Elementare Zahlentheorie, Vorlesungsskript

Prof. Dr. Irene I. Bouw

Sommersemester 2008

Inhaltsverzeichnis

Einleitung

Dies ist ein Skript für der Vorlesung *Elementare Zahlentheorie*. Dies ist ein Vorlesung für Lehrämtler und Bachelorstudenten Mathematik an der Universität Ulm. Ich danke Dr. Robert Carls, Dominik Ufer und Studenten der Vorlesung im SS 2008 und SS 2009 für das sorgfaltige Lesen des Manuskripts.

1 Primzahlen

1.1 Teilbarkeit und der euklidische Algorithmus

Wir schreiben $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ für die Menge der natürlichen Zahlen und $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ für die Menge der ganzen Zahlen. Mit $\mathbb{Q}$ bezeichnen wir die Menge der rationalen Zahlen ("Bruchzahlen").

Definition 1.1.1 Seien $a \neq 0$ und b ganze Zahlen. Wir sagen, dass b durch a *teilbar* ist, falls es eine ganze Zahl c gibt so, dass $b = a \cdot c$. In diesem Fall heißt a ein *Teiler* von b. Falls b durch a teilbar ist, so schreiben wir $a \mid b$. Falls b nicht durch a teilbar ist, so schreiben wir $a \nmid b$.

Beispiel 1.1.2 Die Teiler von 12 sind ± 1, ± 2, ± 3, ± 4, ± 6 und ± 12.

Wir brauchen zuerst einige einfache Eigenschaften der Teilbarkeit.

Lemma 1.1.3 *Seien a, b, c, m, n ganze Zahlen.*

(a) Falls $a \mid b$ und $b \mid c$, so gilt $a \mid c$.

(b) Falls $c \mid a$ und $c \mid b$, so gilt $c \mid (ma + nb)$.

Beweis: (a) Es existieren ganze Zahlen e und f mit $ae = b$ und $bf = c$. Also gilt $c = bf = aef$. Wir schließen daraus, dass c durch a teilbar ist.

(b) Es existieren ganze Zahlen e und f mit $a = ce$ und $b = cf$. Daher gilt $ma + nb = mce + ncf = c(me + nf)$. Also ist $ma + nb$ durch c teilbar. □

Definition 1.1.4 Seien a, b ganze Zahlen (nicht beide 0). Der *größte gemeinsame Teiler* von a und b ist die größte Zahl die sowohl a also auch b teilt. Wir schreiben dafür: $\mathrm{ggT}(a, b)$. Falls $\mathrm{ggT}(a, b) = 1$, so heißen a und b *teilerfremd*. Falls $a \neq 0$, so ist $\mathrm{ggT}(a, 0) = a$. Für $a = b = 0$ ist $\mathrm{ggT}(a, b)$ nicht definiert.

Zwei Beispiele sind $\mathrm{ggT}(16, 12) = 4$ und $\mathrm{ggT}(120, 225) = 15$. Dies kann man zum Beispiel nachrechnen, indem man die Zahlen faktorisiert: $120 = 2^3 \cdot 3 \cdot 5$ und $225 = 3^2 \cdot 5^2$. Für größere Zahlen ist dies allerdings nicht praktikabel. Versuchen Sie zum Beispiel $\mathrm{ggT}(1160718174, 316258250)$ mit Hilfe eines Taschenrechners zu berechnen. Den größten gemeinsamen Teiler berechnet man in Maple mit dem Kommando `igcd`.

Ein sehr effizienter Algorithmus zum Berechnen des ggTs, ist der *euklidische Algorithmus*. Dieser Algorithmus basiert auf *Division mit Rest*.

Satz 1.1.5 *Seien a, b ganze Zahlen mit $b > 0$. Dann existieren eindeutige ganze Zahlen q, r mit $a = bq + r$ und $0 \leq r < b$. Wir nennen q den Quotienten und r den Rest. Falls $r = 0$, so ist b ein Teiler von a.*

Beweis: Sei $q = [a/b]$ die größte ganze Zahl kleiner oder gleich a/b. Es gilt $q \leq a/b < q + 1$. Also gilt

$$qb \leq \frac{a}{b}b = a < (q+1)b = qb + b.$$

Setzen wir $r = a - qb$, so folgt $0 \leq r < b$.

Falls $r = 0$, so gilt $a = qb$. Also ist b ein Teiler von a.

Zur Überprüfung der Eindeutigkeit nehmen wir an, dass

$$a = q_1 b + r_1 = q_2 b + r_2 \qquad \text{mit} \quad 0 \leq r_1, r_2 < b. \tag{1}$$

OBdA dürfen wir annehmen, dass $r_2 < r_1$. (Falls $r_1 = r_2$, so gilt auch $q_1 = q_2$.) Daher gilt $0 < r_1 - r_2 < b$. Insbesondere ist b kein Teiler von $r_1 - r_2$. Aus (1) folgt, dass $(q_1 - q_2)b = r_2 - r_1$. Dies liefert einen Widerspruch. □

Beispiel 1.1.6 Wir erklären zuerst an Hand eines Beispiels wie man den ggT mit Hilfe der Division mit Rest berechnen kann. Wir möchten $\mathrm{ggT}(842, 356)$ berechnen. Wir berechnen zuerst den Rest von $a := 842$ nach Division durch $b := 356$. Aus dem Beweis von Satz 1.1.5 folgt, dass $q = [842/356] = 2$ ist, wie man leicht mit einem Taschenrechner verifiziert. Der Rest ist nun $r = a - qb = 130$. Mit Maple berechnet man q und r mit den Kommandos `iquo` und `irem`. Wir teilen nun 356 durch 130 und machen so weiter, bis wir irgendwann den Rest 0 bekommen. Der vorletzte Rest ist dann $\mathrm{ggT}(a, b)$.

$$\begin{aligned}
842 &= 2 \cdot 356 + 130 \\
356 &= 2 \cdot 130 + 96 \\
130 &= 1 \cdot 96 + 34 \\
96 &= 2 \cdot 34 + 28 \\
34 &= 1 \cdot 28 + 6 \\
28 &= 4 \cdot 6 + 4 \\
6 &= 1 \cdot 4 + \boxed{2} \\
4 &= 2 \cdot 2 + 0.
\end{aligned}$$

Allgemein funktioniert der euklidische Algorithmus wie folgt.

Algorithmus 1.1.7 (Der euklidische Algorithmus) Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Ohne Einschränkung dürfen wir annehmen, dass $0 < b < a$. Wir schreiben $r_{-1} = a$ und $r_0 = b$.

(a) Für $n > 0$ definieren wir nun q_i und r_i rekursiv durch die folgende Gleichung

$$r_{n-2} = q_n \cdot r_{n-1} + r_n, \qquad \text{mit} \quad 0 \leq r_n < r_{n-1}. \tag{2}$$

(b) Sei m minimal so, dass $r_m = 0$. Nun ist $\mathrm{ggT}(a, b) = r_{m-1}$.

Um überflüssiges Schreiben zu vermeiden, bietet es sich an, die Werte von q_n und r_n in einer Tabelle zu notieren. Im obigen Beispiel sieht dies wie folgt aus:

n	r_n	q_n
-1	842	
0	356	
1	130	2
2	96	2
3	34	1
4	28	2
5	6	1
6	4	4
7	$\boxed{2}$	1
8	0	2

Das folgende Lemma beschreibt einige wichtige Eigenschaften des ggTs.

Lemma 1.1.8 *(a)* $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$.

(b) Für jedes $q \in \mathbb{Z}$ *gilt, dass* $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - qb)$.

(c) Falls $g := \mathrm{ggT}(a, b)$*, so gilt* $\mathrm{ggT}(a/g, b/g) = 1$.

Beweis: Aussage (a) ist klar. Wir beweisen nun (b). Sei $q \in \mathbb{Z}$ beliebig und sei d ein gemeinsamer Teiler von a und b. Aus Lemma 1.1.3.(b) folgt, dass d auch ein Teiler von $a - qb$ ist. Umgekehrt, sei e ein gemeinsamer Teiler von b und $a - qb$. Da $a = (a - qb) + qb$ ist folgt aus Lemma 1.1.3.(b), dass e auch ein Teiler von a ist. Daher haben a und b genau die gleichen gemeinsamen Teiler wie b und $a - qb$. Insbesondere ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - qa)$.

Wir beweisen nun (c). Sei $g = \mathrm{ggT}(a, b)$. Wir nehmen an, dass $e > 0$ ein gemeinsamer Teiler von a/g und b/g ist. Es existieren ganze Zahlen x und y, sodass $a/g = xe$ und $b/g = ye$. Also ist ge ein gemeinsamer Teiler von a und b. Da g der größte gemeinsame Teiler von a und b ist, gilt also $e = 1$. Also ist $\mathrm{ggT}(a/g, b/g) = 1$. □

Lemma 1.1.8.(b) zeigt, dass der euklidische Algorithmus den ggT berechnet. Seien nämlich r_n definiert durch (2). Da $(r_n)_{n \geq -1}$ eine streng monoton fallende Folge ganzer Zahlen ist, gilt $r_m = 0$ für m hinreichend groß. Sei m minimal so, dass $r_m = 0$. Wir möchten zeigen, dass $r_{m-1} = \mathrm{ggT}(a, b)$. Da $r_n = r_{n-2} - q_n r_{n-1}$ (2), folgt aus Lemma 1.1.8.(b), dass $\mathrm{ggT}(r_{n-2}, r_{n-1}) = \mathrm{ggT}(r_{n-1}, r_n)$ für $n \geq 1$. Wir schließen, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(r_{-1}, r_0) = \mathrm{ggT}(r_0, r_1) = \cdots = \mathrm{ggT}(r_{m-2}, r_{m-1}) = \mathrm{ggT}(r_{m-1}, 0) = r_{m-1}$.

Lemma 1.1.9 *Seien* $a, b \neq 0$ *ganze Zahlen. Sei* $g := \mathrm{ggT}(a, b)$.

(a) Es existieren $x, y \in \mathbb{Z}$ *so, dass* $xa + yb = g$.

(b) *Jede Zahl d von der Form $d = xa + yb$ mit $x, y \in \mathbb{Z}$ ist teilbar durch* $\mathrm{ggT}(a, b)$.

Beweis: Wir betrachten die Menge $G = \{xa + yb \,|\, x, y \in \mathbb{Z}\}$. Sei $s \in G$ das kleinste positive Element und seien $x_0, y_0 \in \mathbb{Z}$ so, dass $s = x_0 a + y_0 b$.

Behauptung: s teilt jedes Element $\alpha \in G$. Nämlich, sei $\alpha = x_\alpha a + y_\alpha b \in G$ beliebig. Für jedes $c \in \mathbb{Z}$ gilt nun, dass $\alpha - cs = (x_\alpha - cx_0)a + (y_\alpha - cy_0)b \in G$. Insbesondere gilt dies für $c = [\alpha/s]$. Aus $[\alpha/s] \leq \alpha/s < [\alpha/s] + 1$ schließen wir, dass

$$0 \leq \alpha - \left[\frac{\alpha}{s}\right] s < s.$$

Da $\alpha - \left[\frac{\alpha}{s}\right] s \in G$, folgt aus der Wahl von s, dass $\alpha - \left[\frac{\alpha}{s}\right] s = 0$, also dass $s \mid \alpha$.

Aus der Behauptung folgt insbesondere, dass $s = x_0 a + y_0 b$ ein Teiler von a und b ist, da $a, b \in G$. Falls d ein beliebiger gemeinsamer Teiler von a und b ist, so folgt aus Lemma 1.1.3.(b), dass $d \mid s$. Daher ist $s = \mathrm{ggT}(a, b)$ der größte gemeinsame Teiler von a und b. □

Lemma 1.1.9 sagt, dass $g = \mathrm{ggT}(a, b)$ die kleinste positive Zahl ist, die sich als $g = xa + yb$ mit $x, y \in \mathbb{Z}$ schreiben lässt.

Die Zahlen x und y kann man mit Hilfe des euklidischen Algorithmus berechnen. Wir betrachten nur den Fall, dass $0 < b < a$ ist. Der allgemeiner Fall folgt aus diesem Spezialfall.

Sei (r_n) definiert durch (2) und sei m minimal so, dass $r_m = 0$. Also ist $\mathrm{ggT}(a, b) = r_{m-1}$. Wiederholtes einsetzen von (2) liefert, dass $\mathrm{ggT}(a, b) = r_{m-1} = r_{m-3} - q_{m-1} r_{m-2} = (1 + q_{m-1} q_{m-2}) r_{m-3} - q_{m-1} r_{m-4}$. Wir machen dies weiter, bis wir alle Gleichungen (2) benutzt haben.

Eine einfachere Methode zur Berechnung von x und y ist der *erweiterte euklidische Algorithmus*. Dies ist eine Variante des euklidischen Algorithmus, der die Zahlen x, y aus Lemma 1.1.9 gleichzeitig mit dem ggT berechnet. Dies funktioniert wie folgt. Wir definieren zuerst

$$\begin{aligned} x_{-1} &= 1, \qquad y_{-1} = 0, \\ x_0 &= 0, \qquad y_0 = 1. \end{aligned} \tag{3}$$

Für $n \geq 1$ definieren wir

$$\begin{aligned} x_n &= x_{n-2} - q_n x_{n-1}, \\ y_n &= y_{n-2} - q_n y_{n-1}, \end{aligned} \tag{4}$$

wobei q_n der n-te Quotient definiert in (2) ist.

Lemma 1.1.10 *Für jede $n \geq -1$ gilt*

$$r_n = x_n a + y_n b. \tag{5}$$

Insbesondere gilt $\mathrm{ggT}(a, b) = r_{m-1} = x_{m-1} a + y_{m-1} b$.

Beweis: Wir zeigen (5) mittels vollständiger Induktion.

Induktionsanfang: (5) gilt offensichtlich für $n = -1, 0$.

Induktionsschritt: Wir nehmen an, dass (5) für $n-1, n$ gilt und zeigen, dass (5) auch für $n+1$ gilt.

Wir wissen, dass

$$\begin{aligned} r_{n+1} &= r_{n-1} - q_{n+1} r_n, \\ r_{n-1} &= x_{n-1} a + y_{n-1} b, \\ r_n &= x_n a + y_n b. \end{aligned}$$

Also gilt

$$\begin{aligned} r_{n+1} &= r_{n-1} - q_{n+1} r_n = x_{n-1} a + y_{n-1} b - q_{n+1}(x_n a + y_n b) \\ &= a(x_{n-1} - q_{n+1} x_n) + b(y_{n-1} - q_{n+1} y_n) = x_{n+1} a + y_{n+1} b. \end{aligned}$$

□

Beispiel 1.1.11 Sei $a = 93$ und $b = 42$. Wir berechnen nun $\mathrm{ggT}(a, b)$, zusammen mit Zahlen x, y so, dass $\mathrm{ggT}(a, b) = x \cdot a + y \cdot b$. Wie vorher notieren wir r_n, q_n, x_n und y_n in einer Tabelle.

n	r_n	q_n	x_n	y_n
-1	93	$-$	1	0
0	42	$-$	0	1
1	9	2	1	-2
2	6	4	-4	9
3	$\boxed{3}$	1	5	-11
4	0	2	$-$	$-$

Also ist $\mathrm{ggT}(a, b) = 3 = 5 \cdot 93 - 11 \cdot 42$.

1.2 Der Fundamentalsatz der Arithmetik

Definition 1.2.1 Eine natürliche Zahl $n \geq 2$ heißt *Primzahl*, falls 1 und n die einzigen positiven Teiler sind. Falls $n \geq 2$ keine Primzahl ist, so heißt n *zusammengesetzt*.

Die erste Primzahlen sind

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \cdots$$

Primzahlen von der Form $2^n - 1$ heißen *Mersenne-Primzahlen*. Das folgende Lemma zeigt, dass falls $2^n - 1$ eine Primzahl ist, so muss n auch eine Primzahl sein.

Lemma 1.2.2 *(a) Seien d, n natürliche Zahlen, sodass $d \mid n$. Es gilt*

$$(2^d - 1) \mid (2^n - 1).$$

(b) Falls $2^n - 1$ eine Primzahl ist, so ist p auch eine Primzahl.

Beweis: Wir schreiben $n = dt$. Es gilt $x^t - 1 = (x-1)(x^{t-1} + x^{t-2} + \cdots + 1)$. Wi setzen $x = 2^d$ und finden, dass

$$2^n - 1 = 2^{dt} - 1 = (2^d - 1)(2^{d(t-1)} + 2^{d(t-2)} \cdots + 1).$$

Also ist $2^d - 1$ ein Teiler von $2^n - 1$. Dies beweist (a). Teil (b) folgt direkt aus (a). □

Man kann sich fragen, für welche Primzahlen p die Zahl $2^p - 1$ auch eine Primzahl ist. In 1536 fand Hudalricus Regius, dass $2^{11} - 1 = 23 \cdot 89$ keine Primzahl ist. In 1644 behauptete der französische Mönch Marin Mersenne, dass $2^p - 1$ eine Primzahl ist für

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ und } 257,$$

und, dass $2^p - 1$ zusammengesetzt ist für alle andere Primzahlen $p < 257$. Mit der damalige Methoden kann er bestimmt nicht alle Zahlen versucht haben: Erst in 1947 war die genaue Liste der Primzahlen $p \leq 257$, sodass $2^p - 1$ eine Mersenne-Primzahl ist, bekannt. Es stellte sich heraus, dass Mersenne einige Fehler gemacht hat. Zum Beispiel ist $2^{61} - 1$ eine Mersenne-Primzahl, aber $2^{257} - 1$ nicht. Auf der Webseite `http://primes.utm.edu/` können Sie mehr über Mersenne-Primzahlen lesen.

Die größte bekannte Primzahl ist eine Mersenne-Primzahl: Dies ist die Primzahl $2^{32582657} - 1$. Diese Zahl hat 9808358 Dezimalziffern (Stand: Frühjahr 2008). Auf der Webseite `http://www.mersenne.org/status.htm` lesen Sie, wie Sie mitmachen können dieses Rekord zu brechen.

Das folgende Lemma liefert eine charakterisierende Eigenschaft von Primzahlen. Das Lemma ist der wichtigste Schritt im Beweis des Fundamentalsatzes der Arithmetik.

Lemma 1.2.3 *Sei p eine Primzahl. Falls $p \mid ab$, so gilt $p \mid a$ oder $p \mid b$.*

Beweis: Wir nehmen an, dass $p \mid ab$, aber $p \nmid a$. Zu zeigen ist, dass $p \mid b$. Da p eine Primzahl ist, so gilt $\mathrm{ggT}(p, a) = 1$. Lemma 1.1.9.(a) impliziert daher, dass ganze Zahlen x, y mit $1 = xp + ya$ existieren. Wir ergänzen die Gleichung mit b und finden $b = pxb + yab$. Wir haben angenommen, dass p ein Teiler von ab ist. Also ist p auch ein Teiler von b. □

Falls n eine zusammengesetzte Zahl ist, so gibt es Zahlen a und b für die Lemma 1.2.3 nicht gilt. Zum Beispiel nehme $n = 6$, $a = 8$ und $b = 9$. Nun gilt $p \mid ab$, aber $n \nmid a$ und $n \nmid b$.

Theorem 1.2.4 (Fundamentalsatz der Arithmetik) *Sei $n \geq 2$ eine ganze Zahl.*

(a) Die Zahl n kann als Produkt von Primzahlen geschrieben werden.

(b) Die Zerlegung in (a) ist eindeutig bis auf Reihenfolge.

Die Aussage ist klar falls $n = p$ ein Primzahl ist: In diesem Fall ist die Primfaktorzerlegung einfach $p = p$.

Beweis: Wir beweisen (a) mit vollständiger Induktion.

