?

$$a_1 + \frac{1}{a_2 + \frac{1}{1}} = [a_1, a_2, 1] = [a_1, a_2 + 1]$$

Lemma 9.3. *Sei $[a_1, \ldots, a_n] = [b_1, \ldots b_m]$ mit $a_i, b_j \in \mathbb{N}$, $a_n, b_m \neq 1$. Dann gilt $n = m$ und $a_i = b_i$ für alle i.*

Beweis: Sei $n \leq m$. Wir argumentiren mit Induktion nach n. $n = 1$. $a_1 = b_1 + \frac{1}{[b_2, \ldots, b_m]}$. Wegen $[b_2, \ldots, b_m] > 1$ ist der Kehrwert echt kleiner als 1, d.h. die rechte Seite ist nicht ganz, die linke schon. Dieser Widerspruch impliziert $m = 1$, d.h. der gebrochene Anteil ist nicht da.
$n > 1$ Es gilt

$$x = [a_1, \ldots, a_n] = a_1 + \frac{1}{[a_2, \ldots, a_n]} = b_1 + \frac{1}{[b_2, \ldots, b_m]}$$

Die Kehrwerte sind jeweils kleiner als 1, also $a_1 = b_1 = [x]$. Dann folgt

$$[a_2, \ldots, a_n] = [b_2, \ldots, b_m]$$

und nach Induktionsannahme $n = m$, $a_i = b_i$ für $i = 2, \ldots, n$. □

Ab jetzt betrachten wir nur noch irrationale x.

Beispiel. $x = \sqrt{s} = 1,4\ldots$. Es ist

(i) $a_1 = 1$, $x_1 = (\sqrt{2} - 1)^{-1} = \frac{\sqrt{2}+1}{2-1} = 2,4\ldots$

(ii) $a_2 = 2$, $x_2 = (\sqrt{2} + 1 - 2)^{-1} = (\sqrt{2} - 1)^{-1}$

Die Kettenbruchentwicklung ist $[1, 2, 2, \ldots]$.

Aufgabe 9.2. Berechnen Sie die Kettenbruchentwicklung von $\sqrt{5}$, $\sqrt{7} + 3/2$, $\sqrt[3]{2}$

Beispiel. Sei $x = \pi = 3.1416$:

(i) $a_1 = 3$, $x_1 = (\pi - 3)^{-1} = 7,0625\ldots$

(ii) $a_2 = 7$, $x_2 = 15,99\ldots$

Die Kettenbruchentwicklung beginnt $[3, 7, 15, \ldots]$. Die zugehörigen endlichen Kettenbrüche sind

$$3, [3, 7] = 3 + \frac{1}{7} = \frac{22}{7} = 3,1429\ldots,$$
$$[3, 7, 15] = 3 + \frac{1}{7 + \frac{1}{15}} = 3 + \frac{1}{106} = \frac{318 + 15}{106} = \frac{333}{7106} = 3,1415\ldots$$

Aufgabe 9.3. Berechnen Sie zwei weitere Terme der Kettenbruchentwicklung von π (Vorsicht mit der Genauigkeit des Taschenrechners!) Berechnen Sie den Beginn der Kettenbruchentwicklung von e.

Wie steht es mit der Konvergenz? Dafür müssen wir die Kettenbrüche rational machen.

Beispiel.

$$[1, 1, 1] = 1 + \frac{1}{2} = \frac{2+1}{2} = \frac{3}{2}$$
$$[1, 1, 1, 1] = 1 + \frac{1}{\frac{3}{2}} = 1 + \frac{2}{3} = \frac{5}{3}$$
$$[1, 1, 1, 1, 1] = 1 + \frac{3}{5} = \frac{8}{5}$$

Offensichtlich: $[1, \ldots, 1] = \frac{F_n}{F_{n-1}}$ mit $F_0 = 2$, $F_1 = 3$, $F_n = F_{n-1} + F_{n-2}$ die Folge der *Fibonacci-Zahlen.*

