Prof. Dr. K. Mathiak

Einführung in die Zahlentheorie

Braunschweig, Februar 1993

Prof. Dr. K. Mathiak
Technische Universität Braunschweig
Institut für Algebra und Zahlentheorie
Pockelsstraße 14
38106 Braunschweig

Dieses Skript wurde mit dem LaTeX 2$_\varepsilon$-Makropaket $\mathcal{AZ}$-LaTeX 2$_\varepsilon$ erstellt.
Satz: D. Pape
Dr. W. Oelke, Institut für Algebra und Zahlentheorie

Inhaltsverzeichnis

Kapitel 1. Natürliche Zahlen **5**

1. Peano–Axiome **5**

2. Addition und Multiplikation **6**

3. Anordnung in $\mathbb{N}$ **8**

4. Die Elementanzahl einer Menge **10**

5. Aufgaben **11**

Kapitel 2. Primfaktorzerlegung in $\mathbb{N}$ **13**

1. Primzahlen **13**

2. Primfaktorzerlegung **14**

3. Division in $\mathbb{N}$ **17**

4. Vollkommene Zahlen **18**

5. Aufgaben **21**

Kapitel 3. Algebraische Grundlagen **23**

1. Gruppen und Halbgruppen **23**

2. Teilbarkeit in Ringen **27**

3. Euklidische Ringe **29**

4. Der Gaußsche Ring $\mathbb{Z}[i]$ **31**

5. Aufgaben **33**

Kapitel 4. Restklassenringe **35**

1. Kongruenzen **35**

2. Chinesischer Restsatz **38**

3. Allgemeiner chinesischer Restsatz **40**

4. Zerlegung der Restklassenringe **42**

5. Aufgaben **43**

Kapitel 5. Prime Restklassengruppe **45**
1. Eulersche φ-Funktion **45**
2. Primitive Kongruenzwurzeln **47**
3. Die Indexrechnung **51**
4. Anwendungen in der Kryptologie **52**
5. Aufgaben **54**
Kapitel 6. Quadratische Reste **57**
1. Das Legendre-Symbol **57**
2. Das Reziprozitätsgesetz **59**
3. Das Jacobi-Symbol **64**
4. Polynomkongruenzen **66**
5. Aufgaben **69**
Kapitel 7. Summe von Quadraten **71**
1. Pythagoreische Tripel **71**
2. Summe von zwei Quadraten **75**
3. Summe von vier Quadraten **78**
4. Aufgaben **82**
Literatur zur Zahlentheorie **83**
Index **85**

KAPITEL 1

Natürliche Zahlen

1. Peano–Axiome

Gegenstand der elementaren Zahlentheorie sind in erster Linie die natürlichen Zahlen. Will man ihre Grundeigenschaften nicht von vorneherein als bekannt voraussetzen, so wählt man heute üblicherweise folgendes von PEANO stammende Axiomensystem als Ausgangspunkt.

- P1 1 ist eine natürliche Zahl.
- P2 Zu jeder natürlichen Zahl n gibt es eine eindeutig bestimmte natürliche Zahl n^+, die Nachfolger von n heißt.
- P3 Es gibt keine natürliche Zahl, deren Nachfolger die Zahl 1 ist.
- P4 Aus $n^+ = m^+$ folgt $n = m$.
- P5 Ist W eine Menge natürlicher Zahlen, die 1 und mit n auch n^+ enthält, so ist W gleich der Menge aller natürlichen Zahlen.

Die Menge aller natürlichen Zahlen bezeichnet man mit $\mathbb{N}$, die ersten Elemente von $\mathbb{N}$ mit

$$2 = 1^+, \qquad 3 = 2^+, \qquad 4 = 3^+, \quad \ldots$$

Die letzte Bedingung P5 heißt Induktionsaxiom. Hierauf beruhen die Beweise durch vollständige Induktion:

Ist $\mathcal{A}(n)$ eine Aussage über natürliche Zahlen, für die

$$(1) \quad \mathcal{A}(1), \qquad (2) \quad \mathcal{A}(n) \Rightarrow \mathcal{A}(n+1)$$

gilt, so erfüllt die Menge $W = \{n \in \mathbb{N} \mid \mathcal{A}(n)\}$ wegen (1) und (2) die Voraussetzungen von P5. Also ist $W = \mathbb{N}$, d.h. $\mathcal{A}(n)$ gilt für alle $n \in \mathbb{N}$.

Ein Beispiel, wie man direkt Induktionsbeweise nach P5 führen kann, ist

HILFSSATZ 1.1. *Es ist $n \neq n^+$ für alle $n \in \mathbb{N}$.*

BEWEIS. Die Menge $W = \{n \in \mathbb{N} \mid n \neq n^+\}$ erfüllt die Voraussetzungen von P5: Wäre $1 = 1^+$, so wäre 1 ein Nachfolger im Widerspruch zu P3. Folglich liegt 1 in W.

Wäre nun $n \in W$, aber $n^+ \notin W$, also $n^+ = n^{++}$, so würde $n = n^+$ nach P4 folgen, ein Widerspruch zu $n \in W$. Nach P5 ist dann $W = \mathbb{N}$, also gilt $n \neq n^+$ für alle $n \in \mathbb{N}$. □

Die Abbildung

$$\nu : \mathbb{N} \to \mathbb{N}, \qquad n \mapsto n^+$$

heißt Nachfolgerfunktion auf $\mathbb{N}$. Nach P4 ist sie injektiv. Nach P3 ist $1 \notin \text{Bild } \nu$, also ν nicht surjektiv. Genauer gilt

HILFSSATZ 1.2. *Die natürliche Zahl* 1 *ist die einzige ohne Vorgänger.*

BEWEIS. Die Menge $W = \{1\} \cup \text{Bild}\,\nu$ erfüllt die Voraussetzungen von P5, also ist $W = \mathbb{N}$. □

2. Addition und Multiplikation

Um Addition und Multiplikation auf $\mathbb{N}$ zu definieren, verwenden wir folgenden

SATZ *Es sei S eine Menge und $\varphi : S \to S$ eine Abbildung, ferner a ein Element von S. Dann gibt es eine Abbildung $f : \mathbb{N} \to S$ mit*

$$(1) \quad f(1) = a, \qquad (2) \quad f(n^+) = \varphi(f(n)).$$

Man sagt, daß f rekursiv oder induktiv definiert wird, und bezeichnet diesen Satz als *Rekursionssatz*. Wir verweisen hierzu auf

RICHARD DEDEKIND *Was sind und was sollen die Zahlen?* Vieweg 1888

Setzen wir im Rekursionssatz $S = \mathbb{N}$ und φ gleich der Nachfolgerfunktion, so wird die Addition durch folgende Gleichungen induktiv definiert

$$\begin{aligned} 1 + m &= m^+ \\ n^+ + m &= (n + m)^+. \end{aligned}$$

Das folgende Zahlenbeispiel zeigt, wie sich hiermit Additionen ausführen lassen.

$$\begin{aligned} 2 + 3 &= 1^+ + 3 = (1 + 3)^+ = 3^{++} = 4^+ = 5 \\ 3 + 2 &= 2^+ + 2 = (2 + 2)^+ = (1 + 2)^{++} = 3^{++} = 5. \end{aligned}$$

SATZ 1.1. *Die Addition ist assoziativ und kommutativ. Des weiteren gilt die Kürzungsregel*

$$n + k = n + m \quad \Longrightarrow \quad k = m.$$

BEWEIS.

(1) $n + m^+ = (n + m)^+$
Beweis durch Induktion nach n:
Für $n = 1$ ist: $1 + m^+ = m^{++} = (m + 1)^+$
Sei $n + m^+ = (n + m)^+$ bereits bewiesen. Dann ist

$$n^+ + m^+ = (n + m^+)^+ = (n + m)^{++} = (n^+ + m)^+.$$

(2) $n + 1 = n^+$
Beweis durch Induktion nach n:
Für $n = 1$ ist: $1 + 1 = 1^+$.
Sei $n + 1 = n^+$ bereits bewiesen. Dann ist

$$n^+ + 1 = (n + 1)^+ = n^{++}.$$

(3) $n + (m + k) = (n + m) + k$ (Assoziativgesetz)
Beweis durch Induktion nach n:
Für $n = 1$ ist: $1 + (m + k) = (m + k)^+ = m^+ + k = (1 + m) + k$.
Sei das Assoziativgesetz bereits für n bewiesen. Dann ist

$$\begin{aligned} n^+ + (m + k) &= (n + (m + k))^+ = ((n + m) + k)^+ \\ &= (n + m)^+ + k = (n^+ + m) + k. \end{aligned}$$

(4) $n + m = n + m$ (Kommutativgesetz)
Beweis durch Induktion nach n:
Für $n = 1$ ist: $1 + m = m^+ = 1 + m$.
Sei das Kommutativgesetz bereits für n bewiesen. Dann ist

$$n^+ + m = (n + m)^+ = (m + n)^+ = m + n^+.$$

(5) $n + k = n + m \implies k = m$
Beweis durch Induktion nach n:
Für $n = 1$ ist: $1 + k = 1 + m \implies k^+ = m^+ \implies k = m$
Induktionsschluß:

$$\begin{aligned} n^+ + k = n^+ + m &\implies (n + k)^+ = (n + m)^+ \\ &\implies n + k = n + m \\ &\implies k = m. \end{aligned}$$

□

Entsprechend definiert man die Multiplikation durch

$$\begin{aligned} 1 \cdot m &= m \\ n^+ \cdot m &= nm + m. \end{aligned}$$

Wir zeigen zuerst wieder an einem Zahlenbeispiel, wie sich hiermit Multiplikationen ausführen lassen.

$$\begin{aligned} 2 \cdot 3 &= 1^+ \cdot 3 = 1 \cdot 3 + 3 = 3 + 3 = 6 \\ 3 \cdot 2 &= 2^+ \cdot 2 = 2 \cdot 2 + 2 = (1 \cdot 2 + 2) + 2 = 2 + 2 + 2 = 6. \end{aligned}$$

Ähnlich wie für die Addition beweist man

SATZ 1.2. *Die Multiplikation ist assoziativ und kommutativ. Außerdem gilt das Distributivgesetz*

$$n(m + k) = nm + nk.$$

3. Anordnung in $\mathbb{N}$

Eine Menge M heißt bezüglich einer Relation $\leq$ *geordnet*, wenn gilt

(1) $a \leq a$

(2) $a \leq b \ \wedge\ b \leq c \quad \Longrightarrow \quad a \leq c$

(3) $a \leq b \ \wedge\ b \leq a \quad \Longrightarrow \quad a = c$

M heißt *linear* oder *total geordnet*, wenn außerdem gilt

(4) $a \leq b \ \vee\ b \leq a.$

DEFINITION. Für $n, m \in \mathbb{N}$ sei

$$n \leq m \ :\Longleftrightarrow \ \ (n = m \ \ \vee \ \ \exists\, k \in \mathbb{N} : n + k = m)\,.$$

BEMERKUNG. DEDEKIND definiert in der oben zitierten Schrift die Ordnung auf $\mathbb{N}$ ohne Benutzung der Addition. Die Idee, die Addition heranzuziehen, stammt von Landau, siehe

E. LANDAU, *Grundlagen der Analysis*, 1930.

Es gilt $1 \leq n$ für alle $n \in \mathbb{N}$. Ist nämlich $n \neq 1$, so ist n nach Hilfssatz 1.2 Nachfolger eines Element $k \in \mathbb{N}$, also $n = k^+ = k + 1$, also $1 < n$.

Wir zeigen als erstes, daß durch die obige Definition eine lineare Ordnung auf $\mathbb{N}$ erklärt wird.

(1) $n \leq n$: Dies folgt direkt aus der Definition der Ordnung.

(2) $n \leq m \wedge m \leq l \quad \Longrightarrow \quad n \leq l$: Ist $n = m$ oder $m = l$, so folgt sofort $n \leq l$. Sei also $n \neq m$ und $m \neq l$. Dann ist $n + k_1 = m$ und $m + k_2 = l$, also auf Grund des Assoziativgesetzes

$$n + (k_1 + k_2) = (n + k_1) + k_2 = l,$$

also $n \leq l$.

(3) Es sei $n \leq m \ \wedge\ m \leq n$. Wäre $n \neq m$, so existieren $k_1, k_2 \in \mathbb{N}$ mit

$$n + k_1 = m, \qquad m + k_2 = n, \qquad \text{also} \qquad n = n + (k_1 + k_2).$$

Eine Gleichung $n = n + k$ kann jedoch nicht bestehen. Aus $n + 1 = n + k + 1$ würde nämlich nach der Kürzungsregel $1 = k + 1 = k^+$ im Widerspruch zu P3 folgen.

(4) $n \leq m \ \vee\ m \leq n$: Induktion nach n.
Wegen $1 \leq m$ für alle $m \in \mathbb{N}$ gilt die Aussage für $n = 1$.
Für n sei bereits bei gegebenem m die Aussage bewiesen. Wir unterscheiden zwei Fälle.

(a) $m \leq n$. Wegen $n + 1 = n^+$ ist $n \leq n^+$. Nach (3) folgt $m \leq n^+$.

(b) $n \leq m \ \wedge\ n \neq m$, also $n + k = m$. Ist $k = 1$, so ist $n^+ \leq m$. Ist $k \neq 1$, so ist nach Hilfssatz 1.2 $k = l + 1$, also

$$n^+ + l = n + 1 + l = n + k = m,$$

also ebenfalls $n^+ \leq m$.

Wir erhalten

SATZ 1.3. *Durch die obige Relation wird* $\mathbb{N}$ *linear geordnet. Die Ordnung ist mit der Addition und Multiplikation auf* $\mathbb{N}$ *verträglich, d.h.*

(a) $\quad n \leq m \implies n + l \leq m + l,$

(b) $\quad n \leq m \implies nl \leq ml.$

BEWEIS. Für $n = m$ sind $(a), (b)$ trivial. Sei $n+k = m$. Dann ist $n+l+k = m+l$, also $n + l \leq m + l$, ferner $ml = (n + k)l = nl + kl$, also $nl \leq ml$. □

Aus der Existenz der linearen Anordnung auf $\mathbb{N}$ ergibt sich die Kürzungsregel für die Multiplikation

$$nl = nm \implies l = m.$$

Wäre nämlich $l \neq m$, etwa $l < m$, also $l + k = m$ für ein $k \in \mathbb{N}$, so würde

$$nm + 1 = nl + nk + 1 = nm + (nk)^+$$

und damit nach der Kürzungsregel für die Addition $1 = (nk)^+$ im Widerspruch zu P3 folgen.

SATZ 1.4. $\mathbb{N}$ *ist wohlgeordnet, d.h. jede nichtleere Teilmenge* S *von* $\mathbb{N}$ *besitzt ein kleinstes Element* l.

BEWEIS. Die Menge der unteren Schranken von S

$$M = \{m \in \mathbb{N} \mid m \leq s \quad \text{für alle} \quad s \in S\}$$

enthält die 1. Für $s \in S$ ist wegen $s < s^+$ sicher $s^+ \notin M$, also $M \neq \mathbb{N}$. Nach P5 gibt es daher ein $l \in M$ mit $l^+ \notin M$. Daher gibt es ein $s \in S$ mit $s < l^+$, also $l \leq s < l^+$. Da $l < s$, also $l + k = s$ auf $l^+ = l + 1 \leq l + k = s$, einen Widerspruch führt, ist $l = s \in S$. Außerdem ist l untere Schranke von S, also kleinstes Element von S. □

Wir erweitern $\mathbb{N}$ zu

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\}.$$

Hierbei sei 0 kleinstes Element von $\mathbb{N}_0$ und

$$\begin{aligned} 0 + n &= n + 0 = n \\ 0 \cdot n &= n \cdot 0 = 0. \end{aligned}$$

Da jetzt die Null zur Verfügung steht, kann die Ordnung etwas einfacher definiert werden. Es gilt

$$n \leq m \iff \exists\, k \in \mathbb{N}_0 : n + k = m.$$

4. Die Elementanzahl einer Menge

Es sei

$$A_n = \{k \in \mathbb{N} \mid k \leq n\} = \{1, 2, \ldots, n\}$$

der Zahlenabschnitt bis n.

HILFSSATZ 1.3. *Gibt es eine injektive Abbildung $f : A_n \to A_m$, so gilt $n \leq m$.*

BEWEIS. Induktion nach n. Für $n = 1$ ist $n = 1 \leq m$.
Sei $n > 1$ und $f : A_n \to A_m$ injektiv.
1. Fall: Für alle $\nu < n$ gilt $f(\nu) < m$. Dann ist

$$g : A_{n-1} \to A_{m-1}, \qquad k \mapsto f(k)$$

injektiv. Nach Induktion ist $n - 1 \leq m - 1$, also $n \leq m$.
2. Fall: Es gibt ein $\nu < n$ mit $f(\nu) = m$. Weil f injektiv ist, gilt $f(n) \neq m$. Wir definieren

$$g : A_{n-1} \to A_{m-1}, \qquad g(k) = \begin{cases} f(n), & \text{falls } k = \nu \\ f(k), & \text{falls } k < n,\ k \neq \nu. \end{cases}$$

g ist injektiv, also gilt $n - 1 \leq m - 1$, also $n \leq m$. □

DEFINITION. Zwei Mengen A und B heißen *gleichmächtig*, wenn eine Bijektion $f : A \to B$ existiert, geschrieben $A \sim B$.

Die Gleichmächtigkeit ist, wie man leicht sieht, eine Äquivalenzrelation. Ferner, ist A gleichmächtig zu A_n und zu A_m, so ist nach Hilfssatz 1.3 notwendig $n = m$. Wir definieren als Elementanzahl einer Menge A

$$|A| = \begin{cases} 0, & \text{falls } A = \emptyset \\ n, & \text{falls } A \sim A_n \\ \infty, & \text{sonst} \end{cases}$$

Eine Menge A heißt *endlich*, wenn $|A| \in \mathbb{N}_0$ oder anders geschrieben $|A| < \infty$ ist. Dies bedeutet, daß A leer oder zu einem Zahlenabschnitt A_n gleichmächtig ist.

Da es nach Hilfssatz 1.3 keine Injektion von A_{n+1} in A_n gibt, erhält man eine Schlußweise, die man als *Schubfachprinzip* bezeichnet:

> *Verteilt man $n + 1$ Gegenstände auf n Schubfächer, so enthält ein Schubfach mindestens zwei Gegenstände.*

SATZ 1.5. *Gibt es eine injektive Abbildung $f : \mathbb{N} \to A$, so ist A unendlich.* (*Insbesondere ist $\mathbb{N}$ unendlich.*)

BEWEIS. Sicher ist $A \neq \emptyset$. Wir nehmen an, daß A endlich ist, etwa $A \sim A_n$ vermittelt durch eine Bijektion $g : A \to A_n$. Außerdem sei $j : A_{n+1} \to \mathbb{N}$ die Einbettung $k \mapsto k$. Die zusammengesetzte Abbildung

$$A_{n+1} \xrightarrow{j} \mathbb{N} \xrightarrow{f} A \xrightarrow{g} A_n,$$

ist dann eine Injektion, was aber nach dem Hilfssatz auf einen Widerspruch führt. □

SATZ 1.6. *Für disjunkte Mengen gilt*

$$(*) \qquad |A \cup B| = |A| + |B|\,.$$

BEWEIS. Ist A endlich, $f : A \to A_n$ eine Bijektion und $b \notin A$, so ist

$$g : A \cup \{b\} \to A_{n+1}, \quad g(x) = \begin{cases} f(x), & \text{falls } x \in A \\ n+1, & \text{falls } x = b \end{cases}$$

bijektiv, also $|A \cup \{b\}| = |A_{n+1}| = |A| + 1 < \infty$.

Es sei $A \cup B$ endlich. Wir wollen dann durch Induktion nach $n = |A \cup B|$ zeigen, daß dann auch A und B endlich sind.

$n = 0$ bedeutet $A \cup B = \emptyset$, also sind auch A und B leer, also endlich.

Es sei $f : A \cup B \to A_{n+1}$ bijektiv. Ist etwa $f(a) = n+1$, $a \in A$ und $A' = A \setminus \{a\}$, so ist die Restriktion von f

$$g : A' \cup B \to A_n$$

bijektiv, also nach Induktion A' und B endlich. Wie oben gezeigt wurde, ist dann aber auch A endlich.

Durch Kontraposition ergibt sich: Ist A oder B unendlich, so ist es auch $A \cup B$. Damit gilt $(*)$, falls A oder B unendlich ist.

Wir können daher A und B als endlich voraussetzen. Wir beweisen dann $(*)$ durch Induktion nach $n = |B|$.

Ist $|B| = 0$, also $B = \emptyset$, so gilt $(*)$ offensichtlich.

Es sei $B = B' \cup \{b\}$ und $|B'| = n$. Dann ist nach Induktion

$$|A \cup B| = |A \cup B' \cup \{b\}| = |A \cup B'| + 1 = |A| + |B'| + 1 = |A| + |B| . \quad \square$$

In ähnlicher Weise zeigt man für die Produktmenge $A \times B$

$$|A \times B| = |A| \cdot |B|$$

Diese Formel und die Formel aus Satz 1.6 ergeben eine mengentheoretische Interpretation der induktiv definierten Multiplikation und Addition auf den natürlichen Zahlen.

5. Aufgaben

AUFGABE 1.1. Eine andere Form des Axiomensystems von PEANO ist:
Es sei $\mathbb{N}$ eine Menge mit einem ausgezeichneten Element 1 und einer Nachfolgerfunktion $\nu : \mathbb{N} \to \mathbb{N}$, $n \mapsto n^+$, für die gilt

(a) $1 \notin \text{Bild } \nu = \nu(\mathbb{N})$
(b) ν ist injektiv
(c) (P5)

Gib Beispiele für Nachfolgerfunktionen an, in denen jeweils nur zwei der Bedingungen $(a), (b), (c)$ erfüllt sind.

AUFGABE 1.2. Zeige: Jede nicht leere nach oben beschränkte Menge natürlicher Zahlen besitzt ein größtes Element.

AUFGABE 1.3. Es sei N eine Menge mit folgenden Eigenschaften

(a) N ist eine nicht leere linear geordnete Menge.
(b) N besitzt kein größtes Element.
(c) Jede nicht leere nach oben beschränkte Menge besitzt ein größtes Element.
(d) Jede nicht leere Teilmenge besitzt ein kleinstes Element.

Zeige, daß N bezüglich

$$n^+ := \min\{m \in N \mid m > n\}$$

den Peano-Axiomen genügt.

AUFGABE 1.4. Zeige für $m, n, k \in \mathbb{N}$:

(1) $n \neq n + k$.

(2) $n \leq m < n^+ \implies n = m$.

(3) $n = mk \wedge 2 \leq k \implies m < n$.

AUFGABE 1.5. Beweise das Distributivgesetz für natürliche Zahlen.

AUFGABE 1.6. Zeige: $A \subseteq B \implies |A| \leq |B|$.

KAPITEL 2

Primfaktorzerlegung in $\mathbb{N}$

1. Primzahlen

DEFINITION. Sind n und m natürliche Zahlen, so heißt n ein Teiler von m, wenn ein $k \in \mathbb{N}$ mit $nk = m$ existiert, geschrieben

$$n \mid m.$$

EIGENSCHAFTEN.

(A) Die Teilerrelation ist eine Ordnungsrelation auf $\mathbb{N}$ (nicht linear).

(B) $n \mid m \quad \Longrightarrow \quad n \leq m.$
Beweis: Es sei $nk = m$. Aus $1 \leq k$ folgt dann $n \leq nk = m$.

(C) Es sei $n \mid a$. Dann gilt

$$n \mid b \quad \Longleftrightarrow \quad n \mid a + b.$$

Beweis:

(a) Es sei $nk_1 = a, \quad nk_2 = b$. Dann ist $n(k_1 + k_2) = a + b$, also $n \mid a + b$.

(b) Es sei $nk_1 = a, \quad nl = a + b$. Dann ist $k_1 < l$, also $k_1 + k_2 = l$. Aus

$$a + nk_2 = nk_1 + nk_2 = nl = a + b$$

folgt $nk_2 = b$, also $n \mid b$.

DEFINITION. Eine Zahl $p \neq 1$ heißt eine *Primzahl*, wenn sie nur die trivialen Teiler besitzt, formelmäßig

$$p = nm \quad \Longrightarrow \quad (n = 1 \ \vee \ m = 1).$$

$\mathbb{P}$ sei die Menge aller Primzahlen.

SATZ 2.1. *Jede Zahl $n \neq 1$ besitzt einen Primteiler.*

BEWEIS. Die Menge der Teiler $\neq 1$ von n enthält ein kleinstes Element p. Dieses ist eine Primzahl. Ist nämlich $d \neq 1$ ein Teiler von p, so ist d auch Teiler von n. Wegen der Minimalität von p ist dann $d = p$. □

SATZ 2.2 (EUKLID). *Die Menge der Primzahlen ist unendlich.*

BEWEIS. Ist $A = \{p_1, \ldots, p_n\}$ eine endliche Primzahlmenge, so besitzt die Zahl

$$n = p_1 \cdot \ldots \cdot p_n + 1.$$

nach dem obigen Satz einen Primteiler p. Wäre $p \in A$, so würde $p \mid 1$ folgen. □

BEMERKUNG. In der Primzahlfolge treten Lücken beliebiger Länge auf. Die Zahlen

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n$$

sind sämtlich keine Primzahlen.