Induktionsanfang: Sei zuerst $n = 2$. Da 2 selber ein Primzahl ist, ist 2 sicherlich ein Produkt von Primzahlen.

Induktionsschritt: Wir nehmen an, dass wir die Aussage für alle $n < N$ überprüft haben. Wir möchten zeigen, dass die Aussage auch für N gilt. Falls N ein Primzahl ist, so gilt die Aussage für N. Falls N zusammengesetzt ist, existiert ein Teiler $m_1 \neq 1, N$ von N. Wir schreiben $N = m_1 \cdot m_2$. Da nun $1 < m_1, m_2 < N$ können wir m_1 und m_2 laut Induktionshypothese schreiben als Produkt von Primzahlen. Also lässt sich auch N als Produkt von Primzahlen schreiben.

Wir beweisen nun (b). Dazu nehmen wir an, dass wir zwei Primfaktorzerlegungen

$$n = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_\ell$$

von n haben. Die zwei Zerlegungen haben nicht notwendigerweise die gleiche Anzahl von Primfaktoren. Wir dürfen annehmen, dass $m \leq \ell$ ist.

Da $p_1 \mid n$, impliziert Lemma 1.2.3, dass p_1 auch eine der q_is teilt. Da die q_is Primzahlen sind, gibt es ein i_1 sodass $p_1 = q_{i_1}$. Wir kürzen nun p_1 und q_{i_1}. Das gleiche Argument zeigt nun, dass es ein $i_2 \neq i_1$ gibt, sodass $p_2 = q_{i_2}$. Wir kürzen p_2 und q_{i_2}. Dies machen wir so lange weiter bis es keine p_is mehr gibt. (Wir haben angenommen, dass es mehr q_is als p_is gibt.) Falls $m < \ell$, so sagt unsere gekürzte Gleichung, dass 1 ein Produkt von $(\ell - m)$-viele q_is ist. Dies ist unmöglich. Also ist $\ell = m$ und die q_is sind eine Umordnung der p_is. □

Jeder natürliche Zahl n lässt sich also eindeutig schreiben als Produkt

$$n = \prod_p p^{n_p} \qquad \text{mit} \quad n_p \geq 0.$$

Das Produkt läuft über alle Primzahlen. Falls $n = 1$, so ist $n_p = 0$, für alle p.

Schon Euklid bewies in seinem Buch *Elemente*, dass es unendlich viele Primzahlen gibt. Dies ist ein Korollar der Fundamentalsatz der Arithmetik.

Satz 1.2.5 (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis: Wir nehmen an, es gäbe nur endlich viele Primzahlen. Wir bezeignen diese Primzahlen mit $p_1, \ldots, p_n$. Die natürliche Zahl

$$N := p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$$

ist durch keine der Primzahlen $p_1, \ldots, p_n$ teilbar, da sonnst auch 1 durch p_i teilbar wäre (Lemma 1.1.3.(b)). Da jede Zahl größer als 1 durch mindestens eine Primzahl teilbar ist (Theorem 1.2.4), existiert mindestens eine weitere Primzahl p_{n+1}. Aber dies widerspricht der Annahme, dass $p_1, \ldots, p_n$ die einzigen Primzahlen sind. □

Definition 1.2.6 Das *kleinste gemeinsame Vielfache* von a und b ist die kleinste positive Zahl, die sowohl durch a als auch durch b teilbar ist. Bezeichnung: $\mathrm{kgV}(a,b)$.

Lemma 1.2.7 *Seien* $a = \prod_p p^{n_p}$ *und* $b = \prod_p p^{m_p}$ *natürliche Zahlen.*

(a) Es gilt $\mathrm{ggT}(a,b) = \prod_p p^{\min(n_p,m_p)}$ *und* $\mathrm{kgV}(a,b) = \prod_p p^{\max(n_p,m_p)}$.

(b) Zwischen kgV *und* ggT *besteht folgende Beziehung*

$$\mathrm{kgV}(a,b) = \frac{ab}{\mathrm{ggT}(a,b)}.$$

Beweis: Teil (a) ist klar. Für (b) bemerken wir, dass

$$n_p + m_p = \min(n_p, m_p) + \max(n_p, m_p).$$

Also gilt

$$a \cdot b = \prod_p p^{n_p+m_p} = \prod_p p^{\min(n_p,m_p)+\max(n_p,m_p)} = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b).$$

□

Beispiel 1.2.8 Wir haben schon gesehen, dass $\mathrm{ggT}(93,42) = 3$ (Beispiel 1.1.11). Daher ist $\mathrm{kgV}(93,42) = 93 \cdot 42/3 = 31 \cdot 42 = 1302$.

1.3 Probedivision

Der Fundamentalsatz der Arithmetik (Theorem 1.2.4) sagt uns, dass sich jede natürliche Zahl als Produkt von Primzahlen schreiben lässt. Aber wie funktioniert dies in der Praxis? Für kleine Zahlen n findet man die Primfaktorzerlegung durch Ausprobieren. Zum Beispiel gilt

$$180 = 2 \cdot 90 = 2^2 \cdot 45 = 2^2 \cdot 3 \cdot 15 = 2^2 \cdot 3^2 \cdot 5.$$

Für größere Zahlen sollte man ein bisschen geschickter vorgehen. In diesem Abschnitt besprechen wir die einfachste Methode zur Berechnung der Primfaktorzerlegung von einer Zahl n: Die Probedivision. Im Wesentlichen probieren wir alle Primzahlen aus, bis wir ein Faktor d von n gefunden haben. Nun ersetzen wir n durch den Quotient n/d. Eine wichtige Bemerkung ist, dass es reicht die Primfaktoren mit $p \leq \sqrt{n}$ zu betrachten. Der Grund ist, dass wenn $n = a \cdot b$, so ist entweder $a \leq \sqrt{n}$ oder $b \leq \sqrt{n}$.

Wir gehen davon aus, dass wir eine Liste der Primzahlen $p \leq \sqrt{n}$ besitzen. Wie man so eine Liste erstellt, besprechen wir nachher.

Algorithmus 1.3.1 (Probedivision) (a) Wir fangen mit $p = 2$ an und arbeiten die Liste der Primzahlen ab. Für jede Primzahl p probieren wir ob $p \mid n$. Dies machen wir mittels Division mit Rest: $p \mid n$ genau dann wenn der Rest von n nach Division durch p gleich 0 ist.

(b) Falls $p \mid n$, so berechnen wir die höchsten Potenz p^e mit $p^e | n$. Wir ersetzen nun n durch n/p^e und betrachten die nächsten Primzahl.

(c) Sobald $p^2 > n$ ist, sind wir fertig.

Beispiel 1.3.2 Hier ist ein kleines Beispiel. Sei $n = 2331$. Wir finden $2 \nmid n$ und $3 \mid n$. Es gilt $9 \mid n$ aber $3^3 \nmid n$. Also ersetzten wir n durch $n_2 := n/9 = 259$. Wir wissen schon, dass 259 nicht durch 2 und 3 teilbar ist, also gehen wir weiter mit $p = 5$. Wir finden dass $5 \nmid 259$, aber $7 \mid 259$. Da $259 = 5 \cdot 7^2 + 14$, ist 259 nicht durch 7^2 teilbar. Also ersetzten wir 259 durch $n_3 = 259/7 = 37$. Wir wissen dass $n_3 = 37$ nicht durch $2, 3, 5, 7$ teilbar ist. Da $7^2 = 49 > 37$ ist 37 also eine Primzahl. Die Primfaktorzerlegung von n ist nun

$$2331 = 3^2 \cdot 7 \cdot 37.$$

Das Sieb von Eratosthenes Jetzt besprechen wir noch eine Methode, um eine Liste aller Primzahlen $p \leq B$ zu berechnen, wobei B eine vorgegebene Schranke ist. Dies ist das *Sieb von Eratosthenes*. Eratosthenes lebte von 276 bis 194 v. Chr. Er wurde geboren in Cyrene im heutigen Libyen.

Algorithmus 1.3.3 (Sieb von Eratosthenes) Wir machen hierzu eine Liste aller Zahlen von 2 bis B.

(a) Wir fangen mit der ersten nichtdurchgestrichene Zahl p auf der Liste an. Im ersten Durchgang ist dies also $p = 2$.

(b) Wir markieren diese Zahl als Primzahl und streichen alle Vielfachen von p weg. Dieser Schritt heißt *Sieben*: Wir sieben alle Vielfachen von p aus.

(c) Wir wiederholen die Schritte (a) und (b) bis alle Zahlen entweder weggestrichen oder als Primzahl markiert sind.

Als Beispiel wenden wir nun dieses Verfahren auf $B = 49$ an. Wir machen eine Liste alle Zahlen von 2 bis 49, und fangen mit $p = 2$ an. Nachdem wir Schritt (b) für $p = 2$ durchgeführt haben, sieht die Tabelle so aus:

		2	3	~~4~~	5	~~6~~	7	~~8~~	9
~~10~~	11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19
~~20~~	21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29
~~30~~	31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39
~~40~~	41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49.

Als nächstes betrachten wir $p = 3$, usw. Am Ende des Verfahrens sieht die Tabelle dann so aus:

		2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~
~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29
~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~.

Die Primzahlen ≤ 49 sind also $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$.

2 Kongruenzen

2.1 Kongruenzen

In diesem Kapitel studieren wir die Theorie der Kongruenzen. Kongruenzen beschreiben Teilbarkeitsrelationen. Man findet sie auch im tägliche Leben: Uhren geben die Stunden entweder modulo 12 oder modulo 24 an. Die Wochentage rechnen wir modulo 7 und die Monate modulo 12. Sobald wir die richtigen Werkzeuge bereit gestellt haben, können wir genauso gut mit Kongruenzen rechnen wie mit Gleichungen.

Definition 2.1.1 Sei m eine natürliche Zahl und seien a, b ganze Zahlen. Wir sagen, dass a *kongruent zu* b *modulo* m ist, falls $m \mid (b - a)$. Wir schreiben: $a \equiv b \pmod{m}$. Die Zahl m heißt der *Modul* der Kongruenz.

Zum Beispiel ist $200 \equiv 11 \pmod{9}$, da 9 ein Teiler von $200 - 11 = 189$ ist. Anders formuliert: 200 und 11 haben den gleichen Rest nach Division durch 9 nämlich 2.

Satz 2.1.2 *Kongruenz ist eine Äquivalenzrelation, d.h. es gelten die folgenden Eigenschaften:*
Reflexivität $a \equiv a \pmod{m}$, *für alle* $a \in \mathbb{Z}$,
Symmetrie *Falls* $a \equiv b \pmod{m}$, *so gilt auch* $b \equiv a \pmod{m}$,
Transitivität *Falls* $a \equiv b \pmod{m}$ *und* $b \equiv c \pmod{m}$, *so gilt auch* $a \equiv c \pmod{m}$.

Beweis: Übungsaufgabe. □

Satz 2.1.2 impliziert, dass wir die ganze Zahlen für festes m in *Kongruenzklassen* aufteilen können. Eine Kongruenzklasse ist die Menge aller ganzen Zahlen kongruent zu einer festen Zahl $a \in \mathbb{Z}$. Eine solche Zahl heißt *Repräsentant* der Kongruenzklasse. Die Division mit Rest (Satz 1.1.5) impliziert, dass es genau m Kongruenzklassen modulo m gibt.

Beispiel 2.1.3 Für $m = 2$ gilt $a \equiv 0 \pmod{2}$ genau dann wenn a gerade ist und $a \equiv 1 \pmod{2}$ genau dann wenn a ungerade ist. Die Kongruenzklassen modulo 2 sind daher

$$0 \pmod{2} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\},$$
$$1 \pmod{2} = \{\cdots, -5, -3, -1, 1, 3, 5, 7, \cdots\}.$$

Definition 2.1.4 (a) Wir bezeichnen mit $\mathbb{Z}/m\mathbb{Z}$ die Menge der Kongruenzklassen modulo m.

(b) Ein *vollständiges Restsystem* modulo m ist eine Menge ganzer Zahlen so, dass jede ganze Zahl zu genau einem Element des Restsystem kongruent modulo m ist.

Jede ganze Zahl ist zu genau einer der Zahlen $0, 1, \ldots, m-1$ kongruent modulo m, daher ist

$$\mathcal{R} = \{0, 1, \ldots, m-1\}$$

ein vollständiges Restsystem.

Man sieht leicht ein, dass viele Rechenregeln für Gleichungen auch für Kongruenzen gelten. Zum Beispiel, falls $a_1 \equiv b_1 \pmod{m}$ und $a_2 \equiv b_2 \pmod{m}$ so gilt auch $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ und $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$. Wir sagen: die Menge $\mathbb{Z}/m\mathbb{Z}$ ist ein *kommutativer Ring*.

Mit Teilen muss man vorsichtig sein: Aus $ac \equiv bc \pmod{m}$ können wir nicht immer schließen, dass $a \equiv b \pmod{m}$. Zum Beispiel gilt $16 \equiv 10 \pmod{6}$, aber $8 \not\equiv 5 \pmod{6}$.

Der folgende Satz sagt uns, wann wir kürzen dürfen.

Satz 2.1.5 (Kürzungssatz) *Seien a, b, c ganze Zahlen, m eine natürliche Zahl und $g := \mathrm{ggT}(c, m)$. Falls $ac \equiv bc \pmod{m}$, so gilt $a \equiv b \pmod{m/g}$.*

Beweis: Da $ac \equiv bc \pmod{m}$ gilt, existiert eine ganze Zahl x mit $xm = ac - bc = c(a-b)$. Insbesondere ist c ein Teiler von xm. Da $g = \mathrm{ggT}(c, m)$ ist, so gilt $x(m/g) = (c/g)(a-b)$. Aus Lemma 1.1.8.(c) folgt, dass $\mathrm{ggT}(c/g, m/g) = 1$. Also ist m/g ein Teiler von $a - b$. □

Folgendes Korollar ist ein wichtiger Spezialfall von Satz 2.1.5.

Korollar 2.1.6 *Seien a, b, c ganze Zahlen und sei m eine natürliche Zahl mit $\mathrm{ggT}(c, m) = 1$. Falls $ac \equiv bc \pmod{m}$, so gilt $a \equiv b \pmod{m}$.*

Wir benutzen Satz 2.1.5, um lineare Kongruenzen von der Form $ax \equiv b \pmod{m}$ nach x aufzulösen, ähnlich wie man dies in der linearen Algebra mit linearen Gleichungen macht. Zuerst diskutieren wir einige Beispiele.

Beispiel 2.1.7 (a) Wir betrachten die Kongruenz $4x \equiv 3 \pmod{11}$. Um die Kongruenz zu vereinfachen bemerken wir, dass $4 \cdot 3 = 12 \equiv 1 \pmod{11}$. Daher ergänzen wir beide Seiten der Kongruenz mit 3 und finden $12x \equiv 9 \pmod{11}$, was sich vereinfachen lässt zu $x \equiv 9 \pmod{11}$. Also hat die Kongruenz genau eine Lösung (modulo 11).

(b) Wir betrachten nun die Kongruenz $4x \equiv 3 \pmod{12}$. Der Trick von oben funktioniert diesmal nicht, da es keine Zahl c so, dass $4c \equiv 1 \pmod{12}$ gibt. Da $\mathrm{ggT}(3, 4) = 1$ können wir den Term 4 auch nicht kürzen mit Hilfe von Satz 2.1.5. In der Tat hat die Kongruenz keine Lösung, wie man sieht, wenn man die Kongruenz modulo 4 betrachtet.

Satz 2.1.8 (Lösungen linearer Kongruenzen) *Seien a, b, m ganze Zahlen mit $m \geq 1$ und sei $g := \mathrm{ggT}(a, m)$.*

(a) *Falls $g \nmid b$, so hat die Kongruenz $ax \equiv b \pmod{m}$ keine Lösungen.*

(b) *Falls $g \mid b$, so hat die Kongruenz $ax \equiv b \pmod{m}$ genau g verschiedene Lösungen (modulo m).*

Beweis: Wir beweisen zuerst, dass die Kongruenz $ax \equiv b \pmod{m}$ genau dann Lösungen besitzt, wenn $\mathrm{ggT}(a, m) \mid b$.

Sei $g := \mathrm{ggT}(a, m)$. Lemma 1.1.9.(a) impliziert, dass ganze Zahlen y, z existieren mit $y \cdot a + z \cdot m = g$. Falls $g \mid b$, so ist b/g eine ganze Zahl, daher finden wir

$$ay\frac{b}{g} + mz\frac{b}{g} = g\frac{b}{g} = b,$$

Daher ist $x = y(b/g)$ eine Lösung der Kongruenz.

Umgekehrt, falls $x \in \mathbb{Z}$ eine Lösung der Kongruenz $ax \equiv b \pmod{m}$ ist, existiert eine ganze Zahl y mit $ax - ym = b$. Lemma 1.1.9.(b) impliziert, dass $g \mid b$. Also hat die Kongruenz $ax \equiv b \pmod{m}$ genau dann eine Lösung, wenn $g \mid b$.

Wir nehmen nun wieder an, dass $g \mid b$. Wir bestimmen die Anzahl der Lösungen der Kongruenz (modulo m). Wir betrachten zuerst den Spezialfall, dass $g = 1$. Da $g = \mathrm{ggT}(a, m) = 1$ existieren $y, z \in \mathbb{Z}$ mit $ay + mz = 1$ (Lemma 1.1.9.(a)). Insbesondere gilt $ay \equiv 1 \pmod{m}$. Wir ergänzen die Kongruenz $ax \equiv b \pmod{m}$ mit y und finden, dass

$$x \equiv yb \pmod{m}.$$

Insbesondere hat die Kongruenz eine eindeutige Lösung (modulo m).

Falls $g > 1$, so impliziert Satz 2.1.5, dass wir die Kongruenz $ax \equiv b \pmod{m}$ umstellen können zu

$$\left(\frac{a}{g}\right) x \equiv \frac{b}{g} \pmod{\frac{m}{g}}.$$

Da $\mathrm{ggT}(a/g, m/g) = 1$, hat die neue Kongruenz eine Lösung (modulo m/g), und daher g Lösungen in $\{0, 1, \ldots, m-1\}$. □

Der Beweis von Satz 2.1.8 liefert auch ein Verfahren, um alle Lösungen einer Kongruenz zu berechnen. Wir betrachten dazu eine Kongruenz $ax \equiv b \pmod{m}$ mit $g := \mathrm{ggT}(a, m) \mid b$. Eine Lösung $x \in \mathbb{Z}$ der Kongruenz korrespondiert zu eine Lösung $x, y \in \mathbb{Z}$ der Gleichung $ax - my = b$.

Wir berechnen zuerst Zahlen c, d mit $ac - md = g = \mathrm{ggT}(a, m)$ mit Hilfe des erweiterten euklidischen Algorithmus (Lemma 1.1.10). Nun ist $x_0 = cb/g$ eine Lösung der Kongruenz $ax \equiv b \pmod{m}$. Der Beweis von Satz 2.1.8 impliziert, dass die anderen Lösungen der Kongruenz

$$x \equiv x_0 + k\frac{m}{g} \pmod{m}, \qquad k = 0, 1, 2, \ldots, g-1 \tag{6}$$

sind.

Ein bisschen allgemeiner formuliert bekommen wir folgender Satz.

Satz 2.1.9 *Seien a und b ganze Zahlen und $g := \mathrm{ggT}(a, b)$. Falls $g \mid c$ so hat die Gleichung $ax + by = c$ unendlich viele Lösungen $x, y \in \mathbb{Z}$. Falls x_0, y_0 eine Lösung dieser Gleichung ist, so sind alle Lösungen von der Form*

$$x = x_0 + \frac{b}{g}k, \qquad y = y_0 - \frac{a}{g}k$$

für eine ganze Zahl k.

