Elementare Zahlentheorie I

gelesen von Prof. Steuding
Sommersemester 2008
LaTeX von Maximilian Michel

24. Juli 2008

Inhaltsverzeichnis

Teil I.

1. Teil der Vorlesung

Allgemeines

Hinweis

Diese Skript ist meine Vorlesungsmitschrift. Ich lese es zwar „korrektur“ und gleiche es auch mit dem Skript vom Prof. Steuding ab, dennoch sind Fehler niemals auszuschließen. In Absprache mit Prof. Steuding darf ich dieses Skript online stellen, dennoch weise ich daraufhin, dass die Copyrights bei Prof. Steuding liegen. Erreichbar ist Herr Prof. Steuding zur Zeit über diese Emailadresse: steuding“at“mathematik.uni-wuerzburg.de
Wer in diesem Skript Fehler findet bitte ich diese nicht für sich zu behalten sondern eine Mail zu schreiben an: mmichel“at“physik.uni-wuerzburg.de. Kapitelangabe, Seite und das letzte Schlagwort nicht vergessen, Danke!

Übungesbetrieb

Übungsblätter gibt es jede Woche, diese sind bearbeitet am Freitag abzugeben.
Die Übungsblätter und wichitge Termine über die Vorlesung Zahlentheorie findet ihr hier.

Ab sofort findet die Vorlesung in Hörsaal 4 statt

Literaturauswahl:

- A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press 1984
- P. Bundschuh, *Einführung in die Zahlenthorie*, Springer 2002 (5. Auflage)
- G.H. Hardy & E.M. Wright, *An introduction to the theory of numbers*, Clarendon Press 1979 (5th ed.)
- S. Müller-Stach, J. Piontkowski, *Elementare und Algebraische Zahlentheorie*, Vieweg 2006
- J. Steuding, *Diophantine Analysis*, CRC-Press/Chapman Hall 2005
- J. Wolfart, *Einführung in die Zahlentheorie und Algebra*, Vieweg 1996

0. Was ist Zahlentheorie?

Unser „Zahlenuniversum“ besteht (bisher) aus:

$$\mathbb{N} = \{1, 2, \ldots\} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \ldots$$

wobei $\mathbb{N}$ eine **Halbgruppe** mit **Peano-Axiomen** und **Induktionsprinzip** ($\Leftrightarrow$ Wohlordnung), $\mathbb{Z}$ ein **Ring** und $\mathbb{Q}$ ein **Körper** ist. Genauere Definitionen dieser Begriffe, sowie die erklärung der Körper, Ring und Gruppeneigenschaften siehe Analysis 1 (www.uni.jock2.de unter „Skriptesammlung“)

Definition. Wohlordnung Jede nichtleere Teilmenge von $\mathbb{N}$ besitzt ein kleinstes Element.

Wobei $\mathbb{Q}$ auf $\mathbb{R}$ und $\mathbb{C}$ erweiteret werden kann. Erweiterungsmöglichkeiten sind allgebraisch bzw. transzendent Körpererweiterungen

$$\mathbb{Q}\left(\sqrt{2}\right) := \left\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$$
$$\mathbb{Q}\left(\sqrt{-5}\right) \subset \mathbb{C}$$

Dies ist multiplikativ abgeschlossen
Interessant: Teilbarkeitseigenschaften, **diophantische (Un-)Gleichungen**

Bemerkung. Sieb des Erasthostenes
Streiche aus einer der Größe nach geordneten Liste der natürlichen Zahlen sukzessive alle Vielfachen der noch nicht gestrichenen Zahlen ≥ 2 aus, neben der 1 verbleiben die

	1	2	3	~~4~~	5	~~6~~
Primzahlen	7	~~8~~	~~9~~	~~10~~	11	~~12~~
	13	~~12~~	~~15~~	~~16~~	17	~~18~~

- Wieviele Primzahlen gibt es?

  Es gibt dazu eine **Riemannsche Vermutung** (siehe hierzu auch Satz 1.6 auf Seite 11).

- Lässt sich jede grade Zahl ≥ 4 alls Summe zweier Primzahlen darstellen?

  Dazu gibt es auch eine Vermutung, die **Goldbachsche Vermutung**

- Gibt es unendlich viele Primzahlen $p, p + 2$? (**Primzahl-Zwillingsvermutung**)

- Für welche $n \in \mathbb{N}$ ist die Gleichung $x^n + y^n = z^n$ in ganzen Zahlen nicht trivial lösbar? (**Fermatsche Vermutung** bewiesen durch A. Wiles)

1. Teilbarkeit

Bemerkung. In diesem Skriptum werden

- Kleine lateinische Buchstaben für ganze Zahlen
- und kleine griechische Buchstaben für reelle Zahlen

verwendet.

Definition. n heißt **teilbar** durch d, falls es ein b gibt mit $n = b \cdot d$. d teilt n und wir schreiben $d|n$, andernfalls $d \nmid n$.
d heißt **Teiler** von n und n ist ein **Vielfaches** von d.

Problem des diskreten Logarithmus:

Geben eine Primzahl

Rechenregeln.

1. $d|d,\ 1|d, d|0$
2. $0|d \Rightarrow d = 0,\ d|1 \Rightarrow d = \pm 1$
3. $d|n,\ n|m,\ \Rightarrow d|m$
4. $d|a,\ d|b \Rightarrow d|(ax + by)$ *für alle* (x, y)
5. $bd|bn,\ b \neq 0 \Rightarrow b|n$ *kürzen*
6. $d|n,\ n|d \Rightarrow d = \pm n$

Bemerkung. Eine Zahl $\neq 0$ besitzt nur endlich viele Teiler (*6.*), also besitzen $a, b \in \mathbb{Z}$, wenn nicht beide $= 0$ sind einen **größten gemeinsamen Teiler** (ggT) $d \in \mathbb{N}$, kurz $d = \mathrm{ggT}(a, b)$. Ferner $0 := \mathrm{ggT}(0, 0)$. Gilt $\mathrm{ggT}(a, b) = 1$ so sind a und b **teilerfremd**!

Satz 1.1.

1. *(Division mit Rest)*

   Zu $a, b \in \mathbb{Z}$ *mit* $b \neq 0$ *existieren eindeutig bestimmte Zahlen* $q, r \in \mathbb{Z}$ *, sodass*

   $$a = bq + r,\ \textit{mit } 0 \leq r < |b|$$

2. *Für $a, b \in \mathbb{Z}$ gilt:*

$$\begin{aligned} \mathrm{ggT}(a,b)\mathbb{Z} &= \{m \cdot \mathrm{ggT}(a,b) \mid m \in \mathbb{Z}\} \\ &= \{ax + by \mid x, y \in \mathbb{Z}\} \end{aligned}$$

Der ggT *zweier ganzen Zahlen ist die kleinste nicht-negative Zahl, die sich als linearkombination dieser Zahlen schreiben lässt.*

Beweis.

1. Mit der **Wohlordnung** besitzt $\{a - bq \mid q \in \mathbb{Z}\} \cap \mathbb{N}_0$ ein kleinstes Element r, falls $b \nmid a$ ist, gilt $1 \leq r < |b|$
2. ObdA sei $a \neq 0$ und $\mathcal{M} := \{ax,\ by \mid x, y \in \mathbb{Z}\}$, mit $m := \min\{n \in \mathbb{N} \cap \mathcal{M}\}$. Nach *(4.)* teilt $d := \mathrm{ggT}(a,b)$ jede Zahl in $\mathcal{M}$, also $\mathcal{M} \subset d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$ und $d|m$. Mit $a, qm \in \mathcal{M}$ ist auch $a - qm \in \mathcal{M}$. Division mit Rest *(1.)* von a durch m liefert Rest 0 (da m minimal in $\mathbb{N}$). Also $m|a$, analog folgt $m|b$. Somit $m \leq d$. Zusammen mit $d|m$ folgt nach *(7.)* $d = m$ und $d\mathbb{Z} \subset \mathcal{M}$

□

Alternativ kann man das auch mit vollständiger Induktion zeigen.

Rechenregeln.

8. ***Symmetrie:*** $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,a)$
9. ***Assoziativgesetz:*** $\mathrm{ggT}(a, \mathrm{ggT}(b,c)) = \mathrm{ggT}(\mathrm{ggT}(a,b), c)$
10. ***Distributivgesetz:*** $\mathrm{ggT}(ac, bc) = |c| \cdot \mathrm{ggT}(a,b)$

Bemerkung. Teilbarkeit induziert eine Teilordnung auf $\mathbb{N}$ mit der ggT also das maximale Element unter den gemeinsamen Teilern ist.

Definition. Analog zur Definition des ggT definiert man das **kleinste gemeinsame Vielfache** (kgV) von a und b als das **Minimum** aller $m \in \mathbb{N}$, für die $a|m$ und $b|m$ gilt: kurz $\mathrm{kgV}[a,b] = m$. Zum Beispiel gilt:

$$ab = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}[a,b]$$

ggT und kgV von mehr als zwei Zahlen erklärt man induktiv, zum Beispiel:

$$\mathrm{ggT}(a,b,c) = \mathrm{ggT}(a, \mathrm{ggT}(b,c))$$

Zahlen $a_1, \ldots, a_n$ heißen **teilerfremd**, wenn $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ gilt.
Zahlen $a_1, \ldots, a_n$ heißen **paarweise teilerfremd**, wenn $\mathrm{ggT}(a_j, a_k) = 1$ für $k \neq j$ gilt.
Letzteres impliziert Teilerfremdheit, **die Umkehrung gilt nicht**.
Eine effiziente Berechnung des ggT folgt mit dem **Euklidischen Algorithmus**

Beispiel.

$$\begin{aligned} 117 &= 3 \cdot 33 + 18 \\ 33 &= 1 \cdot 18 + 15 \\ 18 &= 1 \cdot 15 + 3 \\ 15 &= 5 \cdot \underline{3} = \mathrm{ggT}(117, 33) \end{aligned}$$

Satz 1.2. ***Euklidischer Algorithmus***
Zu gegebenen $a, b \in \mathbb{N}$ mit $a > b$ sei

$$\left.\begin{array}{rcc} a & = & q_1 b + r_1 \\ b & = & q_2 r_1 + r_2 \\ \vdots & \vdots & \vdots \\ r_{j-2} & = & q_j r_{r-1} + r_j \\ \vdots & \vdots & \vdots \\ r_{n-2} & = & q_n t_{n-1} + r_n \\ r_{n-1} & = & q_{n+1} r_n \end{array}\right\} \text{mit } q_j, r_j \in \mathbb{Z},\ 0 < r_j < r_{j-1}$$

Dann gilt für den letzten nicht verschwindenen Rest $r_n = \mathrm{ggT}(a, b)$.

Beweis. Die Reste r_j bilden eine streng monoton fallende Folge in $\mathbb{N}$, also **terminiert** der Algorithmus. Durchläuft man das Gleichungssystem von unten nach oben, so zeigt sich $r_n | a$ und $r_n | b$ (gemeinsamer Teiler), bzw. von oben nach unten, so folgt aus $c|a$ und $c|b$ schließlich $c|r_n$ (maximal). Also

$$r_n = \mathrm{ggT}(a, b).$$

□

Mit dem euklidischen Algorithmus kann man explizite Lösungen linearer **diophantischer Gleichungen** finden (das heißt ganze/rationalen Lösungen algebraischer/polynomineller Gleichungen, nach **Diophant**, ≈ 200 n.Chr.)

Korollar 1.3. ***Satz von Bezout***
Die Gleichung $aX + bY = c$ ist genau dann in ganzen Zahlen x, y lösbar, wenn $\mathrm{ggT}(a, b) | c$

Beweis. folgt aus Satz 1.1, mit dem euklidischen Algorithmus „rückwärts“ ergibt sich ein **Lösungsverfahren** □

Beispiel.
Die Gleichung $117X + 33Y = 3$

$$\begin{aligned} 3 = 18 \cdot 1 \cdot 15 &= 18 - 1 \cdot (33 - 1 \cdot 18) \\ &= 2 \cdot 18 - 1 \cdot 33 = 2 \cdot (117 - 3 \cdot 33) - 1 \cdot 33 \\ &= \underline{2} \cdot 117 - \underline{7} \cdot 33 \end{aligned}$$

also löst $x = 2,\ y = -7$ die Gleichung

Eine natürliche Zahl $n > 1$ heißt **Primzahl**, bzw. **prim**, wenn die (trivialen) Teiler 1 und n die einzigen positiven Teiler von n sind. Primzahlen sind die multiplikativen Bausteine der ganzen Zahlen.

Satz 1.4. ***Lemma von Euklid***
Sei p prim und $p|(a \cdot b)$. Dann gilt $p|a$ und $p|b$

Die Aussage ist **falsch** für **zusammengesetzte Zahlen**, das heißt Zahlen $n > 1$ der Form $b \cdot d$ mit $1 < b, d < n$. Lemma von Euklid (1.4) charakterisiert Primzahlen.

Beweis. Angenommen $p \not| a$, also $\mathrm{ggT}(a, p) = 1$ (da p prim!). Nach Satz 1.1 *(2.)* gibt es x, y mit $px + ay = 1$ bzw. $pbx + aby = b$. Wegen $p|pbx$ und $p|aby$ folgt $p|b$. □

Satz 1.5. *Jede natürliche Zahl n besitzt eine eindeutige Primfaktorzerlegung, das heißt es gibt eindeutig bestimmte Exponenten, $\nu(n, p) \in \mathbb{N}_0$, sodass*

$$n = \prod_{p \in \mathbb{P}} p^{\nu(n,p)}$$

Hierbei bezeichnet $\mathbb{P} = \{2, 3, 5, \ldots\}$ die Menge aller Primzahlen. Tatsächlich ist das Produkt endlich, das heißt, es gibt nur endlich viele $\nu(n; p) \neq 0$. Für $n = 1$ ist das Produkt ***leer***

18.04.08

Bemerkung. Insbesondere die Eindeutigkeit einer solchen Produktdarstellung ist nicht selbstverständlich, denn etwa

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right) \quad \text{in } \mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$$

Hierbei steht $\mathbb{P}$ für die Menge der Primzahlen $2, 3, \ldots, n$ **??**; tatsächlich ist das Produkt endlich und $n = 1$ wird das **leere Produkt**.

Beweis.

Existenz Ist $n \in \mathbb{N}$ die kleinste Zahl für die die Aussage nicht bekannt ist (**Wohlordnung**), so ist n entweder prim (dann wären wir fertig), oder ein Produkt kleinerer natürlicher Zahlen, für die die Aussage bereits bekannt ist.

Eindeutigkeit Wäre der Satz falsch, dann gäbe es ein kleinstes n mit zwei **wesentlich verschiedenen Primfakatorzerlegeung**.

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s \quad (p_i, q_j \in \mathbb{P})$$

Hierbei benutzen wir **Wohlordnung** und **wesentlich Verschieden**, das bedeutetet, es ist stets $p_i \neq q_j$ (sonst könnte man kürzen). Jedes p_j teilt n, also nach dem Lemma von Euklid (Satz 1.4) auch ein q_k. Da p_i und q_k prim sind, folgt $p_i = q_k$. **Widerspruch**

Damit ist $\mathbb{Z}$ ein **faktorieller Ring** (bzw. **ZPE-Ring**). Die eindeutige Primfaktorzerlegung überträgt sich sofort auf den **Quotientenkörper** $\mathbb{Q}$. □

Satz 1.6. ***Riemannsche Vermutung:***
Es gibt unendlich viele Primzahlen.

Beweis. Zu gegebenen Primzahlen $p_1 = 2,\ p_2, \ldots, p_m$ besitzt $q := p_1 p_2 \ldots p_m + 1$ **(??)** einen von $p_1, \ldots, p_m$ verschiedene Primteiler p. ($p \neq p_j$, denn $p|q$ und falls $p = p_j$ auch $p|(q-1)$, bzw. $p|1$) □

Frage: Wie ist $\mathbb{P}$ in $\mathbb{N}$ verteilt?
Bezeichnet $\pi(x)$ die Anzahl aller Primzahlen $p \leq x$, so wurde von Gauß 1792 mit 17 Jahren vermutet und schließlich durch HADAMARD und DE LA VALLEÉ-POISSON 1986 bewiesen:

Satz. ***Primzahlsatz (?? Fehlt da ein „=“??)***

$$\lim_{x\to\infty} \pi(x)\frac{\log x}{x} = 1$$

mit log *als natürlichen Logarithmus. Der Beweis dieses Satzes kommt in der Analytischen Zahlentheorie.*

Frage: Wie sind die Primzahlen in arithmetischen Progresionen verteilt?

Beispiel.

$4\mathbb{Z}+1:$	1	$\underline{5}$	9	$\underline{13}$	$\underline{17}$	...
$4\mathbb{Z}+2:$	2	6	10	14	18	$\leftarrow$ keine weiteren
$4\mathbb{Z}+3:$	$\underline{3}$	$\underline{7}$	$\underline{11}$	15	$\underline{19}$	
$4\mathbb{Z}:$	4	8	12	16	20	$\leftarrow$ gar keine Primzahlen

Satz 1.7. *Es gibt unendlich viele Primzahlen der Form*

$$p = 4n + 3.$$

Beweis. (wie eben)

Seien $p_1 = 3, p_2, \ldots, p_k$ Primzahlen der Form $4n+3$. Dann ist

$$q := 4(p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1) + 3$$

ebenfalls von der Form. Unter den Primfanktoren von q gibt es einen Primzahl p der Form $p = 4n + 3$, denn

$$(4m+1)\cdot(4n+1) = 4\cdot(4mn + m + n) + 1$$

Das heißt $4\mathbb{Z}+1$ ist multiplikativ abgeschlossen. Diese p kommt **nicht** unter den $p_1, \ldots, p_k$ vor, wie eben. □

Bemerkung. Euklids Beweis versagt für Primzahlen der Form $4n+1$ (denn $(4m+3)\cdot(4n+3) = 4\cdot(4mn+3m+3n+2)+1$). Wir zeigen später, dass es trotzdem unendlich viele Primzahlen dieser Gestalt gibt.

2. Modulare Arithmetik

Für alle $(a, b) \in \mathbb{Z}$ und $m \in \mathbb{N}$ sagen wir a **ist kongruent** b **modulo** m und schreiben $a \equiv b \mod m$ falls $m|(b-a)$, diese Relation heißt **Kongruenz** mit **Modulo** m.

Rechenregeln.

1. ***Reflexivität:*** $a \equiv a \mod m$
2. ***Symmetrie:*** $a \equiv b \mod m \Leftrightarrow b \equiv a \mod m$
3. ***Transitivität:*** $a \equiv b,\ b \equiv c \mod m \Rightarrow a \equiv \mod m$

Bemerkung. Damit ist Kongurenz modulo m eine **Äquivalenzrelation** auf $\mathbb{Z}$ (wie Gleichheit, was „$m = 0$“ entspricht).
Mit den Äquivalenzklassen

$$\begin{aligned} a \mod n :&= \{b \in \mathbb{Z} \mid a \equiv b \mod m\} \\ &= \{a + k \cdot m \mid k \in \mathbb{Z}\} =: a + m \cdot \mathbb{Z}, \end{aligned}$$

die wir als „**Restklassen** modulo m“ bezeichnen. Hierbei ist a ein beliebiger Repräsentant. $a \equiv b \mod m \Leftrightarrow$ die Restklassen $a \mod m$ und $b \mod m$ sind identisch.

Rechenregeln.

4. $a \equiv b,\ c \equiv d \mod m \Rightarrow ax + by \equiv cx + dy \mod m$
5. $a \equiv b,\ c \equiv d \mod m \Rightarrow ac \equiv bd \mod m$
6. $ac \equiv bc \mod m,\ c \equiv c \neq 0 \Rightarrow a \equiv b \mod \frac{m}{\mathrm{ggT}(m,c)}$
7. $a \equiv b \mod m \Rightarrow a^n \equiv b^n \mod m\ \forall_{n \in \mathbb{N}}$
8. $a \equiv b \mod m \Rightarrow \mathcal{P}(a) \equiv \mathcal{P}(b) \mod m$ *für alle Polynome* $\mathcal{P} \in \mathbb{Z}[X]$

Beweis. Zu *(6.)*:$\ldots \Rightarrow m|(a-b)c$ und wegen $\mathrm{ggT}(m, c)|m, c$ folgt

$$\frac{m}{\mathrm{ggT}(m,c)}\cancel{\mathrm{ggT}(m,c)} \mid (a,b) \cdot \frac{c}{\mathrm{ggT}(mc)}\cancel{\mathrm{ggT}(m,c)}$$

mit der Teilerfremdheit von $\frac{m}{\mathrm{ggT}(m,c)}$ und $\frac{c}{\mathrm{ggT}(m,c)}$ folgt die Behauptung.
(4.) und *(5.)* folgen direkt aus der Definition, *(7.)* per Induktion und *(8.)* aus den vorigen Regeln. □

Also lassen sich Kongruenzen zu einem festen Modul addieren und multiplizieren als handle es sich um Gleichungen! Für Restklassen $\mod m$ erklären wir **Addition** und **Multiplikation** von Repräsentanten.

$$\underbrace{(a \mod m) \overbrace{\dot{+}}^{\text{neu}} (b \mod m)}_{\text{Addition/Mulitplikation von Restgliedern}} := \underbrace{a \dot{+} b \mod m}_{\text{in } \mathbb{Z}}$$

Diese Operationen sind wohldefiniert: Die Unabhängigkeit von der Wahl des Repräsentanten folgt sofort aus *(4.)* und *(5.)*

Beispiel.

$$7 \equiv 2 \mod 5 \Rightarrow 21 = 3 \cdot 7 \equiv 3 \cdot 2 = 6 \mod 5$$

Bemerkung. Restklassenbildung ist oft hilfreich um redundante Informationen loszuwerden (beispielsweise Wochentage) mit dem Vorteil von der unendlichen Menge $\mathbb{Z}$ zu endlichen Mengen von Restklassen $\mod m$ übergehen zu können.
Mit Restklassen und obiger Addition und Multiplikation lässt sich rechnen wie in $\mathbb{Z}$ der kürze halber „a“ statt „$a \mod m$“

Beispiel. für $\mod 4$ bezüglich „$\cdot$“ bzw. „$+$“

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Modulo m gibt es genau m verschiedene Restklassen, etwa $0, 1, \ldots, (m-1)$ (Restklassen, keine Zahlen!). Eine Menge von Restklassen $\{a_1, \ldots a_m\}$ heißt **vollständiges Restsystem** $\mod m$, wenn jede Restklassen $\mod m$ genau dann einen der Repräsentanten a_j enthält a_j enthält. Wir sagen „a ist **inkongruent** $b \mod m$“, und in Zeichen $a \not\equiv b \mod m$, falls $m \not| (b-a)$. Dann bilden die m Restklassen $a_j \mod m$ genau dann ein vollständiges Restsystem $\mod m$, wenn die a_j paarweise inkongruent sind $\mod m$.

Definition. $a \mod m$ heißt eine **prime Restklassse** $\mod m$, wenn a und m Teilerfremd sind. Wegen $\mathrm{ggT}(a+km, m) = \mathrm{ggT}(a, m)$ ist mit dem Repräsentanten a auch jedes Element von $a \mod m$ Teilerfremd zu m.

Beispiel. Prime Restklasse $\mod 8 : 1, \not2, 3, \not4, 5, \not6, 7$

Bemerkung. Die Menge der primen Restklassen $\mod m$ ist multiplikativ abgeschlossen. Die Anzahl $\varphi(m)$ der primen Restklassen $\mod m$ zählt die **Eulersche φ-Funktion**. Ein Vertretersystem der $\varphi(m)$ primen Restklassen $\mod m$ heißt **primes Restsystem** $\mod m$.

Satz 2.1. *Mit* $\{a_1, \ldots, a_{\varphi(m)}\}$ *ist auch* $\{aa_1, \ldots aa_{\varphi(m)}\}$ *ein primes Restsystem* $\mod m$, *sofern* $\mathrm{ggT}(a, m) = 1$.

Bemerkung. Die analoge Aussage für vollständige Restsysteme gilt ebenso. Auf die Bedingung der Teilerfremdheit kann **nicht** verzichtet werden: $2 \cdot 3 \equiv 2 \mod 4$ und $\mathrm{ggT}(2,4) > \mathrm{ggT}(3,4)$

Beweis. Wegen $\mathrm{ggT}(a, m) = 1$ ist mit a_j auch $aa_j \mod m$ eine prime Restklasse $\mod m$. Gilt $aa_j \equiv aa_k \mod m$, so auch $a_j \equiv a_k \mod m$ (nach *(6.)*). Also sind mit a_j und a_k auch aa_j und aa_k inkongruent $\mod m$. □

24.04.08

Satz 2.2. *(*Euler*, 1750)*
Für $\mathrm{ggT}(a, m) = 1$ *gilt* $a^{\varphi(m)} \equiv 1 \mod m$.

Beweis. Mit $\{a_1, \ldots, a_{\varphi(m)}\}$ ist **nach Vorraussetzung** auch $\{aa_1, \ldots, aa_{\varphi(m)}\}$ nach Satz 2.1 ein primes Restsystem. Also gilt:

$$\underbrace{\prod_{j=1}^{\varphi(m)} a_j}_{} \overset{2.1}{\equiv} \underbrace{\prod_{j=1}^{\varphi(m)} (aa_j)}_{=a^{\varphi(m)}\prod_{j=1}^{\varphi(m)}}$$

$$\text{Umgruppierung} \quad \mod m : \cdot \downarrow \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 8 \end{matrix} \mod 5 \tag{2.1}$$

Da $\prod_{j=1}^{\varphi(m)} a_j$ (faktorweise) teilerfremd zu m ist, folgt $1 \equiv a^{\varphi(m)} \mod m$, also die Behauptung mittels *6.*. □

Der Satz von Euler besitzt eine Verallgemeinerung auf endliche abelsche Gruppen und heißt dann **Satz von Lagrange**. Dies ist ein wichtiger Satz in der **Algebra**.

Korollar 2.3. ***(Kleiner Fermat)***
Für p *prim und* $p \nmid a$ *gilt*

$$a^{p-1} \equiv 1 \mod p,$$

Dies ist klar, denn $\varphi(p) = p - 1$, *alternativ jedoch ohne jede Restriktion an* a *gilt:*

$$a^p \equiv a \mod p$$

Bemerkung. Insbesondere besitzt also jede prime Restklasse $a \mod m$ ein multiplikatives Inverses, nämlich $a^{-1} \equiv a^{\varphi(m)-1} \mod m$. (gilt nach 2.2)

Beispiel.

a	a^2	a^3	a^4	
1	1	1	1	:(
2	4	3	1	← Orbit erzeugt alle
3	4	2	1	← primen Restklassen
4	1	4	1	:(

Wobei der Orbit aus der letzten Zeile periodisch ist mit minimaler periodischer Länge, die $4 = \varphi(5)$ teilt.
$3^{-1} \equiv 3^{\varphi(5)-1} = 3^3 = 2 \mod 5$
Das multiplikativ Inverse einer primen Restklasse $a \mod m$ berechnet man effizient mit Korollar 1.3 (bzw. dem **Euklidischen Algorithmus**):

Beispiel. Gesucht ist $17^{-1} \mod 19$:

$$\begin{aligned} 19 &= 1 \cdot \boxed{17} + 2 \\ 17 &= 8 \cdot 2 + \underline{1} = (\text{inverses Existiert}) = \text{ggT}(19, 17) \\ &\Downarrow \\ \underline{1} &= 17 - 8 \cdot 2 = 17 - 8 \cdot (19 - 17) = 9 \cdot 17 - 8 \cdot 19 \\ \rightsquigarrow 1 &\equiv 9 \cdot 17 \mod 19 \end{aligned}$$

Für die Lösung allgemeiner linearer Kongruenz gilt:

Satz 2.4. *Die Kongruenz* $aX \equiv b \mod m$ *ist genau dann lösbar, wenn* $\text{ggT}(a, m) | b$ *ist. In diesem Fall gibt es genau* $\text{ggT}(a, m)$ *inkongruente Lösungen* $\mod m$.

Beweis. folgt direkt aus dem Korrollar 1.3 (Satz von Bezout); die Lösungsanzahl ergibt sich aus Rechenregel *(6.)* bzw.

$$m = \underbrace{\frac{m}{\text{ggT}(a, m)}}_{\in \mathbb{Z}} \cdot \text{ggT}(a, m).$$

□

Beispiel.

$$17X \equiv 3 \mod 9 \Leftrightarrow X \equiv 17^{-1} \cdot 17X \equiv 17^{-1} \cdot 3 \equiv 9 \cdot 3 \equiv 8 \mod 19$$

Jetzt behandeln wir Systeme linearer Kongruenzen:

Satz 2.5. ***Chinesischer Restsatz Satz von Sun Tsu*** *(≈ 400 n. Chr:)*

oder in chinesischen Schriftzeichen: 中国剩余定理

Seien $m_1, \ldots m_n \in \mathbb{N}$ *paarweise teilerfremd und* $a_1, \ldots a_n \in \mathbb{Z}$ *beliebig. Dann besitzt das Kongruenzsystem*

$$X \equiv a_1 \mod m_1, \ldots, X \equiv a_n \mod m_n$$

eine eindeutig bestimmte Lösung $X \mod m_1 \cdot \ldots \cdot m_n$.

Beweis.

Existenz:

Sei

$$x = \sum_{j=1}^{n} a_j \underbrace{\left(\frac{m_a \cdot \ldots \cdot m_n}{m_j} \right)^{\varphi(m_j)}}_{\in \mathbb{N}}.$$

Hier ist $\frac{m_1 \cdot \ldots \cdot m_n}{m_j}$ eine ganze Zahl $\equiv 0 \mod m_k$ falls $j \neq k$, bzw. **teilerfremd** zu m_k, falls $j = k$.

Mit dem Satz von Euler (Satz 2.2) folgt:

$$\left(\frac{m_1 \cdot \ldots \cdot m_n}{m_j}\right)^{\varphi(m_j)} \equiv \begin{Bmatrix} 0, & \text{falls } j \neq k \\ 1, & \text{falls } j = k \end{Bmatrix} \mod m_k.$$

Also gilt $x \equiv a_k \mod m_k,\ 1 \leq k \leq n$.

Eindeutigkeit: y ist genau dann eine weitere Lösung, wenn $m_j|(x-y)$ für alle $j = 1, \ldots n$ (nach Satz 2.4). Mit der paarweisen Teilerfremdheit der m_j ist dies äquivalent zu $m_1 \cdot \ldots \cdot m_n|(x-y)$. Also ist $x \equiv y \mod m_1 \cdot \ldots \cdot m_n$.