2. Primfaktorzerlegung

SATZ 2.3. *Es sei m eine von 1 verschiedene natürliche Zahl.*

(a) *m besitzt eine Primfaktorzerlegung $m = p_1 \cdot \ldots \cdot p_n$.*

(b) *Die Zerlegung ist bis auf die Reihenfolge der Primfaktoren eindeutig.*

BEWEIS. (a) Wir machen die Annahme, daß die Aussage falsch ist. Wegen der Wohlordnung von $\mathbb{N}$ gibt es dann eine kleinste natürliche Zahl n ohne Primfaktorzerlegung.

Nach Satz 2.1 ist $n = pk$, wobei p eine Primzahl ist. Es ist dann $k < n$, also hat k eine Primfaktorzerlegung, $k = p_1 \cdot \ldots \cdot p_r$, damit ist $n = p \cdot p_1 \cdot \ldots \cdot p_r$ eine Primfaktorzerlegung von n.

(b) (ZERMELO) Es sei n die kleinste natürliche Zahl mit zwei Primfaktorzerlegungen

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s.$$

Wäre $p_1 = q_1$, so wäre nach der Kürzungsregel

$$a = p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s.$$

Die Zerlegung von $a < n$ ist aber eindeutig bis auf die Reihenfolge der Faktoren, also auch die von n. Analog führt $p_1 = q_j$ auf einen Widerspruch.

Es sei ohne Beschränkung der Allgemeinheit $p_1 < q_1$, also

$$(*) \qquad p_1 + k = q_1 \qquad \text{mit} \qquad k \in \mathbb{N}\,.$$

Dann ist

$$\begin{aligned} n &= (p_1 + k)q_2 \cdot \ldots \cdot q_s \\ &= p_1 q_2 \cdot \ldots \cdot q_s + kq_2 \cdot \ldots \cdot q_s. \end{aligned}$$

n und der erste Summand sind durch p_1 teilbar, also ist nach (C) auch

$$b = kq_2 \cdot \ldots \cdot q_s$$

durch p_1 teilbar.

Für $b < n$ ist die Primfaktorzerlegung eindeutig. Daher ist jeder Primfaktor von b ein Teiler von k oder gleich $q_2, \ldots, q_s$. Da p_1 ungleich $q_2, \ldots, q_s$ ist, ist es ein Teiler von k und damit ein Teiler von $q_1 = p_1 + k$. Da q_1 Primzahl ist, folgt $q_1 = p_1$, ein Widerspruch. □

BEISPIEL. Ein Bereich ohne eindeutige Primfaktorzerlegung ist

$$B = \{2k \mid k \in \mathbb{N}\}$$

die Menge der geraden Zahlen. Sie ist abgeschlossen gegen Addition und Multiplikation, besitzt jedoch kein Einselement. Unzerlegbar sind die Elemente $2(2k+1)$. Beispiel einer nicht eindeutigen Zerlegung ist

$$60 = 2 \cdot 30 = 6 \cdot 10.$$

Man kann die in einer Zerlegung auftretenden gleichen Primfaktoren zu Potenzen zusammenfassen und erhält

KOROLLAR 2.1. *Jede natürliche Zahl $n \neq 1$ besitzt eine eindeutige Darstellung*

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r},$$

wobei $\alpha_i \in \mathbb{N}$ und die Primzahlen der Größe nach geordnet sind:

$$p_1 < p_2 < \ldots < p_r.$$

Wir können die Primfaktorzerlegung formal schreiben

$$n = \prod_{p \in \mathbb{P}} p^{\alpha_p},$$

wobei die Exponenten bis auf endlich viele oder, wie man auch sagt, fast alle Null sind.

Insbesondere sind die Exponenten eindeutig. Wir führen für diese Exponenten eine Bezeichnung ein und definieren zu einer Primzahl $p \in \mathbb{P}$

$$\operatorname{ord}_p(n) = \alpha, \qquad \alpha \in \mathbb{N}_0,$$

falls $n = p^\alpha n'$ und n' nicht durch p teilbar ist. Es ist dann

$$\operatorname{ord}_p(n) = 0 \quad \text{für fast alle} \quad p \in \mathbb{P}.$$

Nach dem obigen Korollar gilt

$$n = m \quad \Longleftrightarrow \quad \operatorname{ord}_p(n) = \operatorname{ord}_p(m) \quad \text{für alle Primzahlen } p \in \mathbb{P}.$$

SATZ 2.4. *Es gilt*

(1) $\operatorname{ord}_p(nm) = \operatorname{ord}_p(n) + \operatorname{ord}_p(m)$.

(2) $\operatorname{ord}_p(n+m) \geq \min(\operatorname{ord}_p n, \operatorname{ord}_p m)$.

BEWEIS. Es sei $n = p^\alpha n'$ und $m = p^\beta m'$. Dann ist

$$nm = p^{\alpha+\beta} n' m',$$

woraus (1) folgt. Ist $\alpha \leq \beta$, so gilt

$$n + m = p^\alpha (n' + p^{\beta-\alpha} m')$$

also, da $n' + p^{\beta-\alpha} m'$ möglicherweise noch weitere p-Potenzen enthält,

$$\operatorname{ord}_p(n+m) \geq \alpha = \min(\operatorname{ord}_p(n), \operatorname{ord}_p(m)). \quad \square$$

Die Teilbarkeit in $\mathbb{N}$ läßt sich vollständig mit Hilfe dieser Funktionen ausdrücken.

SATZ 2.5.

$$n \mid m \iff \operatorname{ord}_p(n) \leq \operatorname{ord}_p(m) \quad \textit{für alle Primzahlen } p \in \mathbb{P}\,.$$

BEWEIS. a) Ist $nk = m$, so folgt sofort

$$\operatorname{ord}_p(n) \leq \operatorname{ord}_p(n) + \operatorname{ord}_p(k) = \operatorname{ord}_p(m).$$

b) Ist

$$\operatorname{ord}_p(n) \leq \operatorname{ord}_p(m)$$

für alle $p \in \mathbb{P}$, so ist

$$\alpha_p = \operatorname{ord}_p(m) - \operatorname{ord}_p(n) = 0$$

für fast alle $p \in \mathbb{P}$. Für $k = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ gilt dann $nk = m$, also $n \mid m$. □

KOROLLAR 2.2. *Die Anzahl der Teiler von m ist*

$$\tau(m) = \prod_{p\in\mathbb{P}} (1 + \operatorname{ord}_p(m)).$$

BEISPIEL.

$$\tau(12) = \tau(2^2 \cdot 3) = 6.$$

Die gleiche Zahl von Teilern besitzt jede Zahl der Form $m = p^2 \cdot q$ mit $p, q \in \mathbb{P}$.

Aus Satz 2.4 ergibt sich weiter

KOROLLAR 2.3. *Zu zwei Zahlen $n, m \in \mathbb{N}$ gibt es einen größten gemeinsamen Teiler*

$$(n, m) = \prod_{p\in\mathbb{P}} p^{\min(\operatorname{ord}_p(n),\operatorname{ord}_p(m))}$$

und ein kleinstes gemeinsames Vielfaches

$$[n, m] = \prod_{p\in\mathbb{P}} p^{\max(\operatorname{ord}_p(n),\operatorname{ord}_p(m))}.$$

Hierfür gilt

$$(n, m)[n, m] = nm.$$

BEWEIS.

$$\begin{aligned} \min(\operatorname{ord}_p(n), \operatorname{ord}_p(m)) + \max(\operatorname{ord}_p(n), \operatorname{ord}_p(m)) &= \\ \operatorname{ord}_p(n) + \operatorname{ord}_p(m) &= \operatorname{ord}_p(nm)\,. \end{aligned}$$ □

DEFINITION. Zwei Zahlen $n, m \in \mathbb{N}$ heißen *teilerfremd*, wenn $(n, m) = 1$ ist.

ANWENDUNG. Gibt es unendlich viele zueinander teilerfremder Zahlen, so gibt es nach Satz 2.1 auch unendlich viele Primzahlen. Offensichtlich sind

$$\begin{aligned} n_1 &= 4 \\ n_2 &= n_1 + 1 \\ n_3 &= n_1 n_2 + 1 \\ &\vdots \\ n_{k+1} &= n_1 n_2 \dots n_k + 1 \\ &\vdots \end{aligned}$$

paarweise teilerfremd, also ist $\mathbb{P}$ unendlich. Dieser Beweis basiert auf Satz 2.1 (wie auch der euklidische Beweis), setzt aber nicht die Kenntnis irgendeiner Primzahl voraus.

3. Division in $\mathbb{N}$

SATZ 2.6. *Zu $n, m \in \mathbb{N}$ gibt es $q, r \in \mathbb{N}_0$ mit*

$$n = qm + r, \qquad 0 \le r < m.$$

BEWEIS. Für $n < m$ haben wir sofort $n = 0 \cdot m + n$ mit $0 \le n < m$. Es sei daher $n \ge m$. Wir betrachten die Menge

$$A = \{k \in \mathbb{N}_0 \mid \exists q \in \mathbb{N} : n = qm + k\}.$$

Sie ist nicht leer: Wegen $n \ge m$ gibt es ein $k \in \mathbb{N}_0$ mit $n = m + k$, also $k \in A$.

Es sei $r = \min A$ kleinstes Element in A. Dann ist $n = qm + r$. Wäre $r \ge m$, also $r = m + k$, so wäre

$$n = (q+1)m + k \qquad \text{mit} \qquad k < r$$

ein Widerspruch zur Minimalität von r. Es folgt $0 \le r < m$. □

Durch wiederholte Anwendung des Satzes ergibt sich

KOROLLAR 2.4. *Ist $g > 1$ eine fest gewählte natürliche Zahl, so besitzt jedes $n \in \mathbb{N}_0$ die Darstellung*

$$n = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_0 \qquad \textit{mit} \qquad 0 \le a_i < g.$$

Für $g = 10$ erhält man die übliche Dezimaldarstellung. Von Bedeutung ist noch das Dualsystem mit der Basiszahl $g = 2$ und historisch das Sexagesimalsystem mit $g = 60$. Hat man die Basiszahl festgelegt, so schreibt man zur Vereinfachung nur die Koeffizientenfolge

$$n = a_k a_{k-1} \dots a_0.$$

Hierbei ist es wichtig, daß die Nullen mitgeschrieben werden, um aus der Stelle, an der die Ziffer steht, die entsprechende Potenz von g abzulesen.

Die Bestimmung des größten gemeinsamen Teilers mittels der Primfaktorzerlegung ist für große Zahlen rechnerisch außerordentlich aufwendig. Das folgende bereits auf Euklid zurückgehende Verfahren ist dagegen sehr viel einfacher. Man bezeichnet es als euklidischen Algorithmus. Er beruht auf folgendem

SATZ 2.7. *Ist $n, m \in \mathbb{N}$ und $n = qm + r$, so gilt*

$$(n, m) = (r, m).$$

BEWEIS. Die Menge der gemeinsamen Teiler von n, m und r, m stimmen wegen (C) überein. Damit sind auch die größten gemeinsamen Teiler gleich. □

Wiederholte Anwendung ergibt den *euklidischen Algorithmus*:
Ist

$$\begin{array}{rcll} n & = & q_1 m + r_1, & 0 \le r_1 < m, \\ m & = & q_2 r_1 + r_2, & 0 \le r_2 < r_1, \\ & \vdots & & \vdots \\ r_{n-1} & = & q_{n+1} r_n + r_{n+1}, & 0 \le r_{n+1} < r_n, \\ r_n & = & q_{n+2} r_{n+1}, & \end{array}$$

so gilt auf Grund von Satz 2.7

$$(n, m) = r_{n+1}.$$

BEMERKUNG. Wegen $m > r_1 > r_2 > \ldots \ge 0$ endet der Algorithmus nach höchstens m Schritten.

BEISPIEL. Um $(963, 657)$ zu berechnen, führt man folgende Divisionen durch

$$\begin{aligned} 963 &= 657 + 306 \\ 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 36 + 9 \\ 36 &= 4 \cdot 9 \end{aligned}$$

Damit ist $(963, 657) = 9$.

4. Vollkommene Zahlen

Die Teiler von

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_1^{\alpha_1}$$

sind die Zahlen

$$d = p_1^{\beta_1} \cdot \ldots \cdot p_1^{\beta_1}, \qquad 0 \le \beta_i \le \alpha_i.$$

Man kann dies benutzen, um die Summe

$$\sigma(m) = \sum_{d|m} d$$

aller Teiler von m zu berechnen.

SATZ 2.8. *Die Summe aller Teiler von*

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$$

ist

$$\sigma(m) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

BEWEIS.

$$\begin{aligned}
\sigma(m) &= \sum_{\substack{\beta_1,\ldots,\beta_r \\ 0\le\beta_i\le\alpha_i}} p_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r} \\
&= \sum_{\substack{\beta_2,\ldots,\beta_r \\ 0\le\beta_i\le\alpha_i}} \Bigg(\sum_{\substack{\beta_1 \\ 0\le\beta_1\le\alpha_1}} p_1^{\beta_1} \Bigg) \cdot p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r} \\
&= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \sum_{\substack{\beta_2,\ldots,\beta_r \\ 0\le\beta_i\le\alpha_i}} p_2^{\beta_2}\cdot\ldots\cdot p_r^{\beta_r} \\
&= \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_r^{\alpha_r+1}-1}{p_r-1}. \qquad \square
\end{aligned}$$

KOROLLAR 2.5. *Für teilerfremde n, m gilt*

$$\sigma(nm) = \sigma(n)\sigma(m).$$

Eine Zahl m heißt *vollkommen*, wenn $\sigma(m) = 2m$ ist.

Beispiele vollkommener Zahlen sind 6, 28, 496, 8128, ...

SATZ 2.9 (EUKLID/EULER). *Eine gerade Zahl m ist genau dann vollkommen, wenn*

$$m = 2^{s-1}b \qquad \textit{und} \qquad b = 2^s - 1 \quad \textit{prim}$$

ist.

BEWEIS. 1.) Hat m die Form, so gilt nach dem obigen Korollar

$$\sigma(m) = (2^s-1)\cdot\frac{b^2-1}{b-1} = 2m.$$

2.) Es sei $m = 2^{s-1}b$ mit b ungerade und $s \ge 2$. Nach dem Korollar ist

$$\sigma(m) = \sigma(2^{s-1})\sigma(b) = (2^s-1)\sigma(b).$$

Setzen wir

$$c = \sum_{\substack{d\mid b \\ d\ne b}} d,$$

so ist $\sigma(b) = b + c$. Ist m vollkommen, also $\sigma(m) = 2m$, so folgt

$$(2^s-1)(b+c) = 2^s b, \qquad \text{also} \qquad b = (2^s-1)c.$$

Folglich ist c selbst ein Teiler von b. Als Summe der echten Teiler kann c nur 1 sein. Damit ist b eine Primzahl und $b = 2^s - 1$. $\square$

BEMERKUNG. Man bezeichnet die Zahlen $M_n = 2^n - 1$ nach MERSENNE (1588–1648) als Mersennesche Zahlen. Von Interesse sind dabei die Mersenneschen Primzahlen. Sie entsprechen nach dem obigen Satz bijektiv den geraden vollkommenen Zahlen. Ist M_n eine Primzahl, so ist auch n eine Primzahl, denn im Fall $n = uv$ gibt es die Zerlegung

$$2^{uv} - 1 = (2^u - 1)(1 + 2^u + \ldots + 2^{u(v-1)}).$$

Bekannt sind zur Zeit 31 Mersennesche Primzahlen. Die ersten sind

$$M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, \ldots$$

Dagegen ist

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

keine Primzahl.

Die Konstruktion vollkommener Zahlen im neunten Buch der Elemente von EUKLID geht bereits auf die Pythagoreer (560–400 v. Chr.) zurück. Siehe

O.BECKER *Das mathematische Denken in der Antike,* Göttingen 1957.

Offen ist die Frage, ob unendlich viele vollkommene Zahlen existieren. Man kennt bisher keine ungeraden vollkommenen Zahlen.

Ein einfacher Satz, der gewisse ungerade Zahlen als vollkommene Zahlen ausschließt, ist folgender

SATZ 2.10. *Es sei*

$$m = p_1^{\alpha_1} p_2^{\alpha_2}, \qquad p_1, p_2 \quad \textit{Primzahlen} > 2.$$

Dann ist $\sigma(m) < 2m$, also m nicht vollkommen.

BEWEIS. Da die Funktion

$$f : (1, \infty) \to \mathbb{R}, f(x) = \frac{x}{x-1}$$

monoton fällt, haben wir

$$\begin{aligned} \sigma(m) &= \frac{p_1^{\alpha_1+1}}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1}}{p_2 - 1} \\ &< \frac{p_1}{p_1 - 1} \cdot \frac{p_2}{p_2 - 1} \cdot m \\ &\leq \frac{3}{3-1} \cdot \frac{5}{5-1} \cdot m < 2m. \quad \square \end{aligned}$$

BEMERKUNG. Seit 1980 ist bekannt, daß eine ungerade vollkommene Zahl, falls sie existiert, mindestens acht verschiedene Primteiler haben muß. Computerrechnungen haben außerdem ergeben, daß es keine ungeraden vollkommene Zahlen $\leq 10^{200}$ gibt.

5. Aufgaben

AUFGABE 2.1. Es sei $n = p^\alpha$ eine Primzahlpotenz. Zeige

$$\sigma(n) = 2n - 1 \quad \Longleftrightarrow \quad p = 2.$$

AUFGABE 2.2. Zeige für $n \geq 0$

(a) 13 teilt $4^{2n+1} + 3^{n+2}$.
(b) 14 teilt $5^{2n+1} + 3^{4n+2}$.
(c) 15 teilt $4^{2n} - 1$.

AUFGABE 2.3. Es sei $(p_1, p_2, \ldots)$ die Folge der Primzahlen nach ihrer Größe geordnet. Benutze den euklidischen Schluß, um

$$p_{n+1} \leq 2^{2^n}$$

zu zeigen.

AUFGABE 2.4. Ist $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$, $2 < p_1 < p_2 < p_3$, eine vollkommene Zahl, so ist $p_1 = 3$, $p_2 = 5$.

AUFGABE 2.5. Es seien n und m teilerfremd, also $(n, m) = 1$. Zeige

(a) $(n^2 + m^2, n + m) = \begin{cases} 2 & \text{falls } n,\ m \text{ ungerade,} \\ 1 & \text{sonst} \end{cases}$

(b) $(7n + 3m, 2n - m) = 1$ oder 13

KAPITEL 3

Algebraische Grundlagen

1. Gruppen und Halbgruppen

Eine Menge G heißt eine *Gruppe*, wenn folgende Axiome gelten

(G1) Auf G ist eine Verknüpfung $G \times G \to G, \quad (b,c) \mapsto a = bc$ definiert.

(G2) Die Verknüpfung ist assoziativ.

(G3) In G gibt es ein neutrales Element, d.h. ein Element e mit $ea = ae = a$ für alle $a \in G$.

(G4) Zu jedem $a \in G$ gibt es ein Element b mit $ab = ba = e$.

Eine nicht-leere Menge H, die (G1) und (G2) erfüllt, heißt eine *Halbgruppe*. Besitzt eine Halbgruppe ein neutrales Element, so ist es eindeutig bestimmt. Wären nämlich e, f neutrale Elemente, so würde $e = ef = f$ folgen. Bei multiplikativer Schreibweise der Verknüpfung bezeichnet man e auch als Einselement.

Es sei H eine Halbgruppe mit Einselement. Ein Element $a \in H$ heißt *invertierbar* oder eine *Einheit*, wenn ein $b \in H$ mit $ab = ba = e$ existiert. Ist $a \in H$ invertierbar, so ist b eindeutig durch a bestimmt: Es sei b' ein weiteres Element mit $ab' = b'a = e$, so gilt

$$b' = b'e = b'(ab) = (b'a)b = eb = b.$$

Man schreibt dann $b = a^{-1}$ und nennt a^{-1} *Inverses* von a.

Satz 3.1. *Es sei H eine Halbgruppe mit Einselement. Die Menge*

$$G = E(H) = \{a \in H \mid a \text{ invertierbar}\}$$

ist eine Gruppe bezüglich der Verknüpfung von H. $E(H)$ heißt Einheitengruppe von H.

Beweis. Es seien $a, b \in H$ invertierbar. Aus

$$(ab)\,(b^{-1}a^{-1}) = (b^{-1}a^{-1})\,(ab) = e$$

folgt, daß ab invertierbar mit dem Inversen $b^{-1}a^{-1}$ ist. Aus

$$a^{-1}a = aa^{-1} = e$$

folgt, daß a^{-1} invertierbar mit dem Inversen a ist. Die Verknüpfung ist in H, also erst recht in $E(H)$ assoziativ. □

BEISPIEL. Es sei $A = \{1, \ldots, n\}$ und H die Menge aller Abbildungen $f : A \to A$. Jedes $f \in H$ läßt sich durch ein Schema

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

beschreiben. Die Verknüpfung in H sei die Hintereinanderschaltung der Abbildungen. Ein Element $f \in H$ ist genau dann invertierbar, wenn f bijektiv, also eine Permutation ist. $E(H)$ ist die symmetrische Gruppe.

Potenzen eines Elements definiert man induktiv durch

$$\begin{aligned} a^1 &= a \\ a^{n+1} &= a^n \cdot a \end{aligned}$$

SATZ 3.2. *Für ein Element a einer Halbgruppe gelten die Potenzregeln*

$$(*) \qquad \begin{aligned} a^n \cdot a^m &= a^{n+m} \\ (a^n)^m &= a^{nm} \end{aligned} \qquad n, m \in \mathbb{N}$$

BEWEIS. Für $m = 1$ ist

$$a^n a^1 = a^n \cdot a = a^{n+1}.$$

Durch Induktion folgt dann

$$\begin{aligned} a^n a^{m+1} &= a^n (a^m a) = (a^n a^m) a \\ &= a^{n+m} a = a^{n+m+1} \end{aligned}$$

Die zweite Formel beweist man analog. □

In einer Gruppe lassen sich auch Potenzen mit negativen Exponenten definieren. Wir setzen

$$\begin{aligned} a^0 &= 1 \quad (\textit{neutrales Element der Gruppe}) \\ a^{-n} &= (a^{-1})^n \qquad \text{für} \quad n \in \mathbb{N} \end{aligned}$$

Wie man leicht zeigt, gelten die Potenzregeln $(*)$ auch für $n, m \in \mathbb{Z}$.

Die Anzahl der Elemente bezeichnet man auch als *Ordnung* der Gruppe.

Die Potenzen eines Elements a sind:

$$\{\ldots, a^{-1}, 1, a, a^2, \ldots\}.$$

Folgende Fälle sind möglich:

1. Alle Potenzen a^n sind verschieden.
2. Es existieren $n, m \in \mathbb{N}$ mit $a^n = a^m$ für $n > m$, also $a^{n-m} = 1$. Es gibt dann ein k mit $a^k = 1$. Dies ist stets bei endlichen Gruppen der Fall.

DEFINITION. Die kleinste natürliche Zahl k mit $a^k = 1$ heißt Ordnung von a, geschrieben $\operatorname{ord} a$. Gibt es kein solches k, so heißt a ein Element unendlicher Ordnung, geschrieben $\operatorname{ord} a = \infty$.

DEFINITION. Eine Gruppe G heißt zyklisch, wenn sie nur aus den Potenzen eines Elementes a besteht, geschrieben $G = \langle a \rangle$.
a heißt dann erzeugendes Element der Gruppe.

SATZ 3.3. *Ist G eine von a erzeugte zyklische Gruppe, so gilt $|G| = \operatorname{ord} a$.*

BEWEIS. Ist $\operatorname{ord} a = \infty$, so sind alle Potenzen von a verschieden, also ist auch $|G| = \infty$.
Es sei $\operatorname{ord} a = k < \infty$. Ist $n = qk + r$, so gilt

$$a^n = (a^k)^q a^r = a^r, \quad 0 \le r < k,$$

also besitzt jedes Element von G die Darstellung a^r mit $0 \le r < k$. Ist $a^r = a^s$ mit $0 \le r \le s < k$, so folgt $a^{s-r} = 1$. Wegen $0 \le s - r < k$ und der Definition der Ordnung ist $r = s$. Also sind alle Potenzen a^r für $0 \le r < k$ verschieden. Folglich ist $|G| = k$. □

Ist ord $a = k < \infty$, so gibt es genau k verschiedene Potenzen. Dies sind

$$\{a^0 = 1, a, a^2, \ldots, a^{k-1}\}.$$

Die Ordnung eines Elements a^n ist, wie man leicht sieht,

$$\operatorname{ord} a^n = \frac{\operatorname{ord} a}{(n, \operatorname{ord} a)},$$

also sind alle Elemente a^n erzeugende Elemente, für die n teilerfremd zu $\operatorname{ord} a$ ist.