Beweis: Der Beweis ist ähnlich dem Beweis von Satz 2.1.8. □

Die Gleichung von Satz 2.1.9 ist eine *lineare Diophantische Gleichung*. Eine Diophantische Gleichung ist eine Gleichung, für die wir ganzzahlige Lösungen suchen. Die Gleichungen sind benannt nach den griechischen Mathematiker Diophant (Alexandria, rund 250 n. Chr.) der solche Gleichungen studiert hatte. Lineare Diophantische Gleichungen wurde zuerst von den indischen Mathematiker Brahmagupta im 7-te Jahrhundert n. Chr. vollständig gelöst.

Das folgende Beispiel gibt eine konkrete Anwendung von Satz 2.1.9.

Beispiel 2.1.10 (Das Briefmarkenproblem) Auf einem Päckchen möchten wir 3,90 Euro an Briefmarken aufkleben. Wir haben nur Briefmarken von 45 und 55 Cent zur Verfügung. Wir fragen uns, ob dies möglich ist. Sei x die Anzahl der Briefmarken von 55 Cent und y die Anzahl der Briefmarken von 45 Cent. Wir möchten also die Gleichung $x \cdot 55 + y \cdot 45 = 390$ lösen. Wir fordern zusätzlich, dass x und y positiv sind.

Zuerst lösen wir die Gleichung $x \cdot 55 + y \cdot 45 = 390$ mit $x, y \in \mathbb{Z}$. Da $\mathrm{ggT}(45, 55) = 5$ ein Teiler von 390 ist, hat das Problem eine Lösung. Mit dem erweiterten euklidischen Algorithmus finden wir, dass $5 = -4 \cdot 55 + 5 \cdot 45$ gilt. Also ist $x = -4 \cdot 390/5 = -312$ und $y = 5 \cdot 390/5 = 390$ eine Lösung unserer Gleichung. Dies ist aber noch keine Lösung des Briefmarkenproblems, da x negativ ist. Da $45/5 = 9$ und $55/5 = 11$, sagt Satz 2.1.9, dass die anderen Lösungen der Gleichung von der Form

$$x = -312 + 9k, \qquad y = 390 - 11k, \qquad \text{mit} \quad k \in \mathbb{Z}$$

sind. Die Bedingung $x, y \geq 0$ liefert, dass $9k \geq 312$ und $11k \leq 390$. Also finden wir $312/9 \leq k \leq 390/11$. Die einzige Lösung ist daher $k = 35$.

Wir schließen also, dass das Briefmarkenproblem genau eine Lösung hat: Wir brauchen $-312 + 9 \cdot 35 = 3$ Briefmarken von 55 Cent und $390 - 11 \cdot 35 = 5$ Briefmarken von 45 Cent.

2.2 Der Kalenderformel

Ziel dieses Abschnittes ist es, eine Formel für den Wochentag eines bestimmten Datums zu geben. Dies ist eine Anwendung des Rechnens modulo 7.

Ein **Jahr** ist die Zeit, welche die Erde braucht, um sich einmal um die Sonne zu drehen. Ein **Tag** ist die Zeit, welche die Erde braucht, um einmal um ihre Achse zu drehen. Ein Jahr ist ungefähr $365,2422$ Tage lang. Dies ist der Grund

dafür, dass Julius Ceasar und seine Berater in 46 v. Chr. das Schaltjahr eingeführt haben, als sie den **julianischen Kalender** einführten. Das julianische Jahr war also im Schnitt $365,25 - 365,2422 \sim 0,0078$ Tage zu lang. Um dies zu kompensieren, führte Papst Gregor IV in 1582 den gregorianischen Kalender ein. Zur Korrektur wurden 10 Tagen gestrichen; auf den 04.10.1582 folgte der 15.10.1582. Es dauerte noch viele Jahre, bis der gregorianische Kalender weltweit eingeführt wurde. In Russland zum Beispiel wurde der gregorianische Kalender erst in 1918 eingeführt. Damals wurden 13 Tage gestrichen. Für die Geschichte des Kalenders siehe zum Beispiel
`http://de.wikipedia.org/wiki/Gregorianischer_Kalender`.

Wir werden jetzt eine Kalenderformel herleiten. Hierzu geben wir jedem Wochentag eine Nummer, wie im folgenden Schema:

So	Mo	Di	Mi	Do	Fr	Sa
0	1	2	3	4	5	6.

Obwohl es das Jahr 0 nicht gegeben hat, betrachten wir dies trotzdem als unser Ausgangsjahr. Sei a der Wochentag des 01.03.0000. Wir werden zuerst a berechnen. Hierzu bemerken wir, dass $365 = 7 \cdot 52 + 1 \equiv 1 \pmod 7$ und $366 \equiv 2 \pmod 7$. Falls 01.03.j auf den Wochentag a' fällt, so gilt

$$a' \equiv a + j + S \pmod 7,$$

wobei S die Anzahl von Schaltjahren zwischen 0 und j ist.

Das Jahr j ist ein Schaltjahr, falls $j \equiv 0 \pmod 4$ und $j \not\equiv 0 \pmod{100}$ ist. Falls $j \equiv 0 \pmod{100}$, so ist j nur dann ein Schaltjahr, wenn $j \equiv 0 \pmod{400}$ ist. Wir finden daher

$$S \equiv [\frac{j}{4}] - [\frac{j}{100}] + [\frac{j}{400}] \pmod 7.$$

Z.B. war 2000 ein Schaltjahr, aber 1900 nicht.

Wir definieren

$$g(j) = j + [\frac{j}{4}] - [\frac{j}{100}] + [\frac{j}{400}] \pmod 7.$$

Also ist der 01.03.j der Wochentag $a' \equiv a + g(j) \pmod 7$. Da der 01.03.2008 ein Samstag war, gilt:

$$6 \equiv a + g(2008) \equiv a + 2008 + [\frac{2008}{4}] - [\frac{2008}{100}] + [\frac{2008}{400}] \equiv a + 3 \pmod 7.$$

Wir schließen, dass $a = 3$, daher war der 01.03.000 ein Mittwoch.

Wie sieht das aus mit einem anderen Datum als dem 1. März? Einfachheitshalber lassen wir das Jahr am ersten März anfangen, da der zusätzliche Tag im Schaltjahr der 29.02. ist. Folgende Tabelle listet den Wochentag des ersten Tages des Monats im Jahre 0000 auf. Wir definieren außerdem eine Funktion

$f(m)$ durch die Eigenschaft, dass $f(m)+1$ die Nummer des Wochentages des $01.m.0000$ ist.

Monat	Nummer	Wochentag	$f(m)$
März	1	3	2
April	2	6	5
Mai	3	1	0
Juni	4	4	3
Juli	5	6	5
August	6	2	1
September	7	5	4
Oktober	8	0	6
November	9	3	2
Dezember	10	5	4
Januar	11	1	0
Februar	12	4	3.

Eine Eselsbrücke für die Zahlen $f(m)$ ist der Satz: My uncle Charles has eaten a cold supper; he eats nothing hot. Die Anzahl der Buchstaben des $m$te Wort ist kongruent zu $f(m) \pmod 7$.

Wir finden daher folgendes Theorem.

Theorem 2.2.1 (Kalenderformel) *Der Tag mit Datum t.m.j ist der Wochentag mit Nummer*

$$t + f(m) + g(j) \pmod 7.$$

Beispiel 2.2.2 (a) Wir berechnen den Tag des Mauerfalls am 09.11.1989. Es gilt $t = 9$, $m = 11 - 2 = 9$ und $j = 1989$. Daher finden wir $f(m) = 2$ und $g(j) = 1989 + 497 - 19 + 4 = 2471 \equiv 0 \pmod 7$, also

$$t + f(m) + g(j) \equiv 9 + 2 + 0 \equiv 4 \pmod 7.$$

Wir schließen also, dass der Mauerfall an einem Donnerstag war.

(b) Wir berechnen den Wochentag, an dem Luther seine 95 Thesen an das Hauptportal der Schlosskirche in Wittenberg geschlagen haben soll (31.10.1517). Wir berechnen, dass $f(m) = 6$ und $g(j) = 1884 \equiv 1 \pmod 7$. Daher war der 31.10.1517, laut Gregorianischem Kalender ein Mittwoch:

$$31 + 6 + 1 \equiv 3 \pmod 7.$$

Da jedoch der Gregorianische Kalender in 1517 noch nicht erfunden war, müssen wir 10 dazu zählen. In Wirklichkeit war der 31.10.1517 daher ein Samstag!

Eine weitere Anwendung der Kalenderformel, für die Abergläubischen unter uns, ist folgendes Lemma.

Lemma 2.2.3 *Jedes Jahr besitzt mindestens einen Freitag den* 13.

Beweis: Wir betrachten den Wochentag vom Monat m im Jahr j, für die Monate $1, \ldots, 10$, also zwischen März und Dezember. Janur und Februar lassen wir hier aus, da sie zum letzten Jahr gerechnet werden. Wir stellen fest, dass $f(m)$ alle Werte von 0 bis 6 annimmt. Wir schließen also, dass es im Jahr j mindestens einen Freitag den 13. gibt. □

Man berechnet leicht, dass es in 2008 genau einen Freitag den 13. gibt, nämlich in Juli. Hierzu sollte man Januar und Februar getrennt betrachten, da sie zu 2007 gerechnet werden.

2.3 Prüfziffer

In diesem Abschnitt geben wir eine weitere Anwendung von Kongruenzen: Wir diskutieren, wie die Prüfziffer bei den ISBN-Nummern funktioniert.

Seit 1.1.2007 gibt es die ISBN-Nummer als eine 13-stellige Zahl zur Kennzeichnung von Büchern und anderen Veröffentlichungen. Vorher gab es eine 10-stellige Zahl. Der Grund für die Änderung war, dass im englischsprachigen Raum die ISBN-Nummern knapp wurden.

Die neue ISBN-13-Nummer besteht aus 4 Bestandteilen. Die Gesamtlänge für (A)–(C) ist 12 Ziffern.

(A) Die Gruppennummer (oder Ländernummer). Beispiele sind:

- 0, 1 englischsprachiger Raum (zB Großbritannien, USA, Australien, Indien)
- 2 französischsprachiger Raum
- 3 deutschsprachiger Raum
- 4 Japan
- 5 Russland

(B) Verlagsnummer: dies ist eine unterschiedlich lange Kennzahl für den Verlag.

(C) Titelnummer.

(D) Prüfziffer.

Die Prüfziffer ermöglicht das Erkennen von Tippfehlern. Eine 13-stellige Zahl $x_1x_2\cdots x_{13}$ ist eine gültige ISBN-13-Nummer, falls

$$x_1 + 3x_2 + x_3 + \cdots + 3x_{12} + x_{13} \equiv 0 \pmod{10}. \tag{7}$$

Diese Gleichung erlaubt auch die Berechnung der Prüfziffer.

Einer der häufigsten gemachten Fehler beim Abtypen von ISBN-Nummer ist die Vertauschung von zwei nebeneinander gelegenen Ziffern. Dies kann man meistens mit Hilfe der Prüfziffer feststellen.

Sei $x_1x_2\cdots x_{13}$ eine gültige ISBN-13-Nummer, also gilt (7). Versehentlich wurde diese ISBN-13-Nummer als $y_1y_2\cdots y_{13} := x_1x_2\cdots x_{i-1}x_{i+1}x_ix_{i+2}\cdots x_{13}$

eingegeben. Wir berechnen die richtige Prüffziffer $\tilde{y}_{13}$ gehörend zu $y_1 \cdots y_{12}$. Diese neue Prüfziffer erfüllt $\tilde{y}_{13} - y_{13} \equiv -(y_1 + 3y_2 + \cdots + 3y_{12}) \pmod{10}$. Also gilt:

$$\begin{aligned}\tilde{y}_{13} - y_{13} &\equiv -(y_1 + 3y_2 + \cdots + 3y_{12}) + x_1 + 3x_2 + \cdots + 3x_{12} \\ &\equiv \begin{cases} -2(x_i - x_{i+1}) \pmod{10} & \text{falls } i \text{ gerade ist,} \\ 2(x_i - x_{i+1}) \pmod{10} & \text{falls } i \text{ ungerade ist.} \end{cases}\end{aligned}$$

Also gilt, dass

$$\tilde{y}_{13} - y_{13} \equiv \tilde{y}_{13} - x_{13} \equiv \pm 2(x_i - x_{i+1}) \pmod{10}.$$

Satz 2.1.5 impliziert daher, dass $\tilde{y}_{13} - y_{13} \equiv 0 \pmod{10}$ genau dann, wenn $x_i - x_{i+1} \equiv 0 \pmod{5}$.

Die Vertauschung von x_i und x_{i+1} kann daher festgestellt werden, außer wenn die Differenz von x_i und x_{i+1} gleich 5 ist.

Der zweithäufigste Fehler ist, dass eine Ziffer falsch eingegeben wird. Wir überlassen es Ihnen als Übungsaufgabe zu überprüfen, dass diese Fehler immer festgestellt werden kann.

Die alte ISBN-10-Nummer gab mehr Möglichkeiten zur Fehlerfeststellung. Da heutzutage die ISBN-Nummer meistens gescannt statt abgetippt wird, hat der Bedarf an einer Fehlerfeststellung abgenommen. Man berechnet die neue ISBN-13-Nummer aus der alten ISBN-13-Nummer, indem man 978- voranstellt. Die Prüfziffer muss neu berechnet werden.

2.4 Teilbarkeitskriterien

Wir stellen eine natürliche Zahl $n \in \mathbb{N}$ im 10er System als

$$\begin{aligned}n &= (a_k a_{k-1} \cdots a_2 a_1 a_0)_{10} \\ &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0\end{aligned}$$

dar. An dieser Darstellung kann man leicht feststellen, ob n durch 2 oder 5 teilbar ist, da dies nur von den letzten Ziffer abhängt. Ähnlich leicht stellt man fest ob n durch $4 = 2^2$ oder $25 = 5^2$ teilbar ist, da dies nur von der letzten 2 Ziffern abhängt. Eine ähnliche Aussage gilt für höhere Potenzen von 2 und 5.

Aus der Schule kennen Sie wahrscheinlich auch die *Dreierregel*: Eine Zahl $n = (a_k a_{k-1} \cdots a_1 a_0)_{10}$ ist genau dann durch 3 teilbar, wenn die Quersumme

$$Q_1(n) := \sum_{i=0}^{k} a_i$$

durch 3 teilbar ist. Diese Regel folgt unmittelbar, wenn man bemerkt, dass $10 \equiv 1 \pmod{3}$ und daher auch $10^i \equiv 1^i \equiv 1 \pmod{3}$ für alle i ist.

In diesem Abschnitt besprechen wir weitere Teilbarkeitskriterien. Dazu definieren wir zuerst einige Verallgemeinerungen des Querschnittes. Wir nennen

$$Q'_1(n) = \sum_{i=0}^{k} (-1)^i a_i = a_0 - a_1 + \cdots + (-1)^k a_k$$

die *alternierende Quersumme*. Allgemeiner nennen wir

$$Q_s(n) = \sum_{i\geq 0} (a_{is+s-1} \cdots a_{is+1} a_{is})_{10} = (a_s a_{s-1} \cdots a_0)_{10} + (a_{s+1} a_s \cdots a_1)_{10} + \cdots$$

die *Quersumme der Stufe s* und

$$\begin{aligned} Q'_s(n) &= \sum_{i\geq 0} (-1)^i (a_{is+s-1} \cdots a_{is+1} a_{is})_{10} \\ &= (a_s a_{s-1} \cdots a_0)_{10} - (a_{s+1} a_s \cdots a_1)_{10} + (a_{s+2} a_{s+1} \cdots a_2)_{10} + \cdots \end{aligned}$$

die *alternierende Quersumme der Stufe s*.

Satz 2.4.1 *Seien $n, s \in \mathbb{N}$. Es gilt*

$$n \equiv Q_s(n) \pmod{10^s - 1} \qquad \textit{und} \qquad n \equiv Q'_s(n) \pmod{10^s + 1}.$$

Beweis: Es gilt

$$n = \sum_{j\geq 0} a_j 10^j = \sum_{i\geq 0} (a_{is+s-1} \cdots a_{is+1} a_{is})_{10} 10^{is}.$$

Da $10^s \equiv 1 \pmod{10^s - 1}$, gilt auch $10^{is} \equiv 1 \pmod{10^s - 1}$ für alle $i \geq 0$. Dies impliziert, dass $n \equiv Q_s(n) \pmod{10^s - 1}$. Die zweite Kongruenz folgt ähnlich aus $10^s \equiv -1 \pmod{10^s + 1}$. □

Für $s = 1$ sagt Satz 2.4.1 zum Beispiel:

$$n \equiv Q_1(n) \pmod 9, \qquad n \equiv Q'_1(n) \pmod{11}.$$

Hieraus folgen die Teilbarkeitskriterien:

$$\begin{aligned} 9 \mid n \quad &\text{genau dann, wenn} \quad 9 \mid Q_1(n), \\ 11 \mid n \quad &\text{genau dann, wenn} \quad 11 \mid Q'_1(n). \end{aligned}$$

Wenn wir allgemeiner ein Teilbareitskriterium für einer Primzahl p suchen, betrachten wir die Primfaktorzerlegung von $10^s - 1$ und $10^s + 1$. Falls p ein Teiler von $10^s - 1$ (b.z.w., von $10^s + 1$) ist, so gilt $p \mid n$ genau dann, wenn $p \mid Q_s(n)$ (bzw. $p \mid Q'_s(n)$). Die Primfaktorzerlegung von $10^s \pm 1$ für kleines s ist

$$99 = 3^2 \cdot 11, \quad 101 = 101, \quad 999 = 3^3 \cdot 37, \quad 1001 = 7 \cdot 11 \cdot 13,$$

wie man leicht feststellt mit Hilfe der Probedivision (§ 1.3). Daher finden wir, dass

$$\begin{aligned} 7 \mid n \quad &\Longleftrightarrow \quad 7 \mid Q'_3(n), \\ 11 \mid n \quad &\Longleftrightarrow \quad 11 \mid Q'_1(n), \\ 13 \mid n \quad &\Longleftrightarrow \quad 13 \mid Q'_3(n). \end{aligned}$$

2.5 Der kleine Satz von Fermat

In § 2.1 haben wir gesehen, dass die Kongruenz $ax \equiv 1 \pmod{m}$ genau dann eine Lösung hat, wenn $\mathrm{ggT}(a, m) = 1$ (Korollar 2.1.6).

Definition 2.5.1 Seien a und m teilerfremd. Eine Lösung x der Kongruenz $ax \equiv 1 \pmod{m}$ heißt die *Inverse* von $a \pmod{m}$. Wir bezeichnen es mit $a^{-1} \pmod{m}$. Ein Element deren Inverse existiert heißt *invertierbar*.

Wir bezeichnen mit $(\mathbb{Z}/m\mathbb{Z})^*$ die Menge der invertierbaren Kongruenzklassen modulo m.

Die Inverse eines Element $a \in \mathbb{Z}/m\mathbb{Z}^*$ kann man mit Hilfe des erweiterten euklidischen Algorithmus berechnen. Sei nämlich $a \in \mathbb{Z}/m\mathbb{Z}^*$, also ist $\mathrm{ggT}(a, m) = 1$. Mit Hilfe des erweiterten euklidischen Algorithmus berechnet man Zahlen x, y, sodass $1 = xa + ym$. Da $xa \equiv 1 \pmod{m}$, ist $x \equiv a^{-1} \pmod{m}$ die Inverse von a modulo m.

Beispiel 2.5.2 Sei $a = 35$ und $m = 111$. Mit Hilfe des erweiterten euklidischen Algorithmus berechnet man, dass $\mathrm{ggT}(a, m) = 1$. Außerdem berechnet man, dass $\mathrm{ggT}(a, m) = 1 = 6 \cdot 111 - 19 \cdot 35$. Wir schließen, dass $a^{-1} = -19 \equiv 111 - 19 = 92 \pmod{111}$.