Allgemein:

Satz 9.4. *Seien* $\alpha_1, \alpha_n \in \mathbb{R}_{\geq 1}$. $p_0 = 1, p_1 = \alpha_1$,

$$p_n = \alpha_n p_{n-1} + p_{n-2}$$

$q_1 = 1, q_2 = \alpha_2$,

$$q_n = \alpha_n q_{n-1} + q_{n-2}$$

Dann gilt

$$[\alpha_1, \ldots, \alpha_n] = \frac{p_n}{q_n}$$

Beweis: Induktion. Für $n = 1$:

$$\frac{p_1}{q_1} = \frac{\alpha_1}{1} = [\alpha_1]$$

Für $n = 2$:

$$\frac{p_2}{q_2} = \frac{\alpha_2\alpha_1 + 1}{\alpha_2} = \alpha_1 + \frac{1}{\alpha_2} = [\alpha_1, \alpha_2]$$

Allgemein $n \geq 2$: $[\alpha_1, \ldots, \alpha_{n+1}] = [\alpha_1, \ldots, \alpha_n + \frac{1}{\alpha_{n+1}}]$. Seien p'_i, q'_i die Folgen zu diesem kürzeren Kettenbruch. Es ist $p_i = p'_i$ und $q_i = q'_i$ für $i <$. Nach Induktionsvorraussetzung gilt dann

$$\begin{aligned}
[\alpha_1 \ldots, \alpha_n + \frac{1}{\alpha_{n+1}}] &= \frac{p'_n}{q'_n} \\
&= \frac{(\alpha_n + \frac{1}{\alpha_{n-1}})p_{n-1} + p_{n-2}}{(\alpha_n + \frac{1}{\alpha_{n-1}})q_{n-1} + q_{n-2}} \\
&= \frac{p_i + \frac{1}{\alpha_{n+1}}p_{n-1}}{q_i + \frac{1}{\alpha_{n+1}}q_{n-1}} \\
&= \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}
\end{aligned}$$

□

Satz 9.5. *Jeder Kettenbruch konvergiert. Ist $a_1, a_2, \cdots \in \mathbb{N}$ die Kettenbruchentwicklung von $x \in \mathbb{R}_{\geq 1}$, dann gilt $x = [a_1, a_2, \ldots]$.*

Beweis: Sei $r_n = \frac{p_n}{q_n}$ mit p_n, q_n wie in Satz 9.4. Dann gilt

$$r_n - r_{n-1} = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n q_{n-1} - p_{n-1}q_n}{fracq_n q_{n-1}}$$

Behauptung. $p_n q_{n-1} - p_{n-1}q_n = (-1)^n$

Induktion nach n: Für $n = 2$:

$$p_2 q_1 - p_1 q_2 = (a_1 a_2 + 1)1 - a_1 a_2 = 1$$

und allgemein

$$p_{n+1}q_n - p_n q_{n+1} = (a_{n+1}p_n + p_{n-1})q_n - p_n(a_{n+1}q_n + q_{n-1}) = p_{n-1}q_n - p_n q_{n-1} = -(-1)^n$$

Die q_n streben gegen Unendlich. Die Differenzen der Folgenglieder r_n bilden eine alternierende Nullfolge, also ist die Folge konvergent.
Sei nun $x \in \mathbb{R}_{\geq 1}$, $[a_1, a_2, \ldots]$ die Kettenbruchentwicklung, also

$$x = [a_1, \ldots, a_n, x_{n+1}]$$

Wir betrachten die Folge der p_i, q_i für diesen Kettenbruch und erhalten

$$x = \frac{p_{n+1}}{q_{n+1}}, [a_1, \ldots, a_n] = \frac{p_n}{q_n}$$

Also folgt

$$x - [a_1, \ldots, a_n] = \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = (-1)^{n+1}\frac{1}{q_{n+1}q_n}$$