Die Verknüpfung in einer endlichen Gruppe läßt sich durch eine Verknüpfungstafel beschreiben, z.B. gibt es zwei Gruppen der Ordnung 4

	1	a	b	c
1	1	a	b	c
a	a	c	1	b
b	b	1	c	a
c	c	b	a	1

und

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Die erste Gruppe ist zyklisch. In der zweiten hat jedes von 1 verschiedene Element die Ordnung 2. Man bezeichnet sie als Kleinsche Vierergruppe.

DEFINITION. Eine Teilmenge U einer Gruppe G heißt eine *Untergruppe* von G, wenn U bezüglich der Verknüpfung von G selbst eine Gruppe ist.

BEISPIEL. Ist $a \in G$, so ist die von a erzeugte zyklische Gruppe $U = \langle a \rangle$ eine Untergruppe von G.

Nebenklassen nach einer Untergruppe

Es sei U eine Untergruppe von G. Wir definieren

$$a \sim b \quad :\Longleftrightarrow \quad a^{-1}b \in U.$$

(A) "$\sim$" ist eine Äquivalenzrelation auf G.
Beweis:
1. $a \sim a$ wegen $a^{-1}a = 1 \in U$.
2. $a \sim b \Rightarrow a^{-1}b \in U \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in U \Rightarrow b \sim a$.
3. $a \sim b \ \wedge \ b \sim c \Rightarrow a^{-1}b, b^{-1}c \in U \Rightarrow a^{-1}bb^{-1}c = a^{-1}c \in U \Rightarrow a \sim c$.

(B) Die Äquivalenzklassen bezüglich $\sim$ sind die Mengen $aU = \{au \mid u \in U\}$.
Beweis: Es ist $au_1 \sim au_2$ wegen $(au_1)^{-1}au_2 = {u_1}^{-1}u_2 \in U$. Ist $a \sim b$, so folgt $a^{-1}b \in U$, also $b = au \in aU$.
Die Mengen aU heißen linke Nebenklassen nach U.

(C) Alle linken Nebenklassen nach U haben gleich viele Elemente.
Beweis: Ist aU eine linke Nebenklasse, so ist die Abbildung

$$f : U \to aU, \quad u \mapsto au$$

nach Definition von aU surjektiv. Sie ist auch injektiv, da aus $au_1 = au_2$ durch Multiplikation mit a^{-1} von links $u_1 = u_2$ folgt. Damit sind U und aU gleichmächtig: $|U| = |aU|$.

Bemerkung. Entsprechend heißen die Mengen Ua rechte Nebenklassen nach U. Es gilt $|U| = |Ua|$. Die Anzahl der rechten und die Anzahl der linken Nebenklassen nach U stimmen überein. (Die Abbildung $x \mapsto x^{-1}$ führt rechte in linke Nebenklassen über.)

Definition. Die Anzahl der (linken oder rechten) Nebenklassen nach U heißt *Index* von U, geschrieben $(G : U)$.

Aus $G = \bigcup aU$ folgt

Satz 3.4 (Lagrange). *Ist G eine Gruppe und U eine Untergruppe von G, so gilt*

$$|G| = |U| \ (G : U).$$

Diese Formel ist auch für unendliche Gruppen richtig, sagt dann jedoch wenig aus. In den folgenden Korollaren sei G endlich.

Korollar 3.1. *Die Ordnung einer Untergruppe ist ein Teiler der Gruppenordnung.*

Korollar 3.2. *Die Ordnung eines Elements ist ein Teiler der Gruppenordnung.*

Beweis. Für $a \in G$ ist $U = \langle a \rangle$ eine Untergruppe der Ordnung $\operatorname{ord} a$. Also teilt $\operatorname{ord} a$ die Gruppenordnung. □

Korollar 3.3. *Ist $|G| = n$, so gilt $a^n = 1$ für alle $a \in G$.*

Beweis. Es sei $k = \operatorname{ord} a$. Nach dem vorigen Korollar ist $rk = n$, also

$$a^n = (a^k)^r = 1^r = 1. \quad \square$$

Korollar 3.4 (Indexformel). *Sind U, V Untergruppen von G mit $U \subseteq V \subseteq G$, so gilt*

$$(G : U) = (G : V)(V : U).$$

Beweis. Aus $|G| = |U|(G : U), ; |G| = |V|(G : V), ; |V| = |U|(V : U)$ folgt die Behauptung. □

2. Teilbarkeit in Ringen

Eine Menge R heißt ein *Ring*, wenn folgende Axiome gelten:

(R1) Auf R ist eine Addition definiert, bezüglich der R eine kommutative Gruppe ist.

(R3) Auf R ist eine Multiplikation definiert, bezüglich der R eine Halbgruppe ist.

(R3) Es gelten die Distributivgesetze

$$\begin{aligned} a(b+c) &= ab+ac \\ (a+b)c &= ac+bc. \end{aligned}$$

Wir werden außerdem stets voraussetzen, daß R ein Einselement 1 besitzt.

Ein Ring R heißt ein *Integritätsbereich*, wenn R kommutativ und nullteilerfrei ist. Nullteilerfrei bedeutet

$$ab = 0 \quad \Longrightarrow \quad (a = 0 \ \vee \ b = 0)\,.$$

Dies ist damit gleichwertig, daß die Kürzungsregel

$$(ca = cb \ \wedge \ c \neq 0) \quad \Longrightarrow \quad a = b$$

gilt.

Ein Element $e \in R$ heißt *invertierbar* oder eine *Einheit*, wenn ein Element $f \in R$ mit $ef = fe = 1$ existiert. Aus Satz 3.2 folgt dann

SATZ 3.5. *Die Einheiten eines Ringes bilden bezüglich der Multiplikation eine Gruppe, die Einheitengruppe E(R).*

DEFINITION. $a, b \in R$ heißen *assoziiert*, geschrieben $a \sim b$, wenn eine Einheit $e \in E(R)$ mit $a = be$ existiert.

Da die Einheiten eine Gruppe bilden, ist $\sim$ eine Äquivalenzrelation auf R.

DEFINITION. Es sei R ein Integritätsbereich. Ein Element a heißt Teiler von b, geschrieben $a \mid b$, wenn ein c mit $ac = b$ existiert.

Eigenschaften

(1) $a \mid a$

(2) $(a \mid b \ \wedge \ b \mid c) \quad \Longrightarrow \quad a \mid c$

(3) $(a \mid b \ \wedge \ b \mid a) \quad \Longrightarrow \quad a \sim b$
Beweis: Es sei $ac_1 = b$ und $bc_2 = a$, also $ac_2c_1 = a$.
Ist $a = 0$, so ist auch $b = ac_1 = 0$, also $a \sim b$.
Ist $a \neq 0$, so folgt nach der Kürzungsregel $c_2c_1 = 1$. Folglich ist c_1 eine Einheit und damit $a \sim b$.

(4) $a \mid b, c \quad \Longrightarrow \quad a \mid b + c$

(5) $a \mid b \iff ca \mid cb$ für $c \neq 0$.

DEFINITION. Ein Element $d \in R$ heißt ein größter gemeinsamer Teiler der Elemente $a_1, \ldots, a_n \in R$, wenn

$$\left.\begin{array}{l} d \mid a_1, a_2, \ldots, a_n \\ t \mid a_1, a_2, \ldots, a_n \end{array}\right\} \quad \Longrightarrow \quad t \mid d\,.$$

gilt. Analog definiert man das kleinste gemeinsame Vielfache.

BEMERKUNG. Im allgemeinen ist der größte gemeinsame Teiler nicht eindeutig bestimmt. Sind d und d' größte gemeinsame Teiler von $a_1, a_2, \ldots, a_n$, so gilt $d \mid d'$ und $d' \mid d$, also $d \sim d'$. Ist umgekehrt d ein größter gemeinsamer Teiler von $a_1, a_2, \ldots, a_n$ und $d \sim d'$, so ist auch d' ein größter gemeinsamer Teiler, d.h. der größte gemeinsame Teiler ist, falls er existiert, nur bis auf Assoziiertheit eindeutig. Wir schreiben

$$d \sim (a_1, a_2, \ldots, a_n).$$

Aus $a_1 \sim a_1', a_2 \sim a_2', \ldots, a_n \sim a_n'$ folgt

$$(a_1, a_2, \ldots, a_n) \sim (a_1', a_2', \ldots, a_n').$$

SATZ 3.6. *Existiert der größte gemeinsame Teiler von je zwei Elementen, so existiert er auch von n Elementen. Es gilt*

$$(a_1, a_2, \ldots, a_n) \sim ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

BEWEIS. Es sei die Existenz von $d' \sim (a_1, a_2, \ldots, a_{n-1})$ bereits gezeigt. Ist $d \sim (d', a_n)$, so gilt $d \mid d', a_n$, also

$$\left.\begin{array}{l} d \mid a_1, a_2, \ldots, a_n \\ t \mid a_1, a_2, \ldots, a_n \end{array}\right\} \quad \Longrightarrow \quad t \mid d', a_n \quad \Longrightarrow \quad t \mid d\,.$$

Folglich ist $d \sim (a_1, a_2, \ldots, a_n)$. □

Rechenregeln

(1) In $(a_1, a_2, \ldots, a_n)$ kann man die Reihenfolge der a_i beliebig ändern und beliebig klammern, z.B. ist

$$(a_1, a_2, a_3, a_4) \sim ((a_2, a_1), (a_3, a_4)).$$

(2) Es gilt

$$(a_1, a_2, \ldots, a_n) \sim (a_1, a_2, \ldots, a_{n-1}),$$

falls

$$a_n = \sum_{i=1}^{n-1} b_i a_i, \qquad b_i \in R$$

ist.

(3)

$$(ba_1, ba_2, \ldots, ba_n) \sim b\ (a_1, a_2, \ldots, a_n).$$

DEFINITION. Es sei R ein Integritätsbereich.

(1) Ein Element $p \neq 0$ heißt *prim* oder *Primelement*, wenn p keine Einheit ist, und wenn gilt

$$p \mid ab \quad \Longrightarrow \quad (p \mid a \ \vee \ p \mid b)\,.$$

(2) Ein Element $q \neq 0$ heißt *unzerlegbar* oder *irreduzibel*, wenn q keine Einheit ist, und wenn gilt

$$q = ab \quad \Longrightarrow \quad (a \text{ Einheit } \vee \ b \text{ Einheit})\,.$$

SATZ 3.7. *Jedes Primelement ist unzerlegbar.*

BEWEIS. Es sei p prim und $p = ab$. Dann gilt $p \mid ab$, also teilt p einen der Faktoren, etwa $p \mid a$. Dann ist $pk = a$, also

$$pkb = ab = p.$$

Weil R nullteilerfrei ist, folgt $kb = 1$. Folglich ist b eine Einheit. □

Die Umkehrung des Satzes gilt nicht. Dies zeigt folgendes

BEISPIEL. $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist ein Teilring von $\mathbb{C}$. Wir definieren die Norm eines Elements durch

$$N\alpha := \alpha\overline{\alpha} = a^2 + 5b^2 \in \mathbb{N}_0.$$

Hierfür gilt

$$N\alpha\beta = \alpha\beta\overline{\alpha\beta} = N\alpha \cdot N\beta.$$

Ein Element α ist genau dann eine Einheit, wenn seine Norm 1 ist. Aus $a^2 + 5b^2 = 1$ folgt $b = 0$, also ist $E = \{1, -1\}$ die Einheitengruppe. Es gilt:

(a) 3 ist unzerlegbar: Aus $3 = \alpha\beta$ folgt $N3 = 9 = N\alpha \cdot N\beta$. Die Gleichung

$$N\alpha = a^2 + 5b^2 = 3$$

besitzt jedoch keine ganzzahlige Lösung, also ist $N\alpha = 1$ oder $N\beta = 1$, d.h. α oder β ist eine Einheit.

(b) 3 ist nicht prim:
3 teilt $9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$, aber 3 teilt keinen der Faktoren $(2 + \sqrt{-5}), (2 - \sqrt{-5})$, denn die Annahme $3(a + b\sqrt{-5}) = 2 \pm \sqrt{-5}$ führt auf die Gleichung $3a = 2$, die in $\mathbb{Z}$ nicht lösbar ist.

3. Euklidische Ringe

DEFINITION. Ein Integritätsbereich R heißt ein *euklidischer* Ring, wenn eine Funktion

$$g : R \setminus \{0\} \to \mathbb{N}_0$$

mit folgender Eigenschaft existiert: Ist $a, b \in R, \quad b \neq 0$, so gibt es $q, r \in R$ mit

$$a = qb + r,$$

wobei $r = 0$ oder $g(r) < g(b)$ ist.

Beispiele sind der Ring der ganzen Zahlen mit $g(a) = |a|$ oder der Ring der Polynome $R = K[x]$ über einem Körper K mit $g(f) = \operatorname{Grad} f$.

Wir nennen die Funktion g regulär, wenn

$$g(a) \leq g(ab)$$

für alle $a, b \in R \setminus \{0\}$ gilt. Man kann stets annehmen, daß g regulär ist. Ist dies nicht der Fall, so betrachtet man die Funktion

$$h(b) = \min_{a \in R \setminus \{0\}} g(ab).$$

Wie man leicht zeigt, ist R auch euklidisch bezüglich h, und h ist offensichtlich regulär.

SATZ 3.8. *Ist R ein euklidischer Ring und $a, b \in R$, so existiert ein größter gemeinsamer Teiler d von a und b. Es gilt*

$$d = xa + yb \qquad mit \qquad x, y \in R.$$

BEWEIS. Der euklidische Algorithmus auf $\mathbb{N}$ läßt sich auf euklidische Ringe übertragen. Wiederholte Anwendung des Divisionsalgorithmus ergibt

$$\begin{array}{rcll} a & = & q_1 b + r_1, & g(r_1) < g(b) \\ b & = & q_2 r_1 + r_2, & g(r_2) < g(r_1) \\ r_1 & = & q_3 r_2 + r_3, & g(r_3) < g(r_2) \\ & \vdots & & \\ r_{n-2} & = & q_n r_{n-1} + r_n, & g(r_n) < g(r_{n-1}) \\ r_{n-1} & = & q_{n+1} r_n. & \end{array}$$

Weil die Werte von g in $\mathbb{N}_0$ liegen, endet das Verfahren nach endlich vielen Schritten. Wegen $(a, b) \sim (a - bq, b)$ ist

$$r_n \sim (a, b).$$

Benutzt man die obigen Gleichungen, so kann man r_n als Linearkombination von a und b darstellen. □

Der Beweis für die Darstellung des größten gemeinsamen Teilers läßt sich leicht durch Induktion auf n Elemente verallgemeinern. Es sei

$$d' \sim (a_1, \ldots, a_{n-1}), \qquad d \sim (d', a_n),$$

also nach Induktion

$$d' = y_1 a_1 + \cdots + y_{n-1} a_{n-1}, \qquad d = x d' + x_n a_n,$$

also

$$d = x(y_1 a_1 + \cdots + y_{n-1} a_{n-1}) + x_n a_n.$$

SATZ 3.9. *In einem euklidischen Ring ist jedes unzerlegbare Element auch prim.*

BEWEIS. Es sei $p \mid ab$, aber p weder Teiler von a noch von b. Ist p unzerlegbar,so sind a und b teilerfremd zu p. Dann ist

$$1 = xp + ya, \qquad 1 = x'p + y'b.$$

Es folgt

$$1 = (xx'p + yax' + xy'b)p + yy'ab.$$

Dies steht im Widerspruch zu $p \mid ab$. □

SATZ 3.10. *Ein euklidischer Ring ist ein Ring mit eindeutiger Primfaktorzerlegung.*

BEWEIS. Wir können annehmen, daß die Funktion g regulär ist. Wir führen einen Widerspruchsbeweis. Es sei a ein von Null verschiedenes Element mit minimalem Wert $g(a)$, das keine Einheit ist und keine Faktorzerlegung in irreduzible Elemente besitzt. a ist dann selbst reduzibel, es gibt daher eine Zerlegung $a = bc$, wobei b und c Nichteinheiten sind. Weil g regulär ist, gilt $g(b) \leq g(a)$. Wäre $g(b) = g(a)$, so hätten wir $b = qa + r$ mit $r = 0$ oder $g(r) < g(a) = g(b)$. Beides führt wegen $r = b(1-qc)$ auf einen Widerspruch. Im Fall $r = 0$ wäre c eine Einheit, im Fall $r \neq 0$ ist wegen der Regularität $g(r) = g(b(1-qc)) \geq g(b)$. Damit ist $g(b) < g(a)$. Analog folgt $g(c) < g(a)$. Wegen der Minimalität von $g(a)$ sind beide Faktoren Produkte von irreduziblen Elementen, also auch a, ein Widerspruch.

Folglich ist jedes von Null verschiedene Element, das keine Einheit ist, ein Produkt irreduzibler Elemente, nach Satz 3.9 ein Produkt von Primelementen.

Es bleibt der Beweis der Eindeutigkeit der Primfaktorzerlegung. Es sei

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s, \qquad p_i, q_j \quad \text{prim.}$$

Wir führen den Beweis durch Induktion nach r. Für $r = 1$ ist $p_1 = q_1$, weil p_1 unzerlegbar ist. Sei $r > 1$.

Aus $p_1 \mid a = q_1 \cdot \ldots \cdot q_s$ folgt wegen der Primeigenschaft von p_1, daß p_1 einen der Faktoren q_j teilt, etwa q_1. Damit gilt $p_1 e = q_1$. Dann ist aber, da q_1 unzerlegbar ist, e eine Einheit und p_1 zu q_1 assoziiert. Nach der Kürzungsregel folgt

$$p_2 \cdot \ldots \cdot p_r = (eq_2) \cdot \ldots \cdot q_s,$$

und daraus nach Induktion die Behauptung. □

4. Der Gaußsche Ring $\mathbb{Z}[i]$

Die Elemente

$$\alpha = a + bi \in \mathbb{Z}[i]$$

bilden in der Gaußschen Zahlenebene ein quadratisches Gitter. Wir betrachten die Normabbildung

$$N : \mathbb{Z}[i] \to \mathbb{N}_0, \quad N(a+bi) = a^2 + b^2.$$

Eigenschaften der Norm

(1) $N(\alpha\beta) = \alpha\beta\overline{\alpha}\overline{\beta} = N(\alpha)N(\beta)$
Wegen $\alpha\beta = (a+bi)(c+di) = (ac-bd) + i(ad+bc)$ folgt

$$(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2).$$

Daraus ergibt sich, daß das Produkt zweier natürlicher Zahlen, die sich als Summe zweier Quadrate schreiben lassen, wieder eine Summe zweier Quadrate ist.

(2) α Einheit in $\mathbb{Z}[i] \iff N(\alpha) = 1 \iff \alpha \in \{1, i, -1, -i\}$

(3) Bezüglich $g(\alpha) = N\alpha$ ist $\mathbb{Z}[i]$ ein euklidischer Ring.
Beweis: Seien $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Berechne in $\mathbb{C}$

$$\frac{\alpha}{\beta} = \gamma + \varepsilon$$

mit $\gamma \in \mathbb{Z}[i]$, $\varepsilon \in \mathbb{C}$ und

$$|\mathrm{Im}(\varepsilon)| \leq \frac{1}{2} \quad \wedge \quad |\mathrm{Re}(\varepsilon)| \leq \frac{1}{2},$$

d.h. γ ist der $\frac{\alpha}{\beta}$ nächstliegende Gitterpunkt. Dann ist

$$\alpha = \gamma\beta + \rho\,,$$

wenn wir $\rho := \varepsilon\beta$ setzen. Es ist

(a) $\rho = \alpha - \gamma\beta \in \mathbb{Z}[i]$

(b) $g(\rho) = N\varepsilon \cdot N\beta \leq \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) N\beta < g(\beta)$ oder $\rho = 0$.

Wegen der Multiplikativität der Norm ist die Funktion g regulär.

(4) Primelemente in $\mathbb{Z}[i]$:

(a) *Ist $N\alpha = p$ eine Primzahl in $\mathbb{N}$, dann ist α Primelement in $\mathbb{Z}[i]$.*
Beweis: Sei $\alpha = \beta\gamma$, also $N\alpha = N\beta \cdot N\gamma = p$. Es folgt $N\beta = 1$ oder $N\gamma = 1$, also ist β oder γ eine Einheit.

(b) *Ist $p \in \mathbb{P}$ zerlegbar in $\mathbb{Z}[i]$, so ist $p = N\alpha = a^2 + b^2$ Summe zweier Quadrate.*
Beweis: Sei $p = \alpha\beta$, $N\alpha, N\beta \neq 1 \Longrightarrow Np = p^2 = N\alpha \cdot N\beta \Longrightarrow N\alpha = p = a^2 + b^2$.

(c) *Ist α prim in $\mathbb{Z}[i]$, so gibt es ein $p \in \mathbb{P}$ mit $\alpha | p$.*
Beweis: Sei $\alpha\overline{\alpha} = N\alpha = p_1 \ldots p_r$ die Primfaktorzerlegung in $\mathbb{N}$, $N\alpha \neq 1$. Weil α prim ist, folgt $\alpha | p_i$ für ein i. (Man erhält also die Primelemente $\alpha \in \mathbb{Z}[i]$ durch Zerlegung der Primzahlen $p \in \mathbb{P}$.)

(d) *Ist α prim und $\alpha | p$, p prim in $\mathbb{N}$, so gilt:*
(a) $\alpha \sim p$ *oder* (b) $N\alpha = p$.
Beweis: Wegen $\alpha | p$ ist $\alpha\beta = p \Longrightarrow Np = p^2 = \underbrace{N\alpha}_{\neq 1} \cdot N\beta$
Fall 1: $N\alpha = p^2 \quad \Longrightarrow \quad N\beta = 1$, β Einheit $\quad \Longrightarrow \alpha \sim p$
Fall 2: $N\alpha = p = a^2 + b^2$.

Ergebnis. Jedes Primelement α ergibt sich durch Zerlegung einer Primzahl $p \in \mathbb{P}$.

Sei $p \in \mathbb{P}$ Primzahl in $\mathbb{N}$

1. Fall: p ist nicht Summe zweier Quadrate. Nach (2) ist p unzerlegbar. Mit p sind auch $-p, ip, -ip$ Primelemente.

2. Fall: $p = a^2 + b^2$, also $p = N\alpha$ mit

$$\alpha \in \{a + bi, -a + bi, a - bi, -a - bi, b + ai, -b + ai, b - ai, -b - ai\}.$$

Man erhält 8 Primelemente, davon sind 4 assoziiert. Im Fall $p \neq 2$ sind alle 8 verschieden.

$p \in \mathbb{P}$	1. Quadrant	2. Quadrant	3. Quadrant	4. Quadrant
$2 = 1^2 + 1^2$	$1 + i$	$-1 + i$	$-1 - i$	$1 - i$
3	3	$3i$	-3	$-3i$
$5 = 1^2 + 2^2$	$1 + 2i$	$-1 + 2i$	$-1 - 2i$	$1 - 2i$
$5 = 2^2 + 1^2$	$2 + i$	$-2 + i$	$-2 - i$	$2 - i$
7	7	$7i$	-7	$-7i$
11	11	$11i$	-11	$-11i$
$13 = 2^2 + 3^2$	$2 + 3i$	$-2 + 3i$	$-2 - 3i$	$2 - 3i$
$13 = 3^2 + 2^2$	$3 + 2i$	$-3 + 2i$	$-3 - 2i$	$3 - 2i$

BEISPIEL. Zerlege $\alpha = 7 + 4i$ in Primfaktoren in $\mathbb{Z}[i]$:

$$N\alpha = 7^2 + 4^2 = 65 = 5 \cdot 13 = (1^2 + 2^2)(2^2 + 3^2) = (1 + 2i)(1 - 2i)(2 + 3i)(2 - 3i)$$

Die rechtsstehenden Ausdrücke sind die möglichen Primfaktoren von α. Welche es sind, stellt man durch Division fest. Weil

$$\frac{7 + 4i}{1 - 2i} = \frac{1}{5}(-1 + 18i)$$

nicht in $\mathbb{Z}[i]$ liegt, tritt $1 - 2i$ nicht als Primfaktor auf. Aus

$$\frac{7 + 4i}{1 + 2i} = 3 - 2i$$

folgt $7 + 4i = (1 + 2i)(3 - 2i)$.

5. Aufgaben

AUFGABE 3.1. Sei $R = \mathbb{Z}[\sqrt{-2}]$
(a) Zeige, daß R euklidisch ist.
(b) Welche Elemente sind Einheiten, welche sind prim?

AUFGABE 3.2. 1. Ermittle im Ring $\mathbb{Z}[i]$ die Primfaktorzerlegung von $\alpha = 3 - 11i$.
2. Ermittle den größten gemeinsamen Teiler von α und $\beta = 3 + 4i$.

KAPITEL 4

Restklassenringe

1. Kongruenzen

Es sei $n \in \mathbb{N}$ fest gewählt. Wir definieren auf $\mathbb{Z}$ folgende Relation

$$a \equiv b \bmod n \quad :\Longleftrightarrow \quad n \mid a-b \quad \Longleftrightarrow \quad \exists\, k \in \mathbb{Z}: \quad nk = a-b$$

gesprochen a kongruent b modulo n.