Definition 2.5.3 Ein *reduziertes Restsystem* modulo m ist eine Menge ganzer Zahlen so, dass jede ganze Zahl, die teilerfremd zu m ist, genau zu einem Element des Restsystem kongruent ist.

Die Menge

$$\{0 < a < m \mid \mathrm{ggT}(a, m) = 1\}$$

ist ein reduziertes Restsystem.

Definition 2.5.4 Die Kardinalität eines reduzierten Restsystems modulo m bezeichnen wir mit $\varphi(m)$. Die Funktion φ heißt die *eulersche φ-Funktion*.

Beispiel 2.5.5 Die Menge

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

ist ein reduziertes Restsystem modulo 12, also ist $\varphi(12) = 4$.

Lemma 2.5.6 *Falls p eine Primzahl ist, so gilt*

$$\varphi(p) = p - 1.$$

Beweis: Falls p eine Primzahl ist, so ist $\{1, 2, \ldots, p-1\}$ ein reduziertes Restsystem. □

Satz 2.5.7 (Euler) *Sei a eine ganze Zahl mit $\mathrm{ggT}(a, m) = 1$. Es gilt*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Beweis: Setze $t = \varphi(m)$. Sei $\mathcal{R} = \{r_1, \dots r_t\}$ ein reduziertes Restsystem modulo m und sei a wie in der Aussage des Satzes. Wir betrachten die Menge

$$A = \{ar_1, \dots ar_t\}.$$

Da $\text{ggT}(a, m) = 1$, so ist $ar_i \equiv ar_j \pmod{m}$ genau dann, wenn $r_i \equiv r_j \pmod{m}$ (Satz 2.1.5). Also sind die Elementen der Menge A alle teilerfremd zu m und paarweise verschieden (modulo m). Die Kardinalität von A ist $t = \varphi(m)$, also ist A auch ein reduziertes Restsystem modulo m. Es folgt daher, dass

$$\prod_{i=1}^{t} r_i \equiv \prod_{i=1}^{t} (ar_i) \equiv a^t \prod_{i=1}^{t} r_i \pmod{m}.$$

Da $\prod_{i=1}^{t} r_i$ teilerfremd zu m ist, so folgt, dass $a^t \equiv 1 \pmod{m}$. □

Folgendes Korollar des Satzes von Euler ist bekannt als der kleine Satz von Fermat. Im Gegensatz zum "großen" Satz von Fermat (siehe Einleitung) wurde diese Aussage von Fermat bewiesen.

Korollar 2.5.8 (Der kleine Satz von Fermat) *Sei p eine Primzahl und $a \in \mathbb{Z}$.*

(a) Falls $p \nmid a$, so gilt $a^{p-1} \equiv 1 \pmod{p}$.

(b) Für alle p und a gilt $a^p \equiv a \pmod{p}$.

Beweis: Teil (a) ist ein Spezialfall von Satz 2.5.7. Falls $p \nmid a$, so folgt (b) aus (a). Falls $p \mid a$, so gilt $a \equiv a^p \equiv 0 \pmod{p}$. □

Definition 2.5.9 Sei $a \in \mathbb{Z}/m\mathbb{Z}^*$. Die *Ordnung* von a modulo m ist die kleinste positive Zahl r, sodass $a^r \equiv 1 \pmod{m}$. Bezeichnung: $r = \text{ord}_m(a)$.

Beispiel 2.5.10 In Beispiel 2.5.5 haben wir gesehen, dass $\varphi(12) = 4$. Es gilt $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$. Also ist $\text{ord}_{12}(5) = \text{ord}_{12}(7) = \text{ord}_{12}(11) = 2$.

Lemma 2.5.11 *Sei $a \in \mathbb{Z}/m\mathbb{Z}^*$. Die Ordnung von a modulo m ist ein Teiler von $\varphi(m)$.*

Beweis: Sei $r = \text{ord}_m(a)$, also gilt $a^r \equiv 1 \pmod{m}$. Der Satz von Euler (Satz 2.5.7) impliziert, dass auch $a^{\varphi(m)} \equiv 1 \pmod{m}$. Wir schreiben $g := \text{ggT}(r, \varphi(m)) = xr + y\varphi(m)$. Es folgt, dass $a^g \equiv a^{rx} \cdot a^{y\varphi(m)} \equiv 1 \pmod{m}$. Da die Ordnung die kleinste positive Zahl mit dieser Eigenschaft ist, folgt $r = g$. Wir schließen, dass r ein Teiler von $\varphi(m)$. □

Beispiel 2.5.12 Sei $m = 37$. Man überprüft leicht, dass m eine Primzahl ist. Also ist $\varphi(m) = 37 - 1 = 36 = 2^2 \cdot 3^2$ (Lemma 2.5.6). Wir berechnen $\text{ord}_m(8)$. Lemma 2.5.11 sagt uns, dass $\text{ord}_m(8) \in \{2, 3, 4, 6, 9, 12, 18, 36\}$ ist. Da

$8^2 \equiv 27 \pmod{37}$, $8^3 = 8^2 \cdot 8 \equiv 31 \pmod{37}$, $8^4 = (8^2)^2 \equiv 26 \pmod{37}$,

$8^6 = 8^4 \cdot 8^2 \equiv 36 \equiv -1 \pmod{37}$, $8^9 = 8^6 \cdot 8^3 \equiv -31 \equiv 6 \pmod{37}$,

$8^{12} = (8^6)^2 \equiv 1 \pmod{37}$.

Wir schließen, dass $\mathrm{ord}_{37}(8) = 12$.

Wir möchten nun $8^{1111} \pmod{37}$ berechnen. Wir bemerken dazu, dass $1111 = 92 \cdot 12 + 7$ ist. (Dies ist Division mit Rest). Da die Ordnung von 8 (modulo 37) gleich 12 ist, gilt

$$8^{1111} = 8^{92 \cdot 12} \cdot 8^7 = (8^{12})^{92} \cdot 8^7 \equiv 8^6 \cdot 8 \equiv -8 \equiv 1 \cdot 8^7 \equiv 29 \pmod{37}.$$

Lemma 2.5.13 *Sei n eine natürliche Zahl. Es gilt, dass*

$$\sum_{d|n} \varphi(d) = n.$$

Beweis: Sei $\mathcal{M} := \{1, \ldots, n\}$. Wir definieren

$$\mathcal{C}_d = \{a \in \mathcal{M} \mid \mathrm{ggT}(a, n) = d\} \subset \mathcal{M}.$$

Offensichtlich ist $\mathcal{C}_d \cap \mathcal{C}_{d'} = \emptyset$ für $d \neq d'$. Also ist

$$\mathcal{M} = \coprod_{d|n} \mathcal{C}_d$$

die disjunkte Vereinigung der $\mathcal{C}_d$s.

Lemma 1.1.8.(c) sagt, dass $\mathrm{ggT}(a, n) = d$ impliziert, dass $\mathrm{ggT}(a/d, n/d) = 1$ ist. Dies impliziert, dass die Kardinalität von $\mathcal{C}_d$ gleich die Kardinalität von $\mathbb{Z}/(n/d)\mathbb{Z}^*$, also $\varphi(n/d)$, ist. Wir schließen, dass

$$n = |\mathcal{M}| = \sum_{d|n} |\mathcal{C}_d| = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$$

ist. □

2.6 Schnelle Exponentiation

Die Berechnung von $b^e \pmod{m}$ kann relativ Zeit aufwendig sein (vergleichen Sie zu Beispiel 2.5.12). Falls der Modul m klein im Vergleich zum Exponenten ist, kann man die Berechnung von $b^e \pmod{m}$ vereinfachen mit Hilfe des Satzes von Euler. Falls dies nicht der Fall ist, braucht man eine andere Idee.

Die schnelle Exponentiotion ist eine Methode zur Berechnung einer großen Potenz

$$b^e \pmod{n}.$$

Wir gehen hier wie folgt vor. **Schnelle Exponentiation**

Schritt 1. Schreibe

$$e = \sum_{i=0}^{k} e_i \cdot 2^i, \qquad e_i \in \{0, 1\}.$$

Dies ist die binäre Entwicklung von e. Die e_i's berechnet man induktiv mit folgendem Algorithmus.

Algorithmus 2.6.1 (Binäre Entwicklung berechnen) Setze $i = 0$.

(a) Falls e ungerade ist, so ist $e_i = 1$. Ersetzte e durch $(e-1)/2$. Falls e gerade ist, ersetzte e durch $e/2$.

(b) Ersetze i durch $i + 1$ und wiederhole Schritt (b) bis $e = 0$.

Beispiel 2.6.2 Sei zum Beispiel $e = 73$. Da e ungerade ist, ist $e_0 = 1$. Wir sehen, dass $(e-1) = 2^3 \cdot 9$. Dies impliziert, dass $e_1 = e_2 = 0$ und $e_3 = 1$. Da $9 - 1 = 8 = 2^3 \cdot 1$ ist, finden wir $e_4 = e_5 = 0$ und $e_6 = 1$. Wir finden nun

$$73 = 1 + 2^3(1 + 2^3) = 1 + 2^3 + 2^6.$$

Schritt 2. Nun berechnen wir

$$b^{2^i} \pmod{n},$$

für alle $i = 1, \ldots, k$. Hierbei benutzen wir, dass

$$b^{2^{i+1}} = b^{2^i \cdot 2} = (b^{2^i})^2.$$

Schritt 3. Wir bemerken, dass

$$b^e = b^{\sum_i e_i \cdot 2^i} = \prod_{i=1}^{k} b^{2^i \cdot e_i} = \prod_{i : e_i \neq 0} b^{2^i}.$$

Mit dieser letzten Formel berechnen wir nun $b^e \pmod{n}$.

Beispiel 2.6.3 Wir berechnen $6^{73} \pmod{100}$. Beispiel 2.6.2 impliziert, dass wir $6^{2^i} \pmod{100}$ berechnen sollen, für $i = 1, 2, \ldots, 6$. Wir finden:

$$6^2 \equiv 36 \pmod{100}, \qquad 6^{2^2} \equiv (6^2)^2 \equiv -4 \pmod{100},$$
$$6^{2^3} \equiv (6^{2^2})^2 \equiv (-4)^2 \equiv 16 \pmod{100}, \qquad 6^{2^4} \equiv (16)^2 \equiv 56 \pmod{100},$$
$$6^{2^5} \equiv (56)^2 \equiv 36 \pmod{100}, \qquad 6^{2^6} \equiv (36^2) \equiv -4 \pmod{100}.$$

Daher gilt:

$$6^{73} \equiv 6^1 \cdot 6^{2^3} \cdot 6^{2^6} \equiv 6 \cdot 16 \cdot (-4) \equiv 16 \pmod{100}.$$

Wir bemerken, dass wir jetzt $6 + 2 = 8$ Multiplikationen gebraucht haben. Falls wir $6^{73} = 6 \cdot 6 \cdot 6 \cdots 6 \pmod{n}$ berechnet hätten und in jedem Schritt modulo n gerechnet hätten, hätten wir 72 Multiplikationen gebraucht, also deutlich mehr! Die schlechteste Strategie wäre einfach 6^{73} zu berechnen und erst im allerletzten Schritt modulo 100 zu rechnen: 6^{73} ist eine Zahl mit 57 Dezimalstellen. Mit einem Taschenrechner kann man diese Zahl nicht einfach ausrechnen. Maple hat damit natürlich noch kein Problem. Man stellt leicht fest, dass falls der Exponent e mindestens 6 Dezimalstellen hat, Maple auch nicht mehr alle Dezimalstellen von b^e angibt. Der obige Algorithmus funktioniert aber trotzdem noch, da alle Zwischenschritte viel kleinere Zahlen ergeben.

2.7 Der chinesische Restsatz

Im § 2.1 haben wir lineare Kongruenzen gelöst. In diesem Abschnitt betrachten wir Systeme von linearen Kongruenzen. Eine solche Aufgabe wurde zuerst in dem Buch *Zhang Qiujians mathematisches Handbuch*, rund 400 n. Chr.) von dem chinesischen Mathematiker Zhang Qiujian gelöst. Für mehr Information siehe `http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Chinese_overview.html` (the MacTutor History of Mathematics archive).

Theorem 2.7.1 (Der chinesische Restsatz) *Seien $m_1, \ldots, m_r \in \mathbb{N}$ Moduli mit $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i \neq j$ und $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig. Setze $m := m_1 \cdots m_r$.*

(a) Es existiert ein $x \in \mathbb{Z}$, sodass $x \equiv a_i \pmod{m_i}$ für alle i.

(b) Die Lösung x wie in (a) is eindeutig (modulo m).

Beweis: Wir definieren $M_j = m/m_j$. Es gilt $\mathrm{ggT}(m_j, M_j) = 1$, also existiert ein $\bar{M}_j \in \mathbb{Z}$, sodass $M_j \cdot \bar{M}_j \equiv 1 \pmod{m_j}$ (Korollar 2.1.6).

Wir definieren

$$x = \sum_{j=1}^{r} M_j \bar{M}_j a_j. \tag{8}$$

Für $i \neq j$ gilt

$$M_j \equiv \frac{m}{m_j} \equiv 0 \pmod{m_i},$$

da $m_i \mid m$. Also schließen wir, dass

$$x \equiv M_j \bar{M}_j a_j \equiv 1 \cdot a_j \pmod{m_j}$$

ist. Wir haben gezeigt, dass x eine Lösung des Systems von Kongruenzen ist.

Wir überprüfen nun noch die Eindeutigkeit der Lösung (modulo m). Sei $y \in \mathbb{Z}$ eine andere Lösung . Da $x \equiv y \equiv a_i \pmod{m_i}$, ist m_i ein Teiler von $x - y$, für alle i. Da die m_i paarweise teilerfremd sind, ist auch $m = m_1 \cdots m_r$ ein Teiler von $x - y$. Wir schließen, dass $x \equiv y \pmod{m}$ ist. □

Beispiel 2.7.2 Wir betrachten die Kongruenzen

$$\begin{cases} x \equiv 2 \pmod{20}, \\ x \equiv 6 \pmod{9}, \\ x \equiv 5 \pmod{7}. \end{cases}$$

Es ist $M_1 = 9 \cdot 7 = 63$, $M_2 = 20 \cdot 7 = 140$, $M_3 = 20 \cdot 9 = 180$ und $m = 20 \cdot 9 \cdot 7 = 1260$. Da $M_1 = 63 \equiv 3 \pmod{20}$ und $3 \cdot 7 \equiv 1 \pmod{20}$ folgt, dass $\bar{M}_1 \equiv 7 \pmod{20}$ ist. Ebenso berechnen wir, dass $\bar{M}_2 \equiv 2 \pmod{9}$ und $\bar{M}_3 = 3 \pmod{7}$. Die Gleichung (8) impliziert daher, dass

$$x = \sum_{j=1}^{3} M_j \cdot \bar{M}_j \cdot a_j = 63 \cdot 7 \cdot 2 + 140 \cdot 2 \cdot 6 + 180 \cdot 3 \cdot 5 = 5262 \equiv 222 \pmod{m}$$

eine Lösung des Systems von Kongruenzen ist.

Alternativ kann man die Lösung x auch wie folgt (durch ausprobieren) berechnen. Die erste Kongruenz sagt uns, dass die gesuchte Lösung von der Form $x = 2 + 20 \cdot i$ ist. Wir versuchen nun die Werte $i = 1, 2, 3, \ldots$ und finden, dass $x = 2 + 20 \cdot 2 = 42 \equiv 6 \pmod 9$ ist. Wir wissen nun also, dass $x = 42 + j \cdot 20 \cdot 9$ ist für eine ganze Zahl j. Wir versuchen die Werte $j = 1, 2, 3, \ldots$, und finden, dass

$$x = 42 + 1 \cdot 180 = 222 \equiv 5 \pmod 7$$

ist. Die gesuchte Lösung ist also $x = 42 + 180 = 222$.

Das folgende Beispiel illustriert, was passiert wenn die Moduln m_i nicht paarweise teilerfremd sind.

Beispiel 2.7.3 (a) Wir betrachten die Kongruenzen

$$\begin{cases} x \equiv 2 \pmod{10}, \\ x \equiv 3 \pmod{14}. \end{cases}$$

Da $\text{ggT}(10, 14) = 2$ ist, liefern beide Kongruenzen eine Kongruenz modulo 2. Die erste Kongruenz liefert $x \equiv 0 \pmod 2$. Die zweite Kongruenz liefert $x \equiv 1 \pmod 2$. Da $1 \not\equiv 0 \pmod 2$, schließen wir, dass das System von Kongruenzen keine Lösung besitzt.

(b) Wir betrachten jetzt die Kongruenzen

$$\begin{cases} x \equiv 3 \pmod{45}, \\ x \equiv 7 \pmod{756}. \end{cases}$$

Nun ist $\text{ggT}(45, 756) = 3^2$. Da $7 \not\equiv 3 \pmod 9$ ist, so besitzt das System von Kongruenzen keine Lösung.

Allgemein gibt es zwei Möglichkeiten für Kongruenzen mit nicht-teilerfremden Moduln:

(I) Die Kongruenzen widersprechen sich. In diesem Fall gibt es keine Lösung. Dies kann man feststellen, indem man die induzierten Kongruenzen modulo den ggT der Moduln berechnet (wie in Beispiel 2.7.3).

(II) Die Kongruenzen widersprechen sich nicht. In diesem Fall kann man das System von Kongruenzen ersetzen durch ein äquivalentes System von Kongruenzen mit paarweise teilerfremden Moduli (siehe Beispiel 2.7.4).

Beispiel 2.7.4 Wir betrachten

$$\begin{cases} x \equiv 7 \pmod{200}, \\ x \equiv 82 \pmod{375}. \end{cases}$$

Wir finden, dass $\mathrm{ggT}(200, 375) = 5^2$ und $200 \equiv 5^2 \cdot 8$ und $375 = 5^3 \cdot 3$. Da $7 \equiv 82 \pmod{25}$, ist das System von Kongruenzen konsistent. Der chinesische Restsatz impliziert, dass die erste Kongruenz äquivalent ist zu

$$x \equiv 7 \pmod{5^2} \qquad \text{und} \qquad x \equiv 7 \pmod{8}.$$

Die zweite Kongruenz ist äquivalent zu

$$x \equiv 82 \pmod{5^3} \qquad \text{und} \qquad x \equiv 82 \equiv 1 \pmod{3}.$$

Insgesamt ist das System von Kongruenzen äquivalent zu

$$\begin{cases} x & \equiv 82 \pmod{5^3}, \\ x & \equiv 7 \pmod{8}, \\ x & \equiv 1 \pmod{3}. \end{cases}$$

Mit der Methode des Beweises von Theorem 2.7.1 überprüft man, dass $x \equiv 1207 \pmod{5^3 \cdot 8 \cdot 3}$ eine Lösung des Systems ist. Man bemerke, dass das System von Kongruenzen eine eindeutige Lösung modulo $5^3 \cdot 8 \cdot 3 = 3000$ statt modulo $200 \cdot 375 = 75000$ hat.