Explizit $q_{n+1} = x_{n+1}q_n + q_{n+1}$, also

$$|x - [a_1, \dots, a_n]| < \frac{1}{q_n^2}$$

q_n hängt nur von $a_1, \dots, a_n$ vor, kommt also auch in der Folge für den unendlichen Kettenbruch vor. Wegen $q_n \to \infty$ gilt $[a_1, \dots, a_n] \to x$. □

Beispiel. Sei $x = [1, 1, \dots]$. Nach dem Satz ist dies die Kettenbruchentwicklung von x. Es gilt

$$x = [1, x] = 1 + \frac{1}{x} \Leftrightarrow x^2 = x + 1 \Leftrightarrow x^2 - x - 1 = 0$$

Diese Gleichung hat die Lösungen $\pm\frac{\sqrt{5}}{2} + \frac{1}{2}$. Wegen $x > 1$ kommt nur $x = \frac{\sqrt{5}}{2} + \frac{1}{2}$ in Frage. Diese Zahl heißt *goldener Schnitt*. Es gilt $\frac{x}{1} = \frac{x+1}{x}$. Die Strecke der Länge $x + 1$ wird von x geteilt wie x zum Rest. Es gilt $\frac{F_n}{F_{n-1}} \to x$.

Aufgabe 9.4. Berechnen Sie den Grenzwert von $[2, 2, 2, \dots]$.

Aufgabe 9.5. Zeigen Sie, dass alle Fibonacci-Zahlen F_n teilerfremd sind. Wieviele Schritte braucht der euklidische Algorithmus? Seien $F_n a > b \in \mathbb{N}$. Zeigen Sie, dass die Laufzeit des euklidischen Algorithmus gegen diese Zahl abgeschätzt werden kann.

Der Beweis hat mehr gezeigt:

Korollar 9.6. *Ist $\frac{p_n}{q_n} = [a_1, \dots, a_n]$ in der Kettenbruchentwicklung von x, so gilt*

$$|x - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$$

Beispiel. $|\pi - \frac{22}{7}| < 1/49$, $|\pi - \frac{333}{106}| < 106^{-1} < 1/10.000$ Zum Vergleich: $3,14 = \frac{314}{100}$ ist bis aus $1/100$ genau!

Kettenbrüche konvergieren sehr schnell, viel besser geht es nicht.

Satz 9.7. *Sei $\theta \in \mathbb{R}_{\geq 1}$ irrational, $a, b \in \mathbb{N}$ mit*

$$|\theta - \frac{a}{b}| < \frac{1}{2b^2}$$

Dann kommt a/b in der Kettenbruchentwicklung von θ vor.

Beweis: Ohne Einschränkung sind a, b teilerfremd. Sei q_m die Folge der Nenner der Kettenbruchentwicklung von θ. Sei $q_m \leq b < q_{m+1}$. Wir betrachten das Gleichungssystem

$$p_m x + p_{m+1} y = a$$
$$q_m x + q_{m+1} y = b$$

Die Determinante der Matrix $\begin{pmatrix} p_m & p_{m+1} \\ q_m & q_{m+1} \end{pmatrix}$ ist ± 1 nach dem Beweis von Satz 9.5. Daher ist das Gleichungsystem eindeutig lösbar mit $x, y \in \mathbb{Z}$.
1. Fall: $x = 0$: Dann gilt $\frac{p_{m+1}y}{q_{m+1}y} = \frac{a}{b}$ und wir wären fertig. Ebenso für $y = 0$.
2. Fall: $x, y \neq 0$. Ist $y < 0$, so folgt $p_{m+1}y = a - p_m x \Rightarrow x > 0$. Ist $y > 0$, so folgt $b < q_{m+1} \leq q_{m+1}b \Rightarrow x < 0$. Auf jeden Fall haben x und y unterschiedliche Vorzeichen. Auch $\theta q_m - p_m$ und $\theta q_{m+1} - p_{m+1}$ haben unterschiedliche Vorzeichen, also haben

$$x(\theta q_m - p_m) \text{ und } y(\theta q_{m+1} - p_{m+1})$$

dasselbe Vorzeichen. Es gilt

$$\theta b - a = \theta(q_m x + q_{m+1} y) - p_m x - p_{m+1} y = x(\theta q_m - p_m) + y(\theta q_{m+1} - p_{m+1})$$