□

Beispiel.

$$\begin{array}{rcl} X \equiv 4 \mod 6 & \overset{(2.2)}{\Longleftrightarrow} & X \equiv 4 \mod 6 \quad \text{(paarw.) teiler-} \\ 2X \equiv 3 \mod 7 & & X \equiv 5 \mod 7 \quad \text{fremde Moduln} \end{array}$$

$$\text{Multiplikation mit } 2^{-1} \equiv 4 \mod 7 \tag{2.2}$$

Lösungsformel:

$$\begin{aligned} x &= 4 \cdot 7^{\varphi(6)} + 5 \cdot 6^{\varphi(7)} \\ &= 4 \cdot \left(\frac{6 \cdot 7}{\cancel{6}}\right)^{\varphi(6)} + 5 \cdot \left(\frac{6 \cdot 7}{\cancel{7}}\right)^{\varphi(7)} \equiv \ldots \equiv 40 \mod 42 \end{aligned}$$

alternativ, aber komplizierter für größere Modulen:

$$\begin{array}{lllllllll} x \equiv 4 \mod 6: & 4 & & 10 & & 16 & & 22 & \\ x \equiv 5 \mod 7: & & 5 & & 12 & & 19 & & 26 \end{array} \quad \begin{array}{lll} 28 & & 34 & 40 \\ & 33 & & 40 \end{array}$$

In einem hinreichend kleinen Bereich ist eine ganze Zahl also eindeutig durch ihre Reste modulo kleinere Primzahlen bestimmt!

Bemerkung. Für einen Primzahlmodul p gilt $a^2 \equiv 1 \mod p$ genau dann , wenn

$$a^2 - 1 = (a-1) \cdot (a+1) \equiv 0 \mod p;$$

also sind in einem primen Restsystem, modulo p genau dann die Restklasse $\pm 1 \mod p$ zu sich selbst invers.

Mit dieser Beobachtung nun ein erster **unpraktikabler** „Primzahltest“:

Satz 2.6. ***Satz von Wilson*** *(18. Jhd.)*
Es ist p genau dann eine Primzahl, wenn

$$(p-1)! \equiv -1 \mod p$$

ist.

Beweis. Besitzt p einen echten Primteiler q, so gilt $q|(p-1)!$ und damit

$$(p-1)! \not\equiv -1 \mod p$$

(-1 ist prime Restklasse $\mod p$).
Ist hingegen $p > 2$ prim, so gilt nach der obigen Beobachtung

$$(p-1)! = \underbrace{1}_{\text{selbstinvers}} \cdot 2 \cdot \ldots \underbrace{a \cdot \ldots \cdot a^{-1}}_{\underbrace{a \cdot a^{-1} \equiv 1 \mod p}_{\text{die Einzige}}} \cdot \ldots \cdot \underbrace{(p-1)}_{\underbrace{\equiv -1 \mod p}_{\text{selbstinvers}}} \equiv -1 \mod p.$$

Für den Spezialfall $p = 2$ ($-1 \equiv +1 \mod 2$) gilt die Kongruenz auch. □

Beispiel.

$$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv -1 \mod 11$$

wobei

$$\begin{aligned} \underbrace{2 \cdot 6 = 3 \cdot 4}_{=12} \mod 11 &\equiv \underbrace{5 \cdot 9}_{=45} \mod 11 \\ &\equiv \underbrace{7 \cdot 8}_{=56} \mod 11 \\ &\equiv 10 \mod 11 \\ &\equiv -1 \mod 11 \end{aligned}$$

3. Restklassenringe

Definition. Bisher haben wir mit Restklassen gerechnet, jetzt untersuchen wir deren Struktur. Wir bezeichnen mit $\mathbb{Z}/m\mathbb{Z}$ die Menge aller m Restklassen modulo m

Satz 3.1.

1. *$\mathbb{Z}/m\mathbb{Z}$ ist (zusammen mit der Addition und der Multiplikation von Restklassen) ein **kommutativer Ring** mit **Einselement** $(= 1 \mod m)$*
2. *$\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein **Körper**, wenn p eine **Primzahl** ist.*

Beweis. Folgt direkt durch Verifizieren der Axiome aus Kapitel 2. Ist $m = p$ prim, so ist jede Restklasse $\not\equiv 0 \mod p$ prim, also invertierbar, ist m zusammengesetzt, etwa $m = a \cdot b$ mit $1 < a, b < m$, so ist $a \cdot b \equiv 0 \mod m$ und es existieren also Nullteiler a, b. □

Bemerkung. $\mathbb{Z}/m\mathbb{Z}$ heißt **Restklassenring** modulo m und mit $(\mathbb{Z}/m\mathbb{Z})^*$ bezeichnen wir dessen (multiplikative) **Einheitsgruppe**, also die Menge der primen Restklassen mod m und bezeichnen diese als die **primen Restklassengruppe** mod m.
„$a \mod m$ ist invertierbar $\overset{\text{Kapitel 2}}{\Longleftrightarrow}$ $a \mod m$ prime Restklassen."

Beispiel. Für $m = 3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$(\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$

Beispiel. Für $m = 6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

sehr einfache Struktur

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

nicht wesentlich komplizierter

wobei für die Spalte „1" und „5" gilt: $(\mathbb{Z}/6\mathbb{Z})^* = \{1, 5 \mod 6\}$. Die Spalten „2", „3", „4" hingegen beschreiben die **Nullteiler**. Man sieht:

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Im Sinne von Produkten von Ringen (komponentenweiser Addition und Multiplikation) ergibt sich folgende algebraische Variante des **chinesischen Restsatzes** 2.5:

Satz 3.2. *Für $m \geq 2$ gilt*

$$\mathbb{Z}/m\mathbb{Z} \cong \overset{bzw.\ \oplus}{\prod_{p|m}} \mathbb{Z}/p^{\nu(m,p)}\mathbb{Z},$$

hierbei ist $\nu(m;p)$ der Exponent von p in der Primfaktorzerelgung von $m = \prod_{p|m}\ p^{\nu(m;p)}$ ist.

Illustration dieser Isomorphie an einem Beispiel:

$$\begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} \quad \mod 6 \leftrightarrow \quad \begin{matrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{matrix} \quad \mod 2 \quad \begin{matrix} 0 \\ 1 \\ 2 \\ 0 \\ 1 \\ 2 \end{matrix} \quad \mod 3$$

Beweis. ist klar. Zunächst sei $m = m_1 \cdot m_2$ mit teilerfremden m_1, m_2. Nach Satz 2.5 gibt es Bijektion: $\mathbb{Z}/m\mathbb{Z},\ m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \ni (a_1, a_2) \mapsto X \in \mathbb{Z}/m\mathbb{Z}$ vermöge

$$\begin{aligned} X &\equiv a_1 \mod m_1 \\ &\equiv a_2 \mod m_2 \end{aligned}$$

Der Rest folgt per Induktion. □

Bemerkung. Vom besonderen Interesse ist die **multiplikative Gruppe** der primen Restklasse, deren Struktur wir im folgenden Kapitel 4 genauer studieren. Für ihre Gruppenanordnung (**Eulers** φ) notieren wir allerdings bereits jetzt:

02.05.08

Korollar 3.3. ***Produktformel***
Für $n \in \mathbb{N}$ gilt:

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Das Produkt geht über die Primteiler p von n. Für $n = 1$ erhalten wir das normale Produkt zurück.

Beweis. Für Teilerfremde m_1, m_2 gilt nach Satz 3.2

$$\varphi(m_1, m_2) = \#(\mathbb{Z}/m_1m_2\mathbb{Z})^* = \#(\mathbb{Z}/m_1\mathbb{Z})^* \cdot \#(\mathbb{Z}/m_2\mathbb{Z})^* = \varphi(m_1) \cdot \varphi(m_2).$$

Für $m = p^\nu$ mit einer Primzahl p und $\nu \in \mathbb{N}$ besitzt $(\mathbb{Z}/p^\nu\mathbb{Z})^*$ aus genau den Restklassen $a \mod p^\nu$, **für die a zu p^ν teilerfremd ist**. Also:

$$\varphi(p^\nu) = \#(\mathbb{Z}/p^\nu\mathbb{Z})^* = \sum_{\substack{0 \leq a < p^\nu \\ p \not| a}} 1 = \sum_{0 \leq a < p^\nu} - \sum_{\substack{0 \leq a < p^\nu \\ p|a}} 1 = p^\nu - p^{\nu-1} = p^\nu \left(1 - \frac{1}{p}\right)$$

(denn genau jede p-te Zahl $0 \leq a < p^\nu$ ist durch p teilbar). Also folgt mit der Primfaktorzerlegung insgesamt

$$\varphi(n) \overset{n=\prod_{p|n} p^{\nu(n;p)}}{=} \prod_{p|n} \varphi\left(p^{\nu(n;p)}\right) = \prod_{p|n} p^{\nu(n;p)} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

□

Bemerkung. Mit dieser Produktformel ist die Eulersche φ-Funktion ein erstes Beispiel einer **multiplikativen** zahlentheoretischen Funktion, das heißt einer Folge $f : \mathbb{N} \to \mathbb{C}$ mit

$$f(m \cdot n) = f(m) \cdot f(n)$$

Für alle teilerfremden $m,\ n$. Multiplikative zahlentheoretische Funktionen werden in der analytischen Zahlentheorie behandelt.

Bemerkung. In der Algebra und Zahlentheorie spielen insbesondere die **Restklassenkörper** $\mathbb{Z}/p\mathbb{Z}$ (zu primen Modul p) eine wichtige Rolle. Tatsächlich besitzt jeder endliche Körper p^ν viele Elemente, wobei p prim und $\nu \in \mathbb{N}$ ist. Hierzu ist $\mathbb{Z}/p\mathbb{Z}$ der **Primkörper** (der Durschnitt aller Unterkörper).

Beweis. Ein Körper der Charakteristik p ist ein endlicher Vektorraum über $\mathbb{Z}/p\mathbb{Z}$. □

Dieser ist bis auf **Isomorphie** eindeutig und wird mit $GF(p^\nu)$ bezeichnet, wobei **GF=Galois-field** bedeutet.

Nun eine moderne Anwendung von Restklassenringen (die unbedingt keine Körperstruktur haben dürfen):
In der sogenannten **public-key-Kryptographie** benutzt man leicht berechenbare Operationen, deren Umkehrung praktisch (!) nicht berechenbar ist.

Beispiel.

$$75\,658\,934\,651 \cdot 15\,643\,985\,657 \underset{\text{schwer}}{\overset{\text{leicht}}{\rightleftarrows}} 1\,183\,607\,288\,504\,144\,300\,707$$

Dies Asymmetrie benutzt das **RSA- Verfahren** (von Ronald L. Rivest, Adi Shamir, Leonard Adleman, 1978), das einer Vielzahl von Nutzern das sichere Austauschen von geheimen Nachrichten ermöglicht. Der Einfachheit halber seien die Texte gemäß $A \mapsto 10, B \mapsto 11, C \mapsto 12, \ldots, Z \mapsto 35$ in Blöcke von Zahlen. $< N$ übersetzt. *Alice* möchte *Bob* eine geheime Nachricht übermitteln:

$$\underbrace{L}_{21}\underbrace{O}_{24}\underbrace{V}_{31}\underbrace{E}_{14} \overset{\Rightarrow M}{\Longrightarrow} \text{public key, } (N, e)$$

Bob hat dazu zwei verschiedene „große“ Primzahlen p, q (in der Praxis ca 100 Stellen) gewählt und $N = pq$, sowie $\varphi(N) = (p-1) \cdot (q-1)$ (nach Korollar 3.3) berechnet; hierzu hat *Bob* ferner $1 < e < \varphi(N)$ teilerfremd zu $\varphi(N)$ gewählt und sein multiplikativ Inverses $e \mod \varphi(N)$, also $de \equiv \mod \varphi(N)$. (schnell mit dem euklidischen Algorithmus). *Bob* veröffentlicht jetzt seinen **öffentlichen** Schlüssel (N, e). Die Zahl d sowie die Primfaktorzerlegung von N und auch $\varphi(N)$ bleiben jedoch geheim.

$$\begin{aligned} p &= 15373 \\ q &= 12373 \\ \rightsquigarrow N &= 190210129, \\ \varphi(N) &= 190\ 182\ 384, \\ e &= 154\ 201\ 933 \\ \rightsquigarrow d &= 37 \end{aligned}$$

Alice verschlüsselt ihren Geheimtext M mit *Bobs* öffentlich Schlüssel gemäß $C = M^e \mod N$:

$$C = 64\ 353\ 547 \equiv (21\ 243\ 114)^{154\ 201\ 933} \mod 190\ 210\ 129$$

und versendet diese Nachricht über einen öffentlichen Kanal. *Bob* dekodiert diese Nachricht mit seinem **geheimen** Schlüssel d gemäß

$$C^d = (M^e)^d = M^{ed} = M^{f\varphi(N)} = M^1 \underline{(M^f)^{\varphi(N)}} \equiv M \mod N$$

Wobei f definiert ist durch $de = 1 + f(\varphi(N),\ f \in \mathbb{Z})$

nach dem Satz von Euler $M^{\varphi(N)} \equiv 1 \mod N$:

$$C^d = 64\ 353\ 547^{37} \equiv 21\ 243\ 114 \mod 190\ 210\ 129.$$

Warum ist dieses Verfahren sicher? (abgesehen von einigen Attacken bei einer unglücklicher Wahl von p, q, e)

Die eifersüchtige *Claudia* müsste, um die Nachricht entschlüsseln zu können, entweder N faktorisieren (weshalb man $p \mod q$ groß gewählt und geheim halten sollte) oder $\varphi(N)$ kennen, denn aus N und $\varphi(N)$ gewinnt man eine quadratische Gleichung in dem unbekannten Primfaktor p

$$\begin{aligned} \varphi(N) &= (p-1)(q-1) \\ &= N - p - q + 1 \\ &= N - \frac{N}{p} - p + 1 \end{aligned}$$

bzw.

$$0 = p^2 + p(\varphi(N) + N) + N - 1$$

Zur Realisierung von RSA sind also effiziente Primzahltests zur Erzeugung großer Primzahlen p und q wichtig. (Satz 2.6 von WILSON ist viel zu „langsam“). Andererseits muss die Wahl ihrer Größen den Möglichkeiten der schnellen Faktorisierungsmethoden großer Zahlen permanent angepasst werden. Es wird vermutet, das es keinen „schnellen“ Faktorisierungsalgorithmus gibt, sogar dass dieses Problem einen Unterschied zwischen den **Komplexitätsklassen** P und NP $[NP \neq p]$ ausmacht. Bereits Gauß wies daraufhin, dass Testen auf **Primalität** sowie das **Faktorisieren großer Zahlen** zu den **fundamentalen Problemen der Zahlentheorie** gehört.

4. Primitivwurzel

Nach dem umformuliertern chinesischen Restsatz 3.2 (in der Urfassung ist es Satz 2.5) zerlegt sich die prime Restklassengruppe $\mod m$ gemäß

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \prod_{p|m} (\mathbb{Z}p^{\nu(m,p)}\mathbb{Z})^*$$

Was kann man über die Struktur dieser Einheitsgruppe sagen? Wir deuten mit dem einfachsten Beispiel $m = p$, wobei p prim ist.

Beispiel. $p = 7$

d	1	2	3	4	5	6	
$a^d \mod 7$	1						
	2	4	1	2	4	1	
	3	2	6	4	5	1	← zwei Zykel :)
	4	2	1				
	5	4	6	2	3	1	← die alles Erzeugen
	6	1					

Definition. Nach dem Satz 2.2 von Euler gibt es zu jedem a teilerfremd zu m ein kleinste natürliche Zahl $o(a;m)$ mit $a^{o(a;m)} \equiv 1 \mod m$; $o(a;m)$ ist unabhängig vom Repräsentanten der Restklasse $a \mod m$ und heißt **Ordnung** von $a \in (\mathbb{Z}/m\mathbb{Z})^*$. Die Menge $\{a^d \mod m \mid 1 \leq d \leq o(a;m)\}$ ist der **Zyklus** von $a \mod m$. Eine prime Restklasse $a \mod m$ heißt **Primitivwurzel modulo** m, falls der Zyklus von a identisch ist mit der primen Restklassengruppe $(\mathbb{Z}/m\mathbb{Z})^*$, diese also von a erzeugt wird. Äquivalent dazu ist, dass die Ordnung von a gleich der Gruppenordnung ist:

$$o(a;m) = \varphi(m)$$

Siehe auch Satz 4.2 *3.* unten.

Unser erstes Ziel ist zu zeigen, dass die primen Restklassengruppe modulo eines Primzahlmoduls stets **zyklisch** ist (siehe obiges Beispiel), also von einem Element (der Primitivwurzel) erzeugt wird.

Satz 4.1. *(von Euler um 1773 formuliert, vervollständigt von Gauß um 1801)*
Sei p eine Primzahl. Dann gibt es genau $\overbrace{\varphi(p-1)}^{stets\ \geq 1}$ Primitivwurzeln modulo p; insbesondere ist die prime Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch.
Im Beispiel $p = 7$ gibt es $\varphi(7-1) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 2$, nämlich Primitivwurzeln $3,\ 5 \mod 7$.

Zum Beweis dieses Satzes brauchen wir ein paar Vorbereitungen. Beginnen wir mit einer Sammlung von Eigenschaften der Ordnung **???**:

Satz 4.2. *Sei a teilerfremd zu m. Dann gilt:*

1. $a^k \equiv 1 \mod m \Leftrightarrow o(a;m) \mid k$
2. $a^s \equiv a^t \mod m \Leftrightarrow s \equiv t \mod o(a;m)$
3. *die Zahlen $a, a^2, \ldots, a^{o(a;m)}$ sind paarweise inkongruent modulo m (das heißt der Zyklus von $a \mod m$ besitzt genau $o(a;m)$ Elemente)*
4. $o(a;m) \mid \varphi(m)$

Beweis. Division mit Rest (Satz 1.1 *1.*) liefert:

$$k = q \cdot o(a;m) + r \text{ für } q, r \in \mathbb{Z} \text{ mit } 0 \leq r < o(a;m)$$

Aus $a^k \equiv 1 \mod m$ folgt damit $a^r \equiv 1 \mod m$ und mit der Minimalität von der Ordnung $o(a;m)$ ergibt sich $r = 0$. Also gilt $o(a;m)|k$. Die umgekehrte Implikation ist trivial (mit dem Satz 2.2 von Euler); *1.* ist beweisen. Zu *2.*: $a^s \equiv a^t \mod m$ ist äquivalent zu $a^{s-t} \equiv 1 \mod m$ (da a teilerfremd zu m ist); also folgt *2.* aus *1.* . Ganz ähnlich folgt Aussage *3.* aus *2.* indirekt sowie *4.* direkt aus *1.* . □

08.05.08

Zur weiteren Beweisvorbereitung von Satz 4.1 untersuchen wir nun die Kongruenz $X^d \equiv 1$ auf Lösbarkeit und Lösungsanzahl (denn jede Lösung führt auf eine Restklasse mit einer in d auftretenden Ordnung). Beispielsweise besitzt die **quadratische Kongruenz** $X^2 \equiv 1$ zwei Lösungen modulo $2, 3, 6$ jedoch vier Lösungen modulo 8. ($1^2, 3^2, 5^2, 7^2 \equiv 1 \mod 8$). Modulo Primzahlen kann es jedoch nicht „zuviele“ Lösunge geben.

Satz 4.3. ***Satz von Lagrange***
Sei p prim und $f \in \mathbb{Z}[X]$ ein Polynom mit ganzzahligen Koeffizienten vom Grad $\deg f = d$ *und* ***Leitkoeffizienten*** $\not\equiv 0 \mod p$. *Dann besitzt die Kongruenz $f(X) \equiv 0 \mod p$ höchstens „d“ Lösungen.*

Bemerkung. Das Polyom f besitzt also höchstens $d = \deg f$ Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ (mit Vielfachheiten gezählt). Dies gilt allgemeiner in **Integritätsbereichen** (wie $\mathbb{Q}$ bzw. $\mathbb{C}$, wo mit dem Fundamentalsatz der Algebra genau $\deg f$ viele Nullstellen existieren), aber nicht alle unbedingt in Ringen mit Nullteilern.

Beweis. (mit Polynomdivision)
Wegen Satz 2.4 (über lineare Kongruenzen) dürfen wir $d \geq 2$ voraussetzen. Angenommen $f(X) \equiv 0 \mod p$ besitzt eine Lösung x (sonst sind wir fertig). Mit der Identität

$$Y^j - Z^j = (Y - Z) \cdot (Y^{j-1} + Y^{j-2}Z^1 + \ldots + Y^1 Z^{j-2} + Z^{j-1})$$

gilt:

$$f(X) - f(Y) = \sum_{j=0}^{d} a_j (X^j - x^j)$$

für gewisse $a_j \in \mathbb{Z}$

$$= (X - x) \cdot \sum_{j=0}^{d-1} \alpha_j X^j$$

für gewisse $\alpha_j = \alpha_j(x) \in \mathbb{Z}$

Aus $f(X) \equiv 0 \mod p$ folgt nun $X \equiv x \mod p$ oder

$$g(X) := \sum_{j=0}^{d-1} \alpha_j X^j \equiv 0 \mod p$$

Mit der Induktion, angewendet auf $g \in \mathbb{Z}[X]$ mit $\deg g = d - 1 < \deg f$, ergibt sich die Behauptung □

Korollar 4.4. *Ist p Primzahl und $d|(p-1)$, so besitzt die Kongruenz $X^d \equiv 1 \mod p$ genau d Lösungen.*

Beweis.

Nach Satz 4.3 hat $X^d - 1$ höchstens d Nullstellen in $\mathbb{Z}/p\mathbb{Z}$. Nach dem kleinen Fermat (Satz 2.3) gilt

$$X^{p-1} - 1 \equiv (X-1) \cdot (X-2) \cdot \ldots \cdot (X-(p-1)) \mod p,$$

also hat $X^{p-1} - 1$ genau $p-1$ Nullstellen $\mod p$. Schreiben wir $p - 1 = db$ so folgt aus der Identität

$$X^{p-1} - 1 = (X^d - 1) \cdot \underbrace{(X^{(b-1)\cdot d} + \ldots + X^d + 1)}_{\text{Polynom vom Grad } p-1-d}$$

das X^{d-1} nach satz 4.3 mindestens $p - 1 - (p - 1 - d) = d$ Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ besitzt.

□

Beispiel. $p = 11$

	„A“			halbe Distanz **„B“**					**„C“**	
1										
2	4	8	5	$10 \equiv -1$	9	7	3	6	1	← Primitivwurzel
3	9	5	4	1						
6	3	7	9	$10 \equiv -1$	5	8	4	2	1	← Primitivwurzel
7	5	2	3	$10 \equiv -1$	4	6	9	8	1	← Primitivwurzel
8	9	6	4	$10 \equiv -1$	3	2	5	7	1	← Primitivwurzel
9	4	3	5	1						
10	1									

wobei die Spalte **„A“**: $X^2 - 1$ zwei, und Spalte **„B“**: $X^5 - 1$ fünf Nullstellen besitzt. Und die Einträge in Spalte **„C“** besitzt $\varphi(10) = 4$ Primitivwurzeln.

Bemerkung. Der Zyklus einer primen Restklassen bildet eine zyklische Untergruppe der primen Restklassengruppe (oben zum Beispiel $\langle 3\rangle = \{3, 9, 5, 4, 13\}$). Wir zeigen nun, dass die prime Restklassengruppe modulo einer Primzahl stets zyklisch ist:

Beweis. von Satz 4.1:

Für primes p bilden $1, 2, \ldots, p-1$ ein vollständig primes Restsystem $\mod p$. Für positives $d|(p-1) = \varphi(p)$ sei

$$\psi_p(d) := \sum_{\substack{1\le a\le p\\ o(a;p)=d}} 1.$$

Nach Satz 4.2 *4.* ist

$$\{a \mid 1 \le a < p\} = \bigcup_{0<d|(p-1)} \{a \mid 1 \le a < p,\ o(a;p) = d\}$$

eine disjunkte Zerlegung des primen Restsystems in Hinblick auf die Ordnung der Restklassen. Also gilt

$$\varphi(p) = \varphi - 1 = \sum_{d|(p-1)} \psi_p(d).$$

Nach Korollar 4.4 besitzt die Kongruenz $X^d \equiv 1 \mod p$ für festes $d|(p-1)$ genau d Lösungen, jedoch hat nicht jede Lösung unbedingt die Ordnung d. Angenommen es gibt eine Lösung $1 \le x < p$ mit $o(x;p) = d$. Nach Satz 4.2 *3.* bilden dann $x, x^2, \ldots x^d$ ein maximiales System paarweise inkongruenter Zahlen $\mod p$, die $X^d \mod p$ erfüllen:

$$x^s \equiv x^t \mod p \qquad \Rightarrow s \equiv t \mod o(x;p) = d$$
$$x^{sd} = (x^d)^s \equiv \mod p$$

(beides gilt nach Satz 4.2) Für jedes a teilerfremd zu p mit $o(a;p) = d$ gilt $a^d \equiv 1 \mod p$ und somit gibt es $1 \le k \le d$ mit $a \equiv x^k \mod p$. Nach Definition ist $o(x^k, p)$ die kleinste natürliche Zahl m mit $a^m \equiv x^{km} \equiv 1 \mod p$. Wegen Satz 4.2 *1.* suchen wir die kleinste Zahl $m \ge 1$ mit $d = o(x;p)|km$. Nach Satz 1.1 *2.* gilt $o(x^k;p) = \frac{d}{\mathrm{ggT}(k,d)}$ und also

$$o(x^k;p) = d \Leftrightarrow \mathrm{ggT}(k,d) = 1$$

Es folgt für die Anzahl der primen Restklassen $\mod p$ der Ordnung d also

$$\psi_p = \varphi(d)$$

unter der Voraussetzung, dass nur **eine** Lösung x der Ordnung d existiert (kurz $\psi_p(d) > 0$).

Zerlegen wir die Zahlen $1, 2, \ldots n$ in disjunkte Teilmengen $\{1 \leq a \leq n \mid \operatorname{ggT}(a,n) = d\}$, so ergibt sich die Formel:

$$n = \sum_{d|n} \underbrace{\#\{1 \leq a \leq n \mid \operatorname{ggT}(a,n) = d\}}_{= \#\left\{1 \leq \tilde{a} \leq \frac{n}{d} \;\middle|\; \operatorname{ggT}\left(\tilde{a}, \frac{n}{d}\right) = 1\right\}} = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d)$$

$$\text{vermöge der Bijektion } \tilde{a} \mapsto ad$$

und dies oben angewandt mit $n = p - 1$ liefert

$$p - 1 = \sum_{d|(p-1)} \psi_p(d) \leq \sum_{d|(p-1)} \varphi(d) = p - 1,$$

summandenweise.

Also gilt hier die Gleichheit und der Fall $\psi_p(d) = 0$ tritt nicht auf. Damit ist stets $\psi_p(d) = \varphi(d)$ für $d|(p-1)$ Primitivwurzeln $\mod p$. □

Bemerkung. Der Beweis zeigt, dass mit g auch alle g^k mit $\operatorname{ggT}(k, p-1) = 1$ Primitivwurzeln $\mod p$ sind!

Beispiel. $p = 31$:

1														
2	4	8	16	1										
3	9	27	19	26	16	17	20	29	25	13	8	24	10	$30 \underbrace{\equiv}_{3^{15}} -1 \mod 31$

$\rightsquigarrow$ 3 ist kleinste Primitivwurzel $\mod 31$, weitere Primitivwurzeln sind $3^7 \equiv 17, 3^{11} \equiv 13,\ 3^{13} \equiv 24,\ 3^{17},\ 3^{19},\ 3^{23},\ 3^{29} \mod 31$, (alle 3^k mit k teilerfremd zu $\varphi(31) = 30$) insgesamt gibt es $\varphi(30) = 30 - \left(1 - \frac{1}{2}\right)) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5}) = 8$ Primitivwurzeln.

Bemerkung. Man kennt keinen effizienten Algorithmus zur Findung von Primitivwurzeln (man geht hierbei nach der Methode **trial and error** vor)! Die kleinste Primitivwurzel $g \mod p$ erfüllt die Abschätzung $g \leq \text{const} \cdot p^{\frac{1}{4}+k}$ (Burgess 1957; Vinogradov vermutete $< p^{\varepsilon}$). Die offene **Artrinschen Vermutung** behauptet, dass jede natürliche Zahl $a > 1$ Primitivwurzel modulo p für unendlich viele primzahlen p ist.
Auch Primitivwurzeln werden in der Kryptographie benutzt. Die Idee der **public-key-Kryptographie** geht zurück auf Diffie und Hellman und ihr Schlüsselaustausch-Verfahren (1976):
Alice und *Bob* wollen ein Geheimnis austauschen und möchten dazu einen **gemeinsamen geheimen** Schlüssel benutzen. Sie vereinbaren eine Primzahl p und eine Primitivwurzel $g \mod p$, ferner wählt *Alice* eine nur ihr bekannte **geheime** Zahl a und *Bob* eine **geheime** Zahl b . Dann berechnet *Alice* $g^a \mod p$ und sendet dies an *Bob*, der berechnet nun $s := g^{ab} = (g^a)^b \mod p$ sowie $g^b \mod p$ und schickt letzteres an *Alice* , die ihrerseits

nun $s = (g^b)^a \mod p$ berechnet. Die Zahl s ist der **gemeinsame geheime** Schlüssel mit dem *Alice* und *Bob* sich geheime Nachrichten zusenden können. *Claudia* „sieht“ nur die Werte g^a beziehungsweise $g^b \mod p$ und kann ohne Kenntnis von b oder a den Schlüssel s nicht berechnen. Die Sicherheit des Schlüsselaustausch- Verfahrens basiert auf dem als schwierig zu „knackend“ eingestuften

Problem des diskreten Logarithmus:

(es gibt auch Varianten in anderen Gruppen)
Gegeben ist hierbei eine Primzahl p, sowie zu p teilerfremden Zahlen g, h, berechne a, sodass $h = g^a$. ($a = \log_g h$ ist gewissermaßen der diskrete Logarithmus).
Wie sieht es mit Primitivwurzeln bei zusammengesetzten Modulo aus?

15.05.08

Beispiel. 1. $m = 8 = 2^3$: $\begin{matrix} 1 & \\ 3 & 1 \\ 5 & 1 \\ 7 & 1 \end{matrix}$ hat keine Primitivwurzeln

2. $m = 25 = 5^2$: $\begin{matrix} 1 & & & & & & & & & & & & \\ 2 & 4 & 8 & 16 & 7 & 14 & 3 & 6 & 12 & 24 & \underbrace{\equiv}_{\text{Hälfte } 10=\frac{1}{2}(\varphi(25))} & & -1 \end{matrix}$ 24 ist Primitivwurzel $\mod 5$ und $\mod 5^2$

Satz 4.5. *Sei $p > 2$ prim. Dann gibt es eine Primitivwurzel $\mod p^k$, $k \in \mathbb{N}$.*

Ausgehend von der Existenz einer Primitivwurzel $\mod p$ (Satz 4.1) zeigen wir konstruktiv die Existenz einer modulo p^ν

Beweis.