Satz 2.7.5 (Multiplikativität der φ-Funktion) *(a) Seien $m_1, m_2 \in \mathbb{N}$ teilerfremd. Es gilt*

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2).$$

(b) Sei p eine Primzahl. Für alle $r \geq 1$ gilt, dass

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

(c) Sei $n = \prod_i p_i^{n_i}$ die Primfaktorzerlegung von n mit p_i paarweise teilerfremd. Es gilt

$$\varphi(n) = \prod_i p_i^{n_i - 1}(p_i - 1) = n \prod_{p \mid n} (1 - \frac{1}{p}).$$

Beweis: Sei $m = m_1 m_2$ mit $\mathrm{ggT}(m_1, m_2) = 1$. Wir definieren die Abbildung

$$\begin{aligned} \Phi : \mathbb{Z}/m\mathbb{Z}^* &\to \mathbb{Z}/m_1\mathbb{Z}^* \times \mathbb{Z}/m_2\mathbb{Z}^* \\ a \pmod{m} &\mapsto (a \pmod{m_1}, a \pmod{m_2}). \end{aligned}$$

Da a genau dann teilerfremd zu m ist, wenn $\mathrm{ggT}(a, m_1) = \mathrm{ggT}(a, m_2) = 1$, ist Φ wohldefiniert. Der chinesische Restsatz (Theorem 2.7.1) impliziert, dass Φ eine Bijektion ist. Teil (a) folgt.

Für (b) bemerken wir, dass $0 < a < p^r$ genau dann teilerfremd zu p^r ist, wenn a teilerfremd zu p ist, also genau dann wenn $p \mid a$. Durch Abzählen findet man, dass genau p^{r-1} Zahlen zwischen 0 und p^r teilbar durch p sind. Also ist $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Teil (c) folgt aus (a) und (b). □

Beispiel 2.7.6 Da $n = 375 = 5^3 \cdot 3$ finden wir, dass

$$\varphi(375) = \varphi(125) \cdot \varphi(3) = 5^2 \cdot 4 \cdot 2 = 200.$$

Alternativ gilt auch

$$\varphi(375) = 375 \cdot (1 - \frac{1}{5})(1 - \frac{1}{3}) = 375 \cdot 4 \cdot 2/15 = 200.$$

3 Kryptographie

Ziel der Kryptographie ist es, eine geheime Botschaft zu verschicken über einen unsicheren Kanal, sodass nur der beabsichtigte Empfänger die Botschaft lesen kann. Dieses Problem beschäftigt Menschen schon seit Jahrtausenden: Das erste Kryptoverfahren, das wir besprechen, wurde von Julius Ceasar benutzt um mit seinen Offizieren zu kommunizieren. Mit der Zunahme des modernen Datenverkehr im Internet, ist die Kryptographie immer wichtiger geworden: eBay und Amazon, wären ohne Kryptographie unmöglich.

Wir führen zuerst einige Begriffe ein. Der *Klartext* ist die eigentliche Nachricht. Die *Verschlüsselung* ändert die Nachricht in einen *Geheimtext* oder eine verschlüsselte Nachricht. Die verschlüsselte Nachricht wird von dem Empfänger *entschlüsselt*. Zum Ver- und Entschlüsseln braucht man in der Regel einen *Schlüssel*.

3.1 Die Caesar-Chiffre

Als Einführung in die Kryptographie besprechen wir in diesem Abschnitt ein sehr altes Kryptoverfahren: Die Caesar-Chiffre. Diese wurde von Julius Caesar benutzt um mit seinen Offizieren zu kommunizieren.

Wir fangen damit an, dass wir jedem Buchstaben eine Zahl zuordnen, wie im folgenden Schema.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
p	q	r	s	t	u	v	w	x	y	z				
15	16	17	18	19	20	21	22	23	24	25				

(9)

Man kann wahlweise den Lesezeichen und den Lehrzeichen auch eine Zahl zuordnen. Wir machen dies hier nicht. Wir machen auch keinen Unterschied zwischen Groß- und Kleinbuchstaben.

Wir möchten nun den Klartext in einen Geheimtext verschlüsseln. Dies machen wir, in dem wir jeden Buchstaben des Klartextes einen neuen Buchstaben des Geheimtextes mittels folgender Vorschrift zuordnen

$$C \equiv B + 3 \pmod{26}, \tag{10}$$

hierbei ist B ein Buchstabe der Nachricht und C ein Buchstabe der verschlüsselten Nachricht. Die Zahl C wird dann mit (9) wieder in eine Buchstabe umgewandelt. Der Effekt ist also, dass jede Buchstabe um 3 verschoben wird: A wird D, B wird E und so weiter.

Zum Entschlüsseln muss man nur das Verfahren umkehren.

Beispiel 3.1.1 Die Verschlüsselung der Nachricht

Es gibt Kuchen

ist

hvjlewnxfkhq.

Eine Verallgemeinerung der Caesar-Chiffre sind die sogenannte affine Chiffren. Diese funktionieren sehr ähnlich wie die Caesar-Chiffre: Auch hier werden einzelne Buchstaben andere Buchstaben zugeordnet. Wir ordnen wieder die Buchstaben einer Zahl zu, wie oben. Statt (10) benutzen wir nun die Vorschrift

$$C \equiv aB + d \pmod{26}, \tag{11}$$

wonach wir die neue Zahl wieder in einen Buchstaben zurückwandeln. Die Zahlen (a, d) sind der *Schlüssel* des Chiffrierverfahrens. Die Caesar-Chiffre hat den Schlüssel $(1, 3)$. Allgemeiner heißt eine affine Chiffre mit Schlüssel $(1, k)$ eine *Verschiebechiffre*: Die Buchstaben werden um k verschoben.

Beispiel 3.1.2 Als Beispiel nehmen wir $a = 7$ und $d = 10$. Die Zuordnung der Buchstaben wird nun:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
k	r	y	f	m	t	a	h	o	v	c	j	q	x	e	l	s
r	s	t	u	v	w	x	y	z								
z	g	n	u	b	i	p	w	d								

(12)

Zum Beispiel, der Buchstabe l hat die Nummer 11. Da $7 \cdot 11 + 10 = 87 \equiv 9 \pmod{26}$ wird l verschlüsselt zu j, und so weiter.

Die geheime Nachricht

fkgglomjognkug

ist entschlüsselt

dasspielistaus.

Ein Schlüssel (a, d) liefert nur dann eine gültiges Chiffrierverfahren, wenn die Abbildung (11) bijektiv ist.

Lemma 3.1.3 *Das Chiffrierverfahren (11) mit Schlüssel (a, d) ist genau dann bijektiv, wenn* $\mathrm{ggT}(a, 26) = 1$ *ist.*

Beweis: Übungsaufgabe. □

Wie sicher sind diese Schlüsseln? Offensichtlich nicht sehr sicher. Nehmen wir an, unsere kleine Schwester hat ihren heimlichen Idol einen Liebesbrief geschrieben und dieser mit einem affinen Schlüssel verschlüsselt. Wir haben den Brief gefunden. Wie schwierig ist es den Brief zu entschlüsseln? Es gibt nur 26 Möglichkeiten für d und $26 - 13 - 2 = 11$ Möglichkeiten für a (Lemma 3.1.3), also insgesamt $26 \cdot 11 = 286$ mögliche affine Schlüsseln. Mit einem Rechner kann man leicht alle Schlüseln durchprobieren. Aber auch ohne Rechner ist es leicht den Schlüssel zu knacken. Der Schwachstelle des affinen Schlüssels ist nämlich, dass jeder Buchstabe einem festen Buchstaben zugeordnet wird. Es ist bekannt, welche Buchstaben am häufigsten vorkommen, zum Beispiel ist e der häufigste Buchstabe. Dies kann man benutzen um zu raten zu welchem Buchstaben e verschlüsselt wird. Nach und nach kann man nun weitere Buchstaben raten.

Hier finden Sie die Häufigkeit (in Prozenten) der Buchstaben in der Deutsche Sprache:

A	B	C	D	E	F	G	H	I	J	K
6,51	1,89	3,06	5,08	17,4	1,66	3,01	4,76	7,55	0,27	1,21
L	M	N	O	P	Q	R	S	T	U	V
3.44	3,53	9,78	2,52	0,79	0,02	7,00	7,27	6,15	4,35	0,67
W	X	Y	Z							
1,89	0,03	0,04	1,13							

Quelle: `http://weddige.eu/tools/kryptix/` . Diese Seite hat auch ein kleines Programm das Verschiebechiffren knacken kann.

3.2 Das RSA-Verfahren

Die Caesar-Ciffre aus § 3.1 ist ein Beispiel eines *symmetrischen Schlüsselverfahrens*: Jeder der verschlüsseln kann, kann auch entschlüsseln. Anders gesagt, der gleiche Schlüssel wird sowohl benutzt um zu verschlüsseln als auch um zu entschlüsseln. Da jeder, der den Schlüssel besitzt, symmetrische Schlüsselverfahren sowohl verals auch entschlüsseln kann, müssen sich Sender und Empfänger des Geheimtextes auf einen Schlüssel geeinigt haben. In modernen Internetanwendungen ist dies oft unmöglich: Man bräuchte dafür einen zweiten sicheren Kommunikationskanal, das, anders als das Internet, nicht abgehört werden kann.

Um dieses Problem zu umgehen benutzt man *asymmetrische Schlüsselverfahren* oder auch Public-Key-Kryptosysteme. Diese Systeme benutzen zwei verschiedene Schlüssel: Ein *öffentlichen Schlüssel* (oder: public key), den jeder benutzen kann um Nachrichten zu verschlüsseln. Der zweite Schlüssel ist der *private Schlüssel* (oder: private key). Nur wer den privaten Schlüssel kennt, kann den Geheintext entschküsseln.

In diesem Abschnitt besprechen wir das RSA-Verfahren. Es wurde in den siebziger Jahren des 20ten Jahrhunderts von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt und von ihnen auch patentiert (siehe `www.RSA.com`). Das Kryptosystem benutzt modulares Potenzieren (§ 2.6).

Der öffentliche Schlüssel besteht aus einen Exponenten e und einen Modulus n, welcher ein Produkt $n = pq$ zweier großen Primzahlen p und q ist. Außerdem gilt, dass $\mathrm{ggT}(e, \varphi(n)) = 1$ ist. Es ist nur n öffentlich bekannt, nicht die Primfaktorzerlegung von n. Da $n = pq$ das Produkt zweier Primzahlen ist, folgt aus Satz 2.7.5, dass $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Schritt 1: Vorbereitung: Zum Verschlüsseln wandeln wir den Klartext in eine Zahlenfolge um (A=00, B=01, ..., Z=25). Dann teilen wir die Nachricht in Blöcke gleicher, vorgegebener, gerader Länge ein. Falls der letzte Block nicht voll ist, ergänzen wir mit Dummies: Ein Dummy entspricht den Wert 26.

Als Beispiel betrachten wir die Nachricht "Hilfe" und nehmen Blöcke der Länge 4. Wir bekommen also die folgenden 3 Blöcke:

$$0708 \quad 1105 \quad 0426. \tag{13}$$

Schritt 2: Verschlüsseln: Der *öffentliche Schlüssel* besteht aus zwei Zahlen (e, n), wobei $n = pq$ das Produkt von 2 großen Primzahlen ist und wobei $\mathrm{ggT}(e, \varphi(n)) = 1$ gilt. Wir bemerken, dass nur n bekannt ist und nicht seine Primfaktorzerlegung.

Ein Block B des Klartextes wird nun mit folgender Vorschrift verschlüsselt:

$$C \equiv B^e \pmod{n}. \tag{14}$$

Wir bemerken, dass n größer als der größte mögliche Block sein soll. In diesem Skript nehmen wir einfachheitshalber Blöcke der Länge 4. Der größte Block ist daher Z+Dummy also 2526. Wir brauchen daher $n > 2526$. In der Praxis braucht man natürlich eine viel größere Schlüssellänge.

Schritt 3: Entschlüsseln: Der *private Schlüssel* ist (d, n), wobei d die Inverse von e modulo $\varphi(n)$ ist. Ist $\varphi(n)$ bekannt, kann man d mit Hilfe des erweiteren euklidischen Algorithmus (Lemma 1.1.9) berechnen. Zum Entschlüsseln berechnen wir nun

$$D(C) \equiv C^d \pmod{n} \tag{15}$$

Um zu sehen, dass wir die Nachricht entschlüsselt haben, schreiben wir $de = 1 + k\varphi(n)$. Der Satz von Euler (Satz 2.5.7) sagt, dass $B^{\varphi(n)} \equiv 1 \pmod{n}$ ist, falls B und n teilerfremd sind. In diesem Fall gilt daher, dass

$$D(C) \equiv C^d \equiv B^{de} = B^{1+k\varphi(n)} = B \cdot (B^{\varphi(n)})^k \equiv B \pmod{n}.$$

Also haben wir die Nachricht B entschlüsselt. Die Wahrscheinlichkeit, dass n und B nicht teilerfremd sind, ist sehr klein: Wir können diese Möglichkeit ignorieren.

Beispiel 3.2.1 (a) Wir verschlüsseln die Nachricht (13) mit Hilfe des Schlüssels $n = 3127$ und $e = 17$:

$$(0708)^{17} \equiv 1357 \pmod{3127}, \quad (1105)^{17} \equiv 3047 \pmod{3127},$$
$$(0426)^{17} \equiv 1222 \pmod{3127}.$$

Der Geheimtext ist daher:

$$1357\ 3047\ 1222.$$

(b) Wir haben den Geheimtext

$$1767 \quad 1087 \quad 0032$$

abgefangen. Der öffentliche Schlüssel ist $(e = 13, n = 2537)$. Um den Code zu knacken, berechnen wir das Inverse von e modulo $\varphi(n)$. Hierzu brauchen wir zuerst $\varphi(n)$. Dies können wir berechnen mit Hilfe von Satz 2.7.5. Hierzu brauchen wir die Primfaktorzerlegung von n. Mit Probedivision (§ 1.3) finden wir, dass $n = 2537 = 43 \cdot 59$. Also folgt, dass $\varphi(n) = (43-1)(59-1) = 2436$.

Wir berechnen $d \equiv e^{-1} \pmod{\varphi(n)}$ mit Hilfe des erweiteren euklidischen Algorithmus. Der erweiterte euklidische Algorithmus liefert uns ganze Zahlen x, y mit $x\varphi(n) + ye = 1$. Da $d = y$ brauchen wir x nicht zu berechnen. Wir finden

i	a_i	q_i	y_i
-1	2436	$-$	0
0	13	$-$	1
1	5	187	-187
2	3	2	375
3	2	1	-562
4	1	1	$\boxed{937}$

Also ist $d = 937$.

Wir entschlüsseln den Geheimtext und finden:

$$(1767)^d \equiv 0613 \pmod{n} \quad (1087)^d \equiv 0003 \pmod{n}, \quad (0032)^d \equiv 0426 \pmod{n}.$$

Die Klartext ist daher: Gnade. Wir beachten, dass die letzten zwei Zahlen ein Dummy darstellen.

Wir haben jetzt gesehen, wie man mit Hilfe des RSA-Verfahern ver- und entschlüsselt. Aber wieso funktioniert die Methode? Die grundlegende Idee ist, dass es einfach ist ein Schlüssel zu bauen und ver- und entschlüsseln schnell geht, aber, dass es schwierig ist ein Code zu knacken.

Um einen Schlüssel zu bauen braucht man zwei große Primzahlen p und q. Im Prinzip könnte man dies mit Hilfe des Siebes von Eratosthenes (Algorithmus 1.3.3) machen. Die aktuelle minimale Sicherheitsstandards schreiben eine Schlüssellänge von 1024 Bits vor, d.h., dass $n \cong 2^{1024}$ ist: Dies ist eine Zahl mit 308 Dezimalstellen. Falls n also das Produkt von 2 ungefähr gleich großen Primzahlen p und q ist, sind p, q Zahlen mit ungefähr 154 Dezimalstellen. Es ist klar, dass wir solche große Primzahlen nicht mit Hilfe des Siebs von Eratosthenes finden möchten. Wie wir dies trotzdem machen können, lernen wir im nächsten Abschnitt (§ 3.3).

Eine andere Anforderung an einen praktikablen Kryptosystem ist, dass das Ver- und Entschlüsseln relativ schnell geht. Zum Ver- und Entschlüsseln muss

man Potenzen modulo n berechnen. Dies macht man mit schneller Exponentiation (§ 2.6).

Wir schauen uns das Knacken eines Codes etwas genauer an (siehe Beispiel 3.2.1.(b)). Der öffentliche Schlüssel (e, n) ist bekannt. Um den Geheimtext zu entschlüsseln, müssen wir aus e und n die Zahl d berechnen. Hierzu brauchen wir $\varphi(n)$. Lemma 3.2.2 sagt uns, dass die Berechung von $\varphi(n)$ äquivalent ist zur Berechnung der Primfaktorzerlegung von n, also zur Berechnung von p und q. Die Sicherheit des RSA-Verfahrens beruht daher darauf, dass es schwierig ist die Primfaktorzerlegung einer großen Zahl zu finden.

Lemma 3.2.2 *Gegeben ist eine RSA-Zahl n. Die Berechnung von $\varphi(n)$ ist äquivalent zur Berechnung der Primfaktorzerlegung $n = p \cdot q$.*

Beweis: So bald wir die Primfaktorzerlegung $n = p \cdot q$ von n gefunden haben, kennen wir auch $\varphi(n) = (p-1)(q-1)$.

Umgekehrt, falls wir n und $\varphi(n) = (p-1)(q-1)$ kennen, kennen wir auch

$$n + 1 - \varphi(n) = pq + 1 - (p-1)(q-1) = p + q$$

und

$$\sqrt{(p+q)^2 - 4n} = \sqrt{p^2 + 2pq + q^2 - 4pq} = \sqrt{(p-q)^2} = |p-q|.$$

Einfachheitshalber nehmen wir an, dass $p \geq q$ ist, dann gilt $|p-q| = p-q$. Wir kennen nun auch

$$p = \frac{1}{2}[(p+q) + (p-q)] \quad \text{und} \quad q = \frac{1}{2}[(p+q) - (p-q)].$$

□

Zahlen, die das Produkt zweier großen Primzahlen sind, heißen RSA-Zahlen. Die größte faktorisierte RSA-Zahl besitzt 200 Dezimalziffern (663 Bits) (Stand: May 2008). Die RSA-Firma, die das Patent auf RSA besitzt, vergab bis vor kurzen Geldpreisen von bis zu $100.000 für das Faktorisieren von RSA-Zahlen. Dies machten sie, um auf dem Laufenden zu bleiben über die schnellsten Faktorisierungstechniken. Diese Herausforderung ist aktuel zurückgezogen. Mehr Informationen über das Faktorisieren von Primzahlen und wie Sie Ihren Rechner mithelfen lassen können neue Rekorde zu brechen, finden Sie auf der Webseite: `http://primes.utm.edu/`.

3.3 Primzahltests

Das RSA-Verfahren basiert auf der Tatsache, dass es viel einfacher ist zu testen ob eine Zahl (wahrscheinlich) prim ist als die vollständige Primfaktorzerlegung zu finden. Um einen privaten Schlüssel füre das RSA-Verfahren zu bauen, sucht man 2 große Primzahlen p und q. Um den RSA-Verfahren zu knacken, muss man die Primfaktorzerlegung des öffentlichen Schlüssels n finden.

In diesem Abschnitt besprechen wir, wie man große Primzahlen konstruiert. Genauer gesagt, besprechen wir Tests, die uns sagen ob eine gegebene natürliche Zahl wahrscheinlich eine Primzahl ist, oder nicht. Hierzu benutzen wir den kleinen Satz von Fermat (Korollar 2.5.8). Dieser sagt uns, dass falls p eine Primzahl ist, so gilt für alle $b \in \mathbb{N}$, dass

$$b^p \equiv b \pmod{p} \tag{16}$$

ist. Wenn wir also eine Zahl b finden, sodass $b^n \not\equiv b \pmod{n}$, so ist n auf jeden Fall keine Primzahl. Dies ist unser erster *Primzahltest*: Gegeben ist eine Zahl n, von der wir wissen möchten ob sie eine Primzahl ist. Wir wählen eine Basis b und berechnen $b^n \pmod{n}$. Falls $b^n \not\equiv b \pmod{n}$, so ist n keine Primzahl. Falls $b^n \equiv b \pmod{n}$, so könnte n eine Primzahl sein. Wir untersuchen nun, wie sicher wir uns sein können, dass n tatsächlich eine Primzahl ist.