Hierbei haben beide Summanden dasselbe Vorzeichen, also

$$|\theta b - a| = |x(\theta q_m - p_m)| + |y(\theta q_{m+1} - p_{m+1})| > |x||\theta q_m - p_m| \geq |\theta q_m - p_m|$$

Nach Voraussetzung ist $|\theta - \frac{a}{b}| < \frac{1}{2b^2}$, also $|\theta b - a| < \frac{1}{2b}$. Es folgt

$$|\theta q_m - p_m| < \frac{1}{2b} \Leftrightarrow |\theta - \frac{p_m}{q_m}| < \frac{1}{2bq_m} \Rightarrow$$
$$\frac{1}{bq_m} \leq \frac{|bp_m - aq_m|}{bq_m} = \left|\frac{p_m}{q_m} - \frac{a}{b}\right| \leq \left|\theta - \frac{p_m}{q_m}\right| + \left|\theta - \frac{a}{b}\right| < \frac{1}{2bq_m} + \frac{1}{2b^2}$$

Also $q_m^{-1} < b^{-1}$ im Widerspruch zu $b \geq q_m$. Der zweite Fall kommt also nicht vor. □

Korollar 9.8. *Sei $d \in \mathbb{N}$ kein Quadrat, x, y eine nicht-tiviale Lösung von $x^2 - dy^2 = 1$. Dann kommt $\frac{x}{y}$ als Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{d}$ vor.*

Beweis: Es gilt

$$(x - \sqrt{d}y)(x + \sqrt{d}y) = 1 \Leftrightarrow \left(\frac{x}{y} - \sqrt{d}\right)\left(\frac{x}{y} + \sqrt{d}\right) = \frac{1}{y^2}$$

Hieraus folgt

$$0 < \frac{x}{y} - \sqrt{d} = \frac{1}{y^2}\left(\frac{1}{\frac{x}{y} + \sqrt{d}}\right) < \frac{1}{2y^2}$$

wegen $x/y \geq \sqrt{d} \geq 1$. □

Beispiel. $d = 2$. Es ist $\sqrt{2} = [1, 2, 2, \dots]$. Es gilt $[1, 2] = 1 + 1/2 = 3/2$. Wir testen: $3^2 - 2 \cdot 2^2 = 1$.

Bemerkung. Wegen $p_n < p_{n+1}$ ist die erste Lösung, die in der Entwicklung vorkommt, die Fundamentallösung.

Aufgabe 9.6. Bestimmen Sie die Fundamentallösung für $d = 12$ und $d = 15$ mit diesem Verfahren.

Definition 9.9. *$x \in \mathbb{R} \setminus \mathbb{Q}$ heißt* quadratische Irrationalzahl, *falls $x \in \mathbb{Q}(\sqrt{d})$ für ein $d \in \mathbb{Q}_{>0}$. Für $x = a + b\sqrt{d}$ schreiben wir $x' = a - b\sqrt{d}$.*

Bemerkung. Wegen $a + b\sqrt{d} = a + b/c\sqrt{dc^2}$ (mit $c > 0$) ist d nicht eindeutig, wohl aber x'.