Es handelt sich um eine Äquivalenzrelation:

(1) $a \equiv a \bmod n$ wegen $n \mid a-a$.

(2) Ist $a \equiv b \bmod n$, also $nk = a-b$, so folgt $n(-k) = b-a$, also $b \equiv a \bmod n$.

(3) Es sei $a \equiv b \bmod n$ und $b \equiv c \bmod n$, also $nk_1 = a-b, \quad nk_2 = b-c$, so folgt $n(k_1+k_2) = a-c$, also $a \equiv c \bmod n$.

Diese Relation wurde von Gauss 1801 in den *Disquisitiones Arithmeticae* eingeführt. Bezüglich dieser Relation wird $\mathbb{Z}$ in n Klassen eingeteilt: Es sei $a \in \mathbb{Z}$. Dann ist

$$a = qn + r, \qquad 0 \le r < n,$$

also $a \equiv r \bmod n$ für ein $r \in \{0, 1, \ldots, n-1\}$. Ist $0 \le r,\, r' < n$ und $r \equiv r' \bmod n$, also $r - r' = kn$, so folgt $k = 0$ wegen $|r - r'| < n$, also $r = r'$. Damit ist

$$\{0, 1, \ldots, n-1\}$$

ein vollständiges Repräsentantensystem.

Da sich die Repräsentanten als Reste bei der Division durch n ergeben, bezeichnet man die Klassen als Restklassen $b \bmod n$. Die Menge der Restklassen bezeichnet man mit $\mathbb{Z}_n$. Für die Elemente von $\mathbb{Z}_n$ schreibt man $\overline{a}$ oder $a \bmod n$.

Satz 4.1. *Bezüglich der Verknüpfungen*

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} \cdot \overline{b} &= \overline{ab} \end{aligned}$$

ist $\mathbb{Z}_n$ ein kommutativer Ring.

Beweis. Die Verknüpfungen sind wohldefiniert: Es sei $\overline{a} = \overline{a'}, \quad \overline{b} = \overline{b'}$, also

$$a = a' + k_1 n, \qquad b = b' + k_2 n.$$

Dann ist

$$\begin{aligned} a+b &= a'+b'+(k_1+k_2)n \\ ab &= a'b'+(k_1b'+k_2a'+k_1k_2n)n, \end{aligned}$$

also

$$\begin{aligned} \overline{a+b} &= \overline{a'+b'} \\ \overline{ab} &= \overline{a'b'}. \end{aligned}$$

Die Ringaxiome und die Kommutativität lassen sich trivial zeigen. □

BEISPIEL. $\mathbb{Z}_4$ besteht aus vier Elementen. Die Multiplikationstafel ist

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Insbesondere erkennt man hieraus, daß $\mathbb{Z}_4$ kein Körper ist. Wegen $\overline{2}\cdot\overline{2} = \overline{0}$ existieren Nullteiler in $\mathbb{Z}_4$.

HILFSSATZ 4.1. *Es sei $d = (a, n)$. Die Kongruenz*

$$(*) \qquad ax \equiv b \bmod n$$

ist genau dann lösbar, wenn d ein Teiler von b ist.

BEWEIS. Ist x eine Lösung von $(*)$, so ist

$$ax = b + kn,$$

also d ein Teiler von b, weil d sowohl a als auch n teilt.

Ist umgekehrt d Teiler von b und $d = au + nv$, so folgt

$$b = dk = auk + nvk, \qquad \text{also} \qquad b \equiv auk \bmod n.$$

Folglich ist $x = uk$ eine Lösung von $(*)$. □

SATZ 4.2. *$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

BEWEIS. 1.) Ist $n = p$ eine Primzahl, so ist $(a, n) = 1$ für alle $\overline{a} \neq 0$. Nach dem Hilfssatz gibt es eine Lösung von $ax \equiv 1 \bmod n$, also ist $\overline{a}$ invertierbar.
2.) Ist $n = ab$ mit $1 < a, b < n$, so ist $\overline{a}\overline{b} = 0$ mit $\overline{a}, \overline{b} \neq 0$. Wäre $\overline{b}$ invertierbar, etwa $\overline{b}\overline{x} = \overline{1}$, so würde $\overline{a} = \overline{a}\overline{b}\overline{x} = 0$ folgen. □

BEISPIEL. Um das Inverse eines Elements $\overline{a}$ im Körper $\mathbb{Z}_p$ zu berechnen, benötigt man eine Darstellung

$$1 = ax + py,$$

die man mittels des euklidischen Algorithmus gewinnt.

Es sei $p = 641, \quad a = 222$. Dann ist

$$\begin{aligned} 641 &= 3 \cdot 222 - 25 \\ 222 &= 9 \cdot 25 - 3 \\ 25 &= 8 \cdot 3 + 1, \end{aligned}$$

also $1 = 25 - 8 \cdot 3 = 25 - 8 \cdot (9 \cdot 25 - 222) = -71 \cdot 25 + 8 \cdot 222 = -71(3 \cdot 222 - 641) + 8 \cdot 222 = -205 \cdot 222 + 71 \cdot 641$. Das Ergebnis ist

$$\overline{222}^{-1} = \overline{-205} = \overline{436}.$$

ANWENDUNGEN. 1.) Neunerprobe. Wegen $10^k \equiv 1 \bmod 9$ ist

$$a = a_0 + a_1 10 + \ldots + a_k 10^k \equiv a_0 + a_1 + \ldots + a_k \bmod 9,$$

also 9 ein Teiler von a, wenn 9 die Quersumme teilt (wobei die Quersumme die Summe der Ziffern im Dezimalsystem ist). Eine Multiplikation zweier Zahlen läßt sich mit Hilfe der Neunerprobe kontrollieren, z.B. $1237 \cdot 568 = 702616$, da $4 \cdot 1 \equiv 4 \bmod 9$ ist. Eine analoge Regel gilt für $n = 3$.

2.) Für $n = 11$ ist

$$10^k \equiv (-1)^k \bmod 11,$$

also

$$a = a_0 + a_1 10 + \ldots + a_k 10^k \equiv a_0 - a_1 + \ldots + a_k (-1)^k \bmod 11.$$

Hiermit läßt sich feststellen, ob 11 ein Teiler von a ist.
Beispiel: $11 \mid 4356$ wegen $11 \mid 6 - 5 + 3 - 4 = 0$.

3.) Bücher versieht man seit 1969 mit der International Standard Book Number, abgekürzt ISBN, z.B.

ISBN 3-540-16099-X.

Die erste Ziffer bedeutet das Land (3=deutsch), die zweite Zifferngruppe den Verlag (540=Springerverlag), die dritte die Buchnummer des Verlages. Die letzte Ziffer ist eine Kontrollziffer $k \in \{0, 1, \ldots, 9, X\}$, wobei X für 10 steht. Die Kontrolle der ersten neun Ziffern $a_1, a_2, \ldots, a_9$ führt man durch, indem man

$$k \equiv \sum_{i=1}^{9} i a_i \bmod 11$$

prüft. Im Beispiel ist

$$10 \equiv 3 + 2 \cdot 5 + 3 \cdot 4 + 5 \cdot 1 + 6 \cdot 6 + 8 \cdot 9 + 9 \cdot 9 \bmod 11.$$

Empirische Versuche haben ergeben, daß Schreibfehler bei Buchbestellungen in 80 Prozent der Fälle Einzelfehler sind, in 10 Prozent durch Vertauschung zweier benachbarter Ziffern entstehen. Bei einem Einzelfehler

$$a_i \quad \mapsto \quad a_i + e_i$$

entsteht eine Abweichung in der Kontrollziffer von $\Delta k = i e_i \not\equiv 0 \bmod 11$, bei einer Vertauschung von a_i mit a_j ist

$$\Delta k = j a_i + i a_j - i a_i - j a_j = (j - i)(a_i - a_j) \not\equiv 0 \bmod 11.$$

In beiden Fällen entstehen Abweichungen von der Kontrollziffer. Bei einer Neunerprobe würde die zweite Gruppe von Fehlern nicht erkennbar sein.

2. Chinesischer Restsatz

Gesucht sind die Lösungen eines Kongruenzsystems

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_k \bmod n_k. \end{aligned}$$

BEISPIEL. Gegeben sei

$$\begin{aligned} x &\equiv 1 \bmod 5 \\ x &\equiv 2 \bmod 6 \\ x &\equiv 3 \bmod 7 \end{aligned}$$

Die Lösungen lassen sich rekursiv ermitteln. Die erste Kongruenz bedeutet $x = 5t + 1$. Eingesetzt in die zweite und dritte Kongruenz ergibt sich

$$\begin{aligned} 5t + 1 &\equiv 2 \bmod 6 \\ 5t + 1 &\equiv 3 \bmod 7 \end{aligned}$$

oder

$$\begin{aligned} t &\equiv 5 \bmod 6 \\ t &\equiv 6 \bmod 7 \end{aligned}$$

Für $t = 6u + 5$ folgt

$$6u + 5 \equiv 6 \bmod 7,$$

also $u \equiv 6 \bmod 7$, also $u = 7v + 6$. Insgesamt ergibt sich

$$x = 5(6(7v + 6) + 5) + 1 = 210v + 206,$$

also

$$x \equiv 206 \bmod 210.$$

SATZ 4.3. *Das System*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \end{aligned}$$

besitzt genau dann eine Lösung, wenn der größte gemeinsame Teiler d von n_1 und n_2 ein Teiler von $a_1 - a_2$ ist.

BEWEIS. 1.) Ist x eine Lösung, so gilt

$$\begin{aligned} x &\equiv a_1 \bmod d \\ x &\equiv a_2 \bmod d, \end{aligned}$$

also durch Subtraktion $0 \equiv a_1 - a_2 \bmod d$, also $d \mid a_1 - a_2$.

2.) Lösungen der ersten Kongruenz haben die Form $x = a_1 + kn_1$. Eingesetzt in die zweite Kongruenz, ergibt sich die Kongruenz

$$kn_1 \equiv a_2 - a_1 \bmod n_2,$$

die lösbar ist, wenn $d = (n_1, n_2)$ ein Teiler von $a_1 - a_2$ ist. □

SATZ 4.4. *Die Lösungen eines Kongruenzsystems*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_k \bmod n_k \end{aligned}$$

sind, falls welche existieren, eindeutig modulo $v = [n_1, \ldots, n_k]$.

BEWEIS. 1.) Sind x und x' Lösungen, so gilt

$$x \equiv a_i \equiv x' \bmod n_i$$

für $i = 1, \ldots, k$, also $n_i \mid x - x'$, also

$$v = [n_1, \ldots, n_k] \mid x - x',$$

also $x \equiv x' \bmod v$.

2.) Ist x eine Lösung und $x' \equiv x \bmod v$, so ist $x' \equiv x \equiv a_i \bmod n_i$, für $i = 1, \ldots, k$, also auch x' eine Lösung des Kongruenzsystems. □

SATZ 4.5. *Sind* $n_1, \ldots, n_k$ *paarweise teilerfremd, so besitzt das System*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \\ x &\equiv a_k \bmod n_k \end{aligned}$$

Lösungen.

BEWEIS. Es sei

$$n = n_1 \cdot \ldots \cdot n_k \qquad \text{und} \qquad N_i = \frac{n}{n_i} \qquad \text{für} \qquad i = 1, \ldots k.$$

Dann sind n_i und N_i teilerfremd, also gibt es ein m_i mit

$$N_i m_i \equiv 1 \bmod n_i, \qquad i = 1, \ldots, k.$$

Die Zahl

$$x = N_1 m_1 a_1 + \ldots + N_k m_k a_k$$

ist dann eine Lösung. □

BEISPIEL. Zu lösen ist das Kongruenzsystem

$$\begin{aligned} x &\equiv 2 \bmod 8 \\ x &\equiv 1 \bmod 9 \\ x &\equiv 6 \bmod 11. \end{aligned}$$

Es ist $n = 8 \cdot 9 \cdot 11 = 792$ und

$$N_1 = 9 \cdot 11 = 99 \qquad N_2 = 8 \cdot 11 = 88 \qquad N_3 = 8 \cdot 9 = 72.$$

Man errechnet nun m_1, m_2, m_3 aus

$$\begin{aligned} 99m_1 &\equiv 1 \bmod 8 \\ 88m_2 &\equiv 1 \bmod 9 \\ 72m_3 &\equiv 1 \bmod 11. \end{aligned}$$

nach dem euklidischen Algorithmus

$$\begin{aligned} 99 &= 12 \cdot 8 + 3 \\ 8 &= 3 \cdot 3 - 1 \end{aligned}$$

also $1 = 3 \cdot (99 - 12 \cdot 8) - 8 \equiv 3 \cdot 99 \bmod 8$, also $m_1 = 3$. Entsprechend erhält man $m_2 = 4$, $m_3 = 2$. Damit ist eine Lösung

$$\begin{aligned} x &= N_1 m_1 a_1 + N_2 m_2 a_2 + N_3 m_3 a_3 \\ &= 99 \cdot 3 \cdot 2 + 88 \cdot 4 \cdot 1 + 72 \cdot 2 \cdot 6 \\ &= 1810 = 2 \cdot 792 + 226 \end{aligned}$$

also $x \equiv 226 \bmod 792$. Hierbei ist 226 die kleinste positive Lösung.

BEMERKUNG. Man bezeichnet den obigen Satz als *chinesischen* Restsatz, da er bei den Chinesen zur Berechnung günstiger Kalenderdaten diente. Bei teilerfremden Moduln existiert stets eine Lösung.

3. Allgemeiner chinesischer Restsatz

HILFSSATZ 4.2. (*Distributivität des Teilerverbandes*)

(1) $(a, [b, c]) = [(a, b), (a, c)]$

(2) $[a, (b, c)] = ([a, b], [a, c])$

BEWEIS. (1) Es sei $\operatorname{ord}_p a = r$, $\operatorname{ord}_p b = i$, $\operatorname{ord}_p c = j$ und etwa $i \leq j$. Dann ist

$$\operatorname{ord}_p(a, [b, c]) = \min(r, j)$$

und

$$\operatorname{ord}_p[(a, b), (a, c)] = \max(\min(r, i), \min(r, j)) = \min(r, j).$$

Die Gleichheit besteht für alle Primzahlen p und daher allgemein.

(2) analog. □

SATZ 4.6. *Das Kongruenzsystem*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_k \bmod n_k \end{aligned}$$

ist lösbar, wenn jeweils zwei der Kongruenzen eine Lösung besitzen (das ist nach Satz 4.3 der Fall, wenn $(n_i, n_j) \mid a_i - a_j$ *gilt).*

BEWEIS. Induktion nach k. Der Induktionsanfang für $k = 1, 2$ ist trivial. Es sei daher $k > 2$. Wir ermitteln zunächst $b_2, \ldots, b_k$ mit

$$\begin{aligned} b_j &\equiv a_1 \bmod n_1 \\ b_j &\equiv a_j \bmod n_j \end{aligned}$$

Setzen wir $m_r = [n_1, n_r]$ für $r = 2, \ldots, k$, so ist

$$\begin{aligned} x &\equiv b_i \bmod m_i \\ x &\equiv b_j \bmod m_j \end{aligned}$$

lösbar, denn es ist

$$\begin{aligned} b_i &\equiv a_1 \bmod n_1 \\ b_j &\equiv a_1 \bmod n_1, \end{aligned}$$

also $b_i - b_j \equiv 0 \bmod n_1$, und

$$\begin{aligned} b_i &\equiv a_i \bmod (n_i, n_j) \\ b_j &\equiv a_j \bmod (n_i, n_j), \end{aligned}$$

also $b_i - b_j \equiv 0 \bmod (n_i, n_j)$. Insgesamt ist

$$b_i - b_j \equiv 0 \bmod [n_1, (n_i, n_j)].$$

Nach dem Hilfssatz ist $[n_1, (n_i, n_j)] = ([n_1, n_i], [n_1, n_j]) = (m_i, m_j)$, also

$$b_i - b_j \equiv 0 \bmod (m_i, m_j).$$

Nach Induktion besitzt dann

$$\begin{aligned} x &\equiv b_2 \bmod m_2 \\ &\vdots \\ x &\equiv b_k \bmod m_k \end{aligned}$$

eine Lösung x. Hiermit ist $x \equiv b_2 \bmod [n_1, n_2]$, also

$$\begin{aligned} x \equiv b_2 &\equiv a_1 \bmod n_1 \\ x \equiv b_2 &\equiv a_2 \bmod n_2 \\ &\vdots \\ x \equiv b_k &\equiv a_k \bmod n_k \end{aligned}$$ □

BEISPIEL. Das Kongruenzsystem

$$\begin{aligned} x &\equiv 10 \bmod 24 \\ x &\equiv 50 \bmod 88 \\ x &\equiv 28 \bmod 99 \end{aligned}$$

ist wegen

$$(24, 88) = 8 \mid 50 - 10, \qquad (24, 99) = 3 \mid 28 - 10, \qquad (88, 99) \mid 50 - 28$$

lösbar. Die Lösung berechnet man durch Zerlegung der einzelnen Kongruenzen

$$\begin{array}{rcrcrcrcr} x & \equiv & 10 \bmod 24 & \Longleftrightarrow & x & \equiv & 1 \bmod 3 & \wedge & x & \equiv & 2 \bmod 8 \\ x & \equiv & 50 \bmod 88 & \Longleftrightarrow & x & \equiv & 2 \bmod 8 & \wedge & x & \equiv & 6 \bmod 11 \\ x & \equiv & 28 \bmod 99 & \Longleftrightarrow & x & \equiv & 1 \bmod 9 & \wedge & x & \equiv & 6 \bmod 11 \end{array}$$

Dieses System ist mit dem Kongruenzsystem

$$\begin{array}{rcl} x & \equiv & 2 \bmod 8 \\ x & \equiv & 1 \bmod 9 \\ x & \equiv & 6 \bmod 11 \end{array}$$

gleichwertig, dessen Lösung, wie oben gezeigt wurde, $x \equiv 226 \bmod 792$ ist.

4. Zerlegung der Restklassenringe

Es seien $R_1, \ldots, R_k$ Ringe. Man definiert auf

$$R = R_1 \times \ldots \times R_k = \{(a_1, \ldots, a_k) \mid a_i \in R_i\}$$

Addition und Multiplikation komponentenweise: Hierdurch erhält man wieder einen Ring, den man direktes Produkt der Ringe R_i nennt. Es ist

$$|R| = |R_1| \cdot \ldots \cdot |R_k|,$$

falls die einzelnen Ringe endlich sind.

Für die Einheitengruppe gilt: $E(R) = E(R_1) \times \ldots \times E(R_k)$, denn ein Element $a = (a_1, \ldots, a_k) \in R$ ist genau dann invertierbar, wenn jede Komponente $a_i \in R_i$ invertierbar ist.

Eine Abbildung $f : R \to R'$ heißt Homomorphismus, wenn

$$\begin{array}{rcl} f(a+b) & = & f(a) + f(b) \\ f(ab) & = & f(a) \cdot f(b) \end{array}$$

für alle $a, b \in R$ gilt. Ein Homomorphismus f heißt Isomorphismus, wenn f bijektiv ist.

SATZ 4.7. *$n_1, \ldots, n_r$ seien paarweise teilerfremd und $n = n_1 \cdot \ldots \cdot n_r$. Die Abbildung*

$$f : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$$

mit

$$x \bmod n \mapsto (x \bmod n_1, \ldots, x \bmod n_r)$$

ist ein Isomorphismus.

BEWEIS. (1) f ist Homomorphismus:

$$\begin{array}{rcl} f(x \bmod n + y \bmod n) & = & f(x + y \bmod n) \\ & = & (x + y \bmod n_1, \ldots, x + y \bmod n_r) \\ & = & (x \bmod n_1 + y \bmod n_1, \ldots, x \bmod n_r + y \bmod n_r) \\ & = & (x \bmod n_1, \ldots, x \bmod n_r) + (y \bmod n_1, \ldots, y \bmod n_r) \\ & = & f(x \bmod n) + f(y \bmod n) \end{array}$$

Analog für die Multiplikation.

(2) f ist surjektiv wegen Satz 4.5 (Chinesischer Restsatz) und injektiv wegen Satz 4.4. □

KOROLLAR 4.1. *$n_1, \ldots, n_r$ seien paarweise teilerfremd und $n = n_1 \cdot \ldots \cdot n_r$. Die Abbildung*

$$f : E(\mathbb{Z}_n) \to E(\mathbb{Z}_{n_1}) \times \ldots \times E(\mathbb{Z}_{n_r})$$

mit

$$x \bmod n \mapsto (x \bmod n_1, \ldots, x \bmod n_r)$$

ist ein Gruppenisomorphismus.

5. Aufgaben

AUFGABE 4.1. Benutze die Tatsache $7 \cdot 11 \cdot 13 = 1001$, um ein Teilbarkeitskriterium für 7, 11 und 13 zu erhalten.

AUFGABE 4.2. Zeige

$$5^n \equiv 1 + 4n \bmod 16 \quad \text{und} \quad 5^{2n} \equiv 1 + 24n \bmod 48\,.$$

AUFGABE 4.3. Es sei $a_1, a_2, \ldots, a_n \in \mathbb{N}_0$.
Zeige, daß eine Teilmenge dieser Zahlen existiert, deren Summe $\equiv 0 \bmod n$ ist.

AUFGABE 4.4. Zeige, daß das System

$$\begin{array}{rcll} 5x & \equiv & 2 & mod\ 13 \\ x & \equiv & 7 & mod\ 20 \\ x & \equiv & 2 & mod\ 35 \\ 3x & \equiv & 13 & mod\ 77 \end{array}$$

lösbar ist und ermittle die Lösungen.

AUFGABE 4.5. Welche der beiden folgenden Kongruenzsysteme sind lösbar? Bestimme im Fall der Lösbarkeit die Lösungen.

$$\text{(a)}\quad \begin{array}{rcrl} x & \equiv & 1 & \bmod 6 \\ 5x & \equiv & 1 & \bmod 14 \\ 8x & \equiv & 17 & \bmod 21 \end{array} \qquad \text{(b)}\quad \begin{array}{rcrl} x & \equiv & 2 & \bmod 6 \\ 5x & \equiv & 1 & \bmod 14 \\ 8x & \equiv & 17 & \bmod 21. \end{array}$$

KAPITEL 5

Prime Restklassengruppe

1. Eulersche φ-Funktion

Unter der primen Restklassengruppe versteht man die Einheitengruppe E_n des Restklassenringes $\mathbb{Z}_n$, also

$$E_n = E(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\}.$$

Die Anzahl der Elemente von E_n bezeichnet man mit $\varphi(n)$. Die Abbildung

$$\varphi : \mathbb{N} \to \mathbb{N}$$

heißt Eulersche φ-Funktion.

BEISPIELE. (1) $n = 12$. Es ist

$$E_{12} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\},$$

also $\varphi(12) = 4$.
E_{12} ist eine Kleinsche Vierergruppe:

	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

(2) $n = 18$. Es ist

$$E_{18} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$$

also $\varphi(18) = 6$. E_{18} ist zyklisch, z.B. ist $\overline{5}$ ein erzeugendes Element.

SATZ 5.1. *Für Primzahlpotenzen gilt*

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

BEWEIS. Wegen $(m, p^k) \neq 1 \iff p \mid m$ ist m genau dann nicht teilerfremd zu p^k, wenn m ein Vielfaches von p ist, also gilt $|E_{p^k}| = p^k - p^{k-1}$. □

Als eine unmittelbare Folgerung von Korollar 4.1 ergibt sich

SATZ 5.2. *Für teilerfremde m und n gilt*

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

KOROLLAR 5.1. *Es sei $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Dann ist*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).$$

BEWEIS. Es gilt

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) \\ &= p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right). \qquad \square \end{aligned}$$

Ist G eine Gruppe der Ordnung $|G| = k$, so gilt nach Korollar 3.3

$$g^k = 1 \quad \forall\, g \in G.$$

Für die primen Restklassengruppen erhalten wir hieraus

SATZ 5.3 (EULER). *Ist $(a, n) = 1$, so gilt*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Speziell für Primzahlen p ist $\varphi(p) = p - 1$. Also gilt

SATZ 5.4 (FERMAT). *Ist $p \in \mathbb{P}$ und $a \in \mathbb{Z}$, dann gilt*

$$a^p \equiv a \bmod p.$$

BEWEIS. Ist p Teiler von a, so sind beide Seiten der Kongruenz $\equiv 0 \mod p$. Ist p kein Teiler von a, so folgt nach dem Eulerschen Satz $a^{p-1} \equiv 1 \mod p$ und damit die obige Kongruenz. $\square$

ANWENDUNGEN. Der Fermatsche Satz läßt sich bei Primzahltests benutzen. Zuerst im negativen Sinn: Ist eine gegebene Zahl n kein Teiler von $2^n - 2$, so ist sie auch keine Primzahl.

Die Umkehrung der Aussage gilt im allgemeinen nicht. Es gibt zusammengesetzte Zahlen n, die $2^n - 2$ teilen. Man bezeichnet sie als *pseudoprim*.