Definition 3.3.1 Eine natürliche Zahl $n > 1$ heißt *Pseudoprimzahl zur Basis* b, falls n zusammengesetzt ist und $b^n \equiv b \pmod{n}$ gilt.

Beispiel 3.3.2 Wir fragen uns ob $n = 123456791$ und $m = 123456793$ Primzahlen sind. Wir könnten dies natürlich mit Hilfe der Probedivision (§ 1.3) machen. Falls n und m Primzahlen wären, müssten wir $\sqrt{n} \cong 11111$ Divisionen mit Rest durchführen.

Wir berechnen mit schnellen Exponentiation (§ 2.6), dass

$$2^{123456791} \equiv 2 \pmod{123456791}, \text{ und } 2^{123456793} \equiv 8474892 \pmod{123456793}.$$

Also ist $m = 123456793$ auf jeden Fall keine Primzahl. Die Zahl $n = 123456791$ ist entweder eine Pseudoprimzahl zur Basis 2 oder eine Primzahl. Es stellt sich heraus, dass 123456791 tatsächlich eine Primzahl ist.

Beispiel 3.3.3 Die kleinste Pseudoprimzahl zur Basis $b = 2$ ist $n = 341$. Es gilt, nämlich, dass $n = 11 \cdot 31$, also ist n zusammengesetzt. Außerdem gilt, dass $2^{341} \equiv 2 \pmod{341}$. Die einzige andere Pseudoprimzahlen zur Basis $b = 2$ kleiner als 1000 sind $561 = 3 \cdot 11 \cdot 17$ und $645 = 3 \cdot 5 \cdot 43$.

Wir fragen uns ob, und wenn ja wie viele, Pseudoprimzahlen n zur Basis b es gibt, also Zahlen die die Kongruenz (16) erfüllen, obwohl sie zusammengesetzt sind. Die folgende Tabelle zeigt wie oft dies passiert für die Basis $b = 2$. Da 2 die einzige gerade Primzahl ist, ignorieren wir die gerade Zahlen.

Anzahl der ungeraden Pseudoprimzahlen $< 10^3$	3
Anzahl der Primzahlen $< 10^3$	168
Anzahl der ungeraden Pseudoprimzahlen $< 10^6$	245
Anzahl der Primzahlen $< 10^3$	78498

Die Tabelle zeigt, dass die Anzahl der ungeraden Pseudoprimzahlen zur Basis $b = 2$ klein ist im Vergleich zur Anzahl der Primzahlen. Falls $2^n \equiv 2 \pmod{n}$ ist, so ist die Wahrscheinlichkeit daher groß, dass n eine Primzahl ist. Trotzdem gibt es unendlich viele Pseudoprimzahlen zur Basis 2.

Satz 3.3.4 *Es gibt unendlich viele Pseudoprimzahlen zur Basis $b = 2$.*

Beweis: Wir zeigen folgende Aussage: Falls n eine ungerade Pseudoprimzahl zur Basis $b = 2$ ist, so ist auch $m := 2^n - 1$ eine ungerade Pseudoprimzahl zur Basis $b = 2$. Da es mindestens eine ungerade Pseudoprimzahl zur Basis $b = 2$ gibt (Beispiel 3.3.3), finden wir so unendlich viele Pseudoprimzahlen zur Basis $b = 2$.

Sei n eine ungerade Pseudoprimzahl zur Basis $b = 2$. Es gilt, dass $2^n \equiv 2 \pmod{n}$. Da n ungerade ist, gilt auch $2^{n-1} \equiv 1 \pmod{n}$ (Satz 2.1.5). Da n eine Pseudoprimzahl ist, ist n zusammengesetzt. Sei $m = 2^n - 1$.

Lemma 1.2.2 impliziert, dass m zusammengesetzt ist, da n keine Primzahl ist. Wir behaupten, dass $2^m \equiv 2 \pmod{m}$ gilt. Hieraus folgt, dass m auch eine Pseudoprimzahl zur Basis $b = 2$ ist.

Da $2^n \equiv 2 \pmod{n}$, gibt es eine Zahl k mit $2^n - 2 = n \cdot k$. Also gilt

$$2^{m-1} = 2^{2^n-2} = 2^{n \cdot k}.$$

Lemma 1.2.2 impliziert, dass $m = (2^n - 1) \mid (2^{nk} - 1)$. Da $n \cdot k = m - 1$, gilt

$$2^{m-1} \equiv 1 \pmod{m}$$

und daher $2^m \equiv 2 \pmod{m}$. □

Man kann den Primzahltest wie folgt verbessern. Falls n den Primzahltest zur Basis $b = 2$ bestanden hat, so berechnen wir $3^n \pmod{n}$, $5^n \pmod{n}$, und so weiter. Zum Beispiel gilt $2^{341} \equiv 2 \pmod{341}$ aber $3^{341} \equiv 168 \not\equiv 3 \pmod{341}$. Die Zahl 341 ist daher keine Pseudoprimzahl zur Basis $b = 3$.

Leider gibt es Zahlen n, die Pseudoprimzahl sind zu alle Basen b. Egal wie viele Basen wir versuchen, wir werden mit dieser Methode nie herausfinden, dass n zusammengesetzt ist.

Definition 3.3.5 Eine zusammengesetzte Zahl $n > 1$ heißt *Carmichael-Zahl*, falls

$$b^n \equiv b \pmod{n}, \quad \text{für alle } b.$$

Lemma 3.3.6 *Die Zahl $n = 561$ ist eine Carmichael-Zahl.*

Beweis: Da $n = 561 = 3 \cdot 11 \cdot 17$ ist, so ist 561 zusammengesetzt. Wir behaupten, dass $b^{561} \equiv b \pmod{561}$ für alle b gilt. Der chinesische Restsatz sagt, dass die Kongruenz $b^{561} \equiv b \pmod{561}$ äquivalent zu dem System von Kongruenzen

$$\begin{cases} b^{561} \equiv b \pmod{3}, \\ b^{561} \equiv b \pmod{11}, \\ b^{561} \equiv b \pmod{17} \end{cases}$$

ist.

Falls $3 \mid b$, so ist gilt sicherlich, dass $b^{561} \equiv b \pmod{3}$. Nehmen wir also an, dass $3 \nmid b$. Da $561 = 1 + 2 \cdot 280$ folgt aus dem kleinen Satz von Fermat

(Korollar 2.5.8), dass $b^{561} \equiv b \cdot 1^{280} \pmod 3$ ist. Die Verifikation der beiden anderen Kongruenzen ist ähnlich. □

Der folgende Satz gibt eine Charakterisierung von Carmichael-Zahlen. Der Satz wurde in 1899 von A. Korselt bewiesen: Dies war 10 Jahren vor Carmichael die erste Beispiele von Carmichael-Zahlen gefunden hat. Korselt war sich sicher, dass solche Zahlen nicht existieren und sah seinen Satz als den ersten Schritt dies zu beweisen. Eine Zahl n heißt *quadratfrei*, falls 1 das einzige Quadrat, das n teilt, ist. Der Beweis des Satzes ist nicht sehr schwierig, aber benutzt den Begriff der Primitivwurzel, den wir erst in § 5.1 einführen werden.

Satz 3.3.7 *Sei n eine quadratfreie, zusammengesetzte, natürliche Zahl, also $n = p_1 \cdot p_2 \cdots p_r$, wobei die p_i paarweise verschiedene Primzahlen sind. Die Zahl n ist genau dann eine Carmichael-Zahl, wenn $(p_i - 1) \mid (n - 1)$ für alle i gilt.*

Mit Hilfe von Satz 3.3.7 können wir einen neuen Beweis von Lemma 3.3.6 geben. Wir haben schon gesehen, dass $561 = 3{\cdot}11{\cdot}17$, also ist $n = 561$ quadratfrei und zusammengesetzt. Da $561 - 1 = 560 = 2^4 \cdot 5 \cdot 7$ ist, folgt, dass $p - 1 \mid 560$ für $p = 3, 11, 17$. Dies zeigt erneut, dass 561 eine Carmichael-Zahl ist.

In 1910 vermutete Carmichael, dass es unendlich viele Carmichael-Zahlen gibt. Dies wurde in 1994 von W.R. Alford, A. Granville und C. Pomerance bewiesen. Obwohl es unendlich viele Carmichael-Zahlen gibt, sind diese sehr selten: Die Anzahl der Carmichael-Zahlen kleiner als $25 \cdot 10^9$ ist 2163.

Die Tatsache, dass Carmichael-Zahlen existieren, zeigt, dass unser Primzahltest noch nicht gut genug ist. Daher besprechen wir nun einen besseren Primzahltest. Dieser basiert auf folgender Beobachtung.

Lemma 3.3.8 *Sei p eine ungerade Primzahl und schreibe*

$$p - 1 = 2^s t, \qquad \text{mit } t \text{ ungerade.}$$

Sei b eine natürliche Zahl, die nicht von p teilbar ist. Es gilt

(a) entweder $b^t \equiv 1 \pmod p$,

(b) oder $b^{2^i t} \equiv -1 \pmod p$ für ein i mit $0 \le i < s$.

Beweis: Der kleine Satz von Fermat (Korollar 2.5.8) impliziert, dass $b^{p-1} \equiv 1 \pmod p$. Da $p - 1 = 2^s t$, so ist eine der Zahlen

$$b^t,\ b^{2t},\ \ldots, b^{2^{s-1}t},\ b^{2^s t}$$

kongruent zu $1 \pmod p$. Falls $b^t \equiv 1 \pmod p$, so tritt Fall (a) des Lemmas auf. Sonst existiert ein $1 \le i \le s$, sodass $b^{2^i t} \equiv 1 \pmod p$, aber $b^{2^{i-1}t} \not\equiv 1 \pmod p$ ist. Die impliziert, dass

$$p \mid (b^{2^i t} - 1) = (b^{2^{i-1}t} - 1)(b^{2^{i-1}t} + 1).$$

Da p eine Primzahl ist mit $p \nmid (b^{2^{i-1}t} - 1)$, folgt, dass $p \mid (b^{2^{i-1}t} + 1)$ (Lemma 1.2.3). Also gilt, dass $b^{2^{i-1}t} \equiv -1 \pmod p$: Fall (b) des Lemmas trifft zu. □

Definition 3.3.9 (a) Eine ungerade, zusammengesetzte Zahl n heißt *starke Pseudoprimzahl* zur Basis b, falls n teilerfremd zu b ist und die Bedingung von Lemma 3.3.8 erfüllt ist.

(b) Falls n keine starke Pseudoprimzahl zur Basis b ist, so heißt b eine *Zeuge* für n.

Beispiel 3.3.10 (a) Wir haben gesehen, dass 341 eine Pseudoprimzahl zur Basis $b = 2$ ist. Wir überprüfen, dass 341 keine starke Pseudoprimzahl zur Basis $b = 2$ ist. Wir schreiben $341 - 1 = 2^2 \cdot 85$, also ist $s = 2$ und $t = 85$. Nun gilt

$$2^{85} \equiv 32 \pmod{341} \pmod{341}, \quad 2^{2\cdot 85} \equiv 1 \pmod{341}.$$

Daher ist sowohl Lemma 3.3.8.(a) als auch Lemma 3.3.8.(b) nicht erfüllt. Wir schließen, dass 341 keine starke Pseudoprimzahl zur Basis $b = 2$ ist.

Wir bemerken, dass $2^{2\cdot 85} \equiv 1 \pmod{341}$ aber $2^{85} \not\equiv \pm 1 \pmod{341}$. Dies illustriert, dass $a^2 \equiv 1 \pmod{341}$ nicht impliziert, dass $a \equiv \pm 1 \pmod{341}$ gilt, wie im Beweis von Lemma 3.3.8. Der Grund ist, dass 341 keine Primzahl ist.

Die kleinste starke Pseudoprimzahl zur Basis $b = 2$ ist 2047.

(b) Sei $n = 91$ und $b = 10$. Wir schreiben $n - 1 = 2 \cdot 45$, also ist $s = 1$ und $t = 45$. Da

$$b^t \equiv 10^{45} \equiv -1 \pmod{91},$$

ist Lemma 3.3.8.(b) erfüllt für $i = 0$. Daher ist n eine starke Pseudoprimzahl zur Basis $b = 10$.

Theorem 3.3.11 *Sei $n > 9$ eine ungerade, zusammengesetzte Zahl. Wir definieren*

$$\mathcal{S}(n) = \{b \in (\mathbb{Z}/n\mathbb{Z})^* \mid n \text{ ist eine starke Pseudoprimzahl zur Basis } b\}.$$

Die Anzahl der Elementen von $\mathcal{S}(n)$ ist kleiner gleich $\varphi(n)/4$.

Beweis: Ein Beweis des Satzes wird zum Beispiel gegeben in [3, Satz 3.2.4]. □

Theorem 3.3.11 bedeutet also, dass mindestens 75 % der Elementen von $(\mathbb{Z}/n\mathbb{Z})^*$ Zeugen für n sind. Insbesondere, gibt es keine starke Carmichael-Zahlen. Wir können Theorem 3.3.11 benutzen um mit beliebig hoher Wahrscheinlichkeit festzustellen ob eine gegebene Zahl eine Primzahl ist. Wir haben eine Zahl n gegeben von der wir vermuten, dass sie eine Primzahl ist. Wir wählen nun zufällig 100 beliebige Basen b mit $0 < b < n$ und überprüfen ob n eine starke Pseudoprimzahl zur Basis b ist. Falls dies der Fall ist für alle 100 Basen b, so ist die Wahrscheinlichkeit, dass n trotzdem zusammengesetzt ist kleiner als $1 - (0,25)^{100} \cong 4 \cdot 10^{-61}$. Man wählt die Anzahl der Basen so groß, dass die erwünschte Genauigkeit erreicht wird. Dieser Primzahltest heißt *Miller–Rabin-Test*.

3.4 Die Pollard-ρ-Methode

In diesem Abschnitt besprechen wir einen anderen Algorithmus zur Berechnung der Primfaktorzerlegung einer Zahl n. Für größere Zahlen ist diese Methode schneller als die Probedivision. In der Praxis wird die Probedivision benutzt um kleine Primfaktoren p zu finden (das heißt $p \leq 10^4$) und Pollard-ρ für Primfaktoren p von mittlere Größe (ungefähr $10^4 \leq p \leq 10^{15}$). Um die wirklich großen Primfaktoren zu finden, braucht man eine weitere Methode, wie zum Beispiel das quadratische Sieb. Diese Methode besprechen wir nicht in der Vorlesung *Elementare Zahlentheorie*.

Die Pollard-ρ-Methode wurde von J. Pollard im Jahre 1975 entdeckt. Ein neuer Bestandteil dieser Methode ist eine gewisse Zufallskomponente.

Wir erklären zuerst die Idee der Methode. Gegeben ist eine (zusammengesetzte) Zahl n. Wir suchen einen Primfaktor $p \mid n$. Es reicht einen nichttrivialen Faktor d von zu n finden: Wir wenden den Algorithmus nun auf d und n/d an und wiederholen dies bis wir die Primfaktorzerlegung von n gefunden haben.

Wie finden wir einen nichttrivialen Faktor von n? Sei p ein Primfaktor von n. Wir betrachten die Funktion

$$f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \qquad x \mapsto x^2 + 1 \pmod{p}.$$

Wir wählen einen Startwert $x_0 \in \mathbb{Z}/p\mathbb{Z}$ und definieren rekursiv $x_{i+1} = f(x_i)$.

Fakt: Die Werte x_0, $x_1 = f(x_0), x_2 = f(x_1), \cdots$ verhalten sich wie eine Zufallsfolge, dass heißt als ob die x_i unabhängig voneinander gewählt wurden.

Da es nur endlich viele Möglichkeiten für $x_i \in \mathbb{Z}/p\mathbb{Z}$ gibt, wiederholen die x_i's sich irgendwann. Sei $i < j$ minimal sodass $x_i \equiv x_j \pmod{p}$. Sobald dies passiert, gilt

$$x_{i+t} \equiv x_{j+t} \pmod{p}, \qquad \text{für alle } t \geq 0.$$

Graphisch kann man sich dies vorstellen wie in Abbildung 1. Die Name der Methode kommt von der Form des Bildes.

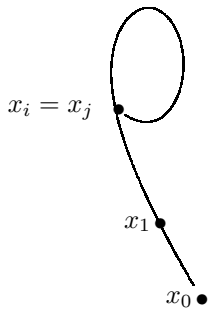


Abbildung 1: Das Pollard-ρ-Verfahren

Wie hilft uns dies, die Zahl n zu faktorisieren? Ein Problem ist dass wir p noch nicht kennen, also $f(x_i) = x_i^2 + 1 \pmod{p}$ nicht berechnen können. Wir definieren daher die Funktion

$$F : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad X \mapsto X^2 + 1 \pmod{n},$$

und setzen $X_0 = x_0$. Für $i > 0$ definieren wir rekursiv $X_i = F(X_{i-1}) \pmod{n}$. Da $p \mid n$ gilt nun $X_i \equiv x_i \pmod{p}$. Falls

$$x_i \equiv x_j \pmod{p},$$

gilt auch

$$p \mid \mathrm{ggT}(X_i - X_j, n).$$

Dies liefert uns folgenden Algorithmus.

Algorithmus 3.4.1 (Die Pollard-ρ-Methode: erste Version) (a) Wähle $X_0 \in \{0, \ldots, n-1\}$. Für $i > 0$ definieren wir X_i durch $X_i = F(X_{i-1}) \pmod{n}$.

(b) Für alle $j < i$ berechnen wir $\mathrm{ggT}(X_i - X_j, n)$.

(c)
- Falls $\mathrm{ggT}(X_i - X_j, n) = 1$, für alle j, so erhöhen wir i und wiederholen Schritt (b).
- Falls wir ein j finden, sodass $\mathrm{ggT}(X_i - X_j, n) \neq 1, n$, so haben wir einen nichttrivialen Faktor gefunden.
- Falls $\mathrm{ggT}(X_i - X_j, n) = n$, so müssen wir einen neuen Startwert X_0 wählen und von vorne anfangen.

Eine Vereinfachung. Wir möchten nicht alle Paare $i < j$ überprüfen, da dies zu aufwendig ist. Stattdessen definieren wir

$$X_0 = Y_0, \qquad X_{i+1} = F(X_i) \pmod{n}, \qquad Y_{i+1} = F(F(Y_i)) \pmod{n}$$

und berechnen nur

$$d = \mathrm{ggT}(X_i - Y_i, n).$$

Man zeigt

Lemma 3.4.2 *Es existiert eine Zahl k mit* $\mathrm{ggT}(X_k - Y_k, n) \neq 1$.

Hier ist die Beweisidee. Man kann sich dies graphisch so vorstellen: X und Y veranstalten ein Rennen über die Rennstrecke (Abbildung 1). Wir wissen nicht wo die unterschiedliche Anfangspositionen sind, aber Y läuft 2 Mal so schnell wie X. (Jedes Mal, wenn wir i erhöhen wenden wir die Funktion F auf X einmal an und auf Y zweimal.) Also überholt Y irgendwann X. Wenn dies passiert, gilt $Y_k \equiv X_k \pmod{n}$, und ist es $\mathrm{ggT}(Y_k - X_k, n) \neq 1$.

Dies liefert uns nun folgenden Algorithmus.

Algorithmus 3.4.3 (Die Pollard-ρ-Methode: zweite Version) (a) Wähle $X_0 \in \{0, \ldots, n-1\}$ beliebig.

(b) Setze $X_{i+1} = F(X_i)$ und $Y_{i+1} = F(F(Y_i))$. Berechne $d_{i+1} = \mathrm{ggT}(X_{i+1} - Y_{i+1}, n)$.