Nach Satz 4.1 gibt es eine Primitivwurzel $g \mod p$. Falls $g^{p-1} \equiv 1 \mod p^2$, so ist

$$\begin{aligned}(g+q)^{p-1} &\equiv g^{p-1} + (p-1)\cdot g^{p-2}\cdot p \mod p^2 \\ &\equiv 1 + ap \mod p^2\end{aligned}$$

mit $a := (p-1)g^{p-2} \not\equiv 0 \mod p$ (**binomische Reihe**). Da mit g auch $g+p$ Primitivwurzel $\mod p$ ist, dürfen wir annehmen, dass g eine Primitivwurzel mit $g^{p-1} \equiv 1 + ap \mod p^2$ für ein $a \not\equiv 0 \mod p$ ist. Dann ist

$$\begin{aligned}\left(g^{(p-1)}\right)^{p^{k-2}} &\equiv (1+ap)^{p^{k-2}} \mod p^k, \\ \text{bzw. per Induktion} \quad \left(g^{(p-1)}\right)^{p^{k-2}} &\equiv 1 + ap^{k-1} \mod p^k, \\ \text{und insbesondere} \quad \left(g^{(p-1)}\right)^{p^{k-2}} &\not\equiv 1 \mod p^k\end{aligned}$$

Für alle anderen Teiler d von $(p-1)p^{k-1} = p^k(1-\frac{1}{p}) = \varphi(p^k)$ (nach Korollar 3.3) gilt aber erst recht $g^d \not\equiv 1 \mod p^k$ (siehe oben für $d = p-1$, andere Fälle analog). Also ist $o(g; p^k) = \varphi(p^k)$ und g somit Primitivwurzel $\mod p^k$. □

Zum Schluss dieses Kapitels erwähnen wir noch ohne Beweis den viel stärkeren

Satz 4.6. ***Satz von Gauß***
$(\mathbb{Z}/m\mathbb{Z})^*$ ist genau dann zyklisch, wenn $m = 1, 2, 4, \ldots p^k$ oder $2 \cdot p^k$ für eine ungerade Primzahlpotenz p^k ist.

Noch ein **Satz von Gauß** ist

Satz 4.7. *Für $2 \not| p$ prim ist folgt für die Anzahl der aufeinanderfolgendenden **Rest-Rest-Paare**:*

$$\frac{1}{4}\left(p - 4 - \underbrace{\left(\frac{-1}{p}\right)}_{\text{Legendre-Symbol (5.1)}}\right)$$

Beweis.

$$\begin{aligned}\sum(a,b) &= \sum_{k=0}^{p-1} \underbrace{\left(\frac{(k+a)\cdot(k+b)}{p}\right)}_{(5.1)} \\ &\overset{l=b-a}{=} \sum_{\underbrace{j}_{=k+a}}^{p-l+q} {}_{=a} \left(\frac{j\cdot(j+l)}{p}\right) \\ &\overset{\text{vollst. Rest-System}}{=} \sum_{j=1}^{p-1} \left(\frac{j\cdot(j+l)}{p}\right),\end{aligned}$$

da für $j = 0$ $\left(\frac{0}{p}\right) = 0$ folgt.

Trick: j durchläuft die primen Restklassen $\mod p$. zu jedem $j \in \{1, \ldots, p-1\}$ gibt es ein Inverses

$$\begin{aligned}j^{-1} \cdot j &= 1 \mod p \\ \left(\frac{j}{p}\right)^2 &= \left(\frac{j^{-1}}{p}\right) = 1\end{aligned}$$

(dies gilt **immer**)

$$\begin{aligned}&= \sum_{j=1}^{p-1} \left(\frac{j^{-1}}{p}\right) \cdot \left(\frac{j\cdot(j+l)}{p}\right) \\ &\overset{\text{Multipl.}}{=} \sum_{j=1}^{p-1} \underbrace{\left(\frac{(j^{-1}j)}{p}\right)}_{\mod p=1} \cdot \left(\frac{j^{-1}(j+l)}{p}\right) \\ &= \sum_{j=1}^{p+1} \left(\frac{1+j^{-1}l}{p}\right)\end{aligned}$$

Dies ist ein volles Restsystem, das heißt, in diesem Zwischenschritt ändert sich **nur** die Reihenfolge der Summanden, mehr nicht. Dies führt dann auf:

$$= \sum_{j=1}^{p-1} \left(\frac{1+jl}{p} \right)$$

für $j = 0, 1, \ldots, p-1$ durchläuft $1 + jl$ wieder ein vollständiges Restsystem (nach Satz 2.1)

$$= \sum_{j=0}^{p-1} \underbrace{\underbrace{\left(\frac{1+jl}{p} \right)}_{=\sum_{h=0}^{p-1}\left(\frac{h}{p}\right)=0}}_{\substack{=\text{Anzahl der Reste} \\ -\ \text{Anzahl der Nicht-Reste}}}$$

$$= \begin{cases} p-1, & \text{wenn } l \equiv \mod p \Leftrightarrow a \equiv b \mod p \\ -1, & \text{sonst} \end{cases}$$

□

5. Quadratisches Restglied

Jetzt untersuchen wir **quadratische Kongruenzen**, wegen $X^2 = X \mod 2$ ist dabei der Fall $p = 2$ trivial.

Definition. Sei p also eine ungrade Primzahl. Eine prime Restklassse $a \mod p$ heißt **quadratischer Rest** $\mod p$ (kurz **Rest**), fall die Kongruenz

$$X^2 \equiv a \mod p$$

lösbar ist. andernfalls ist $a \mod p$ ein **quadratischer Nichtrest** $\mod p$ (kurz: **Nichtrest**) obwohl die Kongruenz $X^2 \equiv 0 \mod p$ dann trivial lösbar ist.

Bemerkung. Um die quadratischen Reste $\mod p$ zu bestimmen, bilden wir die Quadrate des vollständigen primen Restsystems und reduzieren bezüglich eines fest gewählten primen Restsystems (bis auf weiteres sei $\subset [1, p)$). Dies liefert sämtliche **Reste** und die **Nichtreste** bilden dann das **Komplement** dazu.

Beispiel. $p = 11$

X	1	2	3	4	5	6	7	8	9	10
X^2	1	4	9	5	3	3	5	9	4	1

$\mod 11$

Reste sind hier: 1,3,4,5,9, **Nichtreste** sind demzufolge: 2,6,7,8,10. Die Quadrate von a und $p - a$ liefern die selben Reste (Symmetrie), denn:

$$(p - a)^2 \equiv p^2 - 2pa + a^2 \equiv a^2 \mod p,$$

insofern genügt es zur Erzeugung der Reste lediglich die Quadrate des **unteren Halbsystems** $1, 2, \ldots, \frac{p-1}{2}$ zu bilden. Für $1 \leq a, b \leq \frac{p-1}{2}$ gilt

$$a^2 \equiv b^2 \mod p \Leftrightarrow (a - b) \cdot \underbrace{(a + b)}_{\in [2, p-1]} = a^2 - b^2 \equiv 0 \mod p$$

$$\Rightarrow a - b \equiv 0 \mod p$$

also genau für $a = b \mod p$. Damit gibt es also genau $\frac{p-1}{2}$ quadratische Reste $\mod p$ und $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ Nichtreste $\mod p$. Alternative Methode: Die Quadrate bilden eine Untergruppe in $(\mathbb{Z}/p\mathbb{Z})^*$ vom Index 2.

Definition.

Wir definierien das **Legendre-Symbol**:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{falls } a \text{ quadratischer Rest ist,} \\ 0, & \text{falls } p|a \\ -1, & \text{falls } a \text{ quadratischer Nichtrest } \mod p \text{ ist.} \end{cases} \tag{5.1}$$

Sprechweise: „a über p“. Offensichtlich ist das **Legendre-Symbol** p periodisch

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{für } a \equiv b \mod p. \tag{5.2}$$

Satz 5.1. ***Satz über das Euler-Kriterium***
Sei $p > 2$ prim. Dann gilt:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

Beweis.

OBdA sei a teilerfremd zu p (sonst ist die Behauptung trivial, da das Legendre-symbol $= 0$ wird.). Dann ist a nach Satz 4.1 Potenz einer Primitivwurzel $g \mod p$, also $a \equiv g^m \mod p$ für ein $m \in \mathbb{Z}$. Ist $m = 2k$ gerade, so gilt:

$$a \equiv (g^k)^2 \mod p$$

und a ein Rest $\mod p$. Ferner folgt mit dem „kleinen Fermat“ (Korollar 2.3)

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (g^{2k})^{\frac{p-1}{2}} \\ &\overset{2.3}{\equiv} (g^k)^{p-1} \equiv \underbrace{+1}_{=\left(\frac{a}{p}\right)} \mod p. \end{aligned}$$

Also gilt die Behauptung für gerade Exponenten $m = 2k$.

Sei jetzt a ein Nichtrest. Nach Korollar 4.4 besitzt die Kongruenz

$$X^{\frac{p-1}{2}} \equiv 1 \mod p$$

genau $\frac{p-1}{2}$ Lösungen, diese sind genau durch die $\frac{p-1}{2}$ inkongruenten Reste $\mod p$ gegeben. Also gilt für einen Nichtrest

$$a^{\frac{p-1}{2}} \not\equiv 1 \mod p \qquad \text{bzw. } a^{\frac{p-1}{2}} \equiv -1 \mod p$$

(da ja $a^{p-1} \equiv -1 \mod p$). Der Satz ist damit bewiesen.

□

Bemerkung. Der Beweis zeigt, dass Primitivwurzeln stets Nichtreste sind und wie man konstruktiv sämtliche Reste als Potenzen g^{2k} aus einer Primitivwurzel g gewinnt.

Beispiel. $p = 11$:

2 ist Primitivwurzel $\mod 11 \rightsquigarrow$ Reste: $2^2 \equiv 4,\ 2^4 \equiv 5,\ 2^6 \equiv 9,\ 2^8 \equiv 1,\ 2^{10} \equiv 1 \mod 11$

Nichtreste sind $2, 6, 7, 8 \mod 11$ (das sind alles Primitivwurzeln)

Korollar 5.2. *Das Legendre Polynom ist* ***streng*** *multiplikativ, das heißt:*

$$\forall_{a,b\in\mathbb{N}} \left(\frac{a\cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Beweis. Folgt sofort aus dem Euler-Kriterium. □

Beispiel.

$$\left(\frac{28}{11}\right) = \left(\frac{4}{11}\right)\cdot\left(\frac{7}{11}\right) = \left(\frac{2}{11}\right)^2\left(\frac{7}{11}\right) = +1\cdot(-1) = -1$$

Alternativ mit der Periodizität.

$$\left(\frac{6}{11}\right) = -1$$

Bemerkung. Sowohl das Euler als auch Korollar 5.2 eignen sich nicht zur schnellen Berechnung des Legendre Symbols bei großen p, denn die Primfaktorzerlegeung großer Zahlen ist sehr zeitaufwändig.

Ein effizientes Verfahren liefert

Satz 5.3. ***Lemma von Gauß***
Sei $p > 2$ prim und $p \nmid a$. Bezeichnet $m(a;p)$ die Anzahl der Restklassen $la \mod p$ mit $1 \le la < p$ (reduzierte Restklassen) für $1 \le l \le \frac{p-1}{2}$ die dem ***oberen Halbsystem*** *$\frac{p+1}{2}, \dots, p-1$ angehören, so gilt:*

$$\left(\frac{a}{p}\right) = (-1)^{m(a;p)}$$

Bemerkung. m zählt quasi wie oft wir im oberen Halbsystem sind.

Beispiel. $p = 11$ und $a = 5$

l	1	2	3	4	5
la	5	$\underline{10}$	4	$\underline{9}$	3

$\mod 11$

$\rightsquigarrow m(5;11) = 2$, also $\left(\frac{5}{11}\right) = (-1)^2 = +1$. Hier sind 10 und 9 aus dem oberen Halbsystem.

Beweis. Sei $m = m(a;p)$ und $k = \frac{p-1}{2}$. Wir bezeichnen die primen Restklassen $la \mod p$ für $1 \le l \le k$ dementsprechend ob sie dem unteren Halbysystem $1, \dots, \frac{p-1}{2}$ oder dem oberen Halbsystem $\frac{p+1}{2}, \dots, p-1$ angehören mit

$$b_1, \underbrace{\dots}_{\substack{b_j = la \mod p \\ \text{mit } 1 \le b_j \le \frac{p-1}{2}}}, b_{k-m} \mod p$$

bzw.

$$c_1, \underbrace{\dots}_{\substack{c_i = la \mod p \\ \text{mit } \frac{p+1}{2} \le c_i \le p-1}}, c_m \mod p$$

(unter Vernachlässigung der Reihenfolge). Dann gilt (ähnlich wie im Beweis von Satz 2.2 (Satz von Euler) auf Seite 14)

$$a^k k! \equiv \prod_{l=1}^{k} (la) \equiv \left(\prod_{j=1}^{k-m} b_j \right) \cdot \left(\prod_{i=1}^{m} c_i \right) \mod p \tag{5.3}$$

Nach Satz 2.1 sind die Restklassen $la \mod p$ paarweise verschieden, also ebenso die Restklassen b_j und $p - c_i$ dabei gehören die Restklassen alle dem unteren Halbsystem an. Angenommen $b_j \equiv -c_i \mod p$, so folgt über $b_j \equiv l'a \mod p$, $c_i \equiv l''a \mod p$ mit $1 \leq l', l'' \leq k$ aber $a(l' + l'') \equiv b_j + c_i \equiv 0 \mod p$, was wegen $2 \leq l' + l'' \leq 2k = \frac{p-1}{2}$, (wobei $(l' + l'') \in [2, p-1]$, also $a \equiv 0 \mod p$ und $p \not| a$) unmöglich ist. Damit bilden die k inkongruenten Restklassen $b_1, \ldots, b_{k-m}, -c_1, \ldots, -c_m$ das vollständige untere Halbsystem ohne Wiederholung $\mod p$ und es gilt:

$$\left(\prod_{j=1}^{k-m} b_j \right) \cdot \left(\prod_{i=1}^{m} (-c_i) \right) \equiv \prod_{a=1}^{k} a \equiv k! \mod p$$

Im Vergleich mit (5.3) folgt also $a^k \cancel{k!} \equiv (-1)^m \cancel{k!} \mod p$ bzw.

$$\text{(Euler-Kriterium)} \qquad \left(\frac{a}{p} \right) = a^{\frac{p-1}{2}} = a^k \equiv (-1)^m \mod p$$

Mit dem Euler-Kriterium (Satz 5.1) folgt jetzt die Behauptung (mit einer Gleichung statt einer Kongruenz, da $\left(\frac{a}{p}\right) \in \{\pm 1\}$ und $p > 2$). □

23.05.08

Bemerkung. Für das Hauptresultat über quadratische Reste benötigen wir noch eine technische Folgerung aus dem Lemma von Gauß:

Korollar 5.4. *Mit den Behauptungen und Voraussetzungen von Satz 5.3 gilt:*

$$\left(\frac{a}{p} \right) = (-1)^{(a-1)\frac{p-1}{2} + \sum_{l=0}^{\frac{p-1}{2}} \left[\frac{la}{p} \right]}$$

Hierbei steht die ***Gaußklammer*** $[X]$ *für die* ***größere ganze Zahl*** $\leq x$.

Beweis. (wir übernehmen auch die Bezeichnungen aus dem vorigen Beweis)

Es gilt:

$$\frac{la}{p} = \left[\frac{la}{p} \right] + \varrho \qquad \text{mit } \varrho = \varrho(la, p) \in (0, 1)$$

Beziehungsweise:

$$la = \left[\frac{la}{p} \right] \varphi + r \qquad \text{mit } 0 < r = r(la, p) < p$$

Die Zahl r ist der kleinste positive Rest in der Restklasse $la \mod p$. Also liefern die Zahlen $r(la,p)$ für $1 \leq l \leq k$ (nach dem Beweis von Satz 5.3) genau $b_1, \ldots, b_{k-m}, c_1, \ldots, c_m$. Somit folgt

$$a \sum_{k=1}^{k} l = \varphi \underbrace{\sum_{l=1}^{k} \left[\frac{la}{p}\right]}_{=:\Sigma} + \sum_{j=1}^{k-m} b_j + \sum_{i=1}^{m} c_i.$$

Ferner gilt wegen $\{b_1, \ldots, b_{k-m}, p - c_1, \ldots p - c_m\} = \{1, \ldots, k\}$ auch

$$\sum_{l=1}^{k} l = \sum_{j=1}^{k-m} b_j + \sum_{i=1}^{m} (p - c_i),$$

und so ergibt sich durch Subtraktion

$$(a-1) \sum_{l=1}^{k} l = \varphi\,(\Sigma - m) + 2 \sum_{i=1}^{m} c_i$$

wobei gilt:

$$\begin{aligned} \sum_{l=1}^{k} l &= \frac{1}{2} k(k+1) = \frac{1}{2} \frac{\varphi - 1}{2} \frac{\varphi + 1}{2} \\ &= \frac{\varphi^2 - 1}{2} \end{aligned}$$

Also gilt

$$m = m(a,p) \equiv \Sigma + (a-1) \frac{\varphi^2 - 1}{8} \mod 2$$

(denn $-1 \equiv +1 \mod 2$) und die Behauptung folgt aus Satz 5.3 □

Bemerkung. Vermutet von Euler, bewiesen von Gauß spielt der folgende Satz eine zentrale Rolle in der Theorie der quadratischen Reste (sogar in der allgemeinen Zahlentheorie)

Satz 5.5. ***Quadratisches Reziprozitätsgesetz***
Für zwei verschiedene ungerade Primzahlen p und q gilt

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \qquad \textit{(theorem aureum)}$$

Bemerkung. Lesen wir die Kongruenzen modulo Primzahlen als Gleichungen in den entsprechenden Restklassenkörpern, so liefert das Reziprozitätsgesetz Informationen über die Lösbarkeit einer quadratischen Gleichung in $\mathbb{Z}/p\mathbb{Z}$ mit Hilfe der Lösbarkeit einer anderen quadratischen Gleichung über einen anderen Körper $\mathbb{Z}/p\mathbb{Z}$

Beispiel.

$$\left(\frac{7}{11}\right) = \left(\frac{11}{7}\right) (-1)^{\frac{11-1}{2} \cdot \frac{7-1}{2}} = -\left(\frac{4}{7}\right)^2 = -1$$

Beweis. (nach Gauß).
Nach dem Lemma von Gauß bzw. Korollar 5.4 ist

$$\left(\frac{p}{q}\right) = (-1)^m \qquad \text{mit } m = \sum_{l=1}^{\frac{p-1}{2}} \left[\frac{lq}{p}\right] \mod 2,$$

$$\left(\frac{p}{q}\right) = (-1)^n \qquad \text{mit } n = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] \mod 2,$$

denn $(q+1)^{\frac{p^2-1}{8}} \equiv 0$ bzw. $(p+1)^{\frac{q^2-1}{8}} \equiv 0 \mod 2$ (da p und q ungerade). Es ist also $m+n \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \mod 2$ zu zeigen. Hierzu definieren wir

$$f(x,y) = qx - py \qquad \text{für } |x| < \frac{p}{2},\ |y| < \frac{q}{2}.$$

Für $(0,0) \neq (x,y) \in \mathbb{Z}^2$ ist $0 \neq f(x,y) \in \mathbb{Z}$. Ferner nimmt $f(x,y)$ für ganzzahlige $x = 1, \ldots, \frac{p-1}{2},\ y = 1, \ldots, \frac{q-1}{2}$ genau $\frac{p-1}{2}, \frac{q-1}{2}$ verschiedene Werte an, denn

$$f(x,y) - f(x',y') = f(x-x', y-y') \neq 0$$

Für festes x ist $f(x,y)$ genau dann positiv, wenn $x \leq \left[\frac{qx}{p}\right]$. Also ist die Anzahl der positiven Werte

$$P := \sum_{l=1}^{\frac{p-1}{2}} \left[\frac{lq}{p}\right]$$

und analog

$$N := \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right]$$

die Anzahl der negativen Werte von $f(x,y)$. Aus der Gesamtzahl der positiven und negativen Werte von $f(x,y)$ ergibt sich

$$m+n \equiv P+N = \frac{p-1}{2} \cdot \frac{q-1}{2} \mod 2$$

□

Bemerkung. Im Beweis wurden ganzzahlige Gitterpunkte gezählt (ein wichtiges Konzept in der analytischen Zahlentheorie).

Für explizite Berechnungen sind die folgenden beiden Konsequenzen vorangegangener Resultate wichtig:

Korollar 5.6. ***(1. Ergänzungssatz)***
Für $p > 2$ gilt

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \textit{falls } p \equiv +1 \mod 4 \\ -1, & \textit{falls } p \equiv -1 \mod 4 \end{cases}$$

Beweis. Folgt unmittelbar aus dem Euler-Kriterium (Satz 5.2). □

Korollar 5.7. ***(2. Ergänzungssatz)***
Für $p > 2$ gilt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{falls } p \equiv \pm 1 \mod 8, \\ -1, & \text{falls } p \equiv \pm 3 \mod 8. \end{cases}$$

Beweis. Folgt sofort aus ????? □

Bemerkung. jetzt lässt sich „sehr schnell“ entscheiden, ob eine Restklasse quadratisch ist oder nicht.

Beispiel.

$$\begin{aligned} \left(\frac{15}{71}\right) &= \left(\frac{3}{71}\right) \cdot \left(\frac{5}{71}\right) = \left(\frac{71}{3}\right) \cdot (-1)^{\frac{71-1}{2} \cdot \frac{3-1}{2}} \cdot \left(\frac{71}{5}\right) \cdot (-1)^{\frac{71-1}{2} \cdot \frac{5-1}{2}} \\ &= -\left(\frac{2}{3}\right) \cdot \left(\frac{1}{5}\right) = -(-1)^{\frac{3^2-1}{8}} = +1, \end{aligned}$$

also ist 15 quadratischer Rest $\mod 71$

Umgekehrt lassen sich auch alle Primzahlen klassifizieren, für die eine gegebene Restklasse ein quadratischer Rest ist:

Beispiel.

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{p}{3}\right),$$

also ist -3 ein quadratischer Rest für alle Primzahlen $p \equiv +1 \mod 6$ und ein Nichtrest für $p \equiv -1 \mod 6$ (die Restklasse $3 \mod 6$ entfällt).

Wir greifen kurz das alte Problem der Verteilung der Primzahlen in primen Restklassen auf und zeigen in Ergänzung zu Satz 1.7 nun:

Satz 5.8. *Es gibt unendlich viele Primzahlen $p \equiv 1 \mod 4$*

Beweis. Zu einer Menge von Primzahlen $p_1 = 5,\ p_2, \ldots_n \equiv 1 \mod 4$ sei

$$q := (2p_1 \cdot p_2 \cdot \ldots \cdot p_n)^2 + 1.$$

Dann ist $1 < q \equiv 1 \mod 4$ und -1 ein quadratischer Rest modulo aller Primteiler p von q. Nach dem 1. Ergänzungssatz (Korollar 5.6) gilt

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

also $p \equiv 1 \mod 4$, jedoch $p \neq p_j$. □

Bemerkung. Zu einem beliebigen $m \in \mathbb{N}$ heißt eine prime Restklasse $a \mod m$ ein quadratischer Rest $\mod m$, falls $X^2 \equiv \mod m$ lösbar ist, andernfalls ist $a \mod m$ ein Nichtrest $\mod m$. Für ungerade m verallgemeinern wir das **Legendre-Symbol** durch das **Jacobi-Symbol**, definiert durch

$$\left(\frac{a}{m}\right) = \prod_{p|m} \left(\frac{a}{p}\right)^{\nu(m;p)} \qquad \left(\text{gemäß der Primfaktorzerlegung } m = \prod_{p|m} p^{\nu(m;p)}\right)$$

Wir setzen ferner noch $\left(\frac{a}{1}\right) = 1$ und $\left(\frac{a}{m}\right) = 0$, falls $\mathrm{ggT}(a;m) > 1$. Dann übertragen sich sämtliche Eigenschaften inklusive dem Reziprozitivätsgesetz in natürlicher Weise auf das Jacobi-Symbol (Nachrechnen!).

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \qquad \text{für teilerfremde ungerade } m, n$$

Mit diesen Kunstgriff erleichtert sich die Berechnung von Legendre-Symbolen:

Beispiel. 2999 ist prim,

$$\left(\frac{335}{2999}\right) = -\left(\frac{2999}{355}\right) = \left(\frac{-16}{355}\right) = \left(\frac{-1}{355}\right) = +1$$

also ist 355 ein Rest $\mod 2999$.

Bemerkung. Man beachte hierbei, dass f ür zusammengesetzte Moduln ein Jacobi-Symbol $\left(\frac{a}{m}\right) = -1$ impliziert, dass a ein Nichtrest ist (klar), mit $\left(\frac{a}{m}\right) = +1$ ist jedoch a nicht notwendigerweise ein Rest $\mod m$.

Beispiel.

$$\left(\frac{2}{15}\right) = \left(\frac{2}{5}\right) \cdot \left(\frac{2}{5}\right) = (-1)^2 = +1,$$

aber 2 ist kein Rest $\mod 15$ (denn 2 ist kein Quadrat $\mod 3$ und $\mod 5$).

29.05.08

Satz 5.9. *Eine ganze Zahl a ist genau dann ein Quadrat, wenn a ein Quadrat* $\mod p$ *für alle Primzahlen p ist, dabei heißt a ein Quadrat modulo p, wenn*

$$\left(\frac{a}{p}\right) \neq 1$$

(Wenn $X^2 \equiv a$ lösbar ist):

Beweis. ist $a = b^2$ so folgt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)^2 = +1$ für alle $p \not| a$ ansonsten ist $\left(\frac{a}{p}\right) = 0$. Für die Umkehrung genügt es zu einer Nichtquadratzahl a eine Primzahl p mit $\left(\frac{a}{p}\right) = -1$ zu finden bzw., mit dem Jacobi-Symbol genügt es ein ungerades $m \in \mathbb{N}$ mit $\left(\frac{a}{m}\right) = -1$ anzugeben.
Angenommen:

(i) $a = -b^2$: Für $m \equiv 3 \mod 4$ teilerfremd zu b gilt (mit dem 1. Ergänzungsgesetz 5.6)

$$\left(\frac{a}{m}\right) = \left(\frac{-b^2}{m}\right) = \left(\frac{-1}{m}\right) = -1;$$

(ii) $a = \pm 2^\nu b$ mit ungeraden $\nu, b \in \mathbb{N}$: Mit dem chinesischen Restsatz 2.5 sei

$$m \equiv 5 \mod 8 \quad \text{und } m \equiv 1 \mod b;$$

(bzw. $m = 5$ für $b = 1$). Dann ist $\left(\frac{-2^\nu}{m}\right) = \left(\frac{-1^\nu}{m}\right) \cdot \left(\frac{2^\nu}{m}\right) = \left(\frac{2^\nu}{m}\right) = \left(\frac{2}{m}\right) = -1$ (nach dem Ergänzungsgesetz) sowie $\left(\frac{b}{m}\right) = \left(\frac{m}{b}\right) = \left(\frac{1}{b}\right) = +1$ (nach dem Reziprozitätsgesetz). Also folgt

$$\left(\frac{a}{m}\right) = \left(\frac{\pm 2^\nu}{m}\right) \cdot \left(\frac{b}{m}\right) = -1.$$

(iii) $a = \pm 2^{2\nu} q^w b$ mit ungeraden $w, b \in \mathbb{N}$ und $2 < q$ prim, teilerfremd zu b. Für

$$m \equiv 1 \mod 4b \quad \text{und } m \equiv c \mod q$$

mit einem Nichtrest $c \mod q$ folgt $\left(\frac{-2^{2\nu}}{m}\right) = \left(\frac{2^{2\nu}}{m}\right) = +1$, $\left(\frac{b}{m}\right) = \left(\frac{m}{b}\right) = +1$, sowie

$$\left(\frac{q^w}{m}\right) = \left(\frac{q}{m}\right) = \left(\frac{m}{q}\right) = \left(\frac{c}{q}\right) = -1.$$

Diese drei Fälle beinhalten alle möglichen Erscheinungsformen von Nichtquadratzahlen. Der Satz ist bewiesen. □

Dieser Satz ist ein erstes Beispiel für das so genannte **Lokal-Global-Prinzip** (auch **Hasse-Prinzip** genannt): Arithmetische Eigenschaften bezüglich aller Primzahlen (in den „lokalen“ Restklassenkörpern $\mathbb{Z}/p\mathbb{Z}$) übertragen sich auf $\mathbb{Z}$ (bzw. den „globalen“ Körper $\mathbb{Q}$). Leider gilt dies nicht immer, zum Beispiel ist das Analogon von Satz 5.9 für n-ten Potenzen (bzw. n-ten Potenzresten) falsch, wenn $8|n$

6. Summe von Quadraten

Für ein $k \in \mathbb{N}$ bezeichne $\boxed{k}$ die Mengen aller natürlichen Zahlen, die sich als eine Summe von k Quadraten ganzer Zahlen darstellen lassen.

Beispiel.

$$\begin{aligned}
3 &= 1^2 + 1^2 + 1^2 && \in \boxed{3} \\
5 &= 2^2 + 1^2 && \in \boxed{2} \\
7 &= 2^2 + 1^2 + 1^2 + 1^2 && \in \boxed{4} \\
11 &= 3^2 + 1^2 + 1^2 && \in \boxed{3} \\
13 &= 3^2 + 2^2 && \in \boxed{2} \\
17 &= 3^2 + 2^2 + 2^2 && \in \boxed{3} \\
19 &= 3^2 + 3^2 + 1^2 && \in \boxed{3} \\
23 &= 3^2 + 3^2 + 2^2 + 1^2 && \in \boxed{4} \\
29 &= 5^2 + 2^2 && \in \boxed{2}
\end{aligned}$$

Satz 6.1. ***Satz von Fermat und Euler***
Jede Primzahl $p \equiv 1 \mod 4$ *ist darstellbar als Summe von zwei Quadraten.*

$$p \equiv 1 \mod 4 \in \boxed{2}$$

Bemerkung. Erstaunlich ist, dass $p \equiv 1 \mod 4$ immer eine Primzahl ist. Außerdem sind Quadratzahlen sehr „dünn“ in $\mathbb{N}$.