BEISPIEL. Es sei: $n = 341 = 11 \cdot 31$. Wegen $2^{10} \equiv 1 \mod 11$ gilt

$$2^{341} = 2(2^{10})^{31} \equiv 2 \mod 11,$$

also $11 \mid 2^{341} - 2$. Wegen $2^5 = 32 \equiv 1 \mod 31$ gilt

$$2^{341} = 2(2^5)^{68} \equiv 2 \mod 31,$$

also $31 \mid 2^{341} - 2$. Insgesamt ist

$$341 = 11 \cdot 31 \mid 2^{341} - 2.$$

Unterhalb 1000 sind außer 341 nur noch 561 und 645 pseudoprim. Die Anzahl der Primzahlen unter 10^{10} ist 455052512 und die der pseudoprimen Zahlen 14884. Verglichen mit den Primzahlen sind daher die Pseudoprimzahlen selten. Mit großer Wahrscheinlichkeit ist daher eine Zahl n eine Primzahl, wenn sie $2^n - 2$ teilt.

Ist n pseudoprim, so ist es auch $2^n - 1$. Hieraus folgt, daß es unendlich viele Pseudoprimzahlen gibt.

2. Primitive Kongruenzwurzeln

HILFSSATZ 5.1. *Sind a, b Elemente einer abelschen Gruppe mit teilerfremden Ordnungen, so gilt* $\operatorname{ord}(ab) = \operatorname{ord} a \cdot \operatorname{ord} b$.

BEWEIS. Sei $\alpha = \operatorname{ord} a$, $\beta = \operatorname{ord} b$, $\gamma = \operatorname{ord}(ab)$. Aus

$$(ab)^{\alpha\beta} = a^{\alpha\beta} b^{\alpha\beta} = 1 \cdot 1 = 1$$

folgt $\gamma \mid \alpha\beta$. Aus

$$1 = (ab)^{\gamma} = (ab)^{\gamma\alpha} = a^{\gamma\alpha} b^{\gamma\alpha} = b^{\gamma\alpha}$$

folgt $\beta \mid \gamma\alpha$ und, da β teilerfremd zu α ist, $\beta \mid \gamma$.

Analog ergibt sich $\alpha \mid \gamma$. Wieder, weil die Ordnungen teilerfremd sind, ist $\alpha\beta \mid \gamma$ und damit $\alpha\beta = \gamma$. □

HILFSSATZ 5.2. *Sei G eine endliche abelsche Gruppe und $m = \max\{\operatorname{ord} a \mid a \in G\}$. Dann gilt:* $\operatorname{ord} a \mid m$ *für alle $a \in G$.*

BEWEIS. Sei $m = \operatorname{ord} b$ und $\alpha = \operatorname{ord} a$. Annahme: α sei kein Teiler von m, etwa $\alpha = p^k u$, $m = p^l v$, $p \in \mathbb{P}$, $k > l$, $(u, p) = (v, p) = 1$. Dann ist $\operatorname{ord} a^u = p^k$ und $\operatorname{ord} b^{p^l} = v$ mit $(p^k, v) = 1$, also $\operatorname{ord} a^u b^{p^l} = p^k v > p^l v = m$ nach dem obigen Hilfssatz. Widerspruch zur Maximalität von m. □

HILFSSATZ 5.3. *Ein vom Nullpolynom verschiedenes Polynom n-ten Grades über einem Körper K besitzt höchstens n Nullstellen.*

BEWEIS. Induktion nach n: Ist der Grad von f Null, so ist f das konstante Polynom und besitzt keine Nullstellen.
Sei $n = \text{Grad } f > 0$ und $a_1, \ldots, a_r$ verschiedene Nullstellen von f. Ist $f(x) = g(x)(x - a_1) + s$, $s \in K$, so folgt $f(a_1) = s = 0$, also $f(x) = g(x)(x - a_1)$.
Für a_k, $k > 1$, ist $f(a_k) = 0 = g(a_k)(a_k - a_1)$, also $g(a_k) = 0$ für $k = 2, \ldots, r$. Nach Induktion ist $r - 1 \leq \text{Grad } g = n - 1$, also $r \leq n$. □

SATZ 5.5. *Die prime Restklassengruppe E_p, $p \in \mathbb{P}$, ist zyklisch.*

BEWEIS. $\mathbb{Z}_p$ ist ein Körper, $\varphi(p) = p - 1$. Es sei $m = \max\{\operatorname{ord} \overline{a} \mid \overline{a} \in E_p\}$. Nach Hilfssatz 5.2 gilt $\overline{a}^m = \overline{1}$ für alle $\overline{a} \in E_p$. Das Polynom $x^m - \overline{1}$ besitzt also $\varphi(p) = p - 1$ Nullstellen. Also ist nach dem Hilfssatz 5.3 $\varphi(p) \leq m$. Weil aber m ein Teiler von $|E_p| = \varphi(p)$ ist, gilt $\varphi(p) = m$. Damit gibt es ein $\overline{a} \in E_p$ mit $\operatorname{ord} \overline{a} = \varphi(p) = |E_p|$. Folglich ist E_p zyklisch. □

DEFINITION. Ist die prime Restklassengruppe E_n zyklisch und $\overline{a}$ ein erzeugendes Element von E_n, so heißt a eine primitive Kongruenzwurzel mod n.

BEISPIEL. Es sei $p = 13$, $\varphi(p) = 12$. Um zu zeigen, daß 2 eine primitive Kongruenzwurzel ist, berechnen wir mod 13 die Potenzen von 2.

$$\begin{array}{cccc} 2^1 \equiv 2 & 2^2 \equiv 4 & 2^3 \equiv 8 & 2^4 \equiv 3 \\ 2^5 \equiv 6 & 2^6 \equiv 12 & 2^7 \equiv 11 & 2^8 \equiv 9 \\ 2^9 \equiv 5 & 2^{10} \equiv 10 & 2^{11} \equiv 7 & 2^{12} \equiv 1 \end{array}$$

Also hat 2 die Ordnung 12 und ist daher eine primitive Kongruenzwurzel mod 13.

SATZ 5.6 (WILSON). *Ist p eine Primzahl, so gilt*

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

BEISPIEL.

$$\begin{array}{rrl} 1! = & 1 \equiv & -1 \mod 2 \\ 4! = & 24 \equiv & -1 \mod 5 \\ 6! = & 720 \equiv & -1 \mod 7 \end{array}$$

BEWEIS. Es sei a eine eine primitive Wurzel mod p. Dann gilt in $\mathbb{Z}_p$

$$\prod_{\overline{x} \in E_p} \overline{x} = \overline{(p-1)!} = \prod_{k=1}^{p-1} \overline{a}^k = \overline{a}^{\sum_{k=1}^{p-1} k} = \left(\overline{a}^{\frac{p-1}{2}}\right)^p \overset{\text{Fermat}}{=} \overline{a}^{\frac{p-1}{2}}.$$

Weil a eine primitive Wurzel ist, gilt $\overline{a}^{\frac{p-1}{2}} \neq \overline{1}$. Außerdem ist $\left(\overline{a}^{\frac{p-1}{2}}\right)^2 \overset{\text{Fermat}}{=} 1$, also $\overline{a}^{\frac{p-1}{2}}$ Nullstelle von $t^2 - \overline{1}$. Dieses Polynom hat nur zwei Nullstellen, $\overline{1}$ kommt nicht in Frage. Folglich ist $\overline{a}^{\frac{p-1}{2}} = \overline{-1}$. □

HILFSSATZ 5.4. *Ist a eine primitive Wurzel* mod *p, so gibt es auch eine primitive Wurzel b* mod *p, für die $b^{p-1} \not\equiv 1 \mod p^2$ ist.*

BEWEIS. Ist $a^{p-1} \not\equiv 1 \mod p^2$, so wählt man $b = a$. Ist aber $a^{p-1} \equiv 1 \mod p^2$, so gilt für $b = a + p$

$$b^{p-1} = (a+p)^{p-1} \equiv a^{p-1} + \binom{p-1}{1} a^{p-2} p \equiv 1 - a^{p-2} p \not\equiv 1 \mod p^2. \quad \square$$

SATZ 5.7. *Ist $p > 2$ und $m = p^k$ oder $m = 2p^k$, so ist E_m zyklisch.*

BEWEIS. (1) $m = p^k$. Wählt man b wie in Hilfssatz 5.4, so gilt:

$$(*) \qquad b^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k$$

$(*)$ gilt nach Hilfssatz 5.4 für $k = 2$. Sei $(*)$ also für k bereits bewiesen. Wegen

$$b^{\varphi(p^{k-1})} = b^{p^{k-2}(p-1)} \equiv 1 \mod p^{k-1}$$

ist $b^{p^{k-2}(p-1)} = 1 + cp^{k-1}$ mit $(c, p) = 1$. Also

$$b^{p^{k-1}(p-1)} = (1 + cp^{k-1})^p \equiv 1 + \underbrace{cp^k}_{\neq 0} \not\equiv 1 \mod p^{k+1}.$$

Es sei n die Ordnung von $\overline{b}$ in E_{p^k}. Dann ist $b^n \equiv 1 \mod p^k$ also $b^n \equiv 1 \mod p$. Weil b eine primitive Wurzel mod p ist, folgt $p - 1 \mid n$. Außerdem gilt $n \mid \varphi(p^k) =$

$p^{k-1}(p-1)$, also $n = p^l(p-1)$ mit $l \leq k-1$. Auf Grund von $(*)$ ist $n = p^{k-1}(p-1) = \varphi(p^k) = |E_{p^k}|$. Damit ist E_{p^k} ist zyklisch.

(2) $m = 2p^k$. Es ist

$$E_{2p^k} \simeq E_2 \times E_{p^k} \simeq E_{p^k},$$

weil $E_2 = \{1\}$ ist. Damit ist E_{2p^k} zyklisch. Konkret: Sei b eine primitive Wurzel mod p^k. Dann ist b oder $b + p^k$ ungerade. Für ungerade Zahlen a gilt:

$$p^k | a^k - 1 \iff 2p^k | a^k - 1,$$

also ist b oder $b + p^k$ primitiv mod $2p^k$. □

Man kennt kein einfaches Verfahren, um eine primitive Kongruenzwurzel modulo einer Primzahl zu ermitteln. Kennt man aber ein primitives Element b mod p, $p > 2$, so kann man nach dem Beweis des obigen Satzes sofort ein primitives Element mod p^k bzw. mod $2p^k$ angeben. Im Fall $m = p^k$ hat man $b^{p-1} \not\equiv 1 \mod p^2$ zu prüfen. Wenn dies gilt, ist b primitiv für alle p^k, andernfalls hat man b durch $b + p$ zu ersetzen. Im zweiten Fall $m = 2p^k$ ist b oder $b + p^k$ primitiv, je nachdem, welches der beiden Elemente ungerade ist.

BEISPIEL. Es sei $p = 5$. Die prime Restklassengruppe mod 5 ist:

$$E_5 = \{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$$

mit

Element	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
Ordnung	1	4	4	2

Folglich sind 2 und 3 primitiv mod 5.
Es sei zuerst $m = 5^k$: Wegen $2^4 = 16 \not\equiv 1 \mod 25$ ist 2 primitiv mod 5^k für alle $k \in \mathbb{N}$.
Im Fall $m = 2 \cdot 5^k$ ist 3 ungerade und daher primitiv mod $2 \cdot 5^k$ für alle $k \in \mathbb{N}$.
Speziell für $m = 10$ ist $\varphi(10) = 4$ und

$$E_{10} = \{\overline{3},\ \overline{3}^2 = \overline{9},\ \overline{3}^3 = \overline{7},\ \overline{3}^4 = \overline{1}\}$$

also $\operatorname{ord} \overline{3} = 4 = \varphi(10)$, also 3 primitiv mod 10.

SATZ 5.8. *Sei $m = uv$, $(u, v) = 1$, $u, v > 2$. Dann ist E_m nicht zyklisch.*

BEWEIS. Da $\varphi(u)$ und $\varphi(v)$ gerade sind, ist $k = \frac{1}{2}\varphi(u)\varphi(v)$ ein Vielfaches von $\varphi(u)$ und von $\varphi(v)$. Für $\overline{a} \in E_m$ gilt nach Euler:

$$\overline{a}^k \equiv 1 \mod u \wedge \overline{a}^k \equiv 1 \mod v,$$

also

$$\overline{a}^k \equiv 1 \mod uv.$$

Wegen

$$k = \frac{\varphi(u)\varphi(v)}{2} = \frac{\varphi(uv)}{2} < \varphi(uv)$$

gibt es in E_m kein Element der Ordnung $\varphi(m)$, also ist E_m nicht zyklisch. □

BEISPIELE.

$$\begin{array}{lll} E_{12} & = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\} & \text{nicht zyklisch} \\ E_8 & = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} & \text{nicht zyklisch} \\ E_4 & = \{\overline{1}, \overline{3}\} & \text{zyklisch} \\ E_2 & = \{\overline{1}\} & \text{zyklisch} \end{array}$$

SATZ 5.9. *Sei $m = 2^k$, $k \geq 3$. Dann ist E_m nicht zyklisch.*

BEWEIS. Es ist $\varphi(m) = 2^k - 2^{k-1} = 2^{k-1}$. Sei $\overline{a} \in E_m$. Behauptung: Es gilt für ungerade a:

$$(*) \qquad a^{2^{k-2}} \equiv 1 \mod 2^k, \ k \geq 3\,,$$

d.h. die Ordnungen der Elemente aus E_m sind $\leq 2^{k-2}$.

Beweis von $(*)$ durch Induktion nach k:
$k = 3$: Wegen $\overline{a} \in E_m$ ist $a = 2n + 1$ ungerade, also

$$a^2 = 1 + 4n(n+1) \equiv 1 \bmod 8.$$

Sei $k \geq 3$ und $(*)$ für k bewiesen. Dann ist

$$a^{2^{k-2}} = 1 + b2^k, \ b \in \mathbb{Z}.$$

Also

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = (1 + b2^k)^2 = 1 + a2^{k+1} + a^2 2^{2k} \equiv 1 \mod 2^{k+1}\,. \quad \square$$

Wir fassen die bisherigen Ergebnisse zusammen

SATZ 5.10. *Genau die primen Restklassengruppen E_m mit*

$$m \in \{1, 2, 4, p^k, 2p^k\}, \quad p \in \mathbb{P}, \quad p \neq 2$$

sind zyklisch.

SATZ 5.11. *Ist b eine primitive Wurzel mod m, so ist*

$$\{b^k \mid 1 \leq k < \varphi(m), \ (k, \varphi(m)) = 1\}$$

die Menge aller primitiven Wurzeln mod m. Also gibt es $\varphi(\varphi(m))$ primitive Wurzeln.

BEWEIS. Es gilt für Ordnungen der Potenzen eines Elementes einer Gruppe:

$$\operatorname{ord} \alpha^k = \frac{\operatorname{ord} \alpha}{(\operatorname{ord} \alpha, k)}$$

also wegen $\operatorname{ord} \overline{b} = \varphi(m)$

$$\operatorname{ord} \overline{b}^k = \varphi(m) \iff (k, \varphi(m)) = 1\,. \quad \square$$

3. Die Indexrechnung

Wie sich schon der Satz von Wilson sehr einfach unter Verwendung primitiver Kongruenzwurzeln mod p beweisen läßt, kann man die Struktur der multiplikativen Gruppe der Körper $\mathbb{Z}_p$ dazu nutzen, um ein der Logarithmenrechnung ähnliches Verfahren in diesen Körpern einzuführen, das als Indexrechnung bezeichnet wird und auf GAUSS zurückgeht.

Man wählt hierzu eine primitive Kongruenzwurzel b mod p und stellt jedes von Null verschiedene Element $a \in \mathbb{Z}_p$ als Potenz dar

$$a = b^k, \qquad 0 \le k < p.$$

Dabei ist k eindeutig bestimmt und heißt nach GAUSS *Index* von a zur Basis b. Es gilt

$$\operatorname{ind} aa' \equiv \operatorname{ind} a + \operatorname{ind} a' \bmod p - 1,$$

also entspricht dem Produkt zweier Elemente die Summe der Indizes.

BEISPIEL. Wie oben gezeigt wurde, ist 2 eine primitive Wurzel mod 13. Durch Potenzieren von 2 erhält man folgende Tabelle

x	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind} x$	12	1	4	2	9	5	11	3	8	10	7	6

Ist $2^k \equiv x \bmod 13$, so ist $k = \operatorname{ind} x$ zur Basis 2. Man kann diese Tafel ähnlich wie eine Logarithmentafel benutzen.

$$7 \cdot 8 \equiv 2^{11} \cdot 2^3 \equiv 2^{14} \equiv 4 \bmod 13$$
$$7^{-1} \equiv 2^{-11} \equiv 2^1 \equiv 2 \bmod 13$$
$$7^{22} \equiv 2^{11 \cdot 22} \equiv 2^{242} \equiv 4 \bmod 13$$

Es lassen sich mit dieser Methode auch Kongruenzen lösen.

BEISPIEL. Es sei $p = 17$. Wegen $3^8 = 6561 \equiv 16 \bmod 17$ ist 3 ein primitives Element.
Indextafel zur Basis 3

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind} x$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Es gilt: $x = 3^{\operatorname{ind} x}$ und $\operatorname{ord} x = \frac{16}{(16, \operatorname{ind} x)}$.

Um die Kongruenz

$$6x^{12} \equiv 11 \bmod 17$$

zu lösen, betrachten wir die hierzu äquivalente Kongruenz

$$\operatorname{ind} 6 + 12 \cdot \operatorname{ind} x \equiv \operatorname{ind} 11 \bmod 16.$$

Dies ist

$$\iff 12 \cdot \operatorname{ind} x \equiv 7 - 15 \equiv 8 \bmod 16$$
$$\iff 3 \cdot \operatorname{ind} x \equiv 2 \bmod 4$$
$$\iff \operatorname{ind} x \equiv 2 \bmod 4$$
$$\iff \operatorname{ind} x \equiv 2, 6, 10, 14 \bmod 16$$
$$\iff x \equiv 9, 15, 8, 2 \bmod 17.$$

4. Anwendungen in der Kryptologie

Teil A: Lineare Methoden

Schon Julius Caesar benutzte ein einfaches Verschlüsselungsverfahren, indem er das Alphabet „um drei Buchstaben nach rechts verschob“:

Original	A	B	C	...	X	Y	Z
verschoben	D	E	F	...	A	B	C

Beispiel: CAESAR $\hat{=}$ FDHVDU

Jedem Buchstaben sei nun eine Zahl zugeordnet:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Hiermit werden den Buchstaben des Alphabets eineindeutig die Elemente des Restklassenringes $\mathbb{Z}_{26}$ zugeordnet. Eine Verschlüsselung oder Chiffrierung der Buchstaben entspricht einer Abbildung der Zahlen.

(1) Einfache lineare Chiffrierung:

$$y \equiv ax + b \mod 26$$

mit $(a, 26) = 1$
Die Dechiffrierung erfolgt durch:

$$x \equiv a^{-1}y - a^{-1}b \mod 26.$$

Das Verfahren von Caesar ergibt sich für $a = 1,\ b = 3$.

Der Nachteil dieser linearen Verfahren besteht in ihrer einfachen Decodierung aufgrund der Häufigkeitsverteilung der Buchstaben. Sind nämlich (x_1, y_1) und (x_2, y_2) bekannt, so kann man a und b aus

$$\begin{aligned} y_1 &\equiv ax_1 + b \mod 26 \\ y_2 &\equiv ax_2 + b \mod 26 \end{aligned}$$

berechnen. Eine grobe Abschätzung der Häufigkeitsverteilung der Buchstaben in der deutschen Sprache ist:

„E“:	10
„N“:	6
andere Buchstaben:	< 5

Beispiel. Nach einem Linearcode ist

TZEH MIMO HXKY HNMX

verschlüsselt. Die mehrfach auftretenden Buchstaben sind: H, M, X. Die Zuordnung: M$\to$E ($13 \to 5$), X$\to$N ($24 \to 14$) führt auf

$$\left.\begin{aligned} 5 &\equiv 13a + b \mod 26 \\ 14 &\equiv 24a + b \mod 26 \end{aligned}\right\} \Longrightarrow 9 \equiv 11a \mod 26 \Longrightarrow x = 15y + 18.$$

Die Lösung ist: FROH EWEI HNAC HTEN

(2) Blocksysteme (HILL 1930)

Um die Decodierung über die Häufigkeitsverteilung der Buchstaben zu vermeiden faßt man in der gegebenen Buchstabenfolge jeweils l Buchstaben zu Blöcken zusammen, und verschlüsselt die einzelnen Blöcke mittels einer linearen Transformation. z. B. $l = 2$: $(x_1, x_2)(x_3, x_4)\ldots$

$$\begin{aligned} y_1 &\equiv ax_1 + bx_2 \mod 26 \\ y_2 &\equiv cx_1 + dx_2 \mod 26 \end{aligned}$$

wobei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertierbar in $\mathbb{Z}_{26}$ ist. Dies ist genau dann der Fall, wenn $\mathrm{Det}(A) = ad - bc$ eine Einheit in $\mathbb{Z}_{26}$ ist. Die inverse Matrix berechnet sich nach der Formel

$$A^{-1} = \frac{1}{\mathrm{Det}(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Beispiel:

$$A = \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}.$$

$\mathrm{Det}(A) = 7$ ist eine Einheit in $\mathbb{Z}_{26}$. Der Euklidische Algorithmus liefert $26 = 4 \cdot 7 - 2$, $7 = 3 \cdot 2 + 1$, also $1 = 7 - 3(4 \cdot 7 - 26) \equiv 15 \cdot 7 \mod 26$. Daraus ergibt sich

$$A^{-1} = 15 \cdot \begin{pmatrix} 15 & -17 \\ -4 & 5 \end{pmatrix} = \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix}$$

Original	BR	AU	NS	CH	WE	IG
Ziffernpaare (x, y)	(2,18)	(1,21)	(14,19)	(3,8)	(23,5)	(9,7)
$(x, y) \cdot A$	(4,18)	(11,20)	(16,3)	(21,15)	(5,24)	(21,24)
verschlüsselt	DR	KT	PC	UO	EX	UX

Dechiffrierung erfolgt durch Multiplikation mit A^{-1}.

(3) Benutzung eines Schlüsselwortes

Man benutzt zur Codierung ein sogenanntes *Schlüsselwort*, das durch eine Ziffernfolge $(k_1, \ldots, k_n)$ gegeben ist. Setzt man $k_{i+n} = k_i$, so wird die Nachricht mittels

$$y_i = x_i + k_i$$

verschlüsselt. Die Entschlüsselung erfolgt durch Subtraktion.

BEISPIEL. Das Schlüsselwort sei Baum. Hierzu gehören die Ziffern

B	A	U	M	
2	1	21	13	
k_1	k_2	k_3	k_4	$k_{i+4} = k_i$

Beispiel:

Original	B	R	A	U	N	S	C	H	W	E	I	G
als Ziffern	2	18	1	21	14	19	3	8	23	5	9	7
Schlüsselwort	2	1	21	13	2	1	21	13	2	1	21	13
Summe mod 26	4	19	22	8	16	20	24	21	25	6	4	20
verschlüsselt	D	S	V	H	P	T	X	U	Y	F	D	T

Das Verfahren stammt von VIGENÈRE.

Teil B: Exponentenbildung

Als einfache Anwendung des Eulerschen Satzes ergibt sich

SATZ: Sei $m \in \mathbb{N}$ und $(e, \varphi(m)) = 1$. Dann ist die Abbildung $f : E_m \to E_m$, $f(x) = x^e$ bijektiv mit der Umkehrabbildung $g : E_m \to E_m$, $f^{-1}(x) = x^f$, wobei $ef \equiv 1 \mod \varphi(m)$ ist.

BEWEIS. $(g \circ f)(x) = (f \circ g)(x) = x^{ef} = x$, wegen $x^{\varphi(m)} \equiv 1 \mod m$. □

(4) Verfahren von POHLIG, HELMANN 1978

Es sei $m = p \in \mathbb{P}$. Man zerlegt die Buchstabenfolge in Blöcke der Länge l. Jedem Buchstaben entspreche eine Zahl x_i mit $1 \leq x_i \leq 26$. Fasse $x_1 \dots x_l$ als eine natürliche Zahl mit $2l$ Ziffern auf. Sei z. B. $l = 2$: Man wählt eine Primzahl $p > 2626$ und ein e mit $(e, \varphi(p)) = 1$, dann ein f mit $ef \equiv 1 \mod \varphi(p)$.

$$\begin{aligned} \text{Chiffrierungsvorschrift:} &\quad f(x) = x^e \\ \text{Dechiffrierungsvorschrift:} &\quad f^{-1}(x) = x^f \end{aligned}$$

BEISPIEL. $p := 2633$ ist eine Primzahl, $e := 19$ ist teilerfremd zu 2632, da $19 \cdot 2269 \equiv 1 \mod 2632$ ist $f = 2269$.