(c) Wiederhole Schritt (b) bis $d_{i+1} \neq 1$. Falls $d_{i+1} \neq n$ ist, so haben wir einen nicht-trivialen Faktor von n gefunden. Falls $d_{i+1} = n$ ist, so nutzt uns dies nichts. Wir wählen einen neuen Anfangswert X_0 und fangen von vorne an.

Beispiel 3.4.4 Sei $n = 8051$ und $X_0 = Y_0 = 2$. Wir berechnen

i	X_i	Y_i	d_i
1	5	26	1
2	26	7474	1
3	677	871	97

Da $d_3 \neq 1, n$, haben wir einen nicht-trivialen Faktor gefunden. Es gilt $8071 = 97 \cdot 83$. Man stellt leicht fest (zum Beispiel mit Hilfe der Probedivision), dass 83 und 97 Primzahlen sind. Also haben wir die Primfaktorzerlegung von n gefunden.

Bemerkung 3.4.5 Man sollte die Pollard-ρ-Metode nicht auf eine Primzahl anwenden. Falls n eine Primzahl ist, so ist $\mathrm{ggT}(Y_i - X_i, n)$ immer entweder 1 oder n. Also endet der Algorithmus in diesem Fall nie. Bevor man die Pollard-ρ-Methode anwendet um die Primfaktorzerlegung zu finden, sollte man zuerst einen Primzahltest anwenden um auszuschließen, dass n wahrscheinlich eine Primzahl ist.

4 Endliche Körper

4.1 Körper

In diesem Abschnitt geben wir eine kurze Einleitung in die Theorie der Körper. Das Thema wird ausführlicher in der Vorlesung Algebra I behandelt.

Definition 4.1.1 Eine Menge K zusammen mit 2 Verknüpfungen

$$\begin{aligned} + &: K \times K \to K \qquad (a, b) \mapsto a + b, \\ \cdot &: K \times K \to K \qquad (a, b) \mapsto a \cdot b, \end{aligned}$$

heißt *Körper*, falls folgende Bedingungen erfüllt sind:

(K1) $(K, +)$ ist eine kommutative Gruppe, d.h.

(a) die Addition ist assoziativ, d.h. $a + (b + c) = (a + b) + c$ für alle $a, b, c \in K$,

(b) es existiert ein neutrales Element 0, sodass $0 + a = a + 0 = a$ für alle $a \in K$,

(c) für jedes $a \in K$ existiert ein negatives Element $-a$ mit $a + (-a) = (-a) + a = 0$,

(d) die Addition ist kommutativ, d.h. $a + b = b + a$ für alle $a, b \in K$,

(K2) $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe, das heißt

(a) die Multiplikation ist assoziativ, das heißt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in K \setminus \{0\}$,

(b) es existiert ein Einheitselement 1, sodass $1 \cdot a = a \cdot 1 = a$ für alle $a \in K \setminus \{0\}$,

(c) für jedes $a \in K \setminus \{0\}$ existiert ein inverses Element a^{-1} mit $a \cdot a^{-1} = a^{-1} \cdot a = 1$,

(d) die Multiplikation ist kommutativ, das heißt $a \cdot b = b \cdot a$ für alle $a, b \in K \setminus \{0\}$,

(K3) es gelten die Distributivgesetzen:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (a + b) \cdot c = a \cdot c + b \cdot c,$$

für alle $a, b, c, \in K$.

Ein *Unterkörper* eines Körpers L ist eine Teilmenge $K \subset L$, sodass K ein Körper ist bezüglich die Verknüpfungen $+$ und $\cdot$ von L. Falls $K \subset L$ ein Unterkörper ist, so heißt L eine *Körpererweiterung* von K.

Beispiel 4.1.2 Beispiele von Körper sind die rationale Zahlen $\mathbb{Q}$, die reelle Zahlen $\mathbb{R}$ und die komplexe Zahlen $\mathbb{C}$.

Lemma 4.1.3 *Die Menge $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis: Alle Axiomen, außer die Existenz des inversen Elements a^{-1} für alle $a \neq 0$, sind erfüllt.

Sei n eine Primzahl. Korollar 2.1.6 impliziert, dass jedes Element $a \in \mathbb{Z}/n\mathbb{Z}^* = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ ein inverses Element besitzt.

Sei n zusammengesetzt und $d \mid n$ ein nicht-trivialer Teiler von n, das heißt $d \neq 1, n$. Es gilt, dass $\mathrm{ggT}(d, n) = d \neq 1$, also ist $d \notin (\mathbb{Z}/n\mathbb{Z})^*$. Wir schließen daraus, dass $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist. □

Lemma 4.1.3 zeigt, dass für jede Primzahl p ein Körper mit p Elemente existiert. Dieser Körper bezeichnen wir mit $\mathbb{F}_p$. Der Körper $\mathbb{F}_p$ ist nichts anderes als die Menge $\mathbb{Z}/p\mathbb{Z}$. Der Buchstabe F kommt vom englischen Wort für Körper: *field*.

In diesem Kapitel werden wir zeigen, dass für jede Primzahlpotenz $q = p^n$ ein Körper $\mathbb{F}_q$ mit q Elementen existiert. Da $\mathbb{Z}/p^n\mathbb{Z}$ kein Körper ist (Lemma 4.1.3), brauchen wir eine andere Konstruktion.

4.2 Polynome

Bevor wir in § 4.4 Körper mit $q = p^n$ Elementen konstruieren können, brauchen wie einige elementare Eigenschaften von Polynome.

Sei K ein Körper, zum Beispiel $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{F}_p$. Sei

$$K[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in K\}$$

die Menge der Polynome mit Koeffizienten in K. Die Menge $K[x]$ erfüllt alle Axiome aus Definition 4.1.1 außer (K2).(c). Wir nennen $K[X]$ den *Polynomring* über K.

Sei $f = \sum_{i=0}^{n} a_i x^i \in K[x]$ ein Polynom mit Koeffizienten $a_i \in K$. Das *Nullpolynom* $f = 0$ ist das Polynom dessen Koeffizienten alle Null sind. Falls $f \neq 0$ nicht das Nullpolynom ist, so heißt die größte Zahl n, sodass $a_n \neq 0$ ist, der *Grad* von f (Bezeichnung: Grad(f).) Der Grad des Nullpolynoms definieren wir als $-\infty$.

Falls f, g ungleich Null sind, gilt Grad(fg) = Grad(f)+Grad(g). Falls $f(x) = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$ ist, heißt $a_n x^n$ der *führende Term* von f. Ein Polynom von Grad n heißt *normiert*, falls der führende Term x^n ist.

Seien $f(x), g(x) \in K[x]$. Wir sagen, dass $g(x)$ ein *Teiler* von $f(x)$ ist, falls es ein Polynom $h(x) \in K[x]$ gibt mit $f(x) = g(x)h(x)$. Bezeichnung: $g \mid f$.

Im Polynomring $K[x]$ kann man in vielerlei Hinsicht genau so rechnen wie in $\mathbb{Z}$. Zum Beispiel gibt es in $K[x]$ einen euklidischen Algorithmus und man kann den ggT berechnen. Die Berechnung des ggTs basiert auf Polynomdivision. Der folgende Satz ist eine Version von Satz 1.1.5 für Polynome.

Satz 4.2.1 *Sei K ein Körper und seien $f(x), g(x) \in K[x]$ Polynome mit $g(x) \neq 0$. Es existieren eindeutige Polynomen $q(x)$ und $r(x) \in K[x]$ mit*

$$f(x) = q(x)g(x) + r(x),$$

wobei Grad(r) < Grad(g) *ist.*

Wie im Fall der ganzen Zahlen nennen wir $q(x)$ den *Quotient* und $r(x)$ den *Rest* nach Division von $f(x)$ durch $g(x)$.

Beweis: Wir beweisen zuerst die Existenz von q und r. Falls $g(x)$ ein Teiler von $f(x)$ ist, definieren wir $q(x) = f(x)/g(x)$ und $r(x) = 0$.

Falls $g(x)$ kein Teiler von $f(x)$ ist, betrachten wir die Menge

$$\mathcal{M} := \{f(x) - g(x)q(x) \mid q(x) \in K[x]\}.$$

Da $g \nmid f$, ist $0 \notin \mathcal{M}$. Sei $r(x) \in \mathcal{M}$ ein Element kleinsten Grades. Offensichtlich existiert ein Polynom $q(x)$ mit $f(x) = q(x)g(x) + r(x)$.

Wir müssen zeigen, dass Grad(r) < Grad(g) ist. Dazu schreiben wir $r(x) = \sum_{i=0}^{m} r_i x^i$ und $g(x) = \sum_{i=0}^{n} g_i x^i$ mit $r_m \neq 0$ und $g_n \neq 0$. Wir nehmen an, dass

$m = \text{Grad}(r) \geq n = \text{Grad}(g)$ ist. Wir betrachten

$$h(x) = r(x) - \frac{r_m}{g_n} x^{m-n} g(x).$$

Dies ist definiert, da $g_n \neq 0$ ist. Außerdem, ist $h \in \mathcal{M}$. Der Koeffizient von x^m in h ist $r_m - g_n r_m / g_n = 0$, also gilt $\text{Grad}(h) < m = \text{Grad}(r)$. Dies widerspricht den Wahl von r als Polynom in $\mathcal{M}$ kleinsten Grades. Wir schließen, dass $\text{Grad}(r) < \text{Grad}(g)$ ist.

Das Beweis der Eindeutigkeit ist ähnlich am Beweis von Satz 1.1.5. □

Korollar 4.2.2 *Sei $f(x) \in K[x]$ ein Polynom. Ein Element $a \in K$ ist genau dann eine Nullstelle von f, wenn ein Polynom $q(x)$ mit*

$$f(x) = q(x)(x - a)$$

existiert.

Beweis: Dies folgt unmittelbar aus Satz 4.2.1, da $x - a$ genau dann ein Teiler von $f(x)$ ist, wenn der Rest von f nach Division durch $x - a$ gleich 0 ist. Hier haben wir benutzt, dass $\text{Grad}(x - a) = 1$ ist. □

Definition 4.2.3 Seien $f, g \in K[x]$ Polynomen, die nicht beide null sind. Ein *gemeinsamer Teiler* von f und g ist ein Polynom $h(x)$, das sowohl f als auch g teilt. Der *größte gemeinsame Teiler* von f und g ist das normierte Polynom größten Grades, das sowohl f als auch g teilt. Wir bezeichnen den ggT zweier Polynome mit $\text{ggT}(f, g)$.

Wir fordern, dass $\text{ggT}(f, g)$ ein normiertes Polynom ist, da der ggT sonst nicht eindeutig wäre. Wie im Fall ganzer Zahlen, berechnet man den ggT mit Hilfe des euklidischen Algorithmus. Da Division mit Rest für Polynome existiert (4.2.1), funktioniert das euklidischen Algorithmus wie für ganzen Zahlen.

Das Beweis des folgenden Lemmas ist identisch zum Beweis von Lemma 1.1.9. Wir überlassen es der LeserIn.

Lemma 4.2.4 *Seien $f, g \in K[x]$ nicht beide Null. Sei $d(x) = \text{ggT}(f(x), g(x))$.*

(a) Es existieren Polynomen $s, t \in K[x]$, sodass

$$d(x) = s(x)f(x) + t(x)g(x).$$

(b) Jedes Polynom, das sich schreiben lässt als $s(x)f(x) + t(x)g(x)$ ist teilbar durch $d(x)$.

Beispiel 4.2.5 (a) Sei $f(x) := x^5 + x^2 - 4x - 2$ und $g(x) := x^4 + x^3 + 2x^2 + 3x + 1$ Polynomen in $\mathbb{Q}[x]$. Mit Hilfe des erweiterten euklidischen Algorithmus

berechnen wir $\mathrm{ggT}(f(x), g(x))$. Wir benutzen die gleiche Bezeichnung wie in § 1.1.

n	r_n	q_n	s_n	t_n
-1	$x^5 + x^2 - 4x - 2$	$-$	1	0
0	$x^4 + x^3 + 2x^2 + 3x + 1$	$-$	0	1
1	$-x^3 - 2x - 1$	$x - 1$	1	$-x + 1$

Da der ggT normiert ist, finden wir, dass

$$\mathrm{ggT}(f, g) = x^3 + 2x + 1 = (-1)f + (x - 1)g.$$

(b) Wir betrachten nun $K = \mathbb{F}_5$ den Körper mit 5 Elementen und

$$f(x) = x^3 + 4x^2 + x - 1, \quad g(x) = x^3 - x^2 + 2x + 1 \in \mathbb{F}_5[x].$$

Wie oben berechnet man, dass

$$\mathrm{ggT}(f(x), g(x)) = x + 2 = -f + g$$

ist.

Definition 4.2.6 Ein Polynom $f \in K[x]$ ein Polynom mit $f \neq 0$ heißt *reduzibel*, falls ein Teiler $g \in K[x]$ von f mit $1 \leq \mathrm{Grad}(g) < \mathrm{Grad}(f)$ existiert. Sonst heißt f *irreduzibel*.

Lemma 4.2.7 *(a) Jedes Polynom von Grad 1 ist irreduzibel.*

(b) Sei $f \in K[x]$ ein Polynom zweiten oder dritten Grades. Das Polynom f ist reduzibel genau dann, wenn f eine Nullstelle in K besitzt.

Beweis: Teil (a) ist klar. Sei f ein Polynom zweiten oder dritten Grades. Wir nehmen an, dass f reduzibel ist. Also lässt sich f schreiben als $f(x) = g(x)h(x)$ mit $1 \leq \mathrm{Grad}(g) < \mathrm{Grad}(f)$. Es folgt, dass entweder g oder f ein Polynom ersten Grades ist. □

Beispiel 4.2.8 (a) Ob ein Polynom irreduzibel ist oder nicht, hängt von Körper K ab. Zum Beispiel ist das Polynom $x^2 + 1$ irreduzibel in $\mathbb{R}[x]$, aber reduzibel in $\mathbb{C}[x]$. In $\mathbb{C}[x]$ gilt nämlich $x^2 + 1 = (x - i)(x + i)$, aber $i = \sqrt{-1} \notin \mathbb{R}$.

(b) Sei $f(x) = x^4 + 1 \in \mathbb{F}_5[x]$. Durch einsetzen der Werte von $\mathbb{F}_5$ sieht man leicht ein, dass f keine Nullstellen in $\mathbb{F}_5$ besitzt. Falls f reduzibel ist, ist $f = g \cdot h$ also das Produkt zweier Polynome zweiten Grades. Sei $g(x) = a_0 + a_1x + a_2x^2$ und $h(x) = b_0 + b_1x + b_2x^2$. Koeffizientenvergleich zwischen $g \cdot h$ und f liefert, dass

$$x^4 + 1 = (x^2 + 2)(x^2 + 3) \in \mathbb{F}_5[x].$$

Also ist f reduzibel. Die Faktoren sind irreduzibel, da sie keine Nullstellen besitzen.

Sei $f \in K[x]$ ein Polynom und $\alpha \in K$ eine Nullstelle von f. Wiederholtes Anwenden von Korollar 4.2.2 liefert, dass

$$f(x) = (x-\alpha)^m g(x), \qquad \text{mit } g \in K[x] \text{ und } g(\alpha) \neq 0.$$

Wir nennen m die *Vielfachheit* der Nullstelle α. Falls $m > 1$, so heißt α eine *mehrfache Nullstelle* von f.

Sei $f(x) = \sum_{i=0}^{n} a_i x^i$. Wir definieren die *formale Ableitung* von f als

$$f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}.$$

Falls $K = \mathbb{R}$ ist, so ist die formale Ableitung einfach die Ableitung von f nach x. Die formale Ableitung erfüllt die gleichen Rechenregeln wie die Ableitung. Das folgende Lemma zeigt, dass die formale Ableitung ähnliche Eigenschaften wie die Ableitung besitzt.

Lemma 4.2.9 *(a) Es gilt, dass*

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg'.$$

(b) Eine Nullstelle α eines Polynoms $f \in K[x]$ ist genau dann eine mehrfache Nullstelle, wenn $f'(\alpha) = 0$ ist.

Beweis: Teil (a) folgt leicht aus der Definition.

Sei $\alpha \in K$ eine Nullstelle von f mit Vielfachheit $m > 1$. Wir schreiben $f(x) = (x-\alpha)^m g(x)$ mit $g \in K[x]$ und $g(\alpha) \neq 0$. Es gilt, dass

$$f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x).$$

Da $m > 1$ ist, gilt also, dass $f'(\alpha) = 0$. Die Umkehrung beweist man ähnlich. □

Satz 4.2.10 *Sei K ein Körper und sein $f \in K[x]$ ein Polynom von Grad n. So besitzt f höchstens n Nullstellen in K.*

Beweis: Seien $\alpha_1, \ldots, \alpha_r \in K$ die Nullstellen von f gezählt mit Vielfachheit. Korollar 4.2.2 impliziert, dass

$$f(x) = \prod_{i=1}^{r} (x-\alpha_i) g(x)$$

ist, wobei $g(\alpha_i) \neq 0$ für $i = 1, \ldots, r$ ist. Also ist $r \leq \text{Grad}(f) = n$. □

4.3 Polynomkongruenzen

In diesem Abschnitt betrachten wir Polynomkongruenzen: Statt modulo einer natürlichen Zahl rechnen wir modulo einen Polynom. Dies geht sehr ähnlich an das Rechnen mit Kongruenzen ganzer Zahlen (§ 2.1).

Definition 4.3.1 Seien $f, g, h \in K[x]$ Polynome mit $f \neq 0$. Wir sagen, dass g *kongruent zu* h *modulo* f ist falls $f \mid (g - h)$. Bezeichnung: $g \equiv h \pmod{f}$.

Die Menge der Kongruenzklassen modulo f bezeichnen wir mit $K[x]/(f)$.

Lemma 4.3.2 *Seien $f, g \in K[x]$ Polynome mit $f \neq 0$.*

(a) Es existiert ein eindeutiges Polynom h mit $g \equiv h \pmod{f}$ und $\mathrm{Grad}(h) < \mathrm{Grad}(f)$.

(b) Sei nun k ein Körper mit q Elementen und sei $\mathrm{Grad}(f) = n$. Die Menge $k[x]/(f)$ besitzt genau q^n Elemente.

Beweis: Teil (a) folgt mit Hilfe der Division mit Rest für Polynome (Satz 4.2.1). Teil (b) folgt aus (a): Die Kongruenzklassen korrespondieren genau zu den Polynome $h(x) = \sum_{i=0}^{n-1} a_i x^i$ in $k[x]$ mit $\mathrm{Grad}(h) < n$. Da $a_i \in k$ und $|k| = q$ besitzt diese Menge q^n Elemente. □

Beispiel 4.3.3 Jede Kongruenzklasse von $\mathbb{F}_3[x]/(x^2 + x - 1)$ enthält genau ein Polynom von Grad kleiner gleich 1, also gilt

$$R := \mathbb{F}_3[x]/(x^2 + x - 1) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.$$

Die Menge R enthält also 9 Elementen.

Wir addieren und multiplizieren Elementen von $\mathbb{F}_3[x]/(f)$ modulo f. Wir müssen also sowohl modulo 3 als auch modulo f rechnen. Zum Beispiel gilt

$$(2x + 1)(2x + 2) = 4x^2 + 6x + 2 \equiv x^2 + 2 \equiv 1 - x + 2 = -x \in \mathbb{F}_3[x]/(f).$$

Satz 4.3.4 *Seien $f, g \in K[x] \setminus \{0\}$ Polynome. Das Polynom g besitzt genau dann ein inverses Element in $K[x]/(f)$, wenn $\mathrm{ggT}(f, g) = 1$ gilt.*

Beweis: Falls $\mathrm{ggT}(f, g) = 1$, existieren Polynome $s, t \in K[x]$ mit $s \cdot f + t \cdot g = 1$ (Lemma 4.2.4). Also ist $t \equiv g^{-1} \in K[x]/(f)$ das inverse Element von g.