Beweis. **Fermats Methode des Abstieges**
Für $p \equiv 1 \mod 4$ gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = +1$ nach dem 1. Ergänzungssatz (Korollar 5.6). Das heißt, es gibt ein z mit

$$z^2 + 1 = 0 \mod p \qquad \text{und } |z| < \frac{p}{2}$$

bzw. $z^2 + 1 = gp$ für ein $1 \leq g < p$ (denn $gp = z^2 + 1 < \frac{p^2}{4} + 1$). Ist $g = 1$ dann sind wir fertig. Ist $g > 1$ ist, so sei

$$\mathcal{M}(p) := \left\{ m \in \mathbb{N} \mid m < p \text{ und } mp \in \boxed{2} \right\} \neq \emptyset, \qquad \text{denn } g \in \mathcal{M}(p).$$

Sei nun $1 < h \in \mathcal{M}(p)$, dann gibt es x und y mit $x^2 + y^2 = hp$ mit $1 \leq h < p$. Wir wählen nun v, w so, dass

$$\left.\begin{matrix} v \equiv x \mod h \\ w \equiv y \mod h \end{matrix}\right\} \quad \text{und} \quad \begin{matrix} |v| \leq \frac{h}{2} \\ |w| \leq \frac{h}{2} \end{matrix}$$

Dann ist

$$0 \overset{x^2+y^2=ph}{\equiv} x^2 + y^2 = xv + yw \equiv v^2 + w^2 \mod h$$

und

$$xw + yv \equiv xy - yx \equiv 0 \mod h$$

Insbesondere ist $v^2 + w^2 = hk$ für ein k mit $0 \leq k < h$ ($\leftarrow k < h$, denn $|v|, |w| \leq \frac{h}{2}$, also $v^2 + w^2 \leq \frac{h^2}{4} + \frac{h^2}{4} = \frac{h^2}{2}$). Wäre $v = w = 0$, so folgte $h|x$ und $h|y$ bzw. $h|p = (x^2 + y^2)/h$, ein **Widerspruch**, also ist $k > 0$.

Mit der Identität:

$$(xv + yw)^2 + (xw - yv)^2 = (x^2 + y^2) \cdot (v^2 + w^2) \tag{6.1}$$
$$= hp \cdot hk = h^2 kp \tag{6.2}$$

bzw. mit den obigen Kongruenzen $\mod h$ (Division durch k^2).

$$\underbrace{\left(\frac{xv + yw}{h}\right)}_{\in\mathbb{Z}} + \underbrace{\left(\frac{xw + yv}{h}\right)}_{\in\mathbb{Z}} = kp.$$

Hierbei ist der Quotient nach obiger Bedingung eine ganze Zahl. Also ist $k \in \mathcal{M}(p)$. Nun gilt folgende Variante des Wohlordnungsprinzipes: In einer nichtleeren Menge $\mathcal{M} \in \mathbb{N}$ gebe es zu jedem $k \in \mathcal{M}$ mit $h > 1$ ein $k \in \mathcal{M}$ mit $k < h$, dann ist $1 \in \mathcal{M}$.
In unserem Fall folgt $1 \in \mathcal{M}(p)$, also $p \equiv 1 \mod 4 \in \boxed{2}$. □

Bemerkung. Der Beweis ist konstruktiv, sobald man eine Lösung der quadratischen Kongruenz $x^2 + y^2 \equiv 0 \mod p$ besitzt:

Beispiel. $p = 349 \equiv 1 \mod 4$ prim.

$$\underbrace{(174!)^2}_{} \equiv \left(\frac{349 - 1}{2}!\right) \equiv -1 \mod 349$$
$$= 1 \cdot 2 \cdot 3 \cdot \underline{4} \cdot \ldots \cdot \underline{87} \cdot \ldots \cdot 173 \cdot 174 \equiv -136 \mod 349$$
$$\Rightarrow 136^2 + 1^2 = 53 \cdot 349$$

$\rightsquigarrow$ **Fermatsche Abstieg**

x	y	h	v	w	$\frac{1}{h}(xv + yw)$	$\frac{1}{h}(xw + yv)$
136	1	53	-23	1	59	3
$\rightsquigarrow 59$	3	10	-1	3	-5	18
$\rightsquigarrow -5$	18	1				

$5^2 + 18^2 = 1 \cdot 349$

Bemerkung. Die Identität (6.1) aus dem Beweis ist die **Normgleichung** im **Ring der Gaußschen Zahlen** $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}$ mit $i^2 = -1$, wobei die **Norm** über den Betrag in $\mathbb{C}$ definiert ist.:

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

Dies wird in Kapitel 7 vertieft!

Bemerkung. Mit (6.1) ist die Menge aller natürlichen Zahlen, die sich als Summe von zwei Quadraten darstellen lassen, multiplikativ abgeschlossen:

$$m, n \in \boxed{2} \Rightarrow m, n \in \boxed{2}$$

Beispiel.

$$\begin{aligned} 5 \cdot 10 = (2^2 + 1^2) \cdot (3^2 + 1^2) &\overset{(6.1)}{=} (2 \cdot 3 + 1 \cdot 1)^2 + (1 \cdot 1 - 1 \cdot 3)^2 = 7^2 + 1^2 \\ \text{in } \mathbb{C}: \quad (2 - i) \cdot (3 + i) &= 7 - i \\ (2 + i) \cdot (3 + i) &= 5 + 5i \\ m, n \in \boxed{2} &\Rightarrow m \cdot n \in \boxed{2} \end{aligned}$$

Satz 6.2. *Für $n \in \mathbb{N}$ gilt genau dann $n \in \boxed{2}$, wenn der Exponent $\nu(n; p)$ einer jeden Primzahl $p \equiv 3 \mod 4$ in der Primfaktorzerlegung von n gerade ist.*

Beweis. Gegeben ist:

$$n = 2^{\nu(n;2)} \prod_{p \equiv 1 \mod 4} p^{\nu(n;p)} \prod_{p \equiv 3 \mod 4} p^{\nu(n;p)}$$

Es ist $2 \in \boxed{2}$, sowie jede Primzahl $p \equiv 1 \mod 4 \in \boxed{2}$ nach Satz 6.1 sind alle Exponenten $\nu(n; p)$ aller Primteiler $p \equiv 3 \mod 4$ gerade, so ist

$$\left(\prod_{p \equiv 3 \mod 4} p^{\nu(n; \frac{p}{2})} \right)^2$$

ein Quadrat und mit (6.1) folgt $n \in \boxed{2}$.

Angenommen, $n \in \boxed{2}$ und $p \equiv 3 \mod 4$ ein Primfaktor von n. Dann gilt $n = x^2 + y^2$ für gewisse $x, y \in \mathbb{Z}$ und insbesondere

$$x^2 + y^2 \equiv 0 \mod 4$$

Ist $p \nmid$, so gilt

$$xz \equiv 1 \mod p$$

für ein z (das Inverse von $x \mod p$). Damit folgt:

$$1 + (yz)^2 \equiv z^2(x^2 + y^2) \equiv 0 \mod p$$

und insbesondere

$$\left(\frac{-1}{p}\right) = +1$$

im Widerspruch zum 1. Ergänzungssatzes (Korollar 5.6)

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

Also gilt $p|x$ und damit aber auch $p|y$. Damit dann aber $p^2|(x^2+y^2) = n$. Somit ist $n = p^2 m$ mit einem $1 \leq m < n$. Derselbe Schluss angewandt auf m liefert $\nu(n;p) \equiv 0 \mod 2$ für alle Primteiler $p \equiv 3 \mod 4$. □

Für Summen von drei Quadraten gilt der schwierige

Satz. ***Satz von Gauß***

$$\forall_{k,m\in\mathbb{N}_0} \quad n \in \boxed{3} \Leftrightarrow n \neq 4^k(8m+7)$$

Bemerkung. Die Implikation $n = 4^k(8m+7) \Rightarrow n \notin \boxed{3}$ folgt unmittelbar aus der Beobachtung, dass $0, 1$ und 4 die Quadrate $\mod 8$ sind, also $8m+7$ keine Summe von drei Quadraten sein kann, und einer Variante des Fermatschen Abstieges. Die Umkehrung dieser Aussage ist schwierig (und geht mit **ternären quadratischen Formen**).

Kurios

(und unwichtig)

Jede rationale Zahl a ist Summe von drei Kuben rationaler Zahlen

$$a = \left(\frac{a^3 - 3^6}{3^2a^2 + 3a^4 + 3^6}\right)^3 + \left(\frac{-a^3 + 3^5a + 3^6}{3^2a^2 + 3^4a + 3^6}\right)^3 + \left(\frac{a^2 + 3^4}{\cdots}\right)^3$$

30.05.08

Satz 6.3. ***Satz von Lagrange***
$\boxed{4} = \mathbb{N}$, *das heißt jede natürliche Zahl besitzt eine Darstellung als Summe von vier Quadraten.*

Bemerkung. Als Ersatz für (6.1) benutzen wir hier (die Normalgleichung für **Quaternionen**)

$$\begin{cases} (\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2)\cdot(\beta_1^2+\beta_2^2+\beta_3^2+\beta_4^2) & = \gamma_1^2+\gamma_2^2+\gamma_3^2+\gamma_4^2 \quad \text{mit} \\ \gamma_1 & = \alpha_1\beta_1+\alpha_2\beta_2+\alpha_3\beta_3+\alpha_4\beta_4 \\ \gamma_2 & = \alpha_1\beta_2-\alpha_2\beta_1+\alpha_3\beta_4-\alpha_4\beta_3 \\ \gamma_3 & = \alpha_1\beta_3-\alpha_3\beta_1+\alpha_4\beta_2-\alpha_2\beta_4 \\ \gamma_4 & = \alpha_1\beta_4-\alpha_4\beta_1+\alpha_2\beta_3-\alpha_3\beta_2 \end{cases} \tag{6.3}$$

Insbesondere ist $\boxed{4}$ damit multiplikativ abgeschlossen.

Beweis. von Satz 6.3. Wegen $2 \in \boxed{2}$, Satz 6.1 und der multiplikativen Abgeschlossenheit von $\boxed{4}$, genügt es zu zeigen, dass jede Primzahl $p \equiv 3 \mod 4$ in $\boxed{4}$ liegt.
Dies machen wir wieder mit Fermat's Abstieg:

Sei $b \in \{1, 2, \ldots, p-1\}$ der **kleinste quadratische Nichtrest** $\mod p$. Mit dem 1. Ergänzungssatz (Korollar 5.6) gilt:

$$\left(\frac{-b}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{p}{b}\right) = (-1)^{\frac{p-1}{2}}(-1) = -1.$$

Also es existiert ein x mit $x^2 \equiv -b \mod p$. ObdA $|x| < \frac{p}{2}$. Aufgrund der Minimalität von b gibt es ein y mit $|y| < \frac{p}{2}$ und $y^2 \equiv b - 1 \mod p$. Also

$$x^2 + y^2 + 1^2 \equiv -b + b - 1 + 1 \equiv 0 \mod p$$

das heißt

$$x^2 + y^2 + 1^2 = gp \text{ für ein } 1 \leq g < p$$

($g < p$, da $|x|, |y| < \frac{p}{2}$). Ist $g = 1$ dann sind wir fertig. Ist $g > 1$, so sei $\mathcal{M}(p) = \left\{m \in \mathbb{N} \mid m < p,\ mp \in \boxed{4}\right\}$. Wegen $g \in \mathcal{M}(p)$ nicht leer. Sei nun $1 < h \in \mathcal{M}(p)$, dann existieren $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ mit

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp \qquad \text{mit } 1 < h < p$$

Nun definieren wir uns y_j über $y_j \equiv x_j \mod h$ und $|y_j| \leq \frac{h}{2}$ für $j = 1, \ldots, 4$. Dann ist:

$$\begin{aligned} y_1^2 + y_2^2 + y_3^2 + y_4^2 &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \mod h \\ &\equiv 0 \mod h \end{aligned}$$

Wären alle $y_j \equiv 0 \mod h$, so wäre jedes x_j ein Vielfaches von h und damit $h^2 | (x_1^2 + x_2^2 + x_3^2 + x_4^2) = hp$ und insbesondere $h|p$, **Widerspruch** zu $h \in \mathcal{M}(p)$. Also

$$\exists!_{k \in \mathbb{N}}\ y_1^2 + y_2^2 + y_3^2 + y_4^2 = kh \neq 0$$

mit

$$k = \frac{1}{h}(y_1^2 + y_2^2 + y_3^2 + y_4^2) \leq \frac{4}{h}\frac{h^2}{4} = h.$$

Wäre hier $k = h$, so folgte $y_j = \pm\frac{h}{2}$ für alle $j = 1, \ldots, 4$ und insbesondere $2|h$. Dies liefert $x_j^2 \equiv \left(\frac{h}{2}\right)^2 \mod h^2$ und mit obigen $hp \equiv 4\left(\frac{h}{2}\right)^2 \mod h^2$ bzw. $p = h$ folgt ein **Widerspruch**. Also ist $k < h$. Mit $\alpha_i = x_i$, $\beta_i = y_i$ ergibt sich über (6.3) nun

$$\gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_4^2 = hp \cdot kh = kh^2 p$$

(dividiere diese Formel durch h^2)

Hierbei gilt

$$\begin{aligned}\gamma_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod h\end{aligned}$$

und wegen $x_iy_j - x_jy_i \equiv 0 \mod h$ für $i, j \in \{1, \ldots, 4\}$ ist ferner $\gamma_2 \equiv \gamma_3 \equiv \gamma_4 \equiv 0 \mod h$. Es folgt:

$$kp = \frac{1}{h^2}(\gamma_1^2 + \gamma_2^2\gamma_3^2 + \gamma_3^2 + \gamma_4^2) \in \boxed{4} \qquad \text{termweise } \frac{\gamma_j}{h} \in \mathbb{Z}$$

also $k \in \mathcal{M}(p)$. Wegen $k < h$ ergibt sich die Behauptung mit Fermats Abstiegsargument. □

Beispiel.

$$2443 = 7 \cdot 349 = (2^2 + 1^2 + 1^2 + 1^2) \cdot (5^2 + 18^2) = 28^2 + 31^2 + 13^2 + 23^2$$

Bemerkung. Das **Weringsche Problem** fragt, ob zu jedem $k \geq 2$ ein g existiert, sodass jedes $n \in \mathbb{N}$ eine Summe von g vielen k-ten Potenzen ist. Dies wurde positiv durch HILBERT mit einem kombinatorischen Argument positiv beantwortet; mit analytischen Mitteln (Kreismethode) gelingen die Abschätzungen für das minimale g zu gegebenen k.

Teil II.

2. Teil der Vorlesung

Bemerkung. Wie sich angedeutet hat, ist es manchmal sinnvoll, den Zahlenbereich der ganzen oder rationalen Zahlen zu erweitern (zum Beispiel Identität (6.1))!
Eine komplexe Zahl α heißt **algebraisch**, wenn es ein nicht identisch verschwindendes Polynom gibt mit

$$P = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0$$

mit rationalen Koeffizienten und $P(\alpha) = 0$ andernfalls nennt man α transzendent und mit analytischen Methoden bewiesen HERMITE (1873) und LINDEMANN (1882) die Transzendenz von $e = \exp(1)$ und $\pi = 3,14\ldots$ (insbesondere Quadratur des Kreises unmöglich). Die algebraischen Zahlen bilden einen Körper $\bar{\mathbb{Q}}$ und bilden die zentralen Objekte der algebraischen Zahlentheorie. Wir interessieren und im Folgenden speziell für die Nullstellen quadratischer Gleichungen

7. Quadratischer Zahlenkörper

Ein Körper k mit $\mathbb{Q} \leq k \leq \mathbb{C}$ (Oberes Halbsystem **??** von $\mathbb{Q}$, Teilkörper von $\mathbb{C}$) heißt **quadratischer Zahlenkörper** (über $\mathbb{Q}$), wenn die Dimensionen von k als $\mathbb{Q}$ Vektorraum gleich 2 ist; dies macht Sinn, da jeder Teilkörper von $\mathbb{C}$ den Primkörper $\mathbb{Q}$ enthält.

Satz 7.1. *k ist genau dann ein quadratischer Zahlenkörper, wenn es eine ganze quadratfreie Zahl d gibt, sodass*

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

*Verschiedene quadratische Zahlen $d, d' \in \mathbb{Z}$ führen auf verschiedene Zahlenkörper: $\mathbb{Q}\left(\sqrt{d}\right) \neq \mathbb{Q}\left(\sqrt{d'}\right)$ wobei auch der Schnitt $= \mathbb{Q}$ ist. Hierbei heißt d **quadratfrei**, wenn es keine Primzahl p mit $p^2|d$ gibt, ansonsten ist nennt man d **quadratbehaftet**. Ist d eine Quadratzahl, dann gilt $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}(1) = \mathbb{Q}$, reduziert sich also auf den Körper der rationalen Zahlen.*

Beispiel.

$$\mathbb{Q}\left(\sqrt{2}\right) \Rightarrow 1 + \sqrt{2},\ \left(1 + \sqrt{2}\right)^2 = 3 + 2\sqrt{2}$$
$$\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{\left(1+\sqrt{2}\right)\cdot\left(1-\sqrt{2}\right)} = 1 + \sqrt{2} = a + b\sqrt{2}$$

Beweis. Ist k ein quadratischer Zahlenkörper und $\alpha \in k \backslash \mathbb{Q}$, so sind 1 und α eine Basis von k als $\mathbb{Q}$ Vektorraum, das heißt $k = \mathbb{Q} + \mathbb{Q}\alpha$. Wegen $\alpha^2 \in k$ gibt es $r, s \in \mathbb{Q}$ mit $\alpha^2 = r \cdot 1 + s \cdot \alpha$ bzw. teilerfremde Zahlen $a \in \mathbb{N}$ und $b, c \in \mathbb{Z}$, mit $a\alpha^2 + b\alpha + c = 0$. Damit

$$\alpha = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{D} \qquad \text{mit } D := b^2 - 4ac.$$

Wegen $D \in \mathbb{Z}$ gibt es $m, d \in \mathbb{Z}$ mit $D = m^2 d$, d quadratfrei. Also ergibt sich $\alpha \in \mathbb{Q} + \mathbb{Q}\sqrt{d}$ $k \leq \mathbb{Q} + \mathbb{Q}\sqrt{d} = \mathbb{Q}(\sqrt{d})$. Ferner gilt stets $r + s\sqrt{d} \in k$ für $r, s \in \mathbb{Q}$ und damit $k = \mathbb{Q}\left(\sqrt{d}\right)$

Gilt umgekehrt $k = \mathbb{Q}\left(\sqrt{d}\right)$ mit quadratfreien d, so sind die Körperaxiome nachzurechnen. Hier ist höchstens die Existenz des multiplikativen Inversen interessant. Zu $a + b\sqrt{d} \neq 0$ liest man das Inverse ab aus der Indentität

$$(a + b\sqrt{d})^{-1}\frac{a - b\sqrt{d}}{a - b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 + b^2 d} = \frac{a}{a^2 - b^2 d} + \frac{-b}{a^2 - db^2}\sqrt{d}$$

hierbei ist $a^2 - b^2 d \neq 0$, denn d ist quadratfrei. Also ist k ein Teilkörper von $\mathbb{C}$ und da k als $\mathbb{Q}$ Vektorraum Dimension zwei besitzt, ist k ein quadratischer Zahlenkörper. Zum Nachweis der letzten Behauptung nehmen wir

$$\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{d'}\right)$$

mit quadratfreien $d, d' \in \mathbb{Z}$. Wegen $\sqrt{d} \in \mathbb{Q}\left(\sqrt{d'}\right)$ gibt es $a, b \in \mathbb{Q}$ mit $\sqrt{d} = a + b\sqrt{d'}$ bzw. $d = a^2 + 2ab\sqrt{d'} + d'b^2$ ($d \notin \mathbb{Z}$, da d' quadratfrei). Hierbei muss also $ab = 0$ gelten.
$a = 0$ führt auf $d = d'b^2$, geht mit $b = \pm 1$ nur
$b = 0$ führt auf $d = a^2$, das ist Unfug, also bleibt $d = d'$ □

Wir haben hier die Irrationalität von $\sqrt{d}$ für Nicht-Quadrate d bentuzt, die unmittelbar aus den Teilbarkeitseigenschaften ganzer Zahlen folgt.

Definition. Ist $k = \mathbb{Q}\left(\sqrt{d}\right)$ ein quadratischer Zahlenkörper, so ist die **Konjugationsabbildung**

$$' : k \to k, \quad a + b\sqrt{d} \mapsto \left(a + b\sqrt{d}\right)' = a - b\sqrt{d} \qquad (a, b \in \mathbb{Q})$$

ein Automorphismus von k (als Ring bzw. als Körper), denn „ $'$ “ ist offensichtlich bijektiv und es gilt $(\alpha + \beta)' = \alpha' + \beta'$ bzw. $(\alpha \cdot \beta)' = \alpha' \cdot \beta'$ für beliebige $\alpha, \beta \in k$. Ferner definieren wir zu $\alpha = a + b\sqrt{d}$ die **Spur** und die **Norm** von α durch

$$S(\alpha) = \alpha + \alpha' = 2a$$

bzw.

$$\forall_{\alpha,\beta \in k}\ N(\alpha) = \alpha \cdot \alpha' = \left(a + b\sqrt{d}\right) \cdot \left(a - b\sqrt{d}\right) = a^2 - b^2 d.$$

Bemerkung. Sowohl **Spur** als auch **Norm** sind rational für alle Körperselemente. Tatsächlich sind dies gute Bekannte denn für jedes $\alpha \in k \in \mathbb{Q}(\sqrt{d})$ gilt.

$$\begin{aligned} \alpha^2 - S(\alpha)\alpha + N(\alpha) &= 0 \\ \alpha'^2 - S(\alpha)\alpha' + N(\alpha) &= 0 \\ x^2 - (\alpha - \alpha')x + \alpha\alpha' = (x - \alpha) \cdot (x - \alpha') = x^2 - S(\alpha) + N(\alpha) &= 0 \end{aligned}$$

Insbesondere ist damit α algebraisch mit einem annullierenden Polynom

$$P = x^2 - S(\alpha)x + N(\alpha) = (x - \alpha)(x - \alpha').$$

Ferner sind die Abbildungen der Spur $S : k \to \mathbb{Q}$ bzw. $N : k \to \mathbb{Q}$ additiv (Spur) bzw. multiplikativ (Norm). (Im Sinne von Homomorphismen)

$$S(\alpha + \beta) = S(\alpha) + S(\beta)$$

bzw.

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

(vrgl mit (6.1) und dem Normbetrag in $k \in \mathbb{Q}(\sqrt{-1})$)

Definition. In einem quadratischen Zahlenkörper $k \in \mathbb{Q}\left(\sqrt{d}\right)$ heißt ein Element $\alpha \in k$ **ganz**, bzw. **ganzalgebraisch**, falls Spur und Norm von α ganzzahlig sind: $S(\alpha),\ N(\alpha) \in \mathbb{Z}$, Insbesondere sind alle „ganz rationalen" Zahlen $\alpha \in \mathbb{Z}$ auch ganz in jedem quadratischen Zahlenkörper (insofern ist das eine sinnvolle Ausdehnung des **Ganzheitsbegriffserweiterung**).

05.06.08

Satz 7.2. *Sei $k = \mathbb{Q}\left(\sqrt{d}\right)$ ein quadratischer Zahlenkörper. Dann ist die Menge aller ganzen Zahlen in $\mathbb{Q}\left(\sqrt{d}\right)$*

$$\mathcal{O}_d := \left\{\alpha \in \mathbb{Q}(\sqrt{d}) \mid \alpha \text{ ganz}\right\}$$

*ein kommutativer Ring und wird der **Ganzheitsring** (bzw. **Hauptordnung**) von $k \in \mathbb{Q}(\sqrt{d})$ genannt. Es gilt*

$$\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\vartheta = \{a + b\vartheta \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[\vartheta]$$

mit

$$\vartheta := \begin{cases} \frac{1}{2}(1+\sqrt{d}), & \text{falls } d \equiv 1 \mod 4, \\ \sqrt{d}, & \text{falls } d \equiv 3, 2 \mod 4. \end{cases}$$

Bemerkung. Beachte hierbei: mit $\alpha = a + b\vartheta$ ist auch stets das konjugierte Element $\alpha' = a - b\vartheta$, falls $d \equiv 2, 3 \mod 4$ bzw. $\alpha' = a + b - b\vartheta$ falls $d \equiv 1 \mod 4$ ganz ist.

Beweis. Gegeben ist $\alpha = a + b\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right)$, dann gilt

$$\alpha \in \mathcal{O}_d \Leftrightarrow S(\alpha), N(\alpha) \in \mathbb{Z} \Leftrightarrow 2a, a^2 - db^2 \in \mathbb{Z}$$

Die letzte Bedingung ist für beliebige d und für alle $a, b \in \mathbb{Z}$ erfüllt. Ist $d \equiv 1 \mod 4$ und $a = \frac{1}{2}A,\ b = \frac{1}{2}B$ mit $A; B \in \mathbb{Z},\ A \equiv B \mod 2$, so ist

$$a^2 - db^2 = \frac{1}{4}(A^2 - dB^2) \in \mathbb{Z} \text{ und } 2a = A \in \mathbb{Z}$$

und die angegebenen Elemente ganz, insbesondere ist $\alpha = a + b\sqrt{d} = \frac{1}{2}\left(A + B\sqrt{d}\right)$

$$\alpha = \frac{1}{2}(A - B) + \frac{1}{2}\left(1 + \sqrt{d}\right) B \in \mathbb{Z} + \mathbb{Z}\vartheta \text{ mit } \vartheta = \frac{1}{2}\left(1 + \sqrt{d}\right).$$

Nun zeigen wir, dass keine ganzen Zahlen vergessen werden. Wegen $2a \in \mathbb{Z}$ ist

$$4db^2 = (2a)^2 - 4\underbrace{(a^2 + db^2)}_{=N(\alpha)\in\mathbb{Z}} \in \mathbb{Z}$$

und da d quadratisch ist, folgt $2b \in \mathbb{Z}$. Also gibt es $A, B \in \mathbb{Z}$ mit $2a = A,\ 2b = B$ und aus $a^2 - db^2 \in Z$ folgt $A^2 - dB^2 \equiv 0 \mod 4$. Für $d \not\equiv 1 \mod 4$ ist dies nur für gerades A und B möglich (denn die Quadrate $\mod 4$ sind 0,1), was zu $a, b \in \mathbb{Z}$ führt.

Für $d \equiv 1 \mod 4$ ergibt sich als äquivalente Bedingung

$$A \equiv B \mod 2$$

(denn $0 \equiv A^2 + B^2 \equiv A^2 - B^2 = (A-B)(A+B) \mod 4$), wie oben.

Also gilt $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\vartheta$ mit ϑ wie im Satz. Es verbleibt die Ringstruktur nachzuweisen. Nachrechnen: N.a.

$$(\alpha + \beta\vartheta) \cdot (\tilde{\alpha} + \tilde{\beta}\vartheta)R = \alpha\tilde{\alpha} + \underbrace{\beta\tilde{\beta}\vartheta^2}_{\in \mathcal{O}_d} + (\alpha\tilde{\beta} + \tilde{\alpha}\beta)\vartheta;$$

hierin ist $\vartheta^2 = d \in \mathbb{Z}$, falls $d \equiv 2, 3 \mod 4$. bzw.

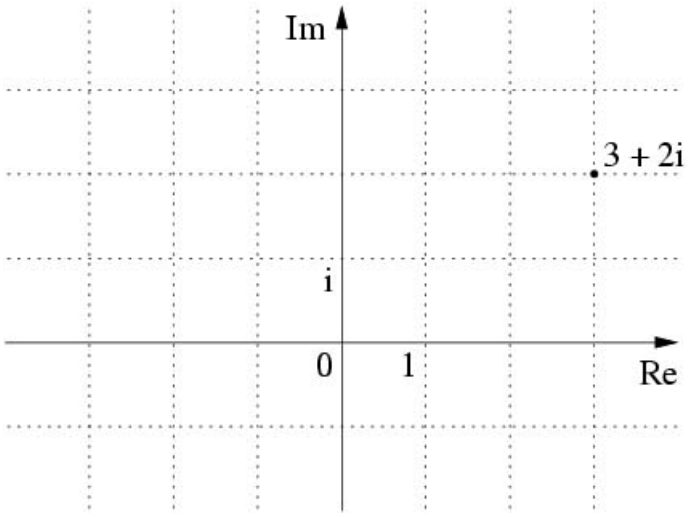
$$\begin{aligned} \vartheta &= \frac{1}{4}(1 + 2\sqrt{d} + d) \text{ falls } d \equiv 1 \mod 4 \\ &= \frac{d-1}{4} + \frac{1}{2}(1 + \sqrt{d}) \in \mathbb{Z} + \mathbb{Z}\vartheta. \end{aligned}$$

□

Bemerkung. Die Zahlen 1 und ϑ aus Satz 7.2 bildet eine so genannte **Ganzheitsbasis** von $\mathcal{O}_d$, das heißt, jede ganze Zahl von $\mathbb{Q}\left(\sqrt{d}\right)$ lässt sich eindeutig darstellen als Linearkombination der jeweils ganzen Zahlen 1 und ϑ.

Beispiel.

1. Die **Gaußschen Zahlen** $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ (vrgl. Kapitel 6) bilden den Ganzheitsring zum quadratischen Zahlenkörper $\mathbb{Q}(i)$. Die Identität (6.1) aus dem Beweis von Satz 6.1 spiegelt die Multiplikativität der Norm in $\mathbb{Z}[i]$ wieder. Betrachtet man die relle und die komplexe Achse, so sieht man hier eine Gitterstruktur. Allgemein haben gewisse Ganzheitsringe eine **Gitterstruktur**!



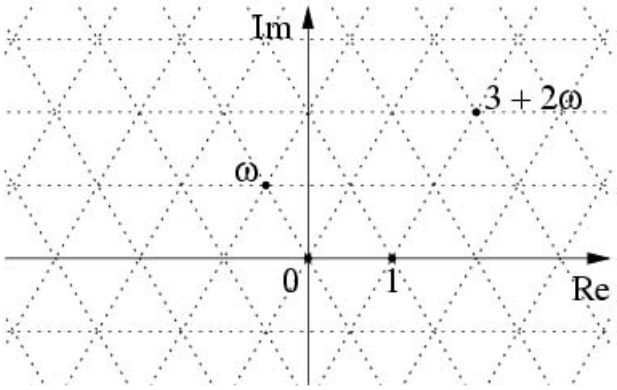
2. Die **Eisensteinschen Zahlen**

$$\mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta \qquad \zeta = \exp\left(\frac{2\pi i}{3}\right) = \frac{-1+\sqrt{-3}}{2},$$

sind der Ganzheitsring zu $\mathbb{Q}(\sqrt{-3})$. Hierbei ist ζ eine **dritte Einheitswurzel** und die Normalabbildung ist hier

$$N(a+b\zeta) = (a+b\zeta)\cdot(a+b\zeta)' = a^2 - a\cdot b + b^2$$

bzw. im Sinne der Funktionentheorie $(a+b\zeta)\cdot\overline{(a+b\zeta)}$.



Bemerkung. In Analogie zu Satz 6.1 kann man zeigen, dass genau die Primzahlen $p = 3$ und $p \equiv 1 \mod 3$ sich durch diese quadratische Form darstellen lassen

$$a^2 - ab + b^2.$$

Beispiel.

$$7 = 3^2 - 3\cdot 1 + 1^2$$

Definition. Ein quadratischer Zahlenkörper heißt **rell quadratisch**, wenn d positiv ist, und **imaginär quadratisch**, wenn d negativ ist (je nachdem ob also $k = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$, bzw. $\not\subset \mathbb{R}$). Die Arithmetrik der quadratischen Zahlenkörper $\mathbb{Q}(\sqrt{d})$ bzw. ihrer Ganzheitsringe hängt stark von der Größe d ab.