Original	BR	AU	NS	CH	WE	IG
x	0218	0121	1419	0308	2305	0907
$f(x)$	2222	2527	0810	0350	0211	2106

$$\text{Chiffrierung:} \quad f(x) \equiv x^{19} \equiv x^{16+2+1} \equiv \left(\left(\left(x^2\right)^2\right)^2\right)^2 \cdot x^2 \cdot x \mod 2633$$

$$\text{Dechiffrierung:} \quad f^{-1}(x) = x^{2355} \mod 2633$$

$$\text{z. B. :} \quad f^{-1}(2222) = 2222^{2355} \equiv 0218 \mod 2633$$

Die Potenzierungen lassen sich sehr schnell mit Computern durchführen, wenn man man die Exponenten im Dualsystem darstellt.

(5) RSA-Verfahren

Das Verfahren beruht darauf, daß Primfaktorzerlegung großer Zahlen selbst mit sehr schnellen Computern außerordentlich zeitaufwendig ist. Für die Zerlegung einer Zahl mit 200 Dezimalen benötigt man zur Zeit circa $4 \cdot 10^9$ Jahre.
Es sei $m = pq$, $p, q \in \mathbb{P}$, $p, q \approx 10^{100}$
Man wählt eine Zahl e mit $(e, \varphi(m)) = 1$ und berechnet eine Zahl f, die zu e invers mod $\varphi(m) = (p-1)(q-1)$ ist. Verschlüsselt man eine Nachricht mittels $f(x) = x^e$, so liefert $f^{-1}(x) = x^f$ die Dechiffrierung. Das Besondere an diesem Verfahren ist, daß hierbei m und e allgemein bekannt sein können. Um jedoch zu dechiffrieren, braucht man f, das sich erst aus der Zerlegung von m berechnen läßt. Das RSA-Verfahren stammt von RIVEST, SHAMIR, ADLEMAN, 1978.

5. Aufgaben

AUFGABE 5.1. Es sei $p \neq 2, 5$ eine Primzahl. Zeige, daß in der Folge

$$1, 11, 111, 1111, \dots$$

ein Element durch p teilbar ist.

AUFGABE 5.2. Zeige: $561 = 3 \cdot 11 \cdot 17$ ist pseudoprim.

AUFGABE 5.3. Löse unter Verwendung der Indizes:

(1) $7x^3 \equiv 3 \mod 13$
(2) $7x^3 \equiv 4 \mod 13$.

AUFGABE 5.4. Zeige: $5^{2^{k-3}} \equiv 1 + 2^{k-1} \mod 2^k,\ k \geq 3$.

AUFGABE 5.5. (1) Zeige, daß 2 eine primitive Wurzel mod 25 ist.

(2) Ermittle die Indizes zur Basis 2 und die Ordnungen der Elemente der primen Restklassengruppe mod 25. Welche Elemente sind primitiv?

(3) Löse die Kongruenz

$$6x^4 \equiv 11 \mod 25$$

unter Benutzung der Indizes.

KAPITEL 6

Quadratische Reste

1. Das Legendre-Symbol

DEFINITION. Eine zu m teilerfremde Zahl a heißt ein quadratischer Rest mod m, wenn ein $x \in \mathbb{Z}$ existiert mit $x^2 \equiv a \bmod m$.
Andernfalls heißt a ein Nichtrest.

BEISPIELE. (1) $m = 13$

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

quadratischer Reste : $\{1, 4, 9, 3, 12, 10\}$
Nichtreste : $\{2, 5, 6, 7, 8, 11\}$

(2) $m = 15$

x	1	2	4	7	8	11	13	14
x^2	1	4	1	4	4	1	4	1

quadratischer Reste : $\{1, 4\}$
Nichtreste : $\{2, 7, 8, 11, 13, 14\}$

BEMERKUNG. Wegen $x^2 = (-x)^2$ erhält man bereits alle Quadrate für $x \leq \frac{\varphi(m)}{2}$. Im Körperfall sind diese auch alle verschieden. Damit gilt

(1) Die Anzahl der quadratischen Reste ist $\leq \frac{\varphi(m)}{2}$ für $m \in \mathbb{N}$.

(2) Die Anzahl der quadratischen Reste ist $= \frac{\varphi(p)}{2}$ für $p \in \mathbb{P}$.

SATZ 6.1 (EULER). *Sei $p > 2$ eine Primzahl, $(a, p) = 1$. a ist genau dann quadratischer Rest* mod p, *wenn gilt*

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

BEWEIS. Fasse $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ zu Paaren (x, y), $x \leq y$, zusammen, für die

$$xy \equiv a \bmod p$$

gilt.

1. Fall: a ist Nichtrest: Dann ist $x \neq y$, also gibt es $\frac{p-1}{2}$ Paare (x, y) mit $x \neq y$, also ist

$$(p-1)! \equiv a^{\frac{p-1}{2}} \bmod p.$$

2. Fall: a sei quadratischer Rest, also $a \equiv x^2 \bmod p$. Dann gilt

$$(p-1)! \equiv a^{\frac{p-3}{2}} \cdot x \cdot (-x) \equiv -a^{\frac{p-1}{2}} \bmod p.$$

Insbesondere für $a = 1$ ergibt sich $(p-1)! \equiv -1 \bmod p$, also der Satz von Wilson. Außerdem ist $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, falls a quadratischer Rest, und $\equiv -1 \bmod p$, falls a Nichtrest ist. Weil beide Fälle sich ausschließen, gilt

$$\begin{array}{lll} a \text{ quadratischer Rest} & \Longleftrightarrow & a^{\frac{p-1}{2}} \equiv 1 \bmod p \\ a \text{ Nichtrest} & \Longleftrightarrow & a^{\frac{p-1}{2}} \equiv -1 \bmod p. \end{array} \qquad \square$$

Spezialfall: $a = -1$ Wegen

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{für } p \equiv 1 \bmod 4 \\ -1 & \text{für } p \equiv 3 \bmod 4 \end{cases}$$

gilt

(a) -1 ist quadratischer Rest für $p \equiv 1 \bmod 4$

(b) -1 ist Nichtrest für $p \equiv 3 \bmod 4$.

DEFINITION. Sei p eine ungerade Primzahl, $(a, p) = 1$. Dann heißt

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest mod } p \\ -1 & \text{sonst} \end{cases}$$

Legendre-Symbol, gesprochen „a nach p“.

SATZ 6.2. (*Eulerkriterium*)

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

BEWEIS. Für $b = a^{\frac{p-1}{2}}$ gilt $b^2 = a^{p-1} \equiv 1 \bmod p$, also ist $b \bmod p$ Nullstelle von $x^2 - \overline{1} \in \mathbb{Z}_p[x]$. Also ist $x \equiv \pm 1 \bmod p$, weil $\mathbb{Z}_p$ ein Körper ist. Nach Satz 6.1 gilt:

$$a \text{ quadratischer Rest} \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p,$$

woraus die Behauptung folgt. $\square$

BEISPIEL. $p = 13$

a	1	2	3	4	5	6	-6	-5	-4	-3	-2	-1
$\left(\frac{a}{p}\right) \equiv a^6$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1
quadratischer Rest	✓		✓	✓					✓	✓		✓

KOROLLAR 6.1. *Sei* $(a, p) = (b, p) = 1$, $p \neq 2$. *Dann gilt*

(1) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *falls* $a \equiv b \bmod p$

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

(3) $\sum\limits_{1 \le a < p} \left(\frac{a}{p}\right) = 0$

(4)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \textit{falls } p \equiv 1 \bmod 4 \\ -1 & \textit{falls } p \equiv 3 \bmod 4. \end{cases}$$

Beweis.

(1) Folgt direkt aus der Definition des Legendre-Symbols.

(2) Nach Satz 6.2 ist

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p\,.$$

Da nur die Werte ± 1 angenommen werden, folgt die Gleichheit.

(3) Für eine Primzahl p gilt: Die Anzahl der quadratischen Reste ist gleich der Anzahl der quadratischen Nichtreste.

(4) Satz 6.2. □

Bemerkung. Ist $a = \pm q_1^{\alpha_1} \dots q_r^{\alpha_r}$ mit $\alpha_1, \dots, \alpha_s$ ungerade, $s \le r$, so folgt nach (2)

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{q_1}{p}\right) \dots \left(\frac{q_s}{p}\right).$$

Um das Legendre-Symbol zu berechnen zu können, braucht man daher nur die Legendre-Symbole $\left(\frac{-1}{p}\right)$ und $\left(\frac{q}{p}\right)$, $p,\ q \in \mathbb{P}$ zu kennen.

2. Das Reziprozitätsgesetz

Neben dem gewöhnlichen Restsystem: $\{0, 1, \dots, p-1\}$ benutzen wir im folgenden das absolut kleinste Restsystem (akR):

$$\{\underbrace{-\frac{p-1}{2}, \dots, -1}_{\text{negative Reste}},\ 0,\ \underbrace{1, \dots, \frac{p-1}{2}}_{\text{positive Reste}}\ \}$$

Satz 6.3. (*Gaußsches Lemma*) *Sei* $p \neq 2$, $(a, p) = 1$. *Ist* μ *die Anzahl der negativen Reste in*

$$A = \left\{a, 2 \cdot a, \dots, \frac{p-1}{2} \cdot a\right\},$$

so ist

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

BEISPIEL. $p = 11$. Ist a quadratischer Rest mod p?

$$\begin{aligned} a = 3: \quad & A = \{3, 2\cdot 3, 3\cdot 3, 4\cdot 3, 5\cdot 3\} \overset{\text{akR}}{=} \{3, -5, -2, 1, 4\} \\ & \left(\tfrac{3}{11}\right) = (-1)^2 = 1 \quad \Longrightarrow \quad 3 \text{ quadratischer Rest} \\ a = 2: \quad & A = \{2, 2\cdot 2, 3\cdot 2, 4\cdot 2, 5\cdot 2\} \overset{\text{akR}}{=} \{2, 4, -5, -3, -1\} \\ & \left(\tfrac{2}{11}\right) = (-1)^3 = -1 \quad \Longrightarrow \quad 2 \text{ quadratischer Nichtrest} \end{aligned}$$

BEWEIS. Seien $u_1, \ldots, u_\mu$ die negativen und $v_1, \ldots, v_\nu$ die positiven Reste von A. Dann sind $-u_1, \ldots, -u_\mu, v_1, \ldots, v_\nu$ paarweise nicht kongruent mod p: sei etwa $-u_i \equiv v_j \bmod p$ mit $u_i = na$, $v_j = ma$, $0 < n, m \leq \frac{p-1}{2}$, $n \neq m$ angenommen. Wegen $(a, p) = 1$ folgt aus $-na \equiv ma \bmod p$ nach Division durch a $-n \equiv m \bmod p$, also $n + m \equiv 0 \bmod p$. Dies steht aber im Widerspruch zu $0 < n, m \leq \frac{p-1}{2}$. Also ist

$$\{-u_1, \ldots, -u_\mu, v_1, \ldots, v_\nu\} = \left\{1, \ldots, \frac{p-1}{2}\right\}.$$

Daraus folgt

$$\frac{p-1}{2}! = (-1)^\mu u_1 \ldots u_\mu \cdot v_1 \ldots v_\nu\,,$$

also

$$\frac{p-1}{2}! \equiv (-1)^\mu 1 \cdot a \ldots \frac{p-1}{2} \cdot a \equiv (-1)^\mu a^{\frac{p-1}{2}} \frac{p-1}{2}! \bmod p\,.$$

Nach dem Eulerkriterium gilt daher

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

also $\left(\frac{a}{p}\right) = (-1)^\mu$ wegen $\left(\frac{a}{p}\right) = \pm 1$. □

Berechnung von μ:
Es sei $k \cdot a = q_k p + r_k$, $\quad 0 < r_k \leq p$ für $0 < k < \frac{p-1}{2}$, also

$$\begin{aligned} 1 \cdot a &= q_1 p & +r_1 \\ 2 \cdot a &= q_2 p & +r_2 \\ &\ldots \\ \tfrac{p-1}{2} \cdot a &= q_{\frac{p-1}{2}} \cdot p & +r_{\frac{p-1}{2}} \end{aligned}$$

Dann ist

$$r_k = \begin{cases} v_j & \text{falls } 1 \leq r_k \leq \frac{p-1}{2} \\ p + u_i & \text{falls } \frac{p-1}{2} < r_k < p. \end{cases}$$

Wegen

$$1 + 2 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8} = -\sum_{i=1}^{\mu} u_i + \sum_{j=1}^{\nu} v_j$$

ergibt sich durch Summation

$$\begin{aligned}\frac{p^2-1}{8}\cdot a &= p\cdot\sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{i=1}^{\mu}(p+u_i) + \sum_{j=1}^{\nu} v_j \\ &= p\cdot\sum_{k=1}^{\frac{p-1}{2}} q_k + \mu p + 2\cdot\sum_{i=1}^{\mu} u_i \underbrace{- \sum_{i=1}^{\mu} u_i + \sum_{j=1}^{\nu} v_j}_{=\frac{p^2-1}{8}}.\end{aligned}$$

Damit ist

$$\frac{p^2-1}{8}(a-1) = p\cdot\sum_{k=1}^{\frac{p-1}{2}} q_k + \mu p - 2\sum_{i=1}^{\mu} u_i.$$

Wegen $p \equiv 1 \bmod 2$ folgt

$$(*) \qquad \mu \equiv \frac{p^2-1}{8}(a-1) + \sum_{k=1}^{\frac{p-1}{2}} q_k \bmod 2\,.$$

SATZ 6.4. *Es gilt*

$$(1) \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$$(2) \qquad \left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} q_k}, \quad a \text{ ungerade.}$$

BEWEIS. (1) Für $k \le \frac{p-1}{2}$ und $a = 2$ ist $k\cdot 2 \le \frac{p-1}{2}\cdot 2 = p-1$. Also ist $q_1 = \cdots = q_{\frac{p-1}{2}} = 0$. Nach $(*)$ ist $\mu \equiv \frac{p^2-1}{8} \bmod 2$, also $\left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{\frac{p^2-1}{8}}$.

(2) Für ungerades a ist $a \equiv 1 \bmod 2$, also nach $(*)$

$$\left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} q_k}. \quad \square$$

BEISPIEL. $p = 17$, $a = 7$. Ist 7 quadratischer Rest mod 17?
Wegen $\frac{p-1}{2} = 8$ sind die Reste > 8 negativ.

$$\begin{array}{lll} 1\cdot 7 = & 0\cdot p & +7 \\ 2\cdot 7 = & 0\cdot p & +14 \quad \text{neg. Rest} \\ 3\cdot 7 = & 1\cdot p & +4 \\ 4\cdot 7 = & 1\cdot p & +11 \quad \text{neg. Rest} \\ 5\cdot 7 = & 2\cdot p & +1 \\ 6\cdot 7 = & 2\cdot p & +8 \\ 7\cdot 7 = & 2\cdot p & +15 \quad \text{neg. Rest} \\ 8\cdot 7 = & 3\cdot p & +5 \end{array}$$

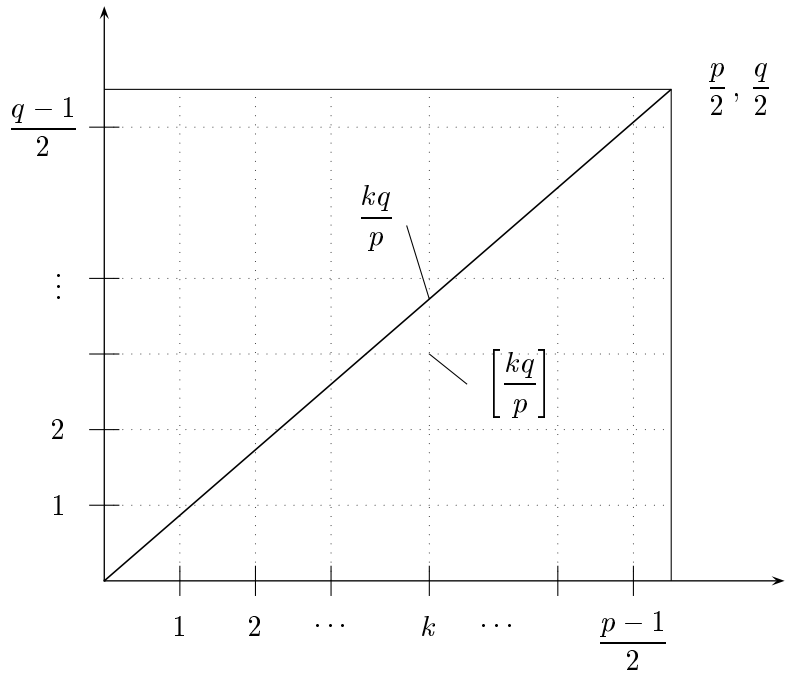

ABBILDUNG 6.1. Geometrische Interpretation von $\sum q_k$

Damit ist $\mu = 3$. Man erhält nach dem

$$\begin{aligned} &\text{Gaußschen Lemma} \quad : \quad \left(\tfrac{7}{17}\right) = (-1)^3 = -1 \\ &\text{Satz 6.4 (2)} \qquad\quad : \quad \left(\tfrac{7}{17}\right) = (-1)^{1+1+2+2+2+3} = (-1)^{11} = -1 \end{aligned}$$

Geometrische Interpretation von $\sum_{k=1}^{\frac{p-1}{2}} q_k$:

Sei $a = q$ ebenfalls eine Primzahl $\neq 2$, $p \neq q$.
Teilt man in der k-ten Zeile $k \cdot q = q_k p + r_k$ durch p, so erhält man

$$\frac{k \cdot q}{p} = q_k + \frac{r_k}{p}, \qquad 0 < \frac{r_k}{p} < 1,$$

also ist

$$q_k = \left[\frac{k \cdot q}{p}\right],$$

wobei $[x]$ die größte ganze Zahl $\leq x$ ist.

Wir betrachten das Rechteck mit den Seiten $\frac{p}{2}$, $\frac{q}{2}$. Die Gleichung der Diagonalen lautet $y = \frac{q}{p} \cdot x$ (s. Abb. 6.1)
Das Gitter $\Gamma = \{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2},\ 1 \leq y \leq \frac{q-1}{2}\}$ enthält

$$|\Gamma| = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Gitterpunkte. Es gilt

(A) Auf der Diagonalen liegt kein Gitterpunkt.
Denn: Es ist $py \neq qx$ für $x, y \in \mathbb{Z}$, weil x und q teilerfremd zu p sind, also p kein Teiler von xq ist.

(B) Unterhalb der Diagonalen liegen $\left[\frac{k\cdot q}{p}\right]$ Gitterpunkte an der Stelle k. Also ist $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{k\cdot q}{p}\right]$ die Anzahl der Gitterpunkte unterhalb der Diagonalen.

(C) Analog ist $\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{k\cdot p}{q}\right]$ die Anzahl der Gitterpunkte oberhalb der Diagonalen.

SATZ 6.5. (*Reziprozitätsgesetz*) *Seien p und q Primzahlen $\neq 2$. Dann gilt*

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

(2) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ (*Ergänzungssätze*)

BEWEIS. (1)

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]} = (-1)^{|\Gamma|} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

(2) Gezeigt in Korollar 6.1 (4) und Satz 6.4 □

BEMERKUNGEN. (1) Der erste Beweis des Reziprozitätsgesetzes stammt von GAUSS (1796), abgedruckt in den Disquisitiones. GAUSS hat danach noch verschiedene weitere Beweise gegeben. Der obige Beweis ist der dritte Beweis (1808), der wesentlich auf dem Gaußschen Lemma beruht.

(2) Wegen $\left(\frac{p}{q}\right) = \pm 1$ läßt sich das Reziprozitätsgesetz in der Form

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{falls } p \equiv 1 \bmod 4 \vee q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & \text{falls } p \equiv 3 \bmod 4 \wedge q \equiv 3 \bmod 4 \end{cases}$$

schreiben. Entsprechend die Ergänzungssätze:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4, \end{cases}$$

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

BEISPIELE. (1) Ist $x^2 \equiv -1457 \bmod 2389$ lösbar?
$p = 2389$ ist Primzahl, $-1457 = (-1)\cdot 31 \cdot 47$. also

$$\left(\frac{-1457}{2389}\right) = \left(\frac{-1}{2389}\right)\left(\frac{31}{2389}\right)\left(\frac{47}{2389}\right)$$

(a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{2388}{2}} = 1$

(b) $\left(\frac{31}{p}\right) = (-1)^{\frac{31-1}{2}\cdot\frac{p-1}{2}} \left(\frac{p}{31}\right) = \left(\frac{p}{31}\right) = \left(\frac{2}{31}\right) = (-1)^{\frac{31^2-1}{8}} = (-1)^{120} = 1$

(c) $\left(\frac{47}{p}\right) = \left(\frac{p}{47}\right) = \left(\frac{39}{47}\right) = \left(\frac{3}{47}\right)\left(\frac{13}{47}\right) = -\left(\frac{47}{3}\right)\left(\frac{47}{13}\right) = \cdots = -1$

$$\Longrightarrow \quad \left(\frac{-1457}{2389}\right) = -1, \text{ also nicht lösbar.}$$

(2) Für welche Primzahlen $p > 3$ ist 3 ein quadratischer Rest?

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

(a) $\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 3 \\ -1 & \text{falls } p \equiv -1 \bmod 3 \end{cases}$

(b) $(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}$

also

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{falls } \begin{cases} p \equiv 1 \bmod 3 \ \wedge \ p \equiv 1 \bmod 4 & \text{oder} \\ p \equiv -1 \bmod 3 \ \wedge \ p \equiv -1 \bmod 4 \end{cases} \\ -1 & \text{falls } \begin{cases} p \equiv 1 \bmod 3 \ \wedge \ p \equiv -1 \bmod 4 & \text{oder} \\ p \equiv -1 \bmod 3 \ \wedge \ p \equiv 1 \bmod 4 \end{cases} \end{cases}$$

$$\overset{\text{Chin. Restsatz}}{\Longrightarrow} \quad \left(\frac{3}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \bmod 12 \\ -1 & \text{falls } p \equiv \pm 5 \bmod 12 \end{cases}$$

Anwendung auf Mersennesche Primzahlen:

Die Mersenneschen Zahlen $M_n = 2^n - 1$ sind nur dann Primzahlen, wenn n selbst eine Primzahl ist (siehe 2.4).

SATZ 6.6. *Sind p und $q = 2p + 1$ Primzahlen und ist $p \equiv 3 \bmod 4$, so gilt $q \mid M_p$, also ist M_p keine Primzahl.*

BEWEIS. Wegen $p \equiv 3 \bmod 4$ ist $q = 2p + 1 = 2(3 + 4k) + 1 = 7 + 8k$, also $q \equiv 7 \bmod 8$. Nach dem Ergänzungssatz ist dann $\left(\frac{2}{q}\right) = 1$. Das Eulerkriterium ergibt $2^p = 2^{\frac{q-1}{2}} \equiv 1 \bmod q$, also $q \mid M_p$. □

BEISPIELE. (1) $p = 11 \equiv 3 \bmod 4 \ \wedge \ q = 2p + 1 = 23 \in \mathbb{P} \quad \Longrightarrow \quad 23 \mid M_{11}$.
(2) $p = 23 \equiv 3 \bmod 4 \ \wedge \ q = 2p + 1 = 47 \in \mathbb{P} \quad \Longrightarrow \quad 47 \mid M_{23}$.

3. Das Jacobi-Symbol

Bei der Berechnung des Legendre-Symbols ist die Primfaktorzerlegung des Zählers notwendig, die bei großen Zahlen auf erhebliche Rechenschwierigkeiten stößt. Eine gewisse Vereinfachung liefert das Jacobi-Symbol:

DEFINITION. Sei $P \in \mathbb{N}$ ungerade und $P = p_1 \dots p_r$ die Primfaktorzerlegung von P. Dann heißt

$$\left(\frac{a}{P}\right) := \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right) \in \{-1, +1\}$$

das Jacobi-Symbol von a nach P.

BEMERKUNG. Das Jacobi-Symbol ist ein formaler Ausdruck. Aus $\left(\frac{a}{P}\right) = -1$ folgt zwar $\left(\frac{a}{p}\right) = -1$ für einen Primteiler p von P und damit, daß a kein Quadrat mod P. Aus $\left(\frac{a}{P}\right) = 1$ folgt jedoch nicht, daß a ein Quadrat mod P ist.

Direkt aus der Definition des Jacobi-Symbols ergeben sich folgende Regeln

(A) $a \equiv b \bmod P \quad \Longrightarrow \quad \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$

(B) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$

(C) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$

SATZ 6.7. *Es seien P und Q ungerade natürliche Zahlen mit $(P, Q) = 1$. Dann gilt*

$$(1) \quad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

$$(2) \quad \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{p^2-1}{8}}.$$

BEWEIS. (nur von (2), 1. Teil)
Es sei $P = p_1 \cdot \ldots \cdot p_r = (1 + (p_1 - 1)) \cdot \ldots \cdot (1 + (p_r - 1))$ die Primfaktorzerlegung von P. Wegen $4 \mid \underbrace{(p_i - 1)}_{\text{gerade}}\underbrace{(p_j - 1)}_{\text{gerade}}$ ist

$$P \equiv 1 + (p_1 - 1) + \cdots + (p_r - 1) \bmod 4,$$

also

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right) \ldots \left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}} = (-1)^{\frac{P-1}{2}}. \quad \square$$

BEISPIEL.

$$\left(\frac{1457}{2389}\right) = \left(\frac{2389}{1457}\right) = \left(\frac{932}{1457}\right) = \left(\frac{4}{1457}\right)\left(\frac{233}{1457}\right) = \left(\frac{1457}{233}\right) =$$

$$\left(\frac{59}{233}\right) = \left(\frac{233}{59}\right) = \left(\frac{56}{59}\right) = \underbrace{\left(\frac{8}{59}\right)}_{=-1}\underbrace{\left(\frac{7}{59}\right)}_{=-\left(\frac{59}{7}\right)} =$$

$$\left(\frac{59}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Abzuspalten sind nur Potenzen von 2. Formal hat man folgende Rechnung durchzuführen und dabei die durch die Umkehrung der Symbole und Abspaltung der 2-Potenzen entstehenden Minuszeichen zu registrieren.