Definition 9.10. *Ein Kettenbruch heißt* periodisch, *falls es $n_0, k \in \mathbb{N}$ gibt mit $a_n = a_{n+k}$ für alle $n \geq n_0$. Wir schreiben*

$$[a_1, a_2, \dots] = [a_1, a_2, \dots, \overline{a_{n_0}, a_{n_0+1}, \dots, a_{n_0+k-1}}]$$

Der Kettenbruch heißt rein periodisch, *falls dabei $n_0 = 1$.*

Lemma 9.11. *Sei $x \in \mathbb{R}_{\geq 1}$ mit periodischer Kettenbruchentwicklung. Dann ist x eine quadratische Irrationalzahl. Ist die Entwicklung rein periodisch, so gilt $-1 < x' < 0$.*

Beweis: $x = [a_1, \dots, a_{n_0-1}, y]$ mit

$$y = [\overline{a_{n_0}, \dots, a_{n_0+k-1}}] = [a_{n_0}, \dots, a_{n_0+k-1}, y] = \frac{yp_k + p_{k-1}}{yq_k - q_{k-1}}$$

Dies liefert eine quadratische Gleichung für y, d.h. $y \in \mathbb{Q}(\sqrt{d})$ für ein geeignetes d. Dann gilt auch

$$x = \frac{yp'_{n_0} + p_{n_0-1}}{yq'_{n_0} + q'_{n_0-1}} \in \mathbb{Q}(\sqrt{d})$$

Wir betrachten die Gleichung für y:

$$y^2 q_k + q_{k-1} y = yp_k + p_{k-1}$$

Das Polynom $F(T) = T^2 q_k + (q_{k-1} - p_k)T - p_{k-1}$ hat die Nullstellen y, y'. Es gilt $F(0) = -p_k < 0$ und $F(-1) = (q_k - q_{k-1}) + (p_k - p_{k-1}) > 0$. Also hat F eine Nullstelle zwischen -1 und 0. Dies muss y' sein. □

Wie steht es mit den Umkehrungen?

Satz 9.12. *Sei $x \in \mathbb{R}_{>1}$ eine quadratische Irrationalzahl mit $-1 < x' < 0$. Dann ist die Kettenbruchentwicklung rein periodisch.*

Tatsächlich ist dies der schwerste Teil der Frage.

Korollar 9.13. *Sei $x \in \mathbb{R}_{>1}$ quadratische Irrationalzahl. Dann ist die Kettenbruchentwicklung periodisch.*

Beweis: Sei $x = [a_1, a_2, \ldots, a_n, x_{n+1}]$ für $x \in \mathbb{Q}(\sqrt{d})$. Dann liegt auch $x_{n+1} \in \mathbb{Q}(\sqrt{d})$. Es ist

$$x = \frac{p_n x_{n+1} + p_{n-1}}{q_n x_{n+1} + q_{n-1}} \Rightarrow x' = \frac{p_n x'_{n+1} + p_{n-1}}{q_n x'_{n+1} + q_{n-1}}$$

Wir lösen nach x'_{n+1} auf:

$$\begin{aligned} q_n x' x'_{n+1} + q_{n-1} x' &= p_n x'_{n+1} + p_{n-1} \\ (q_n x' - p_n) x'_{n+1} &= p_{n-1} - q_{n-1} x' \\ x'_{n+1} &= \frac{p_{n-1} - q_{n-1} x'}{q_n x' - p_n} = \frac{q_{n-1}(r_{n-1} - x')}{q_n (x' - r_n)} \end{aligned}$$

mit $r_n = p_n/q_n = [a_1, \ldots, a_n]$. Wegen $r_n \to x \neq x'$ gilt $x'_{n+1} < 0$ für n groß genug.