8. Euklidische und faktorielle Ganzheitsringe

Wir erweitern die Teilbarkeitsbegriff auf Ringe. Ein kommutativer Ring $\mathcal{R}$ mit Einselement heißt **Integritätsbereich**, wenn $\mathcal{R} \neq \{0\}$ und keine Nullteiler existieren, das heißt, dass keine Ringelemente $r \neq 0$ mit $rs = 0$ für ein $s \neq 0$ existieren. (Vrgl. $\mathbb{Z}/4\mathbb{Z}: \ 2 \cdot 2 \equiv 0 \mod 4$) Sowohl $\mathbb{Z}$ als auch jeder Ganzheitsring eines (quadratischen) Zahlenkörpers sind Integritätsbereiche (klar).

Definition. Ist $\mathcal{R}$ ein Integritätsbereich, so sagen wir, „α teilt β“ für $\alpha, \beta \in \mathcal{R}$, in Zeichen „$\alpha|\beta$“, wenn $\beta = \alpha \cdot \gamma$ für ein $\gamma \in \mathcal{R}$ gilt; ansonsten schreiben wir „$\alpha \not| \beta$“.
Die Teiler des Einselementes $\underline{1}$ heißen **Einheiten** und die Menge aller Einheiten bilden eine mulitplikative Gruppe, die Einheitsgruppe

$$\mathcal{R}^* := \{\varepsilon \in \mathcal{R} \ \ \varepsilon|\underline{1}\}$$

Zwei Elemente $\alpha, \beta \in \mathcal{R}$ heißen **assoziiert**, wenn $\alpha = \varepsilon\beta$ mit einer Einheit $\varepsilon \in \mathcal{R}^*$, sie sich also nur um eine Einheit unterscheiden.

Bemerkung. Die Rechenregeln zur Teilbarkeit übertragen sich ohne wesentliche Einschränkung von $\mathbb{Z}$ auf Integritätsbereiche $\mathcal{R}$. In allgemeinen Ringen können Nullteiler Schwierigkeiten bereiten.

Sei jetzt $k = \mathbb{Q}\left(\sqrt{d}\right)$ und $\beta = \alpha\gamma$ eine Zerlegung im Ganzheitsring $\mathcal{O}_d$. Dann gilt mit der Multiplikativität der Norm:

$$N(\beta) = N(\alpha) \cdot N(\gamma) \qquad \text{(folgt aus der Faktorisierung von } \mathbb{Z})$$

Also hat man die Teiler von β unter den Elementen zu suchen, deren Norm $N(\beta)$ teilt. (ein Teilbarkeitsproblem in $\mathbb{Q}$ bzw. $\mathbb{Z}$) Speziell für $\beta = 1$ folgt, dass ε genau dann eine Einheit in $\mathcal{O}_d$ ist, wenn $N(\varepsilon) = +1$ ist. Mit Satz 7.2 folgt:

- $d \equiv 2, 3 \mod 4: \ \varepsilon = a + b\sqrt{d}$ ist Einheit $\Leftrightarrow \overbrace{a^2 - db^2}^{N(\varepsilon)} = \pm 1$
- $d \equiv 1 \mod 4: \ \varepsilon = \frac{1}{2}\left(a + b\sqrt{d}\right)$ ist Einheit $\Leftrightarrow a^2 - db^2 = \pm 4$

jeweils mit $a, b \in \mathbb{Z}$. Speziell für imaginär-quadratische Zahlenkörper gilt:

Satz 8.1. *Die Einheiten von $\mathcal{O}_d$ mit $d < 0$ sind*

1. $\pm 1, \pm i$ *für* $d = -1$
2. $\pm 1, \pm\omega, \pm\omega^2$ *mit* $\omega = \exp\left(\frac{2\pi i}{6}\right)$ *für* $d = -3$

3. ± 1 *sonst*

Bemerkung. Es treten also nur Einheitswurzeln auf. Es sind die vierten Einheitswurzeln bei den **Gaußschen Zahlen** $\mathbb{Z}[i]$ und die sechsten Einheitswurzeln im Falle der Eisensteinschen Zahlen $\mathbb{Z}[\zeta]$, ansonsten nur ± 1.

Beweis. Für $d < 0$ ist stets $a^2 - db^2 \geq 0$.
Für $d \equiv 2, 3 \mod 4$ gilt

$$1 = a^2 - db^2 = a^2 + |d|\, b^2 \Leftrightarrow \begin{cases} a \text{ oder } b = \pm 1, & ab = 0 \text{ falls } d = -1 \\ a = \pm 1,\ b = 0, & \text{sonst} \end{cases}$$

bzw. für $d \equiv 1 \mod 4$

$$4 = a^2 + |d|\, b^2 \Leftrightarrow \begin{cases} a = \pm 2,\ b = 0, & \text{für } d < -4 \\ a = \pm 2,\ b = 0, & \text{für } d = -3 \\ a = \pm 1,\ b = \pm 1, & \text{für } d = -3 \end{cases}$$

(Man beachte hierbei $\omega = \zeta + 1$ bzw. $\omega^2 = \omega - 1$ im Falle $d = -3$.) □

Bemerkung. Im Gegensatz dazu ist die Einheitengruppe von reell-quadratischen Zahlenkörpern **nicht** endlich. Hierzu gibt es neben ganzrationellen Einheiten ± 1 stets noch mindestens eine weitere Einheit $\varepsilon > 1$ und insbesondere mit all den Potenzen ε^n gleich unendlich viele, zum Beispiel:

$$\begin{aligned} 1 - \left(3 - 2\sqrt{2}\right) \cdot \left(3 + 2\sqrt{2}\right) &= 3^2 - 2 \cdot 2^2 \\ \rightsquigarrow \varepsilon &= 3 + 2\sqrt{2} > 1 \\ \rightsquigarrow \varepsilon^2 &= \left(3 + 2\sqrt{2}\right)^2 = 17 + 12\sqrt{2}, \\ 17^2 - 2 \cdot 12^2 &= +1, \ldots \end{aligned}$$

Eine genauere Beschreibung dieser Einheitengruppen gelingt uns später durch das Studium der **Pellschen Gleichung**

$$X^2 - dY^2 = \pm 1$$

Sei $\mathcal{R}$ ein Integritätsbereich. Dann heißt ein Element $0 \neq \pi \in \mathcal{R} \backslash \mathcal{R}^*$ **prim**, falls für alle $\alpha, \beta \in \mathcal{R}$ aus $\pi | \alpha\beta$, stets $\pi | \alpha$ oder $\pi | \beta$ folgt. π heißt **irreduzibel**, wenn aus $\pi = \alpha\beta$ für $\alpha, \beta \in \mathcal{R}$ folgt, dass π zu α oder β assoziiert ist (der andere Faktor also eine Einheit ist); ein nicht irreduzibles Element ist **reduzibel**. In $\mathbb{Z}$ fallen die Begriffe **prim** und **irreduzibel** zusammen: Das Lemma von Euklid (Satz1.4) rechtfertigt die in $\mathbb{Z}$ irreduziblen Elemente **prim** (Primzahl) nennen zu dürfen. In einem Ganzheitsring können diese Begriffe allerdings verschiedenes Bedeuten!

Beispiel. von **Dedekind**:
$2, 3, 1 \pm \sqrt{-5}$ sind irreduzibel in $\mathbb{Z}\left[\sqrt{-5}\right]$, aber nicht prim, denn: Sei etwa

$$2 = \alpha \cdot \beta \text{ mit } \alpha, \beta \in \mathbb{Z}\left[\sqrt{-5}\right].$$

Mit der Norm

$$N\left(a+b\sqrt{-5}\right)=a^2+5b^2\in\mathbb{Z},$$

aber $\neq\pm2$, ergibt sich aus

$$4=N(2)=N(\alpha)\cdot N(\beta)$$

ohne Einschränkung $N(\alpha)=1$ bzw. $\alpha=\pm1$ nach Satz 8.1, also ist 2 irreduzibel, jedoch nicht prim, da

$$6=2\cdot3=\left(1\sqrt{-5}\right)\cdot\left(1+\sqrt{-5}\right),$$

2 allerdings keinen der Faktoren $1\pm\sqrt{-5}$ teilt. (Ansatz: $2\left(a+b\sqrt{-5}\right)=1\pm\sqrt{-5}$ führt auf $2\cdot a=1,\ 2b=\pm1$, unmöglich!) Bei der anderen ganz algebraischen Zahlen $3,1\pm\sqrt{-5}$ verfährt man ganz genauso.

12.06.08

Definition. Ein **Integritätsbereich**, in dem jedes Element $\neq0$, das keine Einheit ist, in ein Produkt von primen Elementen zerlegt werden kann, heißt **faktorieller Ring**; jedes solche Produkt nennt man eine **Primfaktorzerlegung**. Insbesondere ist $\mathbb{Z}$ (nach Satz 1.5) ein faktorieller Ring, $\mathbb{Z}\left[\sqrt{-5}\right]$ hingegen nicht, neben den wesentlich verschiedenen Zerlegungen $6=2\cdot3=\left(1+\sqrt{-5}\right)\cdot\left(1-\sqrt{-5}\right)$ in irreduzible, aber nicht primen Faktoren, bestehen nämlich bis auf Assoziiertheit keine weitere!

Satz 8.2. *Sei $\mathcal{R}$ ein Integritätsbereich.*

1. *Jedes prime Element von $\mathcal{R}$ ist irreduzibel.*
2. *In einem faktoriellen Ring $\mathcal{R}$ ist jedes irreduzible Element auch prim und die Primfaktorzerlegung ist (bis auf Assoziiertheit und Reihenfolge der Faktoren)* ***eindeutig!***

Beweis. 1. Angenommen π ist **prim** mit $\pi=\alpha\cdot\beta$, dann gilt insbesondere $\pi|\alpha\beta$, bzw. $\pi|\alpha$ etwa. Also $\alpha=\pi\cdot\gamma$ für ein $\gamma\in\mathcal{R}$ und damit $\pi=\alpha\beta=\beta\gamma\pi$. Da $\mathcal{R}$ ein Integritätsbereich ist, folgt $1=\beta\gamma$, das heißt β und γ sind Einheiten und $\alpha=\pi\gamma$ ist assoziiert zu π. Damit ist π irreduzibel.

2. (wie beim Beweis vom Fundamentalsatz 1.5): Da sich jedes irreduzible Element nicht weiter in Primfaktoren zerlegen lässt, muss es in einem faktoriellen Ring prim sein. Gegeben zwei Primfaktorzerlegungen

$$r=\pi_1\cdot\ldots\cdot\pi_m=\omega_1\cdot\ldots\cdot\omega_n\in\mathcal{R}$$

Wegen $\pi_1|r$ teilt π_1 eines der ω_j, oBdA $\pi_1|\omega_1$. Also gilt $\omega_1=\pi_1\cdot\varepsilon$ für ein $\varepsilon\in\mathcal{R}$, da ω_1 irreduzibel ist, muss ε eine Einheit sein. Also sind π_1 und ω_1 assoziiert. Kürzen dieses Faktors π_1 und Wiederholen dieses Arguments bis alle Faktoren abgebaut sind (oder alternativ die Wohlordnung über die Normfunktion) liefert *2.*, also die Behauptung.

□

Bemerkung. Das Analogon der **eindeutigen Primfaktorzerlegung** in $\mathbb{Z}$ ist also nicht notwendig erfüllt in **Ganzheitsringen** von Zahlenkörpern.

Wie entscheidet man, ob ein gegebener Ganzheitsring faktoriell ist?

Definition. Ein **quadratischer Zahlenkörper** $\mathbb{Q}\left(\sqrt{d}\right)$ bzw. sein Ganzheitsring $\mathcal{O}_d$ heißt **normeuklidisch**, wenn

- zu $\alpha, \beta \in \mathcal{O}_d$ mit $\beta \neq 0$ existieren stets $\kappa, \varrho \in \mathcal{O}_d$ mit

  $$\alpha = \kappa \cdot \beta + \varrho$$

  wobei entweder $\varrho = 0$ oder $|N(\varrho)| < |N(\beta)|$ ist. Dies entspricht der Division mit Rest (nach dem Euklidischen Algorithmus)

Hierbei ist $N : \mathcal{O}_d \to \mathbb{Z},\ \alpha \mapsto N(\alpha) = \alpha \cdot \alpha'$, die Norm auf $\mathcal{O}_d$. Dies ermöglicht eine Variante des euklidischen Algorithmus (siehe Saz 1.2) und insbesondere die Definition eines ggT.
Äquivalent zu obiger Bedingung ist: $\mathcal{O}_d$ ist genau dann normeuklidisch, wenn

$\odot$ zu jedem $\gamma \in \mathbb{Q}(\sqrt{d})$ gibt es ein $\kappa \in \mathcal{O}_d$ mit $|N(\gamma - \kappa)| < 1$.
(folgt sofort mit $\gamma = \frac{\alpha}{\beta}$). Nebenrechnung:

$$\begin{aligned} \alpha = \kappa \cdot \eta + \varrho \,|N(\varrho)| &\qquad &< |N(\beta)| \\ \gamma = \frac{\alpha}{\beta} = \kappa \frac{\varrho}{\beta} &\qquad &|N(\gamma \cdot \kappa)| = \left|\frac{N(\varrho)}{N(\beta)}\right| < 1 \end{aligned}$$

Der Nachweis der Normeuklidizität reduziert sich damit auf das Auffinden eines „nahen Gitterpunktes“.

$\mathbb{Z}[i]$ ist normeuklidisch, denn $\gamma \in \mathbb{Q}(i)$

Bemerkung. Betrachtet man das Bild auf der komplexen Ebene so fällt auf, dass mit dem Nullpunkt und den Punkt $\kappa = 1 + i$ wird eine Quadrat aufgespannt wird. Innerhalb dieses Quadrates liegt der Punkt γ.

Satz 8.3. $\mathbb{Q}\left(\sqrt{d}\right)$ *ist normeuklidisch genau für*

1. $d = -1, -2, -3, -7, -11$, *falls* $d < 0$
2. $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$, *falls* $d > 0$.

Ferner gibt es noch quadratische Zahlenkörper wie zum Beispiel $\mathbb{Q}\left(\sqrt{69}\right)$, *die euklidisch sind in dem Sinne, dass die Bedingung der Normeuklidizität zwar nicht mit dem Betrag der Norm, aber einer anderen Funktion* $\mathcal{N} : \mathcal{O}_d \to \mathbb{N}_0$ *erfüllt ist. (*Clark, *1994).*

Beweis. 1. Für $d < 0$ ist der Ganzheitsring $\mathcal{O}_d = \mathbb{Z} + \vartheta\mathbb{Z}$ (mit ϑ gemäß Satz 7.2) ein Gitter in $\mathbb{C}$ und für die Normeuklidizität muss zu gegebenen $\gamma \in \mathbb{Q}\left(\sqrt{d}\right)$ nach $\odot$ ein Gitterpunkt κ mit Abstand < 1 existieren; die Norm $N\left(a + b\sqrt{d}\right) = a^2 - db^2$ ist ja gleich dem Quadrat des euklidischen Abstandes von $a + b\sqrt{d}$ zum Nullpunkt.

Sei zunächst $d = 2, 3 \mod 4$, dann ist $\mathcal{O}_d = \mathbb{Z}+\mathbb{Z}\sqrt{d}$ nach Satz 7.2 und die minimale Norm aller Differenzen $\gamma - \kappa$ maximal für den „Mittelpunkt“ $\gamma = \frac{1}{2}\left(1+\sqrt{d}\right)$ und etwa dem Nullpunkt. Äquivalent zur Normeuklidizität ist also:

$$\frac{1}{4}(1+|d|) = \left|N\left(\frac{1}{2}\left(1+\sqrt{d}\right)\right)\right| < 1 \qquad \text{nach } \odot$$

beziehungsweise

$$|d| < 3, \qquad \text{das heißt } d = -1, -2$$

Im Falle $d \equiv 1 \mod 4$ werden nach Satz 7.2 die Zahlen aus $\mathcal{O}_d = \mathbb{Z} + \frac{1}{2}\left(1+\sqrt{d}\right)\mathbb{Z}$ außer durch die eben betrachteten Gitterpunkte auch noch durch die **Maschenmittelpunkte** dargestellt.

Zu jedem Gitterpunkt κ ist die Menge aller Körperelemente γ, die minimalen Abstand zu κ haben, enthalten in einem Sechseck. (**Vornoi-Zelle**), deren Vereinigung über alle Gitterpunkte γ ganz $\mathbb{C}$ parkettiert. Das maximale Abstandsquadrat eines Punktes γ vom Mittelpunkt eines solchen Sechsecks ist etwa realisiert durch die Eckpunkte auf der positiven Achse $\gamma = \frac{1}{4}\left(\sqrt{d} - \frac{1}{\sqrt{d}}\right)$ und dem Nullpunkt. Somit muss für die Normeuklidizität also gelten:

$$\frac{1}{16}\left(|d| + 2 + \frac{1}{|d|}\right) = \left|N\left(\frac{1}{4}\left(\sqrt{d} - \frac{1}{\sqrt{d}}\right)\right)\right| < 1$$

bzw.

$$|d| < 14 \qquad \text{das heißt } d = -3, -7, -11$$

Das beweist *1.* .
In unserem letzten Argument haben wir benutzt, dass $\mathcal{O}_d$ die Struktur eines Gitters besitzt. (Zum Beispiel impliziert dies, dass alle Sechsecke oben kongruent sind). Dies ist jedoch nicht mehr erfüllt im reell-quadratischen Fall:

2. Beweis hier nur die Normeuklidizität nur für $d = 2$ und $d = 3$. (Das Argument lässt sich auf $d = 5, 13$ und sogar $d < 0$ ausdehnen, liefert aber nicht die volle Behauptung *2.*)
Gegeben ist $\gamma = \mathcal{X} - \mathcal{Y}\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right)$, wähle man $a, b \in \mathbb{Z}$ mit

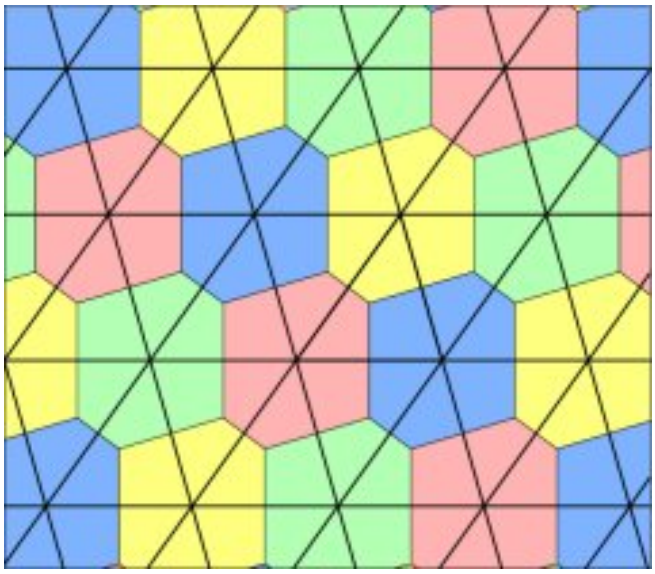
$$|\mathcal{X} - a| \leq \frac{1}{2},$$
$$|\mathcal{Y} - b| \leq \frac{1}{2}$$

Dann ist $\kappa = a + b\sqrt{d} \in \mathcal{O}_d$ (nach Satz 7.2) nahe γ:

$$\begin{aligned} |N(\gamma - \kappa)| &= \left|N\left(\mathcal{X} - a + (\mathcal{Y} - b)\sqrt{d}\right)\right| \\ &= \left|(\mathcal{X} - a)^2 - d(\mathcal{Y} - b)^2\right| < \frac{1}{4}(1+d) \overset{d=2,3}{\leq} 1. \end{aligned}$$

□

Bemerkung. Die eben angesprochene Vornoi-Zelle sieht in etwa so aus



Bemerkung. Die komplette Charakterisierung sämtlicher reell-quadratischer Zahlenkörper, die normeuklidisch sind, gelang Chatlend und Darenpart (1950) bzw. Barnes und Swinnerton-Dyer (1992)

Satz 8.4. *Ist $\mathcal{O}_d$ normeuklidisch, dann auch faktoriell, insbesondere ist $\mathcal{O}_d$ faktoriell für alle Werte von d aus Satz 8.2.*

Beweis. (Vergleich mit Kapitel 1, insbesondere Sätze 1.1 und 1.5). Seien $\alpha, \beta \in \mathcal{O}_d$ teilerfremd, das heißt sie besitzen keine gemeinsamen Faktoren aus $\mathcal{O}_d$ außer höchstens Einheiten sie

$$\mathcal{L} = \{\alpha\mathcal{X} + \beta\mathcal{Y} \mid \mathcal{X}, \mathcal{Y} \in \mathcal{O}_d\}$$

sowie

$$\varepsilon = \alpha\tilde{\mathcal{X}} + \beta\tilde{\mathcal{Y}} \in \mathcal{L}\backslash\{0\}$$

so gewählt, dass $|N(\varepsilon)|$ minimal ist. (möglich wegen der Ganzzahligkeit der Norm $[|N(\varepsilon)| \in \mathbb{N}]$ zusammen mit der Wohlordnung). Mit dem euklidischen Algorithmus angewandt auf α und ε gibt es $\gamma, \delta \in \mathcal{O}_d$, so dass

$$\alpha = \gamma\varepsilon + \delta \qquad \text{mit } |N(\delta)| < |N(\varepsilon)|\,.$$

Es ist

$$\begin{aligned}\delta\alpha - \gamma\varepsilon &= \alpha - \gamma(\alpha\tilde{x} - \beta\tilde{y}) \\ &= \alpha(1 - \gamma\tilde{x}) + \beta(-\gamma\tilde{y}) \in \mathcal{L}\end{aligned}$$

Wegen der Minimalität von $|N(\varepsilon)| \in \mathbb{N}$ muss $N(\delta) = 0$ gelten, was auf $\delta = 0$ bzw. $\alpha = \gamma\varepsilon$ führt. Also gilt $\varepsilon|\alpha$. und analog $\varepsilon|\beta$. Damit ist ε eine Einheit (da α, β teilerfremd), und es gibt daher zu teilerfremden α, β stets $\hat{\mathcal{X}}, \hat{\mathcal{Y}} \in \mathcal{O}_d$ mit

$$1 = \alpha\hat{\mathcal{X}} + \beta\hat{\mathcal{Y}} \tag{8.1}$$

Sei nun $\pi \in \mathcal{O}_d$ irreduzibel sowie $\pi|\alpha\beta$ für alle $\alpha, \beta \in \mathcal{O}_d$. Falls $\pi \nmid \alpha$, so haben π und α außer Einheiten keine gemeinsamen Faktoren. Nach Formel (8.1) existieren somit $\mathcal{X}, \mathcal{Y} \in \mathcal{O}_d$, sodass $\pi\mathcal{X}+\alpha\mathcal{Y} = 1$ bzw. $\beta = \pi\beta\mathcal{X}+\alpha\beta\mathcal{Y}$. Letzteres liefert nun $\pi|\beta$ und per Induktion ergibt sich daraus: Gilt $\pi|\alpha_1 \cdot \ldots \cdot \alpha_n$, wobei π irreduzibel und $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_d$, so teilt π mindestens einen Faktor α_j. Insbesondere ist jedes irreduzible Element $\mathcal{O}_d$ auch prim und der Rest des Beweises ist identisch mit dem Beweis des Fundamentalsatzes 1.5. □

13.06.08

Bemerkung. Die Umkehrung des Satzes gilt nicht. Neben den durch die Sätze 8.3 und 8.4 nachgewiesenen faktoriellen Ganzheitsringen ist ferner $\mathcal{O}_d$ nur faktoriell für

$$d = -19,\ -43,\ -67,\ -163$$

im imaginär-quadratischem Fall ($d < 0$), was einer Vermutung von Gauß bestätigte und erst 1967 von Baker und (unabhängig von ihm) Stark bewiesen wurde. Im schwierigen reell-quadratischen Fall ($d > 0$) werden unendlich viele faktorielle $\mathcal{O}_d$ erwartet...

9. Zerlegung von Primzahlen

Bemerkung. Für jeden Ganzheitsring $\mathcal{O}_d = \mathbb{Z}[\vartheta]$ (mit ϑ gemäß Satz 7.2) gilt $\mathbb{Z}[\vartheta] \cap \mathbb{Q} = \mathbb{Z}$, das heißt die ganzrationalen Elemente eines (quadratischen) Zahlenkörpers sind genau die ganzen Zahlen. Wir untersuchen nun die Teilbarkeitseigenschaften der primen Elemente von $\mathbb{Z}$ (Primzahlen) in $\mathcal{O}_d$.

Unser wichtigstes Werkzeug ist hierbei wieder die **Norm**

Satz 9.1. *Sei $\mathcal{O}_d$ der Ganzheitsring eines Zahlenkörpers $\mathbb{Q}\left(\sqrt{d}\right)$. Dann gibt es zu jedem Primelement $\pi \in \mathcal{O}_d$ genau eine rationale Primzahl p mit $\pi | p$, insbesondere gilt:*

$$N(\pi) = \pm p \qquad \textit{oder } \pm p^2.$$

Beweis. Wegen $\pi | \pi\pi' = N(\pi)$ teilt π einen Primteiler p der ganzen Zahl $N(\pi)$. Wäre ebenso $\pi | q$ für eine weitere Primzahl $q \neq p$, so würde π auch den $\mathrm{ggT}(p, q) = 1$ teilen und π wäre damit eine Einheit. Durch Bildung der Norm wird aus $\pi | p$ nun

$$N(\pi) | N(p) = p^2$$

und wegen $N(\pi) \neq \pm 1$ ergibt sich

$$N(\pi) \in \{\pm p, \pm p^2\}.$$

□

Bemerkung. Satz 9.1 entsprechend gibt es folgende Möglichkeiten wie sich eine rationale Primzahl p in einen Ganzheitsring zerlegen lässt:

- p bleibt auch in $\mathcal{O}_d$ prim
- p ist in $\mathcal{O}_d$ nicht prim, aber irreduzibel
- p ist reduzibel in $\mathcal{O}_d$

Der zweite Fall kann nur eintreten, wenn $\mathcal{O}_d$ **nicht** faktoriell ist (siehe Satz 8.2), was wir im Folgenden aber ausschließen wollen. Am interessantesten ist der **dritte Fall**: Hier ist $p = \alpha\beta$ für Nichteinheiten $\alpha, \beta \in \mathcal{O}_d$. Aus

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

ergibt sich

$$N(\alpha) = N(\beta) = \pm p.$$

Wegen $\pm p = N(\alpha) = \alpha\alpha'$ mit dem Konjugierten α', folgt $\beta = \pm\alpha'$. Mit π statt α gilt also

$$p = \pm\pi\pi',$$

wobei π und π' prim mit Norm $\pm p$ sind.

Definition. Hier stellt sich die Frage, ob π und π' **wesentlich verschieden** sind. Wir sagen

- p ist **träge**, falls p auch in $\mathcal{O}_d$ prim ist,
- p ist **zerlegt**, falls $p = \pm\pi\pi' (= \pm N(\pi))$ für zwei nicht assoziierte, aber algebraisch konjugierte prime Elemente $\pi, \pi' \in \mathcal{O}_d$,
- p ist **verzweigt**, falls $p = \varepsilon\pi^2$ für eine Einheit ε und ein Primelement $\pi \in \mathcal{O}_d$.

Der Zerlegungstyp einer Primzahl p in einem faktoriellen Ganzheitsring lässt sich aus dem Werten des **Legendre-Symbols** ablesen (hier bilder die einzige gerade Primzahl eine Ausnahme). Wir definieren die **Diskriminante** des quadratischen Zahlenkörpers $\mathbb{Q}\left(\sqrt{d}\right)$ durch

$$D = \begin{cases} 4d, & \text{falls } d \not\equiv 1 \mod 4, \\ d, & \text{falls } d \equiv 1 \mod 4 \end{cases}$$

Man beachte, dass stets $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{D}\right)$ ist.

Bemerkung. In Verbindung mit Satz 7.2 beobachten wir, dass für den zugehörigen Ganzheitsring stets $\mathcal{O}_d = \mathbb{Z}\left[\frac{1}{2}\left(D = \sqrt{D}\right)\right]$ gilt, also $1, \frac{1}{2}\left(D + \sqrt{D}\right)$ ungeachtet der Restklasse $d \mod 4$ immer eine Ganzheitsbasis bildet.

Satz 9.2. ***Zerlegungsgesetz für Primzahlen, Satz von Euler, Gauß:***
Es sei $\mathcal{O}_d$ ein faktorieller Ring und p eine ungerade Primzahl. Dann gilt:

$$p \textit{ ist } \left\{ \begin{array}{c} \textit{verzweigt} \\ \textit{zerlegt} \\ \textit{träge} \end{array} \right\} \Leftrightarrow \left(\frac{D}{p}\right) = \begin{cases} 0 \\ +1 \\ -1 \end{cases}$$

sowie

$$2 \textit{ ist } \left\{ \begin{array}{c} \textit{verzweigt} \\ \textit{zerlegt} \\ \textit{träge} \end{array} \right\} \Leftrightarrow \begin{cases} 2|D, & \textit{(wie oben)} \\ D \equiv 1 \mod 8 \\ D \equiv 5 \mod 8 \end{cases}$$

Beweis. 1. Ist $p \neq 2$ ein Teiler von D oder $p = 2$ ein Teiler von d, so ist p ein Teiler von d. Falls $p = |d|$, so folgt $p = \sqrt{d} \cdot \sqrt{d}$ und p ist verzweigt in $\mathcal{O}_d$. Ist $p < |d|$, so schreiben wir $d = p \cdot \underbrace{\frac{d}{p}}_{\in\mathbb{Z}} = \sqrt{d} \cdot \sqrt{d}$, jedoch ist p kein Teiler von $\sqrt{f}$ in $\mathcal{O}_d$ (denn d ist quadratfrei) und somit ist p nicht prim in $\mathcal{O}_d$, das heißt es gibt nach Satz 9.1 ein Primelement $\pi \in \mathcal{O}_d$ mit $p = \pm\pi\pi'$ und $\pi \not| \frac{d}{p}$. Da aber nach obigen π auch $\sqrt{d}$ teilt, also auch $\pi^2 | d$. Es folgt, dass $\pi^2 | p$ und p ist somit verzweigt. Ist $p = 2$ ein Teiler von D, aber nicht von d, so ist $d \equiv 3 \mod 4$. Es gilt:

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

und $2 \not| (d \pm \sqrt{d})$ ist kein Primelement in $\mathcal{O}_d$. Also gibt es ein Primelement $x \pm y\sqrt{d} \in \mathcal{O}_d$ mit

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

Damit ist

$$\varepsilon := \pm \frac{x - y\sqrt{d}}{x + y\sqrt{d}} = \pm \frac{x^2 + dy^2 - 2xy\sqrt{d}}{x^2 - dy^2} = \frac{1}{2}(x^2 + dy^2) - xy\sqrt{d} \in \mathcal{O}_d$$

sowie

$$\frac{1}{\varepsilon} := \pm \frac{x + y\sqrt{d}}{x - y\sqrt{d}} = \ldots = \frac{1}{2}(x^2 + dy^2) + xy\sqrt{d} \in \mathcal{O}_d$$

Insbesondere ist ε eine Einheit und also $x + y\sqrt{d}$ und $x - y\sqrt{d}$ assoziiert. Dies schließt jetzt die Fälle **verzweigt** ab.