2389 =	1·	1457+	932	
1457 =	6·	233+	59	
233 =	3·	59+	56	neg., neg.
59 =	8·	7+	3	neg.
7 =	2·	3+	1	

4. Polynomkongruenzen

DEFINITION. Sei $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. Dann heißt

$$f(x) \equiv 0 \bmod m \tag{1}$$

eine Polynomkongruenz. $a \in \mathbb{Z}$ heißt Lösung von (1), wenn

$$f(a) \equiv 0 \bmod m$$

gilt. Ist a eine Lösung, und gilt $a \equiv a' \bmod m$, so ist auch a' eine Lösung.
Die Anzahl der Lösungen von (1) ist die Anzahl der mod m inkongruenten Lösungen oder der Lösungen a mit $0 \leq a < m$.
(1) heißt lösbar, wenn mindestens eine Lösung existiert.

Aus dem chinesischen Restsatz ergibt sich

SATZ 6.8. *Es sei $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Die Kongruenz (1) ist genau dann lösbar, wenn jede der Kongruenzen*

$$f(x) \equiv 0 \bmod p_i^{\alpha_i}, \quad i = 1, \ldots, r \tag{2}$$

lösbar ist. Sind N_i die jeweiligen Anzahlen der Lösungen von (2), so gibt es $N = N_1 \ldots N_r$ Lösungen von (1).

BEISPIEL.

$$f(x) = x^2 - 1 \equiv 0 \bmod 12 \tag{1}$$

$$\begin{array}{ll} x^2 - 1 \equiv 0 \bmod 4 & \text{Lösungsmenge: } \{1, 3\} \\ x^2 - 1 \equiv 0 \bmod 3 & \text{Lösungsmenge: } \{1, 2\} \end{array} \tag{2}$$

Nach dem Chinesischen Restsatz ergibt sich:

$$\text{(a)} \quad \left.\begin{array}{l} x \equiv 1 \bmod 4 \\ x \equiv 1 \bmod 3 \end{array}\right\} \quad x \equiv 1 \bmod 12$$

$$\text{(b)} \quad \left.\begin{array}{l} x \equiv 1 \bmod 4 \\ x \equiv 2 \bmod 3 \end{array}\right\} \quad x \equiv 5 \bmod 12$$

$$\text{(c)} \quad \left.\begin{array}{l} x \equiv 3 \bmod 4 \\ x \equiv 1 \bmod 3 \end{array}\right\} \quad x \equiv 7 \bmod 12$$

$$\text{(d)} \quad \left.\begin{array}{l} x \equiv 3 \bmod 4 \\ x \equiv 2 \bmod 3 \end{array}\right\} \quad x \equiv 11 \bmod 12$$

Also hat (1) genau vier Lösungen: 1, 5, 7, 11 mod 12.

DEFINITION. Ist $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, so heißt

$$f'(x) := n a_n x^{n-1} + \ldots + a_1$$

die Ableitung von $f(x)$.

HILFSSATZ 6.1. (*Taylorformel*) *Es gilt*

$$f(x + h) = f(x) + f'(x) \cdot h + g(x, h) \cdot h^2$$

mit $g(x, h) \in \mathbb{Z}[x, h]$.

BEWEIS. Nach der binomischen Formel ist

$$(x+h)^k = x^k + kx^{k-1}h + g_k(x,h)\cdot h^2,$$

also

$$f(x+h) = \sum_{k=0}^{n} a_k(x+h)^k = \underbrace{\sum_{k=0}^{n} a_k x^k}_{=f(x)} + \underbrace{\sum_{k=1}^{n} k a_k x^{k-1} h}_{=f'(x)\cdot h} + \underbrace{\sum_{k=0}^{n} a_k g_k(x,h) h^2}_{=g(x,h)h^2} . \quad \square$$

SATZ 6.9. *Besitzen*

$$f(x) \equiv 0 \bmod p \quad \textit{und}$$
$$f'(x) \equiv 0 \bmod p$$

keine gemeinsamen Lösungen, so haben

$$f(x) \equiv 0 \bmod p \quad \textit{und}$$
$$f(x) \equiv 0 \bmod p^\alpha$$

die gleichen Lösungsanzahlen.

BEWEIS. Induktion nach α: $\alpha = 1$ ist trivial.
Sei der Satz also für α bereits bewiesen.
$\alpha \to \alpha + 1$: Seien

$$A := \{a \in \mathbb{Z} \mid f(a) \equiv 0 \bmod p^\alpha,\ 0 \le a < p^\alpha\}$$
$$B := \{b \in \mathbb{Z} \mid f(b) \equiv 0 \bmod p^{\alpha+1},\ 0 \le b < p^{\alpha+1}\} \ .$$

Sei $b \in B$ und $a \equiv b \bmod p^\alpha$, $0 \le a < p^\alpha$. Dann ist $f(a) \equiv f(b) \equiv 0 \bmod p^\alpha$, also ist $a \in A$. Diese Abbildung $B \to A$, $b \mapsto a$, ist bijektiv, denn:
Sei $a \in A$, also $f(a) = up^\alpha$. Setze $b = a + yp^\alpha$ mit $0 \le y < p$.
Nach dem Hilfssatz ist $f(b) = f(a + yp^\alpha) = f(a) + f'(a)yp^\alpha + g(a, yp^\alpha)y^2p^{2\alpha} \equiv (u + f'(a)y)p^\alpha \bmod p^{\alpha+1}$, also

$$f(b) \equiv 0 \bmod p^{\alpha+1} \Leftrightarrow u + f'(a)y \equiv 0 \bmod p.$$

Wegen $f(a) \equiv 0 \bmod p$ ist nach Voraussetzung $f'(a) \not\equiv 0 \bmod p$.

Also gibt es ein eindeutig bestimmtes y mit $u + yf'(a) \equiv 0 \bmod p$, also auch ein eindeutig bestimmtes b, womit die Bijektivität gezeigt ist.

Aus der Bijektivität folgt jetzt $|A| = |B|$. $\square$

SATZ 6.10. *Sei $p > 2$, $(a,p) = 1$. Die Kongruenz*

$$x^2 \equiv a \bmod p^\alpha$$

ist genau dann lösbar, wenn $x^2 \equiv a \bmod p$ lösbar ist. Im Fall der Lösbarkeit gibt es zwei Lösungen.

BEWEIS. $f(x) = x^2 - a \equiv 0 \bmod p$ und $f'(x) = 2x \equiv 0 \bmod p$ haben wegen $(a,p) = 1$ keine gemeinsamen Nullstellen. Satz 6.9 liefert nun sofort die Behauptung. $\square$

SATZ 6.11. *Es sei $m = 2^k$, $k \ge 3$, c ungerade. Dann ist c genau dann ein quadratischer Rest* mod m, *wenn $c \equiv 1 \bmod 8$ ist.*

BEWEIS. „ $\Rightarrow$ “: c quadratischer Rest, also $x^2 \equiv c \bmod 2^k$. Weil c ungerade ist, ist auch x ungerade, also $x = 2y+1 \quad \Longrightarrow \quad x^2 = (2y+1)^2 = 4y^2+4y+1 = 4(y+1)y+1 \quad \Longrightarrow \quad c \equiv 1 \bmod 8$

„ $\Leftarrow$ “: Induktion nach k: $k=3$: $1^2 \equiv c \bmod 8$.

Für k existiere x_0 mit $x_0^2 \equiv c \bmod 2^k$, also $x_0^2 = c + a2^k$. Für $x_1 = x_0 + b2^{k-1}$ mit $a + x_0 b \equiv 0 \bmod 2$ folgt

$$x_1^2 = x_0^2 + x_0 b 2^k + b^2 2^{2k-2} = c + (a + x_0 b)2^k + b^2 2^{2k-2} \equiv c \bmod 2^{k+1},$$

d. h. es existiert eine Lösung für $k+1$. □

SATZ 6.12. *Sei* $(a,2) = 1$. *Die Kongruenz*

$$(*) \qquad x^2 \equiv a \bmod 2^\alpha$$

besitzt im Fall

(i)	$\alpha = 1$	*eine Lösung*
(ii)	$\alpha = 2$	*zwei Lösungen, falls* $a \equiv 1 \bmod 4$
		keine Lösung, falls $a \equiv 3 \bmod 4$
(iii)	$\alpha \geq 3$	*vier Lösungen, falls* $a \equiv 1 \bmod 8$
		keine Lösung, falls $a \not\equiv 1 \bmod 8$.

BEWEIS. $\alpha = 1, 2$ ist trivial. Betrachte also $\alpha \geq 3$. Eine Lösung von $(*)$ kann nur ungerade sein. Wegen

$$(2k+1)^2 = 4k(k+1) + 1 \equiv 1 \bmod 8$$

existieren Lösungen nur für $a \equiv 1 \bmod 8$. Für $\alpha = 3$ sind dann $1, 3, 5, 7$ alle Lösungen von $x^2 \equiv 1 \bmod 8$.
Durch Induktion folgt, daß $(*)$ für $\alpha \geq 3$ gleich viele Lösungen wie $x^2 \equiv a \bmod 2^3$ hat. Der Beweis dafür verläuft analog zum Beweis von Satz 6.9. □

BEISPIEL. Löse $x^2 \equiv 65 \bmod 392$, $392 = 2^3 \cdot 7^2$
(i) $x^2 \equiv 65 \bmod 2^3$:
$65 \equiv 1 \bmod 8 \Longrightarrow$ es existieren 4 Lösungen.
(ii) $x^2 \equiv 65 \bmod 7^2$:
Betrachte $x^2 \equiv 2 \bmod 7$:
$\left(\frac{2}{7}\right) = (-1)^{\frac{49-1}{2}} = 1 \Longrightarrow$ es existieren 2 Lösungen.
Insgesamt gibt es also $4 \cdot 2 = 8$ Lösungen: $\{45, 53, 143, 151, 241, 249, 339, 347\}$

Berechnung der Lösung durch „sukzessive Approximation“ :
(Analog zum Newton-Verfahren der Analysis)

Definiere wie im Beweis von Satz 6.9:

$$A := \{a \in \mathbb{Z} \mid f(a) \equiv 0 \bmod p^\alpha,\ 0 \leq a < p^\alpha\}$$
$$B := \{b \in \mathbb{Z} \mid f(b) \equiv 0 \bmod p^{\alpha+1},\ 0 \leq b < p^{\alpha+1}\}.$$

Sei A bekannt. Für jedes $a \in A$ setze $b := a + yp^\alpha$ mit $0 \leq y < p$. Dann ist $f(a) = up^\alpha$.
Berechnung von y:
$f(a + yp^\alpha) \equiv (u + f'(a)y)p^\alpha \bmod p^{\alpha+1}$

$$(*) \qquad f(b) \equiv 0 \bmod p^{\alpha+1} \iff u + f'(a)y \equiv 0 \bmod p$$

Es sind also drei Fälle zu unterscheiden:

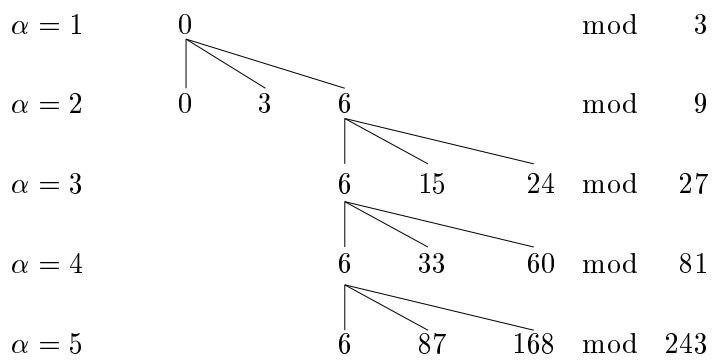

ABBILDUNG 6.2. Splitting-Tafel

(1) $f'(a) \not\equiv 0 \bmod p$: Es gibt genau eine Lösung.
(2) $f'(a) \equiv 0 \bmod p \wedge u \equiv 0 \bmod p$: Es gibt genau p Lösungen.
(3) $f'(a) \equiv 0 \bmod p \wedge u \not\equiv 0 \bmod p$: Es gibt keine Lösung.

BEISPIEL. (vgl. Abb. 6.2)

$$f(x) = x^3 + 3x + 9 \equiv 0 \bmod 3^\alpha, \quad f'(x) = 3(x^2 + 1)$$

(1) $\alpha = 1$: $f(x) \equiv x^3 \equiv 0 \bmod 3$
Lösung: $x = 0$
(2) $\alpha = 2$: Ansatz: $b = 0 + y \cdot 3,\ 0 \le y < 3$
$f(0) = 9 = 3 \cdot 3,\ f'(0) = 3$
$(*) \quad 3 + 3y \equiv 0 \bmod 3$
$\Longrightarrow y = 0, 1, 2$
Lösung: $x = 0, 3, 6$
(3) $\alpha = 3$: Ansatz: $b = a + y \cdot 9$
(a) $a = 0 \Longrightarrow f(0) = 1 \cdot 9 \wedge f'(0) = 3$
$(*) \quad 1 + 3y \equiv 0 \bmod 3$ nicht lösbar
(b) $a = 3 \Longrightarrow f(3) = 5 \cdot 9 \wedge f'(3) = 3 \cdot 10$
$(*) \quad 5 + 3 \cdot 10y \equiv 0 \bmod 3$ nicht lösbar
(c) $a = 6 \Longrightarrow f(6) = 27 \cdot 9 \wedge f'(6) = 3 \cdot 37$
$(*) \quad 27 + 3 \cdot 37y \equiv 0 \bmod 3 \Longrightarrow y = 0, 1, 2$
Lösung: $x = 6, 15, 24$
(4) $\alpha = 4$: Lösung: $x = 6, 33, 60$
(5) $\alpha = 5$: Lösung: $x = 6, 87, 168$

5. Aufgaben

AUFGABE 6.1. Berechne das Legendre-Symbol $\left(\frac{7}{11}\right)$
(a) durch Aufstellen einer Liste aller Quadrate in $\mathbb{Z}_{11}$
(b) mit Hilfe des Eulerkriteriums
(c) mit Hilfe des Gaußschen Lemmas.

AUFGABE 6.2. Für welche Primzahlen ist 10 ein quadratischer Rest?

AUFGABE 6.3. Zeige, daß M_{83} keine Primzahl ist.

AUFGABE 6.4. Zeige

(1) Aus $q \mid M_p$, $p > 2$ folgt $q \equiv 1 \bmod 2p$ und $q \equiv \pm 1 \bmod 8$.
(2) M_{19} ist prim.

AUFGABE 6.5. Beweise $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$, P ungerade.

AUFGABE 6.6. Berechne für $\alpha = 1, 2, 3$ die Lösungen von

$$f(x) = x^3 + 3x + 9 \equiv 0 \bmod 5^\alpha.$$

AUFGABE 6.7. Welche der folgenden Kongruenzen sind lösbar?

(1) $x^2 \equiv 409 \bmod 9000$
(2) $x^2 \equiv 401 \bmod 9000$

Wieviele Lösungen existieren im Fall der Lösbarkeit?

AUFGABE 6.8. Es sei $a \equiv 1 \bmod 4$ sowie p und q zwei verschiedene Primzahlen, deren Summe durch a teilbar ist. Zeige

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

KAPITEL 7

Summe von Quadraten

1. Pythagoreische Tripel

DEFINITION. $(x, y, z) \in \mathbb{N}^3$ heißt ein *pythagoreisches Tripel*, wenn

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

ist.

Es gilt

(A) $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$.

(B) $x^2 + y^2 = z^2 \qquad \Longrightarrow \qquad (xd)^2 + (yd)^2 = (zd)^2$.

Mit Hilfe von (A) lassen sich leicht Beispiele pythagoreischer Tripel konstruieren, z.B. ergibt $m = 2, n = 1$ das Tripel $(3, 4, 5)$.

DEFINITION. Ein pythagoreisches Tripel (x, y, z) heißt *primitiv*, wenn der größte gemeinsame Teiler von x, y, z gleich 1 ist.

Dann sind x, y, z auch paarweise teilerfremd: Wäre z.B. $(x, z) \neq 1$, etwa p ein Primteiler von x, z, so wäre p wegen $y^2 = z^2 - x^2$ auch ein Teiler von y, also ein Teiler aller drei Zahlen im Widerspruch zur Primitivität des Tripels.

HILFSSATZ 7.1. *Ist (x, y, z) ein primitives pythagoreisches Tripel, so gilt*

$$x \not\equiv y \bmod 2, \qquad z \equiv 1 \bmod 2.$$

BEWEIS. Wegen $(x, y) = 1$ sind x, y nicht beide gerade. Wären beide ungerade, so wäre

$$z^2 = x^2 + y^2 \equiv 2 \bmod 4.$$

2 ist jedoch kein Quadrat in $\mathbb{Z}_4$. Folglich ist $x \not\equiv y \bmod 2$, also auch $z \equiv 1 \bmod 2$. □

Wir wählen im folgenden die Bezeichnungen der Zahlen stets so, daß $x \equiv 1 \bmod 2$ und $y \equiv 0 \bmod 2$ ist.

HILFSSATZ 7.2. *Sind $r, s \in \mathbb{N}$ teilerfremd und ist $r \cdot s$ ein Quadrat, so sind auch r und s Quadrate.*

BEWEIS. Es seien

$$r = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \qquad \text{und} \qquad s = q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}$$

die Primfaktorzerlegungen. Wegen $(r, s) = 1$ ist $p_i \neq q_j$. Ist

$$r \cdot s = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}$$

ein Quadrat, so sind wegen der Eindeutigkeit der Primfaktorzerlegung alle Exponenten gerade, also r und s Quadrate. □

SATZ 7.1. *Die Zahlen x, y, z mit $x \equiv 1 \bmod 2$ bilden genau dann ein primitives pythagoreisches Tripel, wenn $m, n \in \mathbb{N}$ mit $(m, n) = 1, m \not\equiv n \bmod 2, m > n$ existieren, so daß*

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2$$

ist.

BEWEIS. (1) Besitzen x, y, z diese Darstellung, so gilt nach (A) $x^2 + y^2 = z^2$. Wäre p Primteiler von x, z, so wäre p auch Teiler von $2m^2 = z + x$ und $2n^2 = z - x$. Wegen $x = m^2 - n^2 \not\equiv 0 \bmod 2$ ist $p \neq 2$, also p auch Teiler von m, n im Widerspruch zu $(m, n) = 1$.

(2) Es sei (x, y, z) ein primitives pythagoreisches Tripel mit $x \equiv 1 \bmod 2$. Dann sind $z + x$ und $z - x$ gerade, also

$$(\frac{y}{2})^2 = \frac{z + x}{2} \cdot \frac{z - x}{2} = r \cdot s.$$

Nach dem obigen Hilfssatz sind r und s Quadrate, etwa

$$r = m^2, \qquad s = n^2.$$

Dann ist $y = 2mn$. Aus

$$z + x = 2r = 2m^2 \qquad z - x = 2s = 2n^2$$

folgt $z = m^2 + n^2$ und $x = m^2 - n^2$. Wäre $(m, n) \neq 1$, etwa p ein Teiler von m und n, so wäre p auch ein Teiler von x und z. Schließlich folgt $m \not\equiv n \bmod 2$ aus $x = m^2 - n^2 \equiv 1 \bmod 2$. □

BEMERKUNG. Die im Satz angegebene Zuordnung der Paare (m, n) mit $(m, n) = 1,\ m > n,\ m \not\equiv n \bmod 2$

$$(m, n) \qquad \mapsto \qquad (x, y, z)$$

ist injektiv.

Beweis: Wegen

$$z + y = (m + n)^2 \qquad z - y = (m - n)^2$$

sind $m + n$ und $m - n$ und damit m, n eindeutig durch z, y bestimmt.

Für $m \leq 6$ ergibt sich folgende Tabelle

m	n	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

Historische Bemerkungen

(A) Plimpton 322 Es handelt sich hierbei um eine altbabylonische Keilschrifttafel mit 15 pythagoreischen Tripeln aus der Plimpton Collection der Columbia University, New York. Sie stammt aus der Zeit um 1900-1600 v. Chr. und ist das älteste bisher bekannte zahlentheoretische Dokument. Siehe

O. NEUGEBAUER *The exact sciences in antiquity*, Dover 1957

Die folgende Tabelle gibt den Inhalt der Tafel im originalen Sexagesimalsystem wieder:

	Breite b	Diagonale d	Nr.
[59,0],15	1,59	2,49	1
[56,56,58],14,50,6,15	56,7	3,12,1*	2
[55,7,41],15,33,45	1,16,41	1,50,49	3
[53,10],29,32,52,16	3,31,49	5,9,1	4
48,54,1,40	1,5	1,37	[5]
47,6,41,40	5,19	8,1	[6]
43,11,56,28,26,40	38,11	59,1	7
41,33,59,3,45	13,19	20,49	8
38,33,36,36	9,1*	12,49	9
35,10,2,28,27,24,26,40	1,22,41	2,16,1	10
33,45	45	1,15	11
29,21,54,2,15	27,59	48,49	12
27,0,3,45	7,12,1*	4,49	13
25,48,51,35,6,40	29,31	53,49	[14]
23,13,46,[40]	28	53	[15]

Die Zahlen in eckigen Klammern sind ergänzt. An den drei markierten Stellen treten Schreibfehler auf. Sieht man hiervon ab, so gilt für die Zahlen b, d der zweiten und dritten Spalte, daß $d^2 - b^2$ ein Quadrat ist, daß sich also b, d zu einem pythagoreischen Tripel ergänzen lassen.

Es gibt verschiedene Theorien darüber, auf welche Weise die Babylonier die Zahlen gefunden haben. Man vermutet, daß der Ausgangspunkt zur Berechnung eine Reziprokentafel gewesen ist. Diese Tafeln dienten den Babyloniern als Hilfsmittel bei der Division. Sie enthalten zweispaltige Tabellen, in denen das Produkt nebeneinanderstehender Zahlen x und y eine Potenz von 60 ist.

Ist $xy = z^2,\ x > y,\ x \equiv y \bmod 2$, so gilt

$$\left(\frac{x+y}{2}\right)^2 = \left(\frac{x-y}{2}\right)^2 + z^2.$$

Man erhält daher ein pythagoreisches Tripel, wenn man von einem Paar (x, y) einer Reziprokentafel mit $xy = 60^{2k}$ ausgeht. Diese Tripel sind im allgemeinen nicht primitiv. Da z eine Potenz von 60 ist, können nur 2, 3 und 5 gemeinsame Primteiler sein.

BEISPIEL. Ist

$$x = 2 \cdot 60^3 + 18 \cdot 60^2 + 53 \cdot 60 + 20, \quad y = 25 \cdot 60^2 + 55 \cdot 60 + 12,$$

so ist $xy = 60^6$. Man erhält

$$\frac{x-y}{2} = 56 \cdot 60^2 + 29 \cdot 60 + 4, \quad \frac{x+y}{2} = 1 \cdot 60^3 + 22 \cdot 60^2 + 24 \cdot 60 + 16,$$

was nach Division durch 16 auf das vierte primitive Paar

$$b = 3 \cdot 60^2 + 31 \cdot 60 + 49 = 12709, \quad d = 5 \cdot 60^2 + 9 \cdot 60 + 1 = 18541$$

der obigen Tabelle führt.

(B) Das folgende Verfahren, pythagoreische Tripel zu gewinnen, soll schon Pythagoras bekannt gewesen sein. Man betrachtet die Folge der Quadratzahlen und ihrer Differenzen

$$\begin{array}{ccccccccccc} 0 & & 1 & & 4 & & 9 & & 16 & & 25 & \cdots \\ & 1 & & 3 & & 5 & & 7 & & 9 & \cdots & \end{array}$$

In der zweiten Zeile stehen sämtliche ungeraden Zahlen. Ist eine davon ein Quadrat, also von der Form $(2n+1)^2$, so erhält man mit den beiden darüberstehenden ein pythagoreisches Tripel. Aus

$$(k+1)^2 - k^2 = (2n+1)^2$$

ergibt sich $k = 2n(n+1)$, also die Formel

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

(C) EUKLID war die allgemeine Formel aus Satz 7.1 bekannt. DIOPHANT beschreibt in den Arithmetica ein allgemeines geometrische Verfahren, um Polynomgleichungen (z.B. der Form $x^2 + y^2 = z^2$) ganzzahlig zu lösen.