Behauptung. $-\frac{1}{x'_{n+1}} - 1 > 0$ *für* n *genügend groß*

Es gilt

$$\begin{aligned} -\frac{1}{x'_{n+1}} - 1 &= -\frac{q_n x' - p_n}{p_{n-1} - q_{n-1} x'} - \frac{p_{n-1} - q_{n-1} x'}{p_{n-1} - q_{n-1} x'} \\ &= \frac{p_n - q_n x' - q_{n-1} x' - p_{n-1}}{p_{n-1} - q_{n-1} x'} \frac{q_{n-1}}{q_{n-1}} \\ &= \frac{1}{q_{n-1}} \frac{q_{n-1} p_n - q_{n-1} q_n x' - q_{n-1}^2 x' - p_{n-1} q_{n-1}}{p_{n-1} - q_{n-1} x'} \\ &= \frac{1}{q_{n-1}} \frac{q_n p_{n-1} - (-1)^n - q_{n-1} q_n x' - q_{n-1}^2 x' - p_{n-1} q_{n-1}}{p_{n-1} - q_{n-1} x'} \\ &= \frac{1}{q_{n-1}} \frac{q_n (p_{n-1} - q_{n-1} x') - q_{n-1}(q_{n-1} x' - p_{n-1}) - (-1)^n}{p_{n-1} - q_{n-1} x'} \\ &= \frac{1}{q_{n-1}} \left(q_n - q_{n-1} - \frac{(-1)^n}{p_{n-1} - q_{n-1} x'} \right) \\ &= \frac{1}{q_{n-1}} \left(q_n - q_{n-1} - \frac{(-1)^n}{q_{n-1}(r_{n-1} - x')} \right) \end{aligned}$$

Es genügt, den Klammerausdruck zu betrachten. Wegen $r_{n-1} \to x \neq x$ und $q_n \to infy$ ist der letzte Summand eine Nullfolge. Andererseits ist $q_n - q_{n-1} \geq q_{n-2} \to infty$, insgesamt ist der Ausdruck in der Klammer also positiv für genügend große n.
Dies bedeutet $x'_{n+1} > -1$ für n genügend groß. Nach Satz 9.12 hat x_{n+1} dann eine periodische Entwicklung. □

Beweis von Satz 9.12. Sei $x = a + b\sqrt{d}$ mit $a, b, d \in \mathbb{Q}$. Ohne Einschränkung ist $d \in \mathbb{N}$. Weiter gibt es $a', b', c' \in \mathbb{Z}$ mit

$$x = \frac{a' + b'\sqrt{d}}{c'} = \frac{a' + \sqrt{b'^2 d}}{c'} = \frac{a'|c'| + \sqrt{b'^2 d}}{c'|c'|}$$

Wir fassen zusammen:

$$x = \frac{m_1 + \sqrt{D}}{k_1}$$

mit ganzen Zahlen D, k_1, m_1 und $k_1 | m_1^2 - D$. Da x irrational ist, ist D keine Quadratzahl. Sei $x = [a_1, a_2, \dots]$. Wir setzen

$$m_{i+1} = a_i k_i - m_i, k_{i+1} = \frac{D - m_{i+1}^2}{k_i}$$

Behauptung. $k_{i+1} \in \mathbb{Z}$, $k_{i+1} | m_{i+1}^2 - D$.

Für $i = 1$ ist die Behauptung erfüllt. Für beliebiges i gilt

$$D - m_{i+1}^2 = D - (a_i k_i - m_i)^2 = D - m_i^2 \mod k_i$$

Nach Induktionsvoraussetzung gilt $k_i | D_m i_i^2$, also nun auch $k_{i+1} \in \mathbb{Z}$. Wegen umgekehrt

$$k_i = \frac{D - m_{i+1}^2}{k_{i+1}}$$

ist k_{i+1} ein Teiler von $D - m_{i+1}^2$.

Behauptung. $x_i = \frac{m_i + \sqrt{D}}{k_i}$

Die Aussage gilt für $i = 1$. Allgemein

$$x_i = a_i + \frac{1}{x_{i+1}} \Rightarrow \frac{m_i + \sqrt{D}}{k_i} - \frac{a_i k_i}{k_i} = \frac{1}{x_{i+1}}$$

$$x_{i+1} = \frac{k_i}{m_i + \sqrt{D} - a_i k_i} = \frac{k_i (m_i a_i k_i - \sqrt{D})}{(m_i - a_i k_i)^2 - D} = \frac{m_{i+1} + \sqrt{D}}{\frac{D - m_{i+1}^2}{k_i}} = \frac{m_{i+1} + \sqrt{D}}{k_{i+1}}$$

Für i genügend groß $x_i' < 0$ (Beweis von Satz 9.13) gilt $x_i - x_i' = \frac{2\sqrt{D}}{k_i} > 0$ (da $x_i > 0$, $x_i' < 0$), also auch $k_i > 0$. Mit

$$0 < k_i k_{i+1} = D - m_{i+1}^2 \leq D$$

folgt $k_{i+1} | m_{i+1}| \leq D$. Nur endlich viele Werte sind möglich für m_{i+1} und für k_{i+1}, also auch für x_{i+1}. Die Kettenbruchentwicklung ist periodisch.