2. Sei nun $p \neq 2$ teilerfremd zu D. Gilt:

$$\left(\frac{d}{p}\right) = \left(\frac{D}{p}\right) = +1,$$

so existiert ein $\mathcal{X} \in \mathbb{Z}$ mit $\mathcal{X}^2 - d \equiv 0 \mod p$. Wäre p prim in $\mathcal{O}_d$, so wäre p ein Teiler von $\mathcal{X} + \sqrt{d}$ und $\mathcal{X} - \sqrt{d}$ ($(\mathcal{X} - \sqrt{d}) \cdot (\mathcal{X} + \sqrt{d}) = \mathcal{X}^2 - d$) und eine der Zahlen $\frac{1}{p}(\mathcal{X} \pm \sqrt{d})$ wäre in $\mathcal{O}_d$ enthalten, was nach Satz 7.2 unmöglich ist.

Also existiert ein Primelement

$$\pi = x + y\sqrt{d} \in \mathcal{O}_d,$$

so dass

$$\pm p = \pi\pi' = \left(x + y\sqrt{d}\right) \cdot \left(x - y\sqrt{d}\right) = x^2 - dy^2.$$

Sei zunächst $d \neq 1 \mod 4$. Angenommen π und $\pi' = x - y\sqrt{d}$ sind **assoziiert**, dann wäre

$$\pm \frac{x + y\sqrt{d}}{x - y\sqrt{d}} = \pm \frac{1}{p}\left(x^2 + dy^2 + 2xy\sqrt{d}\right) \in \mathcal{O}_d$$

und insbesondere p ein Teiler von x und y (!), ein **Widerspruch**. Ist $d \equiv 1 \mod 4$ und wäre π und π' **assoziiert**, so wäre nach Satz 7.2

$$\pm 4p = \left(\mathcal{X} + \mathcal{Y}\sqrt{d}\right) \cdot \left(\mathcal{X} - \mathcal{Y}\sqrt{d}\right) = \mathcal{X}^2 - d\mathcal{Y}^2$$

mit gewissen $\mathcal{X}, \mathcal{Y} \in \mathbb{Z}$. Wie oben folgte der **Widerspruch** durch $p|\mathcal{X}$ und $p|\mathcal{Y}$. Also ist p zerlegt.

3. Sei nun $\left(\frac{D}{p}\right) = -1$. Angenommen, p wäre nicht prim in $\mathcal{O}_d$, dann gäbe es ein Primelement

$$\pi = x + y\sqrt{d} \in \mathcal{O}_d$$

mit

$$\pm p = x^2 - dy^2.$$

Dann ist

$$\pm 4p = (2x)^2 - d(2y)^2$$

bzw.

$$(2x)^2 \equiv d(2y)^2 \mod p$$

mit $2x, 2y \in \mathbb{Z}$. Gilt hier $p|(2x)$ oder $p|(2y)$, so folgte $p^2|(4p)$, ein **Widerspruch**. Also sind $2y$ und p teilerfremd und somit gibt es $z \in \mathbb{Z}$ mit

$$2yz \equiv 1 \mod p$$

bzw.

$$(2xz)^2 \equiv d(2yz)^2 \equiv d \mod p.$$

Es folgt $\left(\frac{d}{p}\right) = +1$, ein **Widerspruch**. Dies schließt die Fälle **zerlegt** und **träge** bei ungeraden Primzahlen ab.

4. Es verbleibt $p = 2$ im Falle der Teilerfremdheit mit D zu untersuchen. In diesem Falle ist $d \equiv 1 \mod 4$. Ist $p = 2$ nicht prim in $\mathcal{O}_d$, so gibt es ein Primelement

$$\pi = \frac{1}{2}\left(x + y\sqrt{d}\right) \in \mathcal{O}_d$$

(nach Satz 7.2), so dass

$$\pm 2 = \frac{1}{4}(x^2 - dy^2)$$

bzw.

$$\pm 8 = x^2 - dy^2$$

Für gerade $x = 2\mathcal{X}$, $y = 2\mathcal{Y}$ folgte $\mathcal{X}^2 - d\mathcal{Y}^2 = \pm 2$, was mit $d \equiv 1 \mod 4$ unvereinbar ist. Also sind x und y ungerade. Wegen

$$x^2 \equiv y^2 \equiv 1 \mod 8$$

folgt aus obigen

$$1 - d \equiv x^2 - dy^2 \equiv 0 \mod 8,$$

also $d \equiv 1 \mod 8$. Damit ist 2 prim in $\mathcal{O}_d$ für

$$D \equiv d \equiv 5 \mod 8.$$

Für $d \equiv 1 \mod 8$ ist

$$\frac{1}{4}(1-d) = 2 \cdot \frac{1}{8}(1-d) = \frac{1}{2}\left(1-\sqrt{d}\right) \cdot \left(1+\sqrt{d}\right),$$

wobei $2 \nmid \frac{1}{2}\left(1 \pm \sqrt{d}\right)$ und 2 ist deshalb nicht prim in $\mathcal{O}_d$. Jetzt hat man wie oben $\pm 2 = \pi\pi'$ mit $\pi = \frac{1}{2}\left(x + y\sqrt{d}\right)$ prim in $\mathcal{O}_d$, $\pi' = \frac{1}{2}(x - dy)$ prim in $\mathcal{O}_d$. π und π' sind nicht assoziiert, denn wiederum mit ungeraden x, y gilt:

$$\frac{x + y\sqrt{d}}{x - y\sqrt{d}} = \pm\frac{1}{8}(x^2 + dy^2) \pm \frac{1}{4}xy\sqrt{d} \in \mathcal{O}_d.$$

Das schließt den Fall $p = 2$ ab.
Der Satz ist also vollständig bewiesen. □

Bemerkung. Der Satz erlaubt einige interessante Anwendungen. Für den Ring $\mathbb{Z}[i]$ ergibt sich mit dem 1. Ergänzungssatz (Korollar 5.6)

- $2 = -i(1+i)^2 = N(1+i)$ ist verzweigt,
- alle rationalen Primzahlen $p \equiv -3 \mod 4$ sind **träge** (denn $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$)
- alle rationalen Primzahlen $p \equiv -1 \mod 4$ sind **zerlegt**.

in $\mathbb{Z}[i]$. Die letzte Behauptung besagt, dass Primzahlen $p \equiv 1 \mod 4$ von der Form $p = \pi\pi'$ nicht assoziierten konjugierten Primelementen $\pi = x + iy$, $\pi' = x - iy \in \mathbb{Z}[i]$; es gilt

$$p = N(\pi) = \pi\pi' = x^2 + y^2.$$

Dies liefert deinen zweiten Beweis für Satz 6.1. Satz 9.2 erlaubt viele weitere ähnliche Darstellungssätze:

Korollar 9.3. *Eine rationale Primzahl p wird genau dann durch die quadratische Form*

$$x^2 - xy + y^2$$

dargestellt, wenn $p \equiv 3$ oder $p \equiv 1 \mod 3$ ist.

19.06.08

Beweis. Der Ring der Eisensteinschen Zahlen $\mathbb{Z}[\zeta]$ mit $\zeta = \frac{-1+\sqrt{-3}}{2}$ (Beispiel 7.*ii*) ist faktoriell (nach Satz 8.3 und 8.4). Die rationalen Primzahlen zerlegen sich nach Satz 9.2 wie folgt:

- $3 = -\left(\sqrt{-3}\right)^2 = N(1-\zeta)$ ist verzweigt,
- alle rationalen Primzahlen $p \equiv 2 \mod 3$ sind träge,
- alle rationalen Primzahlen $p \equiv 1 \mod 3$ sind zerlegt.

Die Norm von $\pi = x + y\zeta$ ist gegeben durch $N(\pi) = x^2 - xy + y^2$ (siehe Beispiel 7.*ii*). Das liefert die Behauptung. □

Bemerkung. Euler entdeckte dasss das Polynom $x^2 + x + 41$ für $x = 0, 1, \ldots, 39$ lauter Primzahlen produziert. (Ein nicht konstantes Polynom in einer (!) Variablen x kann nicht ausschließlich oder auch nur für hinreichend große x Primzahlen liefern). Dieses Phänomen hängt mit der Arithmetik quadratischer Zahlenkörper zusammen.

Satz. ***Satz von Rabinovitch etal.*** *(wobei* RABINOWITCH *die Äquivalenz von 2. und 3. gezeigt hat)*
Sei p eine Primzahl. Dann sind äquivalent:

1. $p = 2, 3, 5, 11, 17, \underline{41}$
2. $x^2 + x + \underline{p}$ *ist prim für* $x = 0, 1, \ldots, p-2$
3. $\mathcal{O}_{1-4p}$ *ist faktoriell*

Bemerkung. Eulers Polynom ensteht mit der Primzahl $p = 41$ und führt zu dem faktoriellen Ganzheitsring $\mathcal{O}_{-163}$ mit minimaler Diksriminante $D = -163 < 0$.
Die Implikation *1.⇒2.* verifiziert man durch Nachrechnen, hingegen benötigt man für *3⇒1.* die komplette Bestimmmung aller faktoriellen Ganzheitsringe (und war Rabinowitch noch nicht bekannt). Jetzt zeigen wir *3.⇒2.* für den Fall $p = 41$.
Im faktoriellen Ring $\mathcal{O}_{-163}$ gilt:

$$N\left(\frac{1}{2}\left(2x + 1 + \sqrt{-163}\right)\right) = x^2 + x + 41, \qquad \text{für } x \in \mathbb{Z},$$

welches insbesondere nicht prim ist. Sei $\pi = \mathcal{X} + \mathcal{Y}\sqrt{-163}$ ein Primfaktor von $x^2 + x + 41$ in $\mathcal{O}_{-163}$, hierbei ist nach Satz 7.2 $\mathcal{X}, \mathcal{Y} \in \frac{1}{2}\mathbb{Z}$ und $\mathcal{X} + \mathcal{Y} \in \mathbb{Z}$. Das heißt:

$$\frac{1}{2}\left(2x + 1 + \sqrt{-163}\right) = \left(\mathcal{X} + \mathcal{Y}\sqrt{-163}\right) \cdot \left(a + b\sqrt{-163}\right)$$

mit gewissen $a, b \in \frac{1}{2}\mathbb{Z}$, $a + b \in \mathbb{Z}$. Trennung von Real- und Immaginärteil liefert

$$\frac{1}{2}(2x + 1) = a\mathcal{X} - 163b\mathcal{Y}$$

und

$$2 = 4(a\mathcal{Y} + b\mathcal{X})$$

Entweder haben wir hier $a\mathcal{Y}$ und $b\mathcal{X}$ verschiedene bzw $a\mathcal{X}$ und -$b\mathcal{Y}$ gleiche Vorzeichen, was auf $x \geq 40\frac{1}{2}$ führt, oder es ist $a = \pm 1,\ b = 0$, was auf $0 \leq x \leq 39$ entspricht.

In diesem Fall ist $\frac{1}{2}\left(2x+1+\sqrt{-163}\right)$ prim in $\mathcal{O}_{-163}$ und x^2+x+41 eine Primzahl. Alternativ mit dem Zerlegungsgesetz 9.2

$$-1 = \left(\frac{-163}{p}\right)$$

Für alle Primzahlen $p > 41$.

Die Mehrdeutigkeit in Primfaktorzerlegungen in Ganzheitsringen beseitigt man durch Einführung so genannter **idealer Zahlen** gemäß KUMMER bzw. (moderner) **Ideale** nach DEDEKIND (1881). So klärt sich Dedekinds Beispiel (Kapitel 8) durch **Primideale** p_i

$$\underbrace{2}_{p_1^2} \cdot \underbrace{3}_{p_2 p_3} = 6 = \underbrace{\left(1+\sqrt{-5}\right)}_{=p_1 p_2} \cdot \underbrace{\left(1-\sqrt{-5}\right)}_{p_1 p_3}$$

Mit dieser Struktur hat man stets eine **eindeutige Primidealzerlegung**. Diese wichtige Fortsetzung des Fundamentalsatzes auf Ganzheitsringe untersucht man in der **Algebraischen Zahlentheorie**.

Teil III.

3.Teil der Vorlesung

Jetzt untersuchen wir diophantische Gleichungen bzw. Approximationen. Hier sollen Gleichungen bzw. Ungleichungen über die ganzen bzw, die rationalen Zahlen (oder algebraische Erweiterungen) gelöst werden. Die Arithmetik quadratischer Zahlenkörper ist dabei oft ein Hilfsmittel.

10. Die Fermat-Gleichung

Wir untersuchen als Erstes die nichtlineare diophantische Gleichung und starten mit:

$$X^2 + Y^2 = Z^2$$

Ein Lösungstripel (X, Y, Z) natürlicher Zahlen heißt **pythagoräisches Tripel** (vergleiche mit dem Satz des Pythagoras); ein solches nennt man **primitiv**, falls $\mathrm{ggT}(X, Y, Z) = 1$.

Bemerkung. Bereits die Babylonier kannten Beispiele

$$3^2 + 4^2 = 5^2$$
$$8^2 + 15^2 = 17^2$$

und nutzten dies zur Konstruktion rechter Winkel. Pythagoras kannte unendlich viele Tripel

$$(2n+1)^2 + (2n^2+2n)^2 = (2n^2+2n+1)^2.$$

Eine Parametrisierung sämtlicher pythagoräischer Tripel gelingt mit:

Satz 10.1. ***Satz von Euklid***
*Seien $a, b \in \mathbb{N}$ teilerfremd und unterschiedlicher **Parität** (das heißt $a \not\equiv b \mod 2$) und $a > b$. Dann ist*

$$x = a^2 - b^2, \qquad y = 2ab, \qquad z = a^2 + b^2$$

ein primitives pythagoräisches Tripel. Alle primitiven pythagoräischen Tripel sind von dieser Form mit eindeutig bestimmten a und b.

Beweis. (geometrisch betrachtet)
Äquivalent zu

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

mit $x, y, z \in \mathbb{Z},\ z \neq 0$ ist

$$u^2 + v^2 = 1$$

mit $u = \frac{x}{z},\ v = \frac{y}{z} \in \mathbb{Q}$. Wir suchen also die **rationalen Punkte** auf dem Einheitskreis

$$U^2 + V^2 = 1$$

Das heißt Punkte mit rationalen Koordinaten.

Die Gerade $V = m(U+1)$ durch den Punkt $P(-1,0)$ mit Steigung m schneidet den Kreis in **genau einem weiteren Punkt**; dieser Punkt besitzt genau dann rationale Koordinaten, wenn $m \in \mathbb{Q}$

$$\begin{aligned} 1 &= U^2 + m^2(U+1)^2 \\ \Rightarrow U^2 + \frac{2m^2}{m^2+1}U + \frac{m^2-1}{m^2+1} &= 0 \\ \Rightarrow U &= \frac{-m^2 \pm 1}{m^2+1} \end{aligned}$$

das heißt, der weitere Schnittpunkt ist $(u,v) = \left(\frac{-m^2+1}{m^2+1}; \frac{2m}{m^2+1}\right)$ (die V-Koordinate schließt Quadratwurzeln für m aus!). Mit $m = \frac{a}{b}$ für ganze Zahlen $a, b \neq 0$ ergibt sich

$$\left(\frac{a^2-b^2}{a^2+b^2}\right)^2 + \left(\frac{2ab}{a^2+b^2}\right)^2 = 1,$$

und damit ein pythagoräisches Tripel (nach Multiplikation mit $(a^2+b^2)^2$). Dabei wird kein Tripel ausgelassen, denn es ist (u,v) ein rationaler Punkt auf dem Kreis, so muss die Gerade durch $(-1,0)$ und (u,v) eine rationale Steigung m besitzen. Die Primitivität der pythagoräischen Tripel ergibt sich leicht aus den Bedingungen an a und b (bzw. umgekehrt) □

Ein „algebraischer Beweis“ benutzt den Fundamentalsatz 1.5 (siehe HARDY & WRIGHT).

Bemerkung. Fermat äußerte (ca. 1635), dass im Gegensatz zum Fall $n = 2$ die Gleichung

$$X^n + Y^n = Z^n \qquad \text{mit } n \geq 3$$

in ganzen Zahlen nur **trivial** lösbar sei, das heißt $X, Y, Z = 0$.
Diese so genannte **Fermatsche Vermutung** wurde erst 1995 durch ANDREW WILES (mit Hilfe von Modulformen und elliptischen Kurven) bewiesen. Wahrscheinlich dachte Fermat fälschlicherweise, dass sich sein Beweis für $n = 4$ verallgemeinern ließe.

Satz 10.2. *Alle ganzzahligen Lösungen der Gleichung*

$$X^4 + Y^4 = z^2$$

(und insbesondere der Fermat-Gleichung für $n = 4$) sind trivial.

Beweis. (Fermats Methode des unendlichen Abstieges [**infinite descente**]).
Angenommen $z \in \mathbb{N}$ ist minimal mit der Eigenschaft, dass

$$X^2 + Y^2 = z^2$$

Lösungen $\mathcal{X}, \mathcal{Y} \in \mathbb{N}$ besitzt. Dann sind $\mathcal{X}$ und $\mathcal{Y}$ teilerfremd (klar, sonst ergibt sich ein **Widerspruch** zu Minimalität von z). OBdA $2 \nmid \mathcal{X}$ und $2 | \mathcal{Y}$ (wären nämlich beide ungerade, so folgte $\mathcal{X}^4 + \mathcal{Y}^4 \equiv 2 \mod 4$, aber $z^2 \equiv 0 \mod 4$ oder $\equiv 1 \mod 4$). Mit Satz 10.1 folgte

$$\begin{aligned} \mathcal{X}^2 &= a^2 - b^2 \\ \mathcal{Y}^2 &= 2a \cdot b \\ z &= a^2 + b^2 \end{aligned}$$

für gewisse teilerfremde $a, b \in \mathbb{N}$, $2 \nmid a,\ 2|b$. Mit $b = 2c$ gilt dann $\boxed{(\mathcal{Y}/2)^2} = ac$ mit $\frac{\mathcal{Y}}{2} \in \mathbb{N}$ und $\mathrm{ggT}(a, c) = 1$.

Mit der eindeutigen Primfaktorzerlegung (Fundamentalsatz 1.5) existieren also teilerfremde $u, v \in \mathbb{N}$ mit $a = \boxed{u^2},\ c = \boxed{v^2}$, wobei $2 \nmid u$. Damit

$$(2v^2)^2 + \mathcal{X}^2 = b^2 + \mathcal{X}^2 = a^2 = (u^2)^2$$

Wiederum mit Satz 10.1 folgt

$$\begin{aligned} 2v^2 &= 2AB, \\ u^2 &= A^2 + B^2 \end{aligned}$$

mit gewissen $A, B \in \mathbb{N}$. Wie oben liefert das gewisse teilerfremde $s, t \in \mathbb{N}$ mit

$$\begin{aligned} A &= s^2, \\ B &= t^2, \end{aligned}$$

und also

$$s^4 + t^4 = u^2$$

Wegen

$$u \leq u^2 = a \leq a^2 < a^2 + b^2 = z$$

(der Fermatsche Abstieg) und das ist ein **Widerspruch** zur Minimalität von z. □

26.06.08

Bemerkung. Für einen Beweis der Fermatschen Vermutung müssen „nur noch“ ungerade Prizahlpotenzen (also $n = p \geq 3$) Betrachtet werden, denn

$$(x^q)^p + (y^q)^p = x^{pq} + y^{pq} = z^{pq} = (z^q)^p.$$

Bereits der Exponent $n = 3$ ist schwierig und wurde erst 1770 von Euler gelöst (wenngleich sein Beweis auch kritisiert wurde). Seine Idee folgend zeigen wir über **Fermats eigentliche Frage hinausgehend**:

Satz 10.3. *Es gibt keine $x, y, z \in \mathbb{Z}[\zeta]\backslash\{0\}$ mit $x^3 + y^3 + z^3 = 0$, insbesondere ist die Fermat-Gleichung zum Exponenten $n = 3$ in ganzen Zahlen nur trivial lösbar.*

Bemerkung. Wegen $(-z)^3 = -z^3$ verhalten sich die Gleichungen $x^3 + y^3 \pm z^3 = 0$ bezüglich nicht trivialer Lösbarkeit völlig gleich. Die Fermat-Gleichung zum Exponenten $n = 3$ ist also sogar im $\mathbb{Z}$ umfassenden Ganzheitsring $\mathcal{O}_{-3} = \mathbb{Z}[\zeta]$ der ganzen Eisensteinschen Zahlen nur trivial lösbar.
Hierbei ist $\zeta = \frac{-1\pm\sqrt{-3}}{2}$ eine dritte Einheitswurzel (vrgl. Beispiel 7 *2.*) und $\mathbb{Z}[\zeta]$ nach Satz 8.3 normeuklidisch und nach Satz 8.4 faktoriell.
Mit Satz 8.2 besitzt jedes Element aus $\mathbb{Z}[\zeta]$ eine **eindeutige Primfaktorzerlegung**. Euler argumentierte hingegen mit dem Ring $\mathbb{Z}\left[\sqrt{-3}\right]$, der keine (!) eindeutige Primfaktorzerlegung besitzt.

Als Vorbereitung zum Beweis bemerken wir, dass

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[\zeta], \qquad (a, b) \mapsto a + b\zeta$$

ein Isomorphismus von additiven Gruppen ist; entsprechend besteht der Isomorphismus

$$\frac{\mathbb{Z}[\zeta]}{3\mathbb{Z}[\zeta]} \cong \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)$$

und dem (Quotienten-) Restklassenring $\mathbb{Z}[\zeta]/3\mathbb{Z}[\zeta]$ besteht somit aus $9 = 3^2$ Elementen. Wir schreiben nun $\alpha \equiv \beta \mod \gamma$ für $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$, falls $\gamma|(\alpha - \beta)$. Dies verallgemeinert unseren Kongruenzbegriff für $\mathbb{Z}$ auf $\mathbb{Z}[\zeta]$, sämtliche Eigenschaften übertragen sich in natürlicher Weise.
Die Restklassen von $\mathbb{Z}[\zeta]/3\mathbb{Z}[\zeta]$ sind also gegeben durch (die Repräsentanten):

$$\underbrace{\pm 1, \pm\zeta, \pm\zeta^2}_{\substack{\text{die Eihnehiten von } \mathbb{Z}[\zeta] \\ \text{(vrgl. Satz 8.1, } \omega = \zeta + 1)}} \qquad 1 - \zeta,\ 1 - \bar{\zeta} (= -\zeta^2(1 - \zeta)), \tag{10.1}$$

(Denn je zwei dieser neun Zahlen sind inkongruent modulo 3: Aus $\alpha \equiv \beta \mod 3$ folgt über $N(3)|N(\alpha - \beta)$, das heißt $9|\,|\alpha - \beta|^2$, bzw. $|\alpha - \beta| < 3$, und das heißt für je zwei verschiedene Zahlen α, β aus (10.1)). Damit ist jeder Kubus in $\mathbb{Z}[\zeta]$ ist modulo 3 kongruent zu einer der drei Zahlen $0, \pm 1$, denn

$$(a + b\zeta)^3 \equiv a^3 + b^3\zeta^3 = a^3 + b^3 = 0 \qquad \text{oder } \pm 1.$$

Insbesondere folgt für $\alpha \in \mathbb{Z}[\zeta]$ und eine Einheit ε mit

$$\varepsilon\alpha^3 \equiv \pm 1 \mod 3 \Rightarrow \varepsilon = \pm 1 \tag{10.2}$$

und somit st $\varepsilon\alpha^3$ ein Kubus in $\mathbb{Z}[\zeta]$ (also etwa $\neq \zeta$!)

Beweis. von Satz 10.3 (nach Gauß). Angenommen es gilt $x^3 + y^3 + z^3 = 0$ für gewisse $x, y, z \in \mathbb{Z}[\zeta]$, $xyz \neq 0$. Wir dürfen annehmen, dass x, y, z keinen gemeinsamen Teiler besitzen (hier geht bereits die Arithmetik von $\mathbb{Z}[\zeta]$ ein!). Damit sind x, y, z sogar **paarweise teilerfremd** (klar). Selbiges gilt auch für

$$\begin{aligned} \alpha &= y + z \\ \beta &= z + x, \\ \gamma &= x + y \end{aligned}$$

denn jeder Primfaktor von etwa γ teilt auch $-z^3 = x^3 + y^3 = (x + y) \cdot (x^2 - xy + y^2)$ und somit z; gemeinsame Primfaktoren von γ und β teilen deshalb z und y. Dann gilt nach Vorraussetzung:

$$(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 = (\alpha + \beta + \gamma)^3 - 24\alpha\beta\gamma = 0.$$

Ferner ist stets

$$(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3 = (\alpha + \beta + \gamma)^3 - 24\alpha\beta\gamma,$$

Sodass sich zusammen also

$$\boxed{(\alpha+\beta+\gamma)^3 = 24\alpha\beta\gamma.}$$

Wegen $3 = -\zeta^2(1-\zeta)$ gilt $(1-\zeta)|(\alpha+\beta+\gamma)^3$. Nun ist $1-\zeta$ prim (denn 3 ist verzweigt in $\mathbb{Z}[\zeta]$ nach dem Zerlegungsgesetz 9.2), also gilt:

$$(1-\zeta)^3|(\alpha+\beta+\gamma)^3 = 2^3 \cdot 3\alpha\beta\gamma$$

Wegen $-\zeta^2(1-\zeta)^2 - 2 = 3 - 2 = 1$ sind $1-\zeta$ und 2 teilerfremd und also folgt (mit dem eindeutigen Primfaktorzerlegung in $\mathbb{Z}[\zeta]$) $(1-\zeta)|\alpha\beta\gamma$. Wiederum mit der Primitivität von $1-\zeta$ folgt, dass $1-\zeta$ eine der Zahlen α, β, γ teilt, etwa γ, dann aber auch z (mit dem Argument von oben).

Sei nun unsere Lösung x, y, z diejenige, für die der Exponent $\nu(z, 1-\zeta)$ in der Primfaktorzerlegung von z bei $1-\zeta$ minimal in $\mathbb{N}$ ist (folgt aus der Wohlordnung). Dann genügt es zu zeigen, dass es eine Lösung $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ unserer Gleichung gibt mit

$$\mathcal{X}\mathcal{Y}\mathcal{Z} \neq 0, \qquad (1-\zeta) \nmid \mathcal{X}\mathcal{Y}$$

und

$$\nu(\mathcal{Z}, 1-\zeta) < \nu(z, 1-\zeta).$$

Wegen der Teilerfremdheit von x und y sind diese nicht durch $1-\zeta$, teilbar, also gilt

$$x, y \equiv \pm 1, \pm\zeta \qquad \text{oder} \pm\zeta^2 \mod 3 \text{ nach (10.1)}$$

Wegen $x^3 = (x\zeta^2)^3 = (x\zeta)^3$ dürfen wir annehmen, dass y und y je zu einer der Zahlen ± 1 kongruent sind. Dabei gilt weder $x \equiv y \equiv +1 \mod 3$ noch $x \equiv y \equiv -1 \mod 3$, denn dann wäre

$$x^3 + y^3 + \underbrace{z^3}_{=0} \equiv \pm 2 \mod 3,$$

(da $(1-\zeta)|z$ impliziert $3|z^3$ und$3 = -\zeta(1-\zeta)^2|z^3$). Wir dürfen also annehmen, dass

$$\begin{aligned} x &\equiv 1 \mod 3 \text{ und} \\ y &\equiv -1 \mod 3 \end{aligned}$$

bzw.

$$\begin{aligned} x &= 1 + 3\alpha, \\ y &= -1 + 3\beta \end{aligned}$$

für gewisse $\alpha, \beta \in \mathbb{Z}[\zeta]$.

Wir definieren uns $A, B, C \in \mathbb{Z}[\zeta]$

$$\begin{aligned} A &= \frac{x+y\zeta}{1-\zeta} = 1-\zeta^2(1-\zeta)\cdot(\alpha+\beta\zeta), \\ B &= \frac{x\zeta+y}{1-\zeta} = -1-\zeta^2(1-\zeta)\cdot(\alpha\zeta+\beta), \\ C &= \frac{\zeta^2(x+y)}{1-\zeta} = -\zeta^2(1-\zeta)\cdot(\alpha+\beta) \end{aligned}$$

Wegen $1+\zeta+\zeta^2=0$ folgt $A+B+C=0$ (klar) und es gilt:

$$A\cdot B\cdot C = (1-\zeta)^{-3}\cdot(x^3+y^3) = \left(\frac{-z}{1-\zeta}\right)^3$$

Es ist außerdem

$$\begin{aligned} -\zeta A+\zeta^2 B &= x, \\ \zeta^2 A-\zeta B &= y \end{aligned}$$

und deshalb sind mit x und y auch A und B teilerfremd, insbesondere sind also A, B, C paarweise teilerfremd.

Also sind A, B, C bis auf Einheiten Kuben in $\mathbb{Z}[\zeta]$. Da aber jedes Primelement $\pi \in \mathbb{Z}[\zeta]$ wegen der Teilerfremdheit nur höchstens eine der Zahlen teilen kann, folgt für die Exponenten von A, B, C

$$\begin{aligned} \nu(A,\pi) &\equiv 0 \mod 3, \\ \nu(B,\pi) &\equiv 0 \mod 3, \\ \nu(C,\pi) &\equiv 0 \mod 3 \end{aligned}$$

bezüglich der Primfaktorzerlegung für alle Primelemente π. Also ist jede der Zahlen A, B, C von der Form $\varepsilon\alpha^3$ mit einen Einheit ε und passendem $\alpha \in \mathbb{Z}[\zeta]$ und Einheiten ε.