Wegen

$$x^2 + y^2 = z^2 \iff \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

gibt es zu jedem primitiven pythagoreischen Tripel einen rationalen Punkt auf dem Einheitskreis. Umgekehrt ergibt jeder rationale Punkt auf dem Einheitskreis durch Erweitern ein pythagoreisches Tripel. Es sei

$$P := \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1,\ x, y > 0\}.$$

g sei die Gerade durch $(-1, 0)$ mit $y = t(x+1)$, $0 < t < 1$.
Schneiden von g mit dem Einheitskreis liefert (vgl. Abb. 7.1):

$$1 - x^2 = y^2 = t^2(x+1)^2.$$

Dies ist eine quadratische Gleichung für x, deren Lösung

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

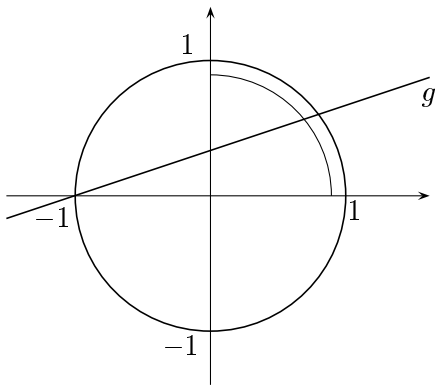

ABBILDUNG 7.1. Einheitskreis

ist. Für $t \in \mathbb{Q}$ ist (x, y) ein rationaler Punkt. Gibt es einen rationalen Punkt $(x, y) \neq (-1, 0)$ auf g, so ist die Steigung t eine rationale Zahl: $t = \frac{y}{x+1} \in \mathbb{Q}$. Damit ist

$$P = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \;\middle|\; t \in \mathbb{Q},\ 0 < t < 1 \right\}$$

die gesuchte Punktmenge.
Setzt man $t = \frac{n}{m}$, $(n, m) = 1$, $m > n$ und erweitert, so erhält man sämtliche pythagoreische Tripel:

$$\begin{aligned} x &= (m^2 - n^2)\lambda \\ y &= 2mn\lambda \\ z &= (m^2 + n^2)\lambda. \end{aligned}$$

BEMERKUNG. Diophant: „Arithmetica“ (um 250 n. Chr.) wurde 1621 von Bachet übersetzt. Fermat hat seine berühmte Vermutung, daß $x^n + y^n = z^n$ nur für $n = 1, 2$ lösbar ist, an den Rand seines Arithmetica-Exemplars geschrieben.

2. Summe von zwei Quadraten

BEISPIELE.

$$\begin{aligned} 2 &= 1^2 + 1^2 \\ 3 &= 1^2 + 1^2 + 1^2 \\ 4 &= 2^2 \\ 5 &= 1^2 + 2^2 \\ 6 &= 1^2 + 1^2 + 2^2 \\ 7 &= 1^2 + 1^2 + 1^2 + 2^2 \end{aligned}$$

Ziel: Welche Zahlen lassen sich als Summe von zwei Quadraten darstellen?
Aus

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

folgt unmittelbar

SATZ 7.2. *Sind n, m Summen von zwei Quadraten, so ist auch $n \cdot m$ Summe zweier Quadrate.*

LEMMA 7.1. *Ist $p \equiv 1 \bmod 4$ eine Primzahl, so gibt es Zahlen $a, k \in \mathbb{N}$ mit $a, k < p$, für die gilt: $pk = a^2 + 1$.*

BEWEIS. Wegen $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ ist $x^2 \equiv -1 \bmod p$ lösbar. Es gibt also ein a mit $1 \leq a < p$ und $a^2+1 = kp$. Wegen $kp = a^2+1 \leq (p-1)^2+1 = p^2-2(p-1) < p^2$ ist $k < p$. □

SATZ 7.3. *Ist $p \equiv 1 \bmod 4$ eine Primzahl, so ist p Summe zweier Quadrate.*

BEWEIS. (Euler) Sei $m \in \mathbb{N}$ minimal gewählt, so daß $mp = x^2 + y^2$, für $x, y \in \mathbb{N}$ gilt. Wegen des obigen Lemmas existiert ein solches m, und es ist $m < p$.

Annahme: $m > 1$

Wir definieren a, b durch

$$\begin{aligned} a &\equiv x \bmod m \\ b &\equiv y \bmod m, \end{aligned} \qquad -\frac{m}{2} < a, b \leq \frac{m}{2}.$$

Dann ist $a^2+b^2 \equiv x^2+y^2 = mp \equiv 0 \bmod m$, also $a^2+b^2 = km$. Wegen $a^2, b^2 \leq \left(\frac{m}{2}\right)^2$ ist

$$km = a^2 + b^2 \leq \frac{m^2}{4} \cdot 2 < m^2,$$

also $k < m$. Wäre $k = 0$, also $a^2 + b^2 = 0$, also $a = b = 0$, so würde hieraus $x \equiv y \equiv 0 \bmod m$, d.h. $m \mid x, y$, also $m^2 \mid x^2 + y^2 = mp$, also $m \mid p$ ein Widerspruch folgen. Damit gilt

$$a^2 + b^2 = km, \quad 1 \leq k < m.$$

Dann ist $(ax + by)^2 + (bx - ay)^2 = (a^2 + b^2)(x^2 + y^2) = km^2p$.

Wegen $ax + by \equiv x^2 + y^2 = mp \equiv 0 \bmod m$ und $bx - ay \equiv yx - xy \equiv 0 \bmod m$ sind $ax + by$ und $bx - ay$ durch m teilbar. Also ist

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{bx - ay}{m}\right)^2 = kp.$$

Dies steht im Widerspruch zur Minimalität von m. Also ist $m = 1$ und damit $p = x^2 + y^2$. □

SATZ 7.4. *$p \in \mathbb{P}$ ist genau dann Summe zweier Quadrate, wenn $p = 2$ oder $p \equiv 1 \bmod 4$ ist.*

BEWEIS. Die eine Richtung wurde eben gezeigt. Für $p = 2$ gilt $p = 1^2 + 1^2$. Es sei umgekehrt $p = x^2 + y^2$. Fallunterscheidung:

(1) $x \equiv y \equiv 0 \bmod 2 \Longrightarrow 4 \mid p$: Widerspruch zu $p \in \mathbb{P}$.

(2) $x \equiv y \equiv 1 \bmod 2 \Longrightarrow p \equiv 0 \bmod 2 \Longrightarrow p = 2$.

(3) $x \not\equiv y \bmod 2 \Longrightarrow p = x^2 + y^2 = (2k)^2 + (2l + 1)^2 \equiv 1 \bmod 4$.

□

SATZ 7.5. *$n \in \mathbb{N}$ ist genau dann Summe zweier Quadrate, wenn in der Primfaktorzerlegung von n alle Primzahlen $\equiv 3 \bmod 4$ in gerader Potenz auftreten.*

BEWEIS. Es sei

$$n = 2^\alpha \underbrace{p_1^{\alpha_1} \cdots p_s^{\alpha_s}}_{p_i \equiv 1 \bmod 4} \underbrace{p_{s+1}^{\alpha_{s+1}} \cdots p_r^{\alpha_r}}_{p_i \equiv 3 \bmod 4}$$

mit $\alpha_i \equiv 0 \bmod 2$ für $s < i \leq r$, also $n = t^2 u$, wobei in der Primfaktorzerlegung von u nur Primzahlen 2 und $\equiv 1 \bmod 4$ auftreten. Dann ist nach Satz 7.2 und 7.4 $u = x^2 + y^2$, also $n = (tx)^2 + (ty)^2$, also n Summe zweier Quadrate.

Es sei nun umgekehrt $n = x^2 + y^2$ und $p \equiv 3 \bmod 4$ ein Primteiler von n, also $x^2 + y^2 \equiv 0 \bmod p$.

Ist $y \not\equiv 0 \bmod p$, so ist $y \bmod p$ invertierbar: $yy_1 \equiv 1 \bmod p$. Es folgt $(xy_1)^2 + 1 \equiv 0 \bmod p$. Also ist -1 ein Quadrat mod p: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, und damit $p \equiv 1 \bmod 4$: Widerspruch zu $p \equiv 3 \bmod 4$.
Folglich ist $y \equiv 0 \bmod p$, also auch $x \equiv 0 \bmod p$. Damit ist p ein Teiler von x, y, also p^2 ein Teiler von $n = x^2 + y^2$.

Man wiederholt den gleichen Schluß mit

$$n_1 = \frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2.$$

Falls p ein Teiler von n_1 ist, so ist auch p^2 ein Teiler, usw. Man kommt schließlich zu dem Fall $p^{2k} \mid n$ und $p^{2k+1} \nmid n$.
Folglich tritt in der Primfaktorzerlegung von n jede Primzahl $p \equiv 3 \bmod 4$ in gerader Potenz auf. □

SATZ 7.6. *Die Darstellung $n = a^2 + b^2$, $(a, b) = 1$, n ungerade, ist genau dann eindeutig bis auf die Reihenfolge der Summanden, wenn n eine Primzahl $\equiv 1 \bmod 4$ ist.*

BEWEIS. 1. Ist p eine Primzahl $\equiv 1 \bmod 4$ so gilt $p = a^2 + b^2 = (a + bi)(a - bi) = c^2 + d^2 = (c + di)(c - di)$, wobei $c + di$ und $c - di$ Primelemente in $\mathbb{Z}[i]$ sind. Wegen der Eindeutigkeit der Primfaktorzerlegung folgt $\{a, b\} = \{c, d\}$.

2. Ist $n = t^2 u$, so ist auch u Summe zweier Quadrate, also $u = c^2 + d^2 \Longrightarrow n = (tc)^2 + (td)^2$. Wegen der Eindeutigkeit der Darstellung ist $t | (a, b) = 1 \Longrightarrow t = 1$, d.h. n ist quadratfrei.
Sei $n = k \cdot m$ eine nicht-triviale Zerlegung. Nach dem vorigen Satz ist

$$\begin{aligned} k = \quad & u^2 + v^2 \quad = (u + iv)(u - iv) \\ m = \quad & x^2 + y^2 \quad = (x + iy)(x - iy), \end{aligned}$$

also

$$(*) \qquad n = \begin{cases} N(u + iv) \cdot N(x + iy) & = (ux - vy)^2 + (vx + uy)^2 \\ N(u + iy) \cdot N(x - iy) & = (ux + vy)^2 + (vx - uy)^2. \end{cases}$$

Aus der Eindeutigkeit der Darstellung folgt

(a) $(ux - vy)^2 = (ux + vy)^2$ oder (b) $(ux - vy)^2 = (vx - uy)^2$.

Es ist

(a) $\Longleftrightarrow 4uxvy = 0 \Leftrightarrow k$ oder m ist Quadrat: Widerspruch zu n quadratfrei.

(b) $\Longleftrightarrow (u^2 - v^2)(x^2 - y^2) = 0$, also ist $u^2 = v^2$ oder $x^2 = y^2 \Longrightarrow m$ oder k ist gerade und damit ist auch n gerade: Widerspruch zu n ungerade.

□

BEMERKUNG. Bei nicht eindeutiger Darstellung liefert $(*)$ verschiedene Zerlegungen:

$$65 = 5 \cdot 13 = (\underbrace{2^2}_{u^2} + \underbrace{1^2}_{v^2})(\underbrace{3^2}_{x^2} + \underbrace{2^2}_{y^2}) = (6 - 2)^2 + (3 + 4)^2 = (6 + 2)^2 + (3 - 4)^2$$

FERMAT bewies mit Hilfe von Satz 7.6 daß 44021 Primzahl ist. Dazu probierte er alle Zahlen $0 < a, b < 209 = \lfloor\sqrt{44021}\rfloor$ aus und stellte fest, daß es nur eine Darstellung von 44021 als Quadratsumme gibt.

Man kann die Anzahl der zu probierenden Zahlen a erheblich einschränken, wenn man beachtet, daß Quadratzahlen nur die Endziffern $0, 1, 4, 5, 6$ oder 9 haben können.

3. Summe von vier Quadraten

SATZ 7.7. *Eine Zahl der Form $n = 4^\alpha(8k+7)$ läßt sich nicht mit weniger als vier Quadraten darstellen.*

BEWEIS. Annahme: $n = x_1^2 + x_2^2 + x_3^2$, $x_i \in \mathbb{N}_0$
Wir betrachten zuerst den Fall $\alpha = 0$:

$$\underbrace{8k+7}_{\text{ungerade}} = x_1^2 + x_2^2 + x_3^2$$

Folgende Fälle sind dann möglich
(a) Alle x_i sind ungerade:
Dann ist $x_i^2 \equiv 1 \bmod 8$ wegen $(2k+1)^2 = 4k(k+1)+1$, also $x_1^2+x_2^2+x_3^2 \equiv 3 \bmod 8$: Widerspruch.
(b) x_1, x_2 gerade, x_3 ungerade:
Wegen $x_3^2 \equiv 1 \bmod 4$ und $x_1^2, x_2^2 \equiv 0 \bmod 4$ ist $8k+7 \equiv 1 \bmod 4$: Widerspruch.

Es sei jetzt $\alpha > 0$:

$$\underbrace{4^\alpha(8k+7)}_{\text{gerade}} = x_1^2 + x_2^2 + x_3^2$$

Folgende Fälle sind dann möglich
(a) x_1, x_2 ungerade, x_3 gerade:
$4^\alpha(8k+7) \equiv 1+1+0 \bmod 4$: Widerspruch.
(b) x_1, x_2, x_3 gerade:
Dann ist

$$4^{\alpha-1}(8k+7) = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2.$$

Diese Reduktion führt bei wiederholter Anwendung entweder auf den Fall (a) oder auf $\alpha = 0$. In jedem Fall erhält man einen Widerspruch. □

SATZ 7.8 (LAGRANGE). *Jede Zahl $n \in \mathbb{N}$ ist Summe von vier Quadraten*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

wobei die x_i aus $\mathbb{N}_0$ sind.

LEMMA 7.2. *Das Produkt zweier Zahlen, die sich als Summe von vier Quadraten darstellen lassen, ist wieder eine Summe von vier Quadraten.*

BEWEIS. (Eulersche Identität)

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) \;=\;& (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\ &+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &+(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2\\ &+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2\end{aligned}$$

□

LEMMA 7.3. *Zu jeder Primzahl p gibt es $a, b, k \in \mathbb{Z}$, $0 < k < p$, mit*

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

BEWEIS. Für $p = 2$ setze $a = 1$, $b = 0$ und $k = 1$. Sei also jetzt $p > 2$.
Betrachte folgende Mengen:

$$A := \{x^2 + 1 | 0 \leq x < \tfrac{p}{2}\}$$
$$B := \{-y^2 | 0 \leq y < \tfrac{p}{2}\}$$

Die Elemente aus A sind mod p inkongruent:
$x^2 + 1 \equiv x'^2 + 1 \bmod p \Longrightarrow (x + x')(x - x') \equiv 0 \bmod p$
Wegen $0 \leq x, x' < \frac{p}{2}$ ist $x + x' \neq p \Longrightarrow x \equiv x' \bmod p \Longrightarrow x = x'$.
Analog folgt dies für B.
Insgesamt liegen $p + 1$ Zahlen in $A \cup B$. Da es p Restklassen mod p gibt, sind nach dem Schubfachprinzip zwei Zahlen mod p kongruent, von denen eine in A und eine in B liegen muß.
Es gibt also $a^2 + 1 \in A$ und $-b^2 \in B$ mit

$$a^2 + 1 \equiv -b^2 \bmod p,$$

also $a^2 + b^2 + 1 = kp$.
Wegen $a, b < \frac{p}{2}$ ist

$$0 < kp = a^2 + b^2 + 1 \leq \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2,$$

also $0 < k < p$. □

LEMMA 7.4. *Jede Primzahl p besitzt die Darstellung*

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

BEWEIS. Sei $m \in \mathbb{N}$ minimal gewählt, so daß

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

für $x_i \in \mathbb{Z}$ ist. Nach Lemma 7.3 gibt es ein solches $m < p$.
Annahme: $m > 1$
1. Fall: m gerade: $\underbrace{mp}_{\text{gerade}} = x_1^2 + x_2^2 + x_3^2 + x_4^2$
Zu jeder ungeraden Zahl auf der rechten Seite gibt es eine zweite ungerade Zahl. Man kann daher $x_1 - x_2$ und $x_3 - x_4$ als gerade annehmen. Dann sind auch $x_1 + x_2$ und $x_3 + x_4$ gerade. Es folgt

$$\left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2$$
$$= \frac{1}{2}(x_1^2 + x_2^2 + x_3^2 + x_4^2) = \frac{m}{2}p.$$

Das steht aber im Widerspruch zur Minimalität von m.
2. Fall: m ungerade, also $m \geq 3$.
Definiere y_1, y_2, y_3, y_4 so, daß

$$y_i \equiv x_i \bmod m, \quad -\frac{m}{2} < y_i \leq \frac{m}{2}.$$

Dann ist $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < m^2$, weil m ungerade und daher $y_i < \frac{m}{2}$ ist. Wegen

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv \underbrace{x_1^2 + x_2^2 + x_3^2 + x_4^2}_{=mp} \equiv 0 \bmod m$$

ist

$$km = y_1^2 + y_2^2 + y_3^2 + y_4^2 < m^2,$$

also $k < m$. Nach der Eulerschen Identität ist

$$(mp)(km) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (\ldots)^2 + \ldots + (\ldots)^2.$$

Es ist zu zeigen, daß die rechten Klammern jeweils durch m teilbar sind.
Es ist $\sum x_i y_i \equiv \sum x_i^2 \equiv 0 \bmod m$, also ist die erste Klammer ist durch m teilbar.
Es ist

$$x_1 y_2 - x_2 y_1 \equiv x_1 x_2 - x_2 x_1 = 0 \bmod m$$

und

$$x_3 y_4 - x_4 y_3 \equiv x_3 x_4 - x_4 x_3 = 0 \bmod m,$$

also auch die zweite Klammer durch m teilbar.
Analog für die dritte und vierte Klammer. Es folgt

$$kp = \left(\frac{\cdots}{m}\right)^2 + \left(\frac{\cdots}{m}\right)^2 + \left(\frac{\cdots}{m}\right)^2 + \left(\frac{\cdots}{m}\right)^2$$

mit $k < m$: Widerspruch zur Minimalität von m.

Also ist $m = 1$. □

Wir kommen nun zum Beweis des Satzes von LAGRANGE.

Sei $n = p_1 \ldots p_r$ die Primfaktorzerlegung von n. Nach Lemma 7.4 ist jedes p_i Summe von vier Quadraten und damit nach Lemma 7.2 auch das Produkt, also n. □

BEMERKUNGEN. (1) BACHET, ein französischer Adeliger, hat 1621 DIOPHANTS „Arithmetica“ ins Lateinische übersetzt und kommentiert. Den 4-Quadrate-Satz hat er bis $n = 355$ verifiziert, weswegen dieser Satz häufig auch Satz von Bachet genannt wird.

FERMAT teilt in einem Brief mit, daß er den Satz bewiesen habe. Aber er hat seinen Beweis nicht veröffentlicht.

Der erste veröffentlichte Beweis des Satzes stammt von LAGRANGE 1770. EULER, der führende Mathematiker jener Zeit, hatte sich lange vergeblich um einen solchen Beweis bemüht. 1773 veröffentlicht er dann die oben dargestellte vereinfachte Version des Beweises von LAGRANGE.

(2) Eine Formel für die Anzahl der Darstellungen: z.B.

$$\begin{aligned} 34 &= 5^2 + 3^2 \\ &= 5^2 + 2^2 + 2^2 + 1^2 \\ &= 4^2 + 4^2 + 1^2 + 1^2 \\ &= 4^2 + 3^2 + 3^2 \end{aligned}$$

hat JACOBI 1829 angegeben.

(3) Der englische Mathematiker EDWARD WARING stellte in seinem Buch „Meditationes algebraicae“ 1770 folgende Vermutungen auf:
(i) Zu jedem k gibt es ein $g(k)$, so daß jede natürliche Zahl n Summe von $g(k)$ k-ten

Potenzen ist: $n = x_1^k + \ldots + x_{g(k)}^k$.
(ii) $g(3) = 9$ und $g(4) = 19$.
Die erste Vermutung wurde 1909 von HILBERT bewiesen. BIBERICH zeigte 1909, daß $g(3) = 9$ ist. Erst 1985 wurde $g(4) = 19$ bewiesen.

SATZ 7.9.

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

BEWEIS. Für

$$n = 2^k \left[\left(\frac{3}{2}\right)^k\right] - 1.$$

gilt

$$n \leq 2^k \left(\frac{3}{2}\right)^k - 1 < 3^k.$$

Bei der Darstellung von n durch k-te Potenzen treten daher nur Potenzen von 1 und 2 auf. Wir nehmen an, daß es

a k-te Potenzen von 1 und b k-te Potenzen von 2 sind.

Also ist $n = a + b \cdot 2^k$, und es gilt somit

$$g(k) \geq a + b = n - b(2^k - 1).$$

Ferner gilt $b < \left[\left(\frac{3}{2}\right)^k\right]$, denn wäre $b \geq \left[\left(\frac{3}{2}\right)^k\right]$, so folgt ein Widerspruch:

$$n \geq b \cdot 2^k \geq 2^k \left[\left(\frac{3}{2}\right)^k\right] = n + 1.$$

Damit ist

$$b \leq \left[\left(\frac{3}{2}\right)^k\right] - 1,$$

also

$$g(k) \geq n - \left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right)\left(2^k - 1\right).$$

Einsetzen von n führt dann auf

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2. \quad \square$$

BEISPIEL. $g(3) \geq 9$. Wähle n wie im Beweis: $n = 8 \cdot 3 - 1 = 23$
Dann ist $23 = 2^3 + 2^3 + 1^3 + \ldots + 1^3 = 2 \cdot 2^3 + 7 \cdot 1^3$

BEMERKUNG. Setzt man

$$g^*(k) := 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2,$$

so ergibt sich folgende Tabelle

k	2	3	4	5	6	7	8
$g^*(k)$	4	9	19	37	73	143	279

Es besteht die Vermutung: $g(k) = g^*(k)$, die bisher mit Computern bis $k = 471.000.000$ verifiziert ist.

4. Aufgaben

AUFGABE 7.1. Es sei $x^2+y^2 = z^2$. Zeige, daß mindestens eine der Zahlen $x, y, z \in \mathbb{N}$

(a) durch 3 (b) durch 4 (c) durch 5

teilbar ist.

AUFGABE 7.2. Benutze die geometrische Methode von Diophant, um sämtliche Lösungen von

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

zu bestimmen.

Literatur zur Zahlentheorie

[1] Borevich & Shafarevich: *Zahlentheorie.*
Birkhäuser 1966

[2] Bundschuh: *Einführung in die Zahlentheorie.*
Springer-Verlag 1988

[3] Dickson: *History of the theory of Numbers.*
Chelsea 1971 (Nachdruck von 1920)

[4] Frey: *Elementare Zahlentheorie.*
Vieweg 1984

[5] Gauss: *Untersuchungen über höhere Arithmetik.*
Chelsea 1965 (Disquisitiones Arithmeticae 1801)

[6] Hasse: *Vorlesungen über Zahlentheorie.*
Springer 1950

[7] LeVeque: *Fundamentals of Number theory.*
Addison-Wesley 1977

[8] Niven & Zuckerman: *Einführung in die Zahlentheorie.*
B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1976

[9] Rosen: *Elementary Number Theory and Applications.*
Wesley 1988

[10] Scheid, H.: *Zahlentheorie.*
B.I. Wissenschaftsverlag Mannheim/Wien/Zürich 1991

[11] Scholz, A. & Schöneberg, B.: *Einführung in die Zahlentheorie.*
Walter de Gruyter 1973

[12] Serre: *Cours d'Arithmetique.*
Hermann 1970

[13] Stark: *An Introduction to Number theory.*
Markham 1970

Index

Ableitung, 66

Dedekind, 6
Direktes Produkt, 42

Elementanzahl einer Menge, 10
Ergänzungssätze, 63
erzeugendes Element, 24
Eulerkriterium, 58
Eulersche φ-Funktion, 45
Eulersche Identität, 78
Exponentenbildung, 54

Fermat, Satz von, 46

Gaußsches Lemma, 59
geordnet, 8
gleichmächtig, 10

Homomorphismus, 42

Index, 51
Induktionsaxiom, 5
Isomorphismus, 42

Jacobi-Symbol, 64

Kleinsche Vierergruppe, 45

Lagrange, Satz von, 78
Landau, 8
Legendre-Symbol, 58
linear geordnet, 8
Lineare Methoden, 52

Nachfolgerfunktion, 11
Nichtrest, 57

Ordnung, 24

Peano, 5
Polynomkongruenz, 66
Primitive Kongruenzwurzel, 47

Quadratischer Rest, 57

Rekursionssatz, 6
Reziprozitätsgesetz, 63
RSA-Verfahren, 54

Schlüsselwort, 53
Schubfachprinzip, 10
Sukzessive Approximation, 68

Taylorformel, 66
total geordnet, 8

Verfahren von Pohlig, Helmann, 54
Verfahren von Vigenère, 54
vollständige Induktion, 5

Waring-Problem, 80
Wilson, Satz von, 48
wohlgeordnet, 9

zyklisch, 24