Behauptung. *Sie ist sogar rein periodisch.*

Sei $x = a_1 + \frac{1}{x_2}$ mit $0 < -x' < 1$. Dann folgt $x' = a_1 + \frac{1}{x_2'}$, also

$$0 < -a_1 - \frac{1}{x_2'} < 1 \Rightarrow a_1 = \left[-\frac{1}{x_2'} \right]$$

mit $0 > x_2' > -1$. Iterativ folgt also $0 < -x_n' < 1$ für alle n und jedesmal

$$a_n = \left[-\frac{1}{x_{n+1}'} \right]$$

Falls $x_{n_0} = x_{n_0+k}$, dann gilt auch $a_{n_0-1} = a_{n_0+k-1}$. Damit ist die Entwicklung rein periodisch. □

Beispiel. Sei $s = \sqrt{d}$, $y = [\sqrt{d}] + \sqrt{d}$, $y' = [\sqrt{d}] - \sqrt{d} \in (0, 1)$. Dann hat y eine rein periodische Entwicklung:

$$y = [\overline{a_1, a_2, \ldots, a_N}], x = [b_1, \overline{a_2, \ldots, a_{N+1}}]$$

Das war genau der Fall, der für die Pellsche Gleichung interessant ist.

Satz 9.14. *Sei $\sqrt{d} = [a_1, a_2, \ldots]$. Mit den Bezeichnungen von oben gilt*

$$p_n^2 - q_n^2 d = (-1)^n k_{n+1}$$

Bemerkung. Speziell für $n = 2jN$ (N die Periodenlänge) erhalten wir eine Lösung der Pellschen Gleichung, da $k_1 = 1$.

Aufgabe 9.7. Wann ist die Gleichung $x^2 - dy^2 = -1$ lösbar?

Beweis:

$$\sqrt{d} = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}} = \frac{\frac{m_n + \sqrt{d}}{k_n} p_{n-1} + p_{n-2}}{\frac{m_n + \sqrt{d}}{k_n} q_{n-1} + q_{n-2}} = \frac{m_n p_{n-1} + \sqrt{d} p_{n-1} + k_n p_{n-2}}{m_n q_{n-1} + \sqrt{d} q_{n-1} + k_n q_{n-2}}$$

Hieraus folgt

$$\begin{gathered} m_n q_{n-1}\sqrt{d} + d q_{n-1} + \sqrt{d} k_n q_{n-2} = m_n p_{n-1} + \sqrt{d} p_{n-1} + k_n p_{n-2} \Leftrightarrow \\ m_n q_{n-1} + k_n q_{n-2} = p_{n-1} \text{ (Mult. mit } p_{n-1}) \\ d q_{n-1} = m_n p_{n-1} + k_n p_{n-2} \text{ (Mult. mit } p_{n-1}) \\ \Rightarrow p_{n-1}^2 + d q_{n-1}^2 = m_n q_{n-1} p_{n-1} + k_n q_{n-2} p_{n-1} - m_m p_{n-1} q_{n-1} - k_n p_{n-2} q_{n-1} \\ = k_n (q_{n-2} p_{n-1} - p_{n-2} q_{n-1}) = k_n (-1)^{n-1} \end{gathered}$$