Nach Konstruktionsvorschrift gilt: $(1-\zeta)|C$ und aufgrund unserer Überlegungen sogar $(1-\zeta)^3|C$. Wegen $3 = -\zeta^2(1-\zeta)^2$ ist C also auch durch 3 teilbar. Wegen $A+B+C=0$ ergibt sich

$$A+B \equiv 0 \mod 3.$$

Wegen $A \equiv 1 \mod (1-\zeta)$ und $B \equiv -1 \mod (1-\zeta)$ folgt aus unseren Vorüberlegungen (10.2)

$$\begin{aligned} A &\equiv \varepsilon \mod 3, \\ B &\equiv -\varepsilon \mod 3, \end{aligned}$$

mit einer passenden Eineheit ε. Wir setzen nun

$$\begin{aligned} A' &= \varepsilon^{-1}A, \\ B' &= \varepsilon^{-1}B, \\ C' &= \varepsilon^{-1}C \end{aligned}$$

Dann gilt

$$A' + B' + C' = 0$$

sowie

$$A'B'C' = \varepsilon^{-3}ABC = \left(\frac{\pm z}{1-\zeta}\right)^3$$

und

$$\begin{aligned} A' &\equiv 1 \mod 3, \\ B' &\equiv -1 \mod 3 \end{aligned}$$

Nach (10.2) sind A' und B' also Kuben in $\mathbb{Z}[\zeta]$, damit aber C' ebenso. Es gibt also $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \in \mathbb{Z}[\zeta]$ mit $A' = \mathcal{X}^3,\ B' = \mathcal{Y}^3,\ C' = \mathcal{Z}^3$. Es folgt:

$$\mathcal{X}^3 + \mathcal{Y}^3 + \mathcal{Z}^3 = 0$$

sowie

$$\mathcal{X}^3\mathcal{Y}^3\mathcal{Z}^3 = \left(\frac{\pm z}{1-\zeta}\right)$$

Da $(1-\zeta) \nmid \mathcal{X}\mathcal{Y}$ (nach Konstruktion). folgt

$$\nu(\mathcal{Z}, 1-\zeta) = \nu(z, 1-\zeta) - 1,$$

der gewünschte **Widerspruch**. □

Bemerkung. Entscheidend für den Beweis war die Euklidizität des Ringes $\mathbb{Z}[\zeta]$ der Eisensteinschen Zahlen und die damit verbundenen eindeutige Primfaktorzerlegung.
Im Hinblick auf Satz 8.3 kann man die Begrenztheit der Fermatschen Abstiegsmethode für die Fermatsche Gleichung erahnen. Die Fermatsche Abstiegsmethode mag in Hinblick auf die wenige faktoriellen Ganzheitsringen also kein probates Mittel für einen elementaren Beweis der Fermatschen Vermutung sein!
Die Idee der Faktorisierung in Zahlenkörpern ist jedoch oft ein hilfreiches Mittel bei der Behandlung diophantischer Gleichungen.

Hilberts 10. Problem

27.06.08

Gibt es einen universellen Algorithmus, der enstscheidet, ob eine beliebige, gegebene polynomielle diophantische Gleichung mit ganzzahligen Koeffizienten lösbar ist?
Dies wurde 1970 durch Matjasewitsch **negativ** beantwortet! Für Gleichungen bestimmten Typs mag jedoch Hoffnung bestehen:

Die *abc*- Vermutung

Gegeben sind teilerfremde, ganze Zahlen a, b, c mit

$$\boxed{a + b = c}.$$

(Diese Vermutung ist allerdings sehr allgemein). Dann gilt:

$$\forall_{\varepsilon>0} \qquad \max\{|a|, |b|, |c|\} \leq c(\varepsilon) \prod_{p|abc} p^{1+\varepsilon},$$

wobei $c(\varepsilon)$ eine nur von ε abhängige Konstante ist und das Produkt über alle Primteiler p von abc erhoben wird.

Bemerkung. Für Polynome ist die Annahme richtig, allerdings weiß man noch nichts über die ganzen Zahlen...

Bemerkung. Die *abc*-Vermutung impliziert unter anderem die Fermatsche Vermutung für alle hinreichenden Exponenten $n = n(\varepsilon)$ ($\leftarrow$ Beweis ist leicht! Am besten selbst ausprobieren)

Teil IV.

4. Teil der Vorlesung

Im folgenden wollen wir mit der **Pellschen Gleichung** (vrgl. Kapitel 8) eine wichtige diophantische Gleichung lösen. Hilfsmittel hierbei entstammen der Theorie der diophantsichen Aproximationen (Ungleichungen).

Definition. Die **Pellsche Gleichung** hat die Form:

$$X^2 + dY^2 = \pm 1, \qquad d \in \mathbb{N}$$

11. Kettenbrüche

Bemerkung. Wir starten mit einer Variante des euklidischen Allgorithmus:

$$\begin{aligned} 1730 &= \underline{4} \cdot 419 + 54 \rightsquigarrow \frac{1730}{419} = 4 + \frac{54}{419} \\ 419 &= \underline{7} \cdot 54 + 41 \rightsquigarrow \frac{419}{54} = 7 + \frac{41}{54} \\ 54 &= \underline{1} \cdot 41 + 13 \rightsquigarrow \frac{54}{41} = 1 + \frac{13}{41} \end{aligned}$$

Dies gibt für das **tropische Jahr** (365 Tage, 5 Stunden,48 Minuten und 45,8 Sekunden)

$$\begin{aligned} 365 + \frac{419}{1730} &= 365 + \frac{1}{\frac{1730}{419}} = 365 + \frac{54}{419} \\ &= 365 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6 + \frac{1}{2}}}}}} \end{aligned}$$

Dies führte dazu, dass der Julianische Kalender (nach Julius Caesar) alle 4 Jahre am Ende des Jahres einen **Schalttag** eingeführt hat. Verbessert wurde dieses System durch Papst Gregor, der den **Gregorianischen Kalender** einführte. Dieser beinhaltet Ausnahmen für Schaltjahre.

Allgemeiner gilt: Für Variable $a_0, a_1, \ldots, a_m$ heißt

$$[a_0, a_1, \ldots, a_m] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{m-1} + \frac{1}{a_m}}}}}$$

(endlicher) **Kettenbruch** mit **Teilnennern** $a_0, a_1, \ldots a_m$. Es gilt:

$$\begin{aligned} [a_0, a_1, \ldots, a_{m-1}, a_m] &= \left[a_0, a_1, \ldots a_{m-1} + \frac{1}{a_m}\right] \\ &= a_0 + \frac{1}{[a_1, \ldots, a_m]} = [a_0, [a_1, \ldots, a_m]] \end{aligned}$$

Für $n \leq m$ nennt man $[a_0, a_1, \ldots, a_n]$ den n-ten **Näherungsbruch** an $[a_0, a_1, \ldots, a_m]$. Zu gegebenen Zahlen $a_0, a_1, \ldots, a_m$ erklären wir rekursiv:

$$(pq) \begin{cases} p_{-1} = 1,\ p_0 = a_0,\ p_n = a_n p_{n-1} + p_{n-2}, & \text{für } n \leq m \text{ (bzw. } n \in \mathbb{N}) \\ q_{-1} = 0,\ q_0 = 1,\ q_n = a_n q_{n-1} + q_{n-2}, & \text{für } n \leq m \text{ (bzw. } n \in \mathbb{N}) \end{cases}$$

Satz 11.1. *Für $n \in \mathbb{N}$ gilt:*

1. $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$ *(leicht berechenbar!)*
2. $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, *insbesondere sind p_n und q_n teilerfremd für $a_j \in \mathbb{Z}$*
3. $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$.

Beweis. 1. per Induktion nach n; $n = 0$ ist klar, für $n = 1$ gilt:

$$\frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0, a_1]$$

$n \mapsto n + 1$:

$$\begin{aligned}
[a_0, a_1, \ldots, a_n, a_{n+1}] &= \left[a_0, \ldots a_n + \frac{1}{a_{n+1}}\right] \\
&= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n-1}}\right) q_{n-1} + q_{n-2}} \\
\frac{(a_{n+1} a_n + 1)\, p_{n+1} + a_{n+1} p_{n-2}}{(a_{n-1} a_n + 1) q_{n-1} + a_{n+1} q_{n-2}} &= \frac{a_{n+1} p_n + q_{n-1}}{a_{n+1} q_n + q_{n-1}} \\
&= \frac{p_{n+1}}{q_{n+1}}
\end{aligned}$$

2. folgt aus (pq) durch einsetzen

$$\begin{aligned}
p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_n) \\
&= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\
&= \ldots \\
&= (-1)^n \left(p_0 q_{-1} - p_{-1} q_0\right) \\
&= (-1)^{n-1}.
\end{aligned}$$

3. folgt analog.

□

Bemerkung. Jede rationale Zahl besitzt (offensichtlich) eine Darstellung als endlicher Kettenbruch $[a_0, a_1, \ldots, a_m]$ mit Teilnenner $a_0 \in \mathbb{Z},\ a_1, \ldots a_m \in \mathbb{N}$ (dies ist nichts anderes als der euklidische Algorithmus (1.2) angewandt auf p_m, q_m!) Dies ist eindeutig unter der Forderung $a_m \geq 2$:

$$[a_0, a_1, \ldots, a_m] = [a_0, a_1, \ldots, a_m - 1, 1]$$

Definition. Der **Kettenbruchalgorithmus** besteht aus der Iteration

$$\begin{aligned}
\alpha &=: \alpha_0, \\
\alpha_n &= \lfloor \alpha_n \rfloor + \frac{1}{\alpha_{n+1}} && \text{für } n = 0, 1, 2, 3, \ldots, \\
a_n &:= \lfloor \alpha_n \rfloor.
\end{aligned}$$

Für $\alpha \in \mathbb{Q}$ ist dies der euklidische Algorithmus und terminiert somit. Für $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ bricht die Iteration nicht ab (klar) und liefert einen unendlichen Kettenbruch:

$$\begin{aligned}
\alpha = \alpha_0 &= \lfloor \alpha_0 \rfloor + \frac{1}{\alpha_1} \\
&= a_0 + \frac{1}{\lfloor \alpha_1 \rfloor + \frac{1}{\alpha_2}} \\
&= a_0 + \frac{1}{a_1 + \frac{1}{\lfloor \alpha_2 \rfloor + \frac{1}{\alpha_3}}} \\
&= \dots \\
&= [a_0, a_1, \dots] \qquad \text{Konvergiert das ganze eventuell?}
\end{aligned}$$

Satz 11.2. *Für $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ gilt:*

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{a_{m+1} q_n^2};$$

insbesondere ist

$$[a_0, a_1, \dots] = \lim_{n \to \infty} \frac{p_1}{q_1} = \alpha.$$

Beweis. Nach Satz 11.1 gilt:

$$\begin{aligned}
\alpha - \frac{p_n}{q_n} &= [a_0, a_1, \dots, a_n, \alpha_{n+1}] - \frac{p_n}{q_n} \\
&= \frac{\alpha_{n+1} p_n + p_{n1}}{\alpha_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n} \\
&= \frac{p_{n-1} q_n - p_n q_{n-1}}{(\alpha_{n+1} q_n + q_{n-1}) q_n} \\
&= \frac{(-1)^{n-1}}{q_n (\alpha_{n+1} q_n + q_{n-1})}
\end{aligned} \tag{11.1}$$

Die Ungleichung folgt aus (11.1) mit $a_{n+1} = \lfloor \alpha_{n+1} \rfloor \leq \alpha_{n+1}$. Die Konvergenz bei $n \to \infty$ ergibt sich aus der streng wachsenden Monotonie der q_n für $n \geq 2$ gegen $\to +\infty$, da $q_n \in \mathbb{N}$. □

Bemerkung. Der Beweis zeigt ferner, dass die Näherung alternierend gegen α konvergieren

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \alpha < \dots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Bemerkung. Auch die unendlichen Kettenbruchentwicklung für irrationale Zahlen ist eindeutig (und erlaubt damit eine alternative Konstruktion von $\mathbb{R}$)!

Wir interessieren uns hier aber für die Approximationseigenschaften:

Satz 11.3. ***Gesetz über die beste Nährung*** *(nach Lagrange um 1770).*
Sei $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ mit Näherungsbrüchen $\frac{p_n}{q_n}$. Ist $n \geq 2$ und $p, q \in \mathbb{Z}$ (wobei p und q nicht notwendigerweise prim sein müssen) mit $0 < q \leq q_n$ und $\frac{p}{q} \neq \frac{p_n}{q_n}$, so gilt:

$$|q_n \alpha - p_n| < |q\alpha - p|.$$

Bemerkung. Die Näherung an die Kettenbruchentwicklung einer Irrationalzahl α liegen also die besten rationalen Approximationen:

$$\begin{aligned}\left|\alpha - \frac{p_n}{q_n}\right| &= \frac{1}{q_n}\left|q_n\alpha - p_n\right| < \frac{1}{q_n}\left|q\alpha - p\right| \\ &= \frac{q}{q_n}\left|\alpha - \frac{p}{q}\right| \leq \left|\alpha - \frac{p}{q}\right|.\end{aligned}$$

Beweis. OBdA sei $\mathrm{ggT}(p,q) = 1$ und $q_{n-1} < q \leq q_n$ (denn $\mathbb{N} \ni q_n \to +\infty$). Ist $q = q_n$, so ist:

$$p \neq p_n$$

und

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \frac{|pq_n - p_nq|}{qq_n} = \left|\frac{p - p_n}{q_n}\right| \geq \frac{1}{q_n}.$$

Mit Satz 11.2 gilt:

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_nq_{n+1}} < \frac{1}{2q_n}$$

(denn $q_{n+1} \geq 3$). Also ist

$$\begin{aligned}\left|\alpha - \frac{p}{q}\right| &\geq \left|\frac{p}{q} - \frac{p_n}{q_n}\right| - \left|\alpha - \frac{p_n}{q_n}\right| \\ &> \frac{1}{q_n} - \frac{1}{2q_n} = \frac{1}{2q_n} \\ &> \left|\alpha - \frac{p_n}{q_n}\right|\end{aligned}$$

beziehungsweise

$$\begin{aligned}\left|q_n\alpha - p_n\right| &= q_n\left|\alpha - \frac{p_n}{q_n}\right| \\ &= q_n\left|\alpha - \frac{p}{q}\right| \\ &= \left|q\alpha - p\right|\end{aligned}$$

Sei jetzt $q_{n-1} < q < q_n$. Nach Satz 11.1 besitzt das System linearer diophantischer Gleichungen

$$\begin{aligned}p_nX + p_{n-1}Y &= p, \\ q_nX + q_{n-1}Y &= q\end{aligned}$$

die eindeutige (!) Lösung

$$\begin{pmatrix} x \\ y \end{pmatrix} = \underbrace{\frac{1}{p_n q_{n-1} - p_{n-1} q_n}}_{=\pm 1} \begin{pmatrix} pq_{n-1} + qp_{n-1} \\ pq_n - qp_n \end{pmatrix} \in \mathbb{Z}^2.$$

Hierbei gilt $xy \neq 0$ sowie, dass x und y verschiedene Vorzeichen haben (denn $q_n X + q_{n-1} Y = q \in (q_{n-1}, q_n)$), selbiger gilt nach (11.1) für $q_n\alpha - p_n$ und $q_{n-1}\alpha - p_{n-1}$. Also besitzen $X(q_n\alpha - p_n)$ und $Y(q_{n-1}\alpha - p_{n-1})$ das selbe Vorzeichen. Wegen

$$q\alpha - p = X(q_n\alpha - p_n) + Y(q_{n-1}\alpha - p_{n-1})$$

folgt:

$$|q\alpha - p| > |q_{n-1}\alpha - p_{n-1}| \overset{(11.1)}{>} |q_n\alpha - p_n|.$$

□

12. Quadratische Irrationalzahlen

03.07.08

Die **Fibonacci Zahlen** 0,1,1,2,3,5,8,13,21,... sind rekursiv definiert durch

$$\begin{aligned} F_0 &= 0, \quad F_1 = 1, \\ F_{n+1} &= F_n + F_{n-1} \qquad \text{für } n \in \mathbb{N} \end{aligned}$$

Es gilt:

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = [1,1,1,\ldots] = \frac{\sqrt{5}+1}{2} =: G \qquad \textbf{Goldener Schnitt}$$

denn $G = 1 + \frac{1}{G}$ bzw. $G^2 - G - 1 = 0$, sowie

$$\begin{aligned} F_{n+1}F_{n-1} - F_n^2 &= (-1)^n && \text{(mit Satz 11.1 } \textit{2.}\text{)} \\ F_n &= \frac{1}{\sqrt{5}}\left(G^n - \left(\frac{-1}{G}\right)^n\right) && \text{(per Induktion)} \end{aligned}$$

Ein weiteres Beispiel ist:

$$\begin{aligned} \underline{\sqrt{2}} &= 1 + \frac{1}{\frac{1}{\sqrt{2}-1}\cdot\frac{\sqrt{2}+1}{\sqrt{2}+1}} = 1 + \frac{1}{1+\underline{\sqrt{2}}} \\ &= 1 + \frac{1}{2 + \frac{1}{2+\ddots}} = [1,2,2,\ldots] \end{aligned}$$

Bemerkung. Das ist eine Folge von Näherungsbrüchen.

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \underline{\frac{99}{70}}, \ldots \to \sqrt{2}$$

wobei $\frac{99}{70}$ die rationale Approximation für das **DinA4**

Definition. Eine Zahl $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ heißt **quadratisch irrational**, wenn es ein (irreduzibles) Polynom $P \in \mathbb{Z}[x]$ vom Grad $\deg P = 2$ mit $P(\alpha) = 0$ gibt, Alternativ: wenn $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)\backslash\mathbb{Q}$ für ein $d \in \mathbb{N}$ (um einen reell-quadratischen Zahlenkörper zu haben).

Satz 12.1. *$\alpha \in \mathbb{R}\backslash\mathbb{Q}$ ist genau dann quadratisch irrational, wenn die Kettenbruchzerlegung **periodisch** ist.*
*Hierbei besitzt α eine **periodische** Kettenbruchzerlegung, wenn*

$$\begin{aligned} \alpha &= [a_0, a_1, a_2, \ldots] && \textit{mit } a_{n+k} = a_n \ \forall_{n\geq r} \\ &= [a_0, a_1, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+k}}] \end{aligned}$$

(Geht analog zur periodischen Dezimalentwicklung)

das Minimale k mit dieser Eigenschaft heißt ***Periode****, das Minimale r* ***Vorperiode****.*

Nun der wunderschöne Beweis:

Beweis. Sei zunächst $\alpha = [\overline{a_0, a_1, \ldots, a_{k-1}}]$. Dann gilt nach Satz 11.1

$$\alpha = [a_0, a_1, \ldots, a_{k-1}] = \frac{\alpha p_{k-1} + p_{k-2}}{\alpha q_{k-1} + q_{k-2}}$$

bzw. $q_{k-1}\alpha^2 + (q_{k-2} + p_{k-1})\alpha - p_{k-2} = 0$. Wegen $\alpha \notin \mathbb{Q}$ ist α quadratisch irrational.

Sei jetzt

$$\begin{aligned} \alpha &= [a_0, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+k}}] \\ &= [a_0, \ldots, a_r, \beta] \end{aligned}$$

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

Hierin ist β quadratisch irrational und damit auch

$$\alpha = \frac{\beta p_r - p_{r-1}}{\beta q_r + q_{r-1}} \in \mathbb{Q}(\beta),$$

denn $\mathbb{Q}(\beta)$ ist quadratischer Zahlenkörper (Siehe auch Satz 11.1 und die Definition der (p_n) und (q_n))

Ist umgekehrt $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$ quadratisch irrational, so gibt es also ein irreduzibles Polynom

$$P = a \cdot X^2 + bX + c$$

mit $a, b, c \in \mathbb{Z}$ und $P(\alpha) = 0$

Mittels

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

folgt über

$$P\left(\frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}\right) = 0$$

jetzt

$$A_n\alpha_n^2 + B_n\alpha_n + C_n = 0 \text{ mit } \begin{cases} A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \\ B_n &= 2ap_{n-1}p_{n-2}b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_nq_{n-1} \\ C_n &= ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2 = A_{n-1} \end{cases}$$

Hierin ist $A_n \neq 0$, da sonst $\alpha_n \in \mathbb{Q}$ und damit sowohl $\frac{p_{n-1}}{q_{n-1}}$ auch $\alpha \in \mathbb{Q}$, **Widerspruch**. Also ist $A_nX^2 + B_nX + C_n$ ein irreduzibles quadratisches Polynom mit Nullstelle α_n und Diskriminante

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)\overbrace{(p_{n-1}q_{n-2} - p_{n-2}q_{n-2})}^{=\pm 1 \text{ nach Satz 11.1}} = \pm\text{Diskriminante}(P) \tag{12.1}$$

Nach Satz 11.2

$$p_{n-1} = \underbrace{\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}} \qquad \text{mit } |\delta_{n-1}| < 1$$

es folgt

$$\begin{aligned} A_n &= a\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + bq_{n-1}\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right) + cq_{n-1}^2 \\ &= \underbrace{(a\alpha^2 + b\alpha + c)}_{P(\alpha)=0} q_{n-1}^2 + 2a\alpha\delta_{n-1} + a\left(\frac{\delta_{n-1}}{q_{n-1}}\right)^2 + b\delta_{n-1} \end{aligned}$$

und somit

$$|A_n| < 2 \cdot |a\alpha| + |a| + |b|$$

Wegen $C_n \subset A_{n-1}$ gilt dieselbe Abschätzung auch für $|C_n|$. Mit (12.1) gilt

$$\begin{aligned} B_n^2 &\leq 4\,|A_nC_n| + \left|b^2 - 4ac\right| \\ &< 4(2\,|a\alpha| + |a| + |b|)^2 + \left|b^2 - 4ac\right|. \end{aligned}$$

Die Schranken für A_n, B_n, C_n sind **unabhängig von** n; die Tripel (A_n, B_n, C_n) nehmen nur endlich viele Werte an, wiederholen sich also. Es gibt daher (A, B, C) mit

$$(A, B, C) = (A_{n_1}, B_{n_1}, C_{n_1}) = (A_{n_2}, B_{n_2}, C_{n_2}) = (A_{n_3}, B_{n_3}, C_{n_3})$$

mit $n_1 < n_2 < n_3$. Entsprechend sind die Zahlen $\alpha_{n_1}, \alpha_{n_2}, \alpha_{n_3}$ Nullstellen sind von $AX^2 + BX + C$ und somit sind mindestens zwei identisch, oBdA. $\alpha_{n_1} = \alpha_{n_2}$, was auf $a_{n_1} = \lfloor \alpha_{n-1} \rfloor = \lfloor \alpha_{n_2} \rfloor a_{n_2}, a_{n_1+1}, \ldots$ führt. □

Bemerkung. Insbesondere sind die Teilnenner der Kettenbruchentwicklung quadratischer Irrationalzahlen beschränkt, also ist

$$e = \exp(1) = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots 1, 2n, , 1, \ldots]$$

keine quadratische Irrationalität. Es ist unbekannt, ob die Teilnenner algebraischer Zahlen „höheren Grades“ (etwa $\sqrt[3]{2}$) unbeschränkt ist.

Definition. Eine quadratische Irrationalzahl α heißt **reduziert**, falls $\alpha > 1$ und $-1 < \alpha' < 0$. (Hier ist α' das Konjugierte zu α).

Satz 12.2. ***Satz von Galois***
*Die Kettenbruchentwickung einer quadratischen Irrationalzahl α ist genau dann **reinperiodisch**, das heißt*

$$\alpha = [\overline{a_0, a_1, \ldots, a_k}],$$

wenn α reduziert ist.

Beweis. Der für uns relevanten Richtung!
Sei

$$\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$$

reduziert. Nun gilt

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} \qquad \text{und } \alpha'_n = a_n + \frac{1}{\alpha'_n}$$

für $n = 0, 1, \ldots$ (denn rationale Operationen sind verträglich mit der Konjugation). Also $\alpha_n > 1$. Gilt $\alpha'_n < 0$,so folgt

$$-1 \overset{\text{Def.}}{<} \alpha'_{n+1} = \frac{1}{\alpha'_n + a_n} \underbrace{<}_{\alpha'_n < 0 < 1 < \alpha_n} 0.$$

Mit Induktion sind alle α_n reduziert. Insbesondere gilt dann

$$0 < -\alpha'_n = -a_n - \frac{1}{\alpha'_n + 1} < 1$$

bzw

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

Da α quadratisch irrational ist, folgt aus Satz 12.1 die Existenz von $k < l$ mit $\alpha_k = \alpha_l$ bzw. $a_k = a_l$ sowie $\alpha'_k = \alpha'_l$. Damit ist

$$a_{k-1} = \left[\frac{1}{\alpha'_k} \right] = \left[-\frac{1}{\alpha'_l} \right] = a_{l-1}$$

Dies impliziert die Reinperiodizität. □

Bemerkung. Tatsächlich gilt:

$$-\frac{1}{\alpha} := [\overline{a_k, \ldots, a_1, a_0}]$$

Korollar 12.3. ***Legendre/Lagrange***
Für $d \in \mathbb{N}$ mit $\sqrt{d} \notin \mathbb{Q}$ ist

$$\sqrt{d} = \left[\lfloor\sqrt{d}\rfloor, \overline{a_1, a_2, a_3, \ldots a_{N-1}, 2\lfloor\sqrt{d}\rfloor}\right].$$

Beweis. Es ist $-1 < \lfloor\sqrt{d}\rfloor - \sqrt{d} < 0$, also ist $\sqrt{d} + \lfloor\sqrt{d}\rfloor$ reduziert und nach Satz 12.2 reinperiodisch. Es gilt

$$\sqrt{d} = \lfloor\sqrt{d}\rfloor = \left[\overline{2\lfloor\sqrt{d}\rfloor, a_1, \ldots, a_{n-1}}\right] \overline{2\lfloor\sqrt{d}\rfloor}.$$

□

10.07.08

Bemerkung. Tatsächlich gilt:

$$\sqrt{d} = \left[\lfloor\sqrt{d}\rfloor, \overline{\underbrace{a_1, a_2, \ldots, a_2, a_1}_{\text{Symmetrie}}, 2\lfloor\sqrt{d}\rfloor}\right].$$

Beispiel.

$$\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 14}]$$

13. Die Pellsche Gleichung

Archimedes stellte Eratosthemes bereits die Aufgabe, die diophantische Gleichung

$$X^2 - 4\ 729\ 494Y^2 = 1$$

zu lösen (das sogenannte **Rinderproblem**).
Allgemeiner nennt man

$$X^2 + dY^2 = \pm 1$$

mit $1 < d \in \mathbb{N},\ d \notin \boxed{1}$ (ist Trivial für $d =$ „Quadratzahl“, da man sie dann faktorisieren kann) die **Pellsche „$\pm$“- Gleichung**. Die Menge der ganzzahligen Lösungen ist geometrisch der Schnitt einer Hyperbel mit dem Gitter $\mathbb{Z}^2$. Aufgrund der Symmetrie genügt es sich auf den ersten Quadranten zu beschränken. Stets löst $(x, y) = (1, 0)$, aber gibt es Lösungen in $\mathbb{N}^2$?

Euler hatte die Idee die Gleichung im Ring $\mathbb{Z}\left[\sqrt{d}\right]$ zu faktorisieren. Ist $\mathcal{X}, \mathcal{Y} \in \mathbb{N}$ eine Lösung, so gilt:

$$\left(\mathcal{X} - \mathcal{Y}\sqrt{d}\right) \cdot \left(\mathcal{X} + \mathcal{Y}\sqrt{d}\right) = \mathcal{X}^2 - d\mathcal{Y}^2 = \pm 1$$

und damit

$$\mathcal{X} - \mathcal{Y}\sqrt{d} = \pm \frac{1}{\mathcal{X} + \mathcal{Y}\sqrt{d}}$$

bzw.

$$\left|\sqrt{d} - \frac{\mathcal{X}}{\mathcal{Y}}\right| = \frac{1}{\mathcal{Y}^2\left(\sqrt{d} + \frac{\mathcal{X}}{\mathcal{Y}}\right)} < \frac{1}{2\mathcal{Y}^2}.$$

Also liefern die Lösungen (x, y) der Pellschen Gleichung sehr gute rationale Approximationen an die Irrationalität $\sqrt{d}$. Nach einem Satz von Lagrange (siehe Übungsblatt 12?, Aufgabe 1) muss damit $\frac{\mathcal{X}}{\mathcal{Y}}$ bereits ein Näherungsbruch an $\sqrt{d}$ sein.