□

Beispiel. $d = 11$, $N = 2$, also $k_3 = k_1 = 1$, $(-1)^2 k_3 = 1$, $(-1)^4 k_5 = 1$. Zugehörige Zahlen:

$$\begin{gathered} \frac{p_2}{q_2} = [a_1, a_2] = [3, 3] = 3 + 1/3 = 10/3 \Rightarrow 10^2 - 11 \cdot 3^2 = 1 \\ \frac{p_4}{q_4} = [3, 3, 6, 3] = 3 + \frac{1}{3 + \frac{1}{6 + \frac{1}{3}}} = 3 + \frac{1}{3 + \frac{3}{19}} = 3 + \frac{19}{60} = \frac{199}{60} \\ 199^2 - 11 \cdot 60^2 = 39601 - 39600 = 1 \end{gathered}$$

Aufgabe 9.8. Lösen Sie die Pellsche Gleichung für $d = 19$.

Kapitel 10

Zusammenfassung

Was haben wir behandelt?

- Der wichtigste Satz der gesamten Vorlesung war Satz 2.5: In $\mathbb{Z}$ gilt die Eindeutigkeit der Primfaktorzerlegung. Wir haben gleichzeitig die Beispiele $\mathbb{Z}[i]$ und $\mathbb{Z}[\varrho]$ behandelt. (Weil es dafür Anwendungen gab, undum die abstrakte Struktur des Beweisen herauszuarbeiten.) Wesentliches Hilfsmittel war der euklidische Algorithmus.

- Rechnen in Restklassenringen, meist $\mod p$ für Primzahlen p. Hier haben wir den chinesischen Restsatz 3.3 gezeigt: um Gleichungen modulo nm zu lösen, genügt es, sie getrennt modulo n und m zu lösen. (m, n teilerfremd).

- Schon etwas schwieriger: Strukturtheorie für Restklassenkörper: $\mathbb{F}_p^*$ ist zyklisch.

- Die Frage nach der Lösbarkeit der Gleichung $x^2 = a \mod p$ führte zum quadratischen Reziprozitätsgesetz 3.3:

  $$\left(\frac{l}{p}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

  für ungerade Primzahlen p, l. Zusammen mit den Ergänzungssätzen und der Multiplikativität des Restsymboles erlaubt dies schnelle Entscheidung ob a Quadrat $\mod p$ ist oder nicht. Dies ist wohl der tiefste Satz der Vorlesung.

- Beispiele für quadratische Gleichungen: $x^2 + y^2 = z^2$ führte zu pythagoräischen Tripeln.

- $x^3 + y^3 = z^3$ hat keine nicht-trivialen Lösungen (mit Rechnen in $\mathbb{Z}[\varrho]$).

- $x^2 - dy^{=}1$ (Pellsche Gleichung) hat immer unendlich viele Lösungen. Die Theorie der Kettenbrüche erlaubt die Berechnung der Lösungen.

- Darstellbarkeit von Primzahlen durch quadratische Ausdrücke: Hier haben wir den Zweiquadratesatz 5.1 und den Vierquadratesatz 6.1 bewiesen.

Wie geht es weiter? Es gibt mehrere interessante Forschungsrichtungen, die hier beginnen:

- Die Theorie der quadratischen Formen in zwei oder mehr Variablen, über $\mathbb{Z}$, $\mathbb{Q}$ oder auch anderen Ringen/Körpern.
- Nichtquadratische algebraische Erweiterungen von $\mathbb{Q}$ (z.B. $\mathbb{Q}(\sqrt[3]{2})$). Dies ist algebraische Zahlentheorie. Es gibt Struktursätze über die Einheitengruppe (verallgemeinern unsere Ergebnisse zu Pellschen Gleichung). Auch das quadratische Reziprozitätsgesetz hat Verallgemeinerunge, Stichwort Klassenkörpertheorie für Erweiterungen von $\mathbb{Q}$ mit abelscher Galoisgruppe. Der allgemeine Fall ist aktuelle Forschung.
- Systeme von Polynomgleichungen in mehreren Variablen über $\mathbb{Q}$ oder $\mathbb{Z}$. Dies ist algebraische bzw. arithmetische Geometrie, mein Arbeitsgebiet.

Inhaltsverzeichnis