Beispiel. $d = 2$

$$\frac{p_n}{q_n} = \frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70} \qquad \to \sqrt{2} = \left[1, \overline{2}\right]$$

tatsächlich ist hier $p_n^2 - 2q_n^2$ abwechselnd ∓ 1, also $x^1 2 - 2y^2 = \mp 1$

Sei N minimale Periode der Kettenbruchentwicklung von

$$\sqrt{d} = \left[\lfloor\sqrt{d}\rfloor, a_1, a_2, \ldots, a_{n-1}, \alpha_n\right] = \left[\lfloor\sqrt{d}\rfloor, \overline{a_1, a_2, \ldots, a_N}\right]$$

(nach Korrollar 12.3). Es ist dann

$$\alpha_1 = \frac{\sqrt{d} + \lfloor\sqrt{d}\rfloor}{d - \lfloor\sqrt{d}\rfloor^2} =: \frac{P_1 + \sqrt{d}}{Q_1}$$

mit $P_1, Q_1 \in \mathbb{Z}$, $Q_1 | (d - P_1^2)$. Angenommen

$$\alpha_n = \frac{P_n + \sqrt{d}}{Q_n} \tag{13.1}$$

mit $P_n,\ Q_n \in \mathbb{Z},\ Q_n | (d - P_n^2)$, dann

$$\begin{aligned}
\alpha_{n+1} &= \frac{1}{\alpha_n - a_n} \\
&= \frac{Q_n}{P_n - a_n Q_n + \sqrt{d}} \\
&= \frac{Q_n (P_n - a_n Q_n - \sqrt{d})}{(P_n - a_n Q_n)^2 - d} \\
&= \frac{P_{n+1} + \sqrt{d}}{Q_{n+1}},
\end{aligned}$$

wobei $P_{n+1} = a_n Q_n - P_n \in \mathbb{Z}$,

$$\begin{aligned}
Q_{n+1} &= \frac{d - (P_n - a_n Q_n)^2}{Q_n} \\
&\overset{(13.1)}{=} \frac{d - P_n^2}{Q_n} + 2a_n P_n - a_n^2 Q_n \in \mathbb{Z}
\end{aligned}$$

Ferner gilt

$$\begin{aligned}
Q_n &= \frac{d - (P_n - a_n Q_n)^2}{Q_{n+1}} \\
&= \frac{d - P_{n+1}^2}{Q_{n+1}}
\end{aligned}$$

und damit $Q_{n+1} | (d - P_{n+1}^2)$

Per Induktion folgt (13.1) also für alle $n \in \mathbb{N}$, insbesondere gilt

$$\begin{aligned}
\sqrt{d} &\overset{(p,q)\text{-Formel}}{=} \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \\
&\overset{(13.1)}{=} \frac{\left(P_n + \sqrt{d}\right) p_{n-1} + p_{n-2} Q_n}{\left(P_n + \sqrt{d}\right) q_{n-1} + q_{n-2} Q_n}
\end{aligned}$$

bzw.

$$\sqrt{d}\left(\left(P_n+\sqrt{d}\right)q_{n-1}+q_{n-2}Q_n\right)=\left(P_n+\sqrt{d}\right)p_{n-1}+p_{n-2}Q_n.$$

zerlegen wir diese Gleichung in den **rationalen Anteil**:

$$dq_{n-1}=P_np_{n-1}+p_{n-2}Q_n \tag{13.2}$$

und den **irrationalen Anteil**:

$$p_{n-1}=P_nq_{n-1}+q_{n-2}Q_n \tag{13.3}$$

Multipliziert man (13.2) mit q_{n-1} und Gleichung (13.3) mit p_{n-1} mit substraktion liefert:

$$\begin{aligned}p_{n-1}^2-dq_{n-1}^2&=P_n\underbrace{\left(\underbrace{p_{n-1}q_{n-1}}_{\text{Irrational}}-\underbrace{p_{n-1}q_{n-1}}_{\text{Rational}}\right)}_{=0}+Q_n\underbrace{\left(\underbrace{p_{n-1}q_{n-2}}_{\text{irrationalteil}}-\underbrace{p_{n-2}q_{n-1}}_{\text{irrationalteil}}\right)}_{=(-1)^n\ \text{Nach Satz 11.1 1.}}\\&=(-1)^nQ_n\end{aligned}$$

Ist $n=k\cdot N$ (mit $N=$ minimale Periode), so ist

$$\frac{P_{kN}+\sqrt{d}}{Q_{kN}}=\alpha_{kN}\overset{s.o}{=}[0,\overline{a_1,\ldots,a_{N-1}}]\overset{s.o}{=}\sqrt{d}\lfloor\sqrt{d}\rfloor,$$

Im Vergleich mit (13.1) folgt $Q_{kN}=1$

Dies liefert unendlich viele Lösungen der Pellschen Gleichung (konstruktiv!):

Satz 13.1. *Die Pellsche Gleichung*

$$X^2-dY^2=+1$$

mit $\sqrt{d}\notin\mathbb{Q}$ besitzt unendlich viele Lösungen $\mathcal{X}_k,\ \mathcal{Y}_k$ gegeben durch

$$(\mathcal{X}_k,\ \mathcal{Y}_k)=\begin{cases}(p_{kN-1},q_{kN-1}), & \text{für } 2|N,\\(p_{2kN-1},q_{2kN-1}), & \text{für } 2\not|N.\end{cases}$$

Bemerkung. Die Lösung $\mathcal{X},\mathcal{Y}\in\mathbb{N}$ mit minimalem $\mathcal{X}$ heißt **Fundamentallösung** für dieses $\mathcal{X}$ gilt stets

$$1<\mathcal{X}\leq\mathcal{Y}_1=\begin{cases}P_{n-1}, & 2|N,\\P_{2N-1}, & 2\not|N\end{cases}$$

ist also nicht „zu groß“!
Tatsächlich gilt stets $\mathcal{X}=\mathcal{X}_1$ (ohne Beweis). Durch potenzieren der Fundamentallösung enstehen weitere Lösungen:

Beispiel. $d=2$

$$\left(3+2\sqrt{2}\right)^2=17+12\sqrt{2}$$
$$3^2-2\cdot2^2=1\quad17^2-2\cdot12^2=1$$

Wir schreiben nun Lösungen als $x + y\sqrt{d}$ und notieren die Fundamentallösung mit $\mathcal{X} + \mathcal{Y}\sqrt{d}$.

Satz 13.2. *Sämtliche Lösungen $x + y\sqrt{d}$ der Pellschen „+“ Gleichung ergeben sich durch Potenzieren der Fundamentallösung:*

$$x + y\sqrt{d} = (\mathcal{X} + \mathcal{Y}\sqrt{d})^{\pm n}$$

für ein $n \in \mathbb{N}_0$.
Die Lösungen bilden also eine zyklische Gruppe, erzeugt durch die Fundamentallösung. (vermöge $\begin{pmatrix} x & dy \\ y & x \end{pmatrix}$ Untergruppe der $SL_2(\mathbb{Z})$.)

Beweis. Für Lösungen gilt

$$\frac{\pm 1}{x + y\sqrt{d}} = \pm\frac{x - y\sqrt{d}}{x^2 + dy^2} = \pm x \mp y\sqrt{d}, \tag{13.4}$$

also genügt es zu zeigen, dass alle Lösungen $x, y \in \mathbb{N}$ gegeben sind durch $x + y\sqrt{d} = \varepsilon^n$, wobei $\varepsilon = \mathcal{X} + \mathcal{Y}\sqrt{d}$ und $n \in \mathbb{N}$ gilt. Zu jeder Lösung $x, y \in \mathbb{N}$ gibt es ein $n \in \mathbb{N}$ mit $\varepsilon^n \leq x + y\sqrt{d} < \varepsilon^{n+1}$, denn $\varepsilon^n \overset{n\to\infty}{\longrightarrow} +\infty$. Sei

$$X + Y\sqrt{d} = \varepsilon^{-n}(x + y\sqrt{d})$$

so ist

$$X + Y\sqrt{d} = 1$$

zu zeigen.

Wegen $\sqrt{d} \notin \mathbb{Q}$ liefert die Konjugation (13.4)

$$X - Y\sqrt{d} = \varepsilon^n \left(x - y\sqrt{d}\right)$$

und mittels Multiplikation

$$\begin{aligned} X^2 - dY^2 &= \left(X - Y\sqrt{d}\right) \cdot \left(X + Y\sqrt{d}\right) \\ &= \varepsilon^{n-n} \left(x - y\sqrt{d}\right) \cdot \left(x + y\sqrt{d}\right) \\ &= x^2 + dy^2 = +1 \end{aligned}$$

Angenommen $1 < X + Y\sqrt{d} < \varepsilon$, dann wiederum mit (13.4)

$$0 < \varepsilon^{-1} < \left(X + Y\sqrt{d}\right)^{-1} = X - Y\sqrt{d} < 1$$

Damit

$$\begin{aligned} 2X &= \left(X + Y\sqrt{d}\right) + \left(X - Y\sqrt{d}\right) > 1 + \varepsilon^{-1} > 0 \\ 2Y\sqrt{2} &= \left(X + Y\sqrt{d}\right) - \left(X - Y\sqrt{d}\right) > 1 - 1 = 0 \end{aligned}$$

Also ist X, Y, eine Lösung in $\mathbb{N}$ mit

$$1 < X + Y\sqrt{d} < \varepsilon = \mathcal{X} + \mathcal{Y}\sqrt{d},$$

ein **Widerspruch zur Minimalität** der Fundamentallösung. □

Bemerkung. Die Größe der Fundamentallösung variiert recht unabhängig von der Größe von d, es gilt:

$$\mathcal{X}, \mathcal{Y}\sqrt{d} < 2d^{\sqrt{d}}$$

Beispiel.
$$\begin{array}{lll} \sqrt{2} & = [1, \bar{2}] & (\mathcal{X}, \mathcal{Y}) = (3, 2) \\ \sqrt{61} & = \left[7, \overline{7, 1, 4, 3, , 1, 2, 2, 1, 3, 4, 1, 14}\right] & (1766319049, 226153980) \end{array}$$

Beim Rinderproblem hat die Fundamentallösung ca. 200 000 Stellen.

Wir kehren zurück zum Problem der Einheiten in reell-quadratischen Zahlenkörpern $\mathbb{Q}\left(\sqrt{d}\right)$ aus Kapitel 8.

Korollar 13.3. *Jede reell-quadratische Zahlenkörper besitzt unendlich viele Einheiten.*

11.07.08

Bemerkung. Denn nach Satz 7.2 ist ε-Einheit in $\mathcal{O}_d$, wenn

- $\varepsilon = \mathcal{X} + \mathcal{Y}\sqrt{d}$ eine der Gleichungen $X^2 + dY^2 = \pm 1$ löst, falls $d \equiv 2, 3 \mod 4$ mit $\mathcal{X}, \mathcal{Y} \in \mathbb{Z}$
- $\varepsilon = \frac{1}{2}(\mathcal{X} + \mathcal{Y})$ eine der Gleichunge $X^2 - dY^2 = \pm 4$, falls $d \equiv 1 \mod 4$, mit $\mathcal{X}, \mathcal{Y} \in \mathbb{Z}$ und $2|(\mathcal{X} - \mathcal{Y})$

Lösungen der Pellschen „+“ Gleichungen führen auf jeden Fall stets zu Einheiten $\varepsilon \in \mathcal{O}_d$. Unter Umständen kommen über die „−“ Gleichungen noch weitere hinzu.

14. Faktorisierungsmethoden und Primzahltests

11.07.08

Das Sieb des Erastothenes (Siehe Kapitel 0) liefert „zuviele“ Informationen, um eine „schnelle“/effiziente Faktorisierungsmethode zu sein oder als **Primzahltest** zu fungieren. Wir beginnen mit dem Faktorisierungsproblem, eine gegebene „große“ ganze Zahl N zu faktorisieren.

Bemerkung. Sei $1 \neq d \in \mathbb{Z}$ quadratfrei und

$$D = \begin{cases} d, & \text{für } d \equiv 1 \mod 4, \\ 4d, & \text{für } d \equiv 2,3 \mod 4 \end{cases} \qquad \text{(wie in Kapitel 9)}$$

Dann wird durch die Gleichung $X^2 - DY^2 = 4$ eine **affine Kurve** (vom **Geschlecht** Null) beschrieben und wir notieren ihre Punkte mit $\mathcal{C}(\mathcal{R})$, je nachdem welchen Ring $\mathcal{R}$ wir für die Koordinaten x, y zu Grunde legen. Ist $\mathcal{R} = k$ ein Körper der Charakteristik $\neq 2$, so gilt $(2,0) \in \mathcal{C}(k)$ stets und mit der Addition

$$(x_1, y_1) \oplus (x_2, y_2) = \frac{1}{2}(x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1)$$

wird $\mathcal{C}(k)$ zu einer Gruppe. Geometrisch beschreibt das Gruppengesetz die Konstruktion eines k-rationalen Punktes $P_1 \oplus P_2$ zu gegebenen $P_1, P_2 \in \mathcal{C}(k)$:

Die Gerade durch $(2,0)$ parallel zu der Geraden durch P_1 und P_2 schneidet $\mathcal{C}(k)$ in **genau einem weiteren Punkt** von $\mathcal{C}(k)$; dieser sei $P_1 \oplus P_2$. Man beachte, dass für $P_1 = (2,0)$ dabei $P_1 \oplus P_2 = P_2$ gilt, also $(2,0)$ das neutrale Element der additiven Gruppe $(\mathcal{C}(k), \oplus)$ ist.

Speziell für den Restklassenkörper $k \in \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl $p > 2$ gilt

$$\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = P - \left(\frac{D}{p}\right) =: q \qquad \text{bzw. } \mathcal{C}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z},$$

denn etwa für einen Rest $D \mod p$ gilt:

$$\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = \sum_{x \mod p} \underbrace{\left(1 + \left(\frac{x^2-4}{p}\right)\right)}_{\equiv 2 \text{ oder } \equiv 0} = p + \sum_{x \mod p} \left(\frac{(x-2)\cdot(x+2)}{p}\right)$$

je nachdem, ob $(x^2-4)D^{-1} \equiv Y^2$ ist.

$$= p + \sum_{\mathcal{X}}^{P-1} \underbrace{\left(\frac{\mathcal{X}^{-1}}{p}\right)}_{=1} \cdot \left(\frac{\mathcal{X}(\mathcal{X}+4)}{p}\right) = P + \sum_{\mathcal{X}=1}^{P-1} \left(\frac{1+\mathcal{X}^{-1}}{p}\right)$$
$$= P - 1 = P + \left(\frac{D}{p}\right)$$

denn mit $\mathcal{X}$ durchläuft auch $1 + 4\mathcal{X}^{-1}$ ein vollständiges primes Restsystem $\mod p$, hierbei ist $\mathcal{X}^{-1}$ das Inverse zu $\mathcal{X} = x - 2 \mod p$.

Sei nun eine große, zusammengesetze Zahl N gegeben. Der Ring $\mathbb{Z}/N\mathbb{Z}$ ist kein Körper (Satz 3.1) und der Kegelschnitt $\mathcal{C}(\mathbb{Z}/N\mathbb{Z})$ zerlegt sich in ein Produkt von Restklassenringen, jeweils von einer Ordnung echt kleiner $\#\mathcal{C}(\mathbb{Z}/N\mathbb{Z})$. Ist nun p ein Primteiler von N, so gilt mit $q = \#\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = p - \left(\frac{D}{p}\right)$, dass $qP = P \oplus \ldots \oplus P = (2,0)$ (mit der Lagrangeschen Erweiterung des Eulerschen Satzes 2.2) für jeden Punkt $P \in \mathcal{C}(\mathbb{Z}/N\mathbb{Z})$. Setzen wir $qP = (x,y)$, so folgt also

$$x \equiv 2 \qquad \text{und } y \equiv 0 \mod p.$$

Gilt nun $N \not| y$, so kann man durch die (schnelle) Berechnung von $\mathrm{ggT}(x-2, N)$ bzw. $\mathrm{ggT}(y, N)$ einen echten Teiler von N finden; vorteilhaft ist hierbei, wenn q nur kleine Primfaktoren besitzt.

Beispiel. Sei $N = 35$ mit $\mathcal{C} : X^2 - 12Y^2 = 4$ (siehe oben); es ist $(4,1) \in \mathcal{C}(\mathbb{Z}/35\mathbb{Z})$

$$\rightsquigarrow 2(4,1) = (14,1),$$
$$4(4,1) = 2(14,1) = (10,28)$$
$$\text{und } (3!)(4,1) = (14,1) \oplus (10,28) = (7,6)$$

was über $\mathrm{ggT}(7-2, 35) = 5$ den Primfaktor 5 von $N = 35$ liefert; hier ist $q = 5 - \left(\frac{12}{5}\right) = 6$, aber tatsächlich ist $k!$ für kleines k oft ein guter Ersatz für die Unbekannte q.

Bemerkung. Dieser Faktorisierungsalgorithmus basiert auf der „(p,q)-Methode“ von Pollard, vorgeschlagen von Lemmermeyer als „Ersatz“ für elliptische Kurven (algebraische Kurven vom Geschlecht 1, wie etwa die Fermat-Gleichung zum Exponenten $n = 3$). Allerdings erlaubt H.W. Lenstras Faktorisierungsmethode mit elliptischen Kurven (ECM, 1986) eine höhere Variabilität bei der Wahl der Gruppe (Kurve). Die Laufzeit ist **erwartet subexponentiell**, die erste **subexponentielle Methode** nach Brillhart und Morrison (1973) benutzte Kettenbrüche. Die zur Zeit schnellste (aber nicht polynominelle) Methode ist das **Zahlenkörpersieb**, welches kubsiche Irratioanlzahlen (algebraische Zahlen vom Grad 3) benutzt. Mit ihm gelang 1999 die Faktorisiserung einer 512-Bit-Zahl (**RSA-155**, 155 Stellen!).

17.07.08

Bemerkung. Die **größte bekannte Primzahl** ist:

$$2^{32\,582\,657} - 1.$$

Sie hat **fast eine Millionen Stellen** (**GIMPS 2006**).

Definition. Eine **Mersennesche Zahl**

$$M_p := 2^p - 1$$

kann nur dann prim sein, wenn p Primzahl ist, ansonsten kann man faktorisieren:

$$2^{ab} - 1 = (2^a - 1) \cdot \left(2^{(b-1)\cdot a} + \ldots + 2^a + 1\right).$$

Für Mersennesche Zahlen gibt es einen „sehr schnellen“, die spezielle Struktur von $2^p - 1$ ausnutzenden Primzahltest:

Satz 14.1. ***Lucas-Lehmer-Test***
Sei $p > 2$ prim und die Folge (S_n) rekursiv definiert durch

$$S_1 = 4, \quad S_n = S_{n-1}^2 - 2 \qquad (n \in \mathbb{N}).$$

Dann ist $M_p = 2^p - 1$ genau dann prim, wenn $Mp | S_{n-1}$.

Beispiel.

$$\begin{aligned} & S_1 = 4 \\ \rightsquigarrow\ & S_2 = 14 = 2 \cdot \underbrace{7}_{M_3} \\ \rightsquigarrow\ & S_3 = 194 \\ \rightsquigarrow\ & S_4 = 37\,634 = \underbrace{31}_{M_5} \cdot 1214 \\ \rightsquigarrow\ & S_5 = \ldots \end{aligned}$$

Beweis. Wir rechnen im Ring $\mathbb{Z}\left[\sqrt{3}\right]$. Sei $\omega = 2 + \sqrt{3}$. Wegen $N(\omega) = \omega\omega' = \left(1 + \sqrt{3}\right) \cdot \left(2 - \sqrt{3}\right) = 1$ ist ω eine Einheit im Ganzheitsring $\mathcal{O}_3 = \mathbb{Z}\left[\sqrt{3}\right]$. Per Induktion verifiziert man

$$S_n = \omega^{2^{n-1}} + (\omega')^{2^{n-1}}. \tag{14.1}$$

Also ist $M_p | S_{n-1}$ äquivalent zu

$$\omega^{2^{p-2}} + (\omega')^{2^{p-2}} \mod M_p \equiv 0 \quad \underbrace{\text{und}}_{(\omega\omega'=1)} \quad \omega^{2^{p-1}} + 1 \equiv \underbrace{0 \mod M_p}_{\text{in } \mathbb{Z}\left[\sqrt{3}\right]}. \tag{14.2}$$

Einschub: Beweis der Formel (14.2) mittels der Vollständigen Induktion:

$$\begin{aligned} & N = 1 && \Rightarrow 4 = \omega\omega' \\ n - 1 \mapsto n \ :\ & S_n = S_{n-1}^2 - 2 = \left(\omega^{2^{n-2}} + (\omega')^{2^{n-2}}\right)^2 - 2 \\ & \qquad = \omega^{2^{n-1}} + (\omega')^{2^{n-1}} + \underbrace{2(\omega\omega')^{2^{n-1}}}_{=1} - 2 \end{aligned}$$

Angenommen, M_p besitzt einen **nicht trivialen Primteiler** q, oBdA $q^2 \leq M_p$ sowie $q > 2$. Der Resklassenring (vrgl. *Beweis von* $\mathrm{X}^3 + Y^3 = Z^3$).

$$\mathbb{Z}\left[\sqrt{3}\right]/q\mathbb{Z}\left[\sqrt{3}\right] \cong (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})\sqrt{3}$$

hat genau q^2 Elemente und seine Einheitengruppe höchstens $q^2 - 1$ viele Elemente, darunter insbesondere $-1 \not\equiv 1 \mod q$ sowie $\omega \mod q$. Aus (14.2) folgt:

$$\omega^{2^{p-1}} \equiv -1 \mod q$$

und damit

$$\omega^{2^p} \equiv 1 \mod q.$$

folgt, dass $\omega \mod q$ ohne Ordnung 2^p in $\mathbb{Z}\left[\sqrt{3}\right]/q\mathbb{Z}\left[\sqrt{3}\right]$ hat. Damit ist 2^p die Ordnung von $\mod q$. (hierbei ist die Ordnung genauso definiert, wie in $\mathbb{Z}/m\mathbb{Z}$). Also teilt 2^p die Gruppenordnung q^2 (nach dem Satz 2.2 von Euler bzw. seine Verallgemeinerung nach Lagrange).

$$2^p \leq q^2 - 1 \leq M_p - 1 = 2^p - 2, \qquad \text{ein } \textbf{Widerspruch}$$

Ist umgekehrt M_p prim, so ist die Gleichung (14.2) zu zeigen. Definiere

$$\tau = \frac{1 + \sqrt{3}}{\sqrt{2}}$$

und auch

$$\tau' = \frac{1 - \sqrt{3}}{\sqrt{2}},$$

so gelten $\tau^2 = \omega$, $(\tau')^2 = \omega'$ und $\tau\tau' = -1$. Dies ersetzt Formel (14.2) durch

$$\tau^{2^p} = \tau^{M_p+1} \equiv -1 \mod M_p,$$

dies kann sowohl als Kongruenz in $\mathbb{Z}\left[\sqrt{3}\right]$ als auch in $\mathbb{Z}\left[\sqrt{2}, \sqrt{3}\right]$ interpretiert werden (wenn wir auch solche Ringe bislang nicht betrachtet haben). Nach dem Euler-Kriterium (Satz 5.1) und den Reziprozitätsgesetz mit seinen Ergänzungen (Sätze 5.5, 5.6 und 5.7) gilt

$$2^{\frac{M_p-1}{2}} \overset{5.1}{\equiv} \left(\frac{2}{M_p}\right) \mod M_p \overset{5.7}{=} (-1)^{\frac{M_p^2-1}{8}} = +1 \mod M_p \tag{14.3}$$

und

$$3^{\frac{M_p-1}{2}} \equiv \left(\frac{3}{M_p}\right) = \left(\frac{M_p}{3}\right) = -\left(\frac{(-1)^p - 1}{3}\right) = -\left(\frac{-2}{3}\right) = -1 \mod M_p. \tag{14.4}$$

Wegen

$$(a+b)^p = a^p + \underbrace{pa^{p-1}b + \ldots + pab^{n-1}}_{\equiv 0 \mod p} + b^p \equiv a^+ b^p \mod p \qquad (14.5)$$

für jede Primzahl p folgt:

$$\begin{aligned}\tau^{2^p} = \tau^{M_p+1} &= \left(1+\sqrt{3}\right)^{M_p+1} 2^{-\frac{M_p+1}{2}} \overset{14.5}{\equiv} \left(1+\left(\sqrt{3}\right)^{M_p}\right)\cdot\left(1+\sqrt{3}\right)\cdot 2^{-\frac{M_p+1}{2}}\cdot 2^{-1} \\ &\overset{14.3}{\equiv} \left(1+\sqrt{3}^{M_p}\right)\cdot\left(1+\sqrt{3}\right)2^{-1} = \left(1+3^{\frac{M_p-1}{2}}\sqrt{3}\right)\cdot\left(1+\sqrt{3}\right)2^{-1} \mod M_p \\ &\overset{14.4}{\equiv} \left(1-\sqrt{3}\right)\cdot\left(1+\sqrt{3}\right)\cdot 2^{-1} = -1 \mod M_p,\end{aligned}$$

was zu zeigen war. □

Bemerkung. Man vermutet, dass es unendlich viele **Mersennesche Primzahlen** gibt, interpretiert man nämlich den Primzahlsatz so, dass eine natürliche Zahl n mit „Wahrscheinlichkeit“ $\frac{1}{\log n}$ prim ist, so berechnet sich der Erwartungswert für die Anzahl der Mersenneschen Primzahlen als

$$\sum_p \frac{1}{\log M_p} \sim \sum_p \frac{1}{\log 2^p \cancel{-1}} = \frac{1}{\log 2}\sum_p \frac{1}{p} = +\infty$$

denn (bereits nach Euler) ist die Summe über die Reziproken der Primzahlen divergent (was man in der **analytischen Zahlentheorie** beweist).

Für Anwendungen in der Kryptographie sind Mersennesche Primzahlen jedoch unwichtig. Hier liegt es nahe, die Umkehrung des kleinen Fermatschen Satzes (Korrolar 2.3) benutzen zu wollen, diese ist allerdings im Allgemeinen **falsch**. Betrachten wir ein Beispiel:

$$2^{340} \equiv 1 \mod 341 \qquad \text{aber } 341 = 11\cdot 31$$

zusammengesetzte Zahlen $n > 1$ für die es ein $a \geq 2$ mit $a \not\equiv 1 \mod n$ gibt und

$$a^{n-1} \equiv 1 \mod n$$

erfüllen, heißen **Pseudoprimzahlen zur Basis** a. Zahlen n, die pseudoprim zu allen mit n teilerfremden Basen $a \geq 2$ sind, nennt man **Carmichael-Zahl**, die kleinste dieser Zahlen ist

$$561 = 3\cdot 11\cdot 17.$$

Es gibt (leider) unendlich viele Carmichael-Zahlen. 1994 zeigten Alford, Granville und Pomerance, dass die Anzahl $\mathcal{C}(x)$ aller Carmichael Zahlen kleiner gleich x für hinreichend große x der Ungleichung

$$x^{\frac{2}{7}} < \mathcal{C}(x) < \text{const}\cdot x^{1-\frac{\log\log\log x}{\log\log x}}$$

genügt. Glücklicherweise treten Carmichael-Zahlen seltener auf als Primzahlen bis zur Stelle x, weshalb in der Praxis der kleine Fermat zur Erzeugung von **Primzahlkandidaten** benutzt wird.

Erinnern wir uns an dieser Stelle an die Abschätzung über die Anzahl der Primzahlen:

$$\pi(x) \sim \frac{x}{\log x} > \mathcal{C}(x)$$

Ein Verfahren zum Auffinden von Carmichael-Zahlen liefert folgende einfache Charakterisierung:

Satz 14.2. *Eine ungerade, zusammengesetzte Zahl $n \geq 3$ ist genau dann eine Carmichael-Zahl wenn gilt:*

1. *n ist quadratfrei,*
2. *für jeden Primteiler p von n gilt $(p-1)|(n-1)$.*

Beweis. Zeigen wir zunächst, dass *1.* und *2.* **hinreichende** Bedingungen sind.
Sei $n = p_1, \ldots, p_k$ die Primfaktorzerlegung von n in verschiedene Primzahlen p_j. Nach Satz 3.2 gilt

$$(\mathbb{Z}/n\mathbb{Z})^4 \cong (\mathbb{Z}p_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}p_k\mathbb{Z})^*,$$

also

$$a \mod n \leftrightarrow (a_1 \mod p_1, \ldots, a_k \mod p_k),$$

für $\mathrm{ggT}(a;n) = 1$. Wegen *2.* folgt $a_j^{n-1} \equiv p_j$ für alle j und mit dem chinesischen Restsatz 2.5, also $a^{n-1} \equiv 1 \mod n$.

Nun zur **Notwendigkeit** der Bedingung; Zunächst *1.*: Ist n nicht quadratfrei , so gilt $n = p^k m$ mit einer Primzahl p, einem Exponenten $k \geq 2$ und einer zu p teilerfremden Zahl m. Nach Satz 4.5 gibt es eine Primitivwurzel $g \mod p^k$. Mit dem chinesischen Restsatz existiert ferner eine zu n teilerfremde Zahl a, so dass

$$a \equiv g \mod p^k$$

und

$$a \equiv 1 \mod m.$$

Wäre nun $a^{n-1} \equiv 1 \mod n$, so auch $g^{n-1} \equiv 1 \mod n$ bzw. $g^{n-1} \equiv 1 \mod p^k$. Da die Primitivwurzel g die Ordnung

$$\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^k - p^{k-1} = p^{k-1}(p-1)$$

besitzt, folgt $p^{k-1}(p-1)|(n-1)$, also $p|(n-1)$ im **Widerspruch** zu $p|n$. damit ist n keine Carmichael-Zahl.

Jetzt zu *2.*: Ist n eine Carmichael-Zahl, so ist n nach *1.* **quadratfrei**. Sei also $n = p \cdot m$ mit p prim und $m > 1$ teilerfremd zu p. Dasselbe Argument wie bei *1.* liefert hier $(p-1)|(n-1)$. □

Bemerkung. Damit findet man leicht einige weitere „kleine“ Carmichael-Zahlen:

$$\begin{aligned} 1105 &= 5 \cdot 13 \cdot 17, \\ 12^3 + 1^3 = 10^3 + 9^3 = 1729 &= 7 \cdot 13 \cdot 19, \\ \vdots &= \vdots \end{aligned}$$

Bemerkung. Die Zahl 1729 ist die kleinste natürliche Zahl, die sich aus der Summer zweier Kuben berechnen lässt.

18.07.08

Bemerkung. Es ist naheliegend nach Verschärfungen des kleinen Fermat zu suchen, die Primzahlen tatsächlich charakterisieren und dabei auch einen „schnellen“ Test ermöglichen. 2002 gelang Agrawahl, Kayal und Saxena die Konstruktion eines deterministischen Primzahltests in **Polynomialzeit** (das heißt polynomielle Schrittanzahl in der Eingabegröße); im Gegensatz zu so genannten **probabilistischen Primzahltests** (wie Solova-Strassen etwa) ist dieser AKS-Primzahltest in der Praxis zwar langsamer, liefert aber sicher das exakte Ergebnis.

Die Grundlage dieses Tests ist folgende einfache Ausdehnung des kleinen Fermats auf Polynome:

Satz 14.3. *Eine natürliche Zahl n ist genau dann prim, wenn gilt:*

$$(X + a)^n \equiv X^n + a^n \mod n \qquad \forall a \in \mathbb{Z}.$$

Vorsicht!
Diese Kongruenz ist im Polynomring $\mathbb{Z}[X]$ (alle Polynome mit ganzzahligen Koeffizienten) zu verstehen.

Beweis. Falls n prim ist, so ergibt sich die Kongruenz durch die binomische Reihe (wie bei $(a+b)^p \equiv a^p + b^p \mod p$). Falls n nicht prim ist, also $n = p^k m$ mit einer zu p teilerfremden Zahl $m \in \mathbb{N}$ (und $k \geq 2$, wenn $m = 1$), so ist der Koeffizient im Polynom X^p in $(X+1)^n$ gleich

$$\binom{n}{p} = \frac{n!}{(n-p)!p!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-p+1)}{1 \cdot 2 \cdot \ldots \cdot p}$$

Unter den p aufeinanderfolgenden Zahlen des Zählers ist genau **eine** durch p teilbar, nämlich $n = p^k m$, selbiges gilt für den Nenner. Also gilt:

$$\binom{n}{p} = p^{k-1} m$$

für ein $m' \in \mathbb{N}$ mit

$$\mathrm{ggT}(p, m') = 1.$$

Insbesondere ist $\binom{n}{p} \not\equiv 0 \mod p^k$ und somit auch $\not\equiv 0 \mod n$. Damit ist $(X+1)^n \not\equiv X^n + 1 \mod n$. □

Bemerkung. Wichtig für den AKS-Primzahltest ist hierbei, diese Kongruenzen (aus Satz 14.3) nicht in $\mathbb{Z}/n\mathbb{Z}[X]$ zu testen, sondern zusätzlich noch modulo eines Polynoms $X^r - 1$ mit kleinem Exponenten r (von der Größenordnung $(\log n)^{\frac{15}{2}}$). Damit wird der AKS-Primzahltest zu einem Polynomialzeittest.
Insbesondere ist also das Testen auf Primalität schnell durchführbar (Komplexitätsklasse P); für das (verwandte) Faktorisierungsproblem „erwartet“ man keine vergleichbar schnelle Methode (das liegt an der Komponentenklasse) (NP). Diese Asymmetrie nutzt man in der modernen Kryptographie aus (vergleiche mit RSA).
Es ist eine offene Vermutung, ob $P \neq NP$ gilt...

Index