Wir nehmen an, ein inverses Element $t = g^{-1} \in K[x]/(f)$ von g existiert. Also gilt, dass $t \cdot g \equiv 1 \pmod{f}$ ist. Daher existiert ein Polynom $s \in K[x]$, sodass $t \cdot g + s \cdot f = 1$ ist. Lemma 4.2.4.(b) impliziert, dass $\mathrm{ggT}(f, g) = 1$. □

Korollar 4.3.5 *Die Menge $K[x]/(f)$ ist genau dann ein Körper, wenn $f \in K[x]$ irreduzibel ist. Falls f irreduzibel ist, so heißt $K[x]/(f)$ der* Stammkörper *von f.*

Beweis: Alle Körperaxiomen außer K2.(c) (die Existenz des inversen Elements) sind automatisch erfüllt. Satz 4.3.4 sagt uns, dass $g \in K[x]/(f)$ genau dann ein inverses Element besitzt, wenn $\mathrm{ggT}(f, g) = 1$ ist. Falls f reduzibel ist, existieren daher nicht-invertierbare Elementen in $K[x]/(f)$, nämlich die Restklassen der nicht-triviale Teiler von f. Falls f irreduzibel ist, gilt, dass $\mathrm{ggT}(f, g)$ genau dann gleich 1 ist, wenn $f \nmid g$ gilt. Also besitzt jede nicht-triviale Restklasse in $K[x]/(f)$ ein inverses Element. □

Lemma 4.3.6 *Sei $f \in K[x]$ ein irreduzibles Polynom und $L = K[x]/(f)$ der Stammkörper von f. Das Polynom f besitzt mindestens eine Nullstelle $\alpha \in L$, nämlich die Restklasse α von x.*

Beweis: Dies folgt sofort aus der Definition des Stammkörpers und der Definition von α. □

Bezeichnung 4.3.7 Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom von Grad n. Sei $L = K[x]/(f)$ der Stammkörper von f. Wir definieren $\alpha \in L$ als die Restklasse von x in L. Lemma 4.3.6 impliziert, dass $\alpha \in L$ eine Nullstelle von $f(x)$ ist. Die Elemente von L können wir wie folgt darstellen:

$$L = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}.$$

Beispiel 4.3.8 (a) Man überprüft leicht, dass $f(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$ irreduzibel ist, also ist $L = \mathbb{F}_3[x]/(x^2 + x - 1)$ ein Körper mit 9 Elementen (Beispiel 4.3.3). Sei $\alpha \in L$ die Restklasse von x. Die Elementen von L können wir nun darstellen als

$$L = \{a_0 + a_1\alpha \mid a_i \in \mathbb{F}_3\},$$

wobei $\alpha^2 + \alpha - 1 = 0$ ist.

Da L ein Körper ist, existiert das inverse Element $1/\alpha$ von α. Wir schreiben $1/\alpha = b_0 + b_1\alpha$. Mit Hilfe der Relation $\alpha^2 = -\alpha + 1$ finden wir, dass

$$1 \stackrel{!}{=} \alpha(b_0 + b_1\alpha) = b_0\alpha + b_1(-\alpha + 1) = b_1 + (b_0 - b_1)\alpha.$$

Die b_i erfüllen daher das Gleichungssystem

$$\begin{cases} b_1 = 1 \\ b_0 - b_1 = 0 \end{cases}$$

Also gilt $b_0 = b_1 = 1$. Wir schließen, dass $1/\alpha = 1 + \alpha$ ist.

Alternativ finden wir mit Hilfe des erweiterten euklidischen Algorithmus, dass

$$\mathrm{ggT}(x, x^2 + x - 1) = 1 = (1 + x) \cdot x - 1 \cdot (x^2 + x - 1)$$

gilt. Hieraus folgt auch, dass $1/\alpha = 1 + \alpha$ ist.

(b) Das Polynom $f(x) = x^2 + x - 1$ ist irreduzibel in $\mathbb{F}_3[x]$. Wir überprüfen, dass dies in $L[x]$ nicht mehr gilt. In L besitzt f eine Nullstelle α (Lemma 4.3.6). Division mit Rest in $L[x]$ zusammen mit der Relation $\alpha^2 = 1 - \alpha$ liefert, dass

$$f(x) = (x - \alpha)(x + 1 + \alpha) \in L[x]$$

gilt.

Lemma 4.3.9 *Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom von Grad n. Sei $L = K[x]/(f)$ der Stammkörper von f. Nun ist L ein K-Vektorraum der Dimension n. Wir nennen n den* Grad *der Körpererweiterung $K \subset L$. Bezeichnung: $n = [L : K]$.*

Beweis: Die Tatsache, dass L ein K-Vektorraum ist, folgt aus den Körperaxiomen (Definition 4.1.1). Bezeichnung 4.3.7 impliziert, dass

$$(1, \alpha, \ldots, \alpha^{n-1}) \tag{17}$$

ein K-Basis von L ist. Also ist n die Dimension von L als K-Vektorraum. □

4.4 Endliche Körper

Definition 4.4.1 Ein Körper mit endlich vielen Elementen heißt *endlicher Körper.*

Satz 4.4.2 *Sei k ein endlicher Körper. Es existiert eine Primzahl p, sodass k den Körper $\mathbb{F}_p$ enthält. Falls $\mathbb{F}_p \subset k$ ein Unterkörper ist, so heißt p die* Charakteristik *von k. Bezeichnung:* $\mathrm{Char}(k)$.

Beweis: Sei $1 \in k$ das Einheitselement (Axiom (K2.(b)). Da k nur endlich viele Elementen besitzt, existiert ein $n > 0$, sodass $n \cdot 1 = 1 + \cdots + 1 = 0$ ist. Sei $n > 0$ minimal mit dieser Eigenschaft. Wir betrachten die Teilmenge

$$\mathcal{N} := \{0, 1, \ldots, n - 1\}$$

von k.

Wir nehmen an, dass n eine zusammengesetzte Zahl ist. Sei $n = d \cdot e$ mit $d \neq 1, n$. Wir fassen $d \in \mathcal{N}$ als Element von k auf. Wir behaupten, dass d kein inverses Element in k besitzt. Da $d \neq 0$ liefert dies ein Widerspruch zur Annahme, dass k ein Körper ist. Also folgt, dass n eine Primzahl ist. Dies beweist den Satz.

Wir beweisen die Behauptung, dass d kein inverses Element d^{-1} in k besitzt. Falls $d^{-1} \in k$ existieren würde, so würde gelten, da $n = d \cdot e \equiv 0 \in \mathbb{F}_p$ ist, dass

$$0 = d^{-1} \cdot 0 \equiv d^{-1} \cdot n = d^{-1} \cdot d \cdot e = 1 \cdot e = e$$

ist. Dies liefert ein Widerspruch zur Annahme, dass e ein Teiler von n, also insbesondere ungleich Null, ist. Also besitzt d kein inverses Element in k. □

Satz 4.4.3 *Sei k ein endlicher Körper der Charakteristik p. Die Kardinalität von k ist p^n für ein $n \geq 1$.*

Beweis: Der Beweis von Satz 4.4.2 impliziert, dass $\mathbb{F}_p \subset k$ ein Unterkörper ist. Wie im Beweis von Lemma 4.3.9 zeigt man, dass k ein $\mathbb{F}_p$-Vektorraum ist. Sei n die $\mathbb{F}_p$-Dimension von k und sei $(e_1, \ldots e_n)$ ein Basis von k als $\mathbb{F}_p$-Vektorraum. Es gilt, dass

$$k = \{\sum_{i=1}^{n} a_i e_i \mid a_i \in \mathbb{F}_p\}.$$

Also besitzt k genau p^n Elementen. □

Falls $k = \mathbb{F}_p[x]/(f)$ der Stammkörper eines irreduziblen Polynoms ist, folgt Satz 4.4.3 aus Lemma 4.3.2. Theorem 4.4.6 impliziert, dass jeder endliche Körper der Stammkörper eines irreduziblen Polynoms ist.

Satz 4.4.4 (Kronecker) *Sei K ein Körper und $f \in K[x]$ ein Polynom. Es existiert eine Körpererweiterung $K \subset L$ von K, sodass f in $L[x]$ in Linearfaktoren zerfällt.*

Bemerkung 4.4.5 Ein Polynom $f(x) \in K[x]$ zerfällt genau dann in Linearfaktoren, wenn Zahlen $c, \alpha_i \in K$ existieren, sodass

$$f(x) = c \prod_i (x - \alpha_i) \in K[x].$$

Falls $f \in K[x]$ in Linearfaktoren zerfällt, so besitzt f daher $\mathrm{Grad}(f)$ Nullstellen in K gezählt mit Vielfachheit.

Beweis: Wir schreiben

$$f = \prod_i f_i \in K[x]$$

als Produkt von irreduziblen Faktoren. Falls $f \in K[x]$ in Linearfaktoren zerfällt, d.h. wenn $\mathrm{Grad}(f_i) = 1$ für alle i, so sind wir fertig.

Wir nehmen an, dass $f \in K[x]$ nicht in Linearfaktoren zerfällt. Es existiert daher ein irreduzibler Faktor g_1 von f vom Grad mindestens zwei. (Es ist möglich, dass $g_1 = f$ gilt.) Sei $L_1 = K[x]/(g_1)$ der Stammkörper von g_1. Da g_1 irreduzibel ist, so ist L_1 eine Körpererweiterung von K (Korollar 4.3.5). Wir betrachten $f \in L_1[x]$ nun als Polynom mit Koeffizienten in L_1. Das Polynom g_1 besitzt in L_1 mindestens eine Nullstelle (Lemma 4.3.6). Das Polynom f besitzt in L_1 daher mehr Nullstellen als in K.

Wir betrachten f als Polynom in $L_1[x]$ und wiederholen das Argument: Falls f in $L_1[x]$ in Linearfaktoren zerfällt, so sind wir fertig. Sonst definieren wir L_2 als den Stammkörper eines irreduziblen Faktors von f von Grad mindestens zwei. Und so weiter.

Dies liefert eine Kette $K \subset L_1 \subset L_2 \subset \cdots$ von Körpererweiterungen. Da Grad(f) endlich ist, ist diese Kette endlich. Sei L_m der größte Körper der Kette. So zerfällt f in L_m in Linearfaktoren. □

Theorem 4.4.6 *Sei $q = p^n$ eine Primzahlpotenz. Es existiert ein Körper k mit q Elementen.*

Beweis: Sei $q = p^n$ eine Primzahlpotenz. Wir betrachten das Polynom

$$g(x) = x^q - x \in \mathbb{F}_p[x].$$

Satz 4.4.4 impliziert, dass eine Körpererweiterung L von K existiert, sodass g in $L[x]$ in Linearfaktoren zerfällt.

Wir behaupten, dass g keine mehrfache Nullstellen in L besitzt. Da $q = p^n \equiv 0 \in \mathbb{F}_p$ gilt, dass $g'(x) = qx^{q-1} - 1 \equiv -1 \in \mathbb{F}_p[x]$. Also gilt, dass $\mathrm{ggT}(g, g') = 1$ ist. Lemma 4.2.9 impliziert, dass g keine mehrfache Nullstellen besitzt. Insbesondere besitzt g genau q Nullstellen in L.

Sei $F \subset L$ die Menge der Nullstellen von g. Wir behaupten, dass F ein Körper ist. Die Definition der Menge F impliziert, dass $\alpha \in F$ genau dann, wenn $\alpha^q = \alpha$ ist. Seien nun $\alpha, \beta \in F$. Es gilt

$$(\alpha\beta)^q = \alpha^q\beta^q, \quad (-\alpha)^q = -\alpha, \quad (1/\alpha)^q = 1/\alpha^q.$$

Wir behaupten, dass $(\alpha + \beta)^q = \alpha^q + \beta^q$ für alle $\alpha, \beta \in F$. Zuerst bemerken wir, dass es reicht zu zeigen, dass $(\alpha+\beta)^p = \alpha^p+\beta^p$ gilt. Die allgemeine Aussage folgt mit widerholtes Anwenden, da $q = p^n$. Es gilt, dass

$$(\alpha + \beta)^p = \sum_{i=0}^{p} \binom{q}{i} \alpha^i \beta^{p-i},$$

wobei

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

ist. Sei $i \neq 0, p$. Wir sehen, dass p der Zähler der Ausdrück aber nicht der Nenner teilt. Daher ist $\binom{p}{i} \equiv 0 \pmod{p}$ für $i \neq 0, p$. Es folgt, dass $(\alpha+\beta)^q = \alpha^q + \beta^q \in F$. Wir schließen, dass F ein Körper ist. □

Bemerkung 4.4.7 Man kann zeigen, dass für jede Primzahlpotenz $q = p^n$ genau ein Körper mit q Elementen gibt, bis auf *Körperisomorphie*. Wir beweisen dies hier nicht und definieren auch nicht was ein Körperisomorphismus ist. Mehr Details finden Sie in [2, § 4.5]. Der Körper mit $q = p^n$ Elementen bezeichnen wir mit $\mathbb{F}_q$.

Beispiel 4.4.8 Sei $q = 3^2 = 9$. Wir faktorisieren das Polynom $x^q - x$ in irreduziblen Faktoren in $\mathbb{F}_3[x]$, zum Beispiel mit Hilfe des Maple-Kommando `Factor(`$x^q - x$`) mod 3`:

$$x^q - x = x(x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1).$$

Um den Körper mit 9 Elementen darzustellen, wählen wir einen der irreduziblen Faktoren von g von Grad 2, zum Beispiel $h(x) = x^2 + 1$. In Beispiel 4.3.8 haben wir $x^2 + x - 1$ gewählt. Wir können $\mathbb{F}_9$ nun darstellen als

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1) = \{a_0 + a_1\alpha \mid a_j \in \mathbb{F}_3\},$$

wobei α die Relation $\alpha^2 = -1$ erfüllt. Also ist $\alpha \in \mathbb{F}_9$ eine Nullstelle des Polynoms $x^2 + 1$.

Der Beweis von Theorem 4.4.6 impliziert, dass $x^q - x$ über $\mathbb{F}_9$ in Linearfaktoren zerfällt. Wir rechnen dies nach. Wir suchen dazu die Nullstellen von $x^2 + 1$, $x^2 - x - 1$ und $x^2 + x - 1$ in $\mathbb{F}_9$. Wie in Beispiel 4.3.8 finden wir, dass

$$x^2 + 1 = (x + \alpha)(x - \alpha), \qquad x^2 - x - 1 = (x + \alpha + 1)(x - \alpha + 1),$$
$$x^2 + x - 1 = (x - \alpha - 1)(x + \alpha - 1).$$

Die Eindeutigkeit des Körpers mit 9 Elementen kann man so verstehen: Da alle irreduzible Polynomen in $\mathbb{F}_3[x]$ von Grad 2 in $\mathbb{F}_9[x]$ in Linearfaktoren zerfallen, ist es egal ob man $\mathbb{F}_9$ konstruiert in dem man eine Nullstelle von x^2+1 oder von $x^2 + x - 1$ an $\mathbb{F}_3$ hinzufügt.

5 Der diskrete Logarithmus

5.1 Primitivwurzeln

Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd zu m. In § 2.5 haben wir die Ordnung $\mathrm{ord}_m(a)$ von a modulo m definiert. Wir haben gezeigt (Lemma 2.5.11), dass $\mathrm{ord}_m(a)$ ein Teiler von $\varphi(m)$ ist.

Definition 5.1.1 Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $\mathrm{ggT}(a, m) = 1$. Die Zahl a heißt *Primitivwurzel* modulo m, falls $\mathrm{ord}_m(a) = \varphi(m)$ ist.

Beispiel 5.1.2 (a) Sei $m = 7$, also ist $\varphi(m) = 6$. Man berechnet:

a	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	1	3	6	3	6	2

.

Also sind 3 und 5 Primitivwurzeln modulo 7.

(b) Sei $m = 12$, also ist $\varphi(12) = \varphi(3)\varphi(4) = 4$. Man berechnet:

a	1	5	7	11
$\mathrm{ord}_{12}(a)$	1	2	2	2

.

Wir schließen, dass keine Primitivwurzeln modulo 12 existieren.

Lemma 5.1.3 *Sei a eine Primitivwurzel modulo m. So ist*

$$\mathcal{R} := \{a, a^2, \ldots, a^{\varphi(m)}\}$$

ein reduziertes Restsystem modulo m.

Beweis: Seien $1 \leq i < j \leq \varphi(m)$. Die Definition der Ordnung modulo m impliziert, dass

$$a^{j-i} \not\equiv 1 \pmod{m}.$$

Also ist $a^j \not\equiv a^i \pmod{m}$. Außerdem gilt offensichtlich, dass $\mathrm{ggT}(a^i, m) = 1$ für alle i. Da die Kardinalität der Menge $\mathcal{R}$ gleich $\varphi(m)$ ist, ist $\mathcal{R}$ ein reduziertes Restsystem modulo m. □

Lemma 5.1.4 *Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$ Zahlen mit $\mathrm{ggT}(a, m) = 1$. Für alle $k \in \mathbb{N}$ gilt, dass*

$$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{\mathrm{ggT}(\mathrm{ord}_m(a), k)}$$

ist.

Beweis: Übungsaufgabe. □

Beispiel 5.1.5 In Beispiel 5.1.2 haben wir gesehen, dass $a = 3$ eine Primitivwurzel modulo 7 ist. Es gilt

k	1	2	3	4	5	6
a^k	3	2	6	4	5	1
$\mathrm{ord}_m(a^k)$	6	3	2	3	6	1

.

Dies bestätigt Lemmata 5.1.3 und 5.1.4.

Sei p eine Primzahl. Ziel dieses Abschnittes ist die Existenz von Primitivwurzel modulo p zu beweisen (Korollar 5.1.8). Der folgende Satz ist ein erster Schritt in diesem Beweis.

Satz 5.1.6 *Sei p eine Primzahl und $d \mid (p-1)$ ein Teiler. Die Kongruenz*

$$x^d \equiv 1 \pmod{p}$$

besitzt genau d Lösungen.

Beweis: Sei d ein Teiler von $p-1$. Wir schreiben $p - 1 = d \cdot e$. Wie im Beweis von Lemma 1.2.2 finden wir, dass

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1) =: (x^d - 1)g(x).$$

Der kleine Satz von Fermat (Korollar 2.5.8) impliziert, dass die Kongruenz $x^{p-1} \equiv 1 \pmod{p}$ genau $p-1$ Lösungen besitzt, nämlich die Elementen von $\mathbb{Z}/p\mathbb{Z}^*$.

Satz 4.2.10 mit $K = \mathbb{F}_p$ impliziert, dass die Kongruenz $g(x) \equiv 0 \pmod{p}$ höchstens $\mathrm{Grad}(g) = d(e-1) = p-1-d$ Lösungen besitzt. Es gibt also mindestens d Zahlen $\alpha \in \mathbb{Z}/p\mathbb{Z}^*$ mit $g(\alpha) \not\equiv 0 \pmod{p}$ und $\alpha^{p-1} \equiv 1 \pmod{p}$. Diese Zahlen α erfüllen also $\alpha^d \equiv 1 \pmod{p}$. Da die Kongruenz $x^d \equiv 1 \pmod{p}$ höchstens d Lösungen besitzt, schließen wir, dass genau d Zahlen $\alpha \in \mathbb{Z}/p\mathbb{Z}$ mit $\alpha^d \equiv 1 \pmod{p}$ existieren. □

Theorem 5.1.7 *Sei p eine Primzahl und $d \mid (p-1)$ ein Teiler von $p-1$. Wir definieren*

$$\psi(d) = |\{1 \leq a < p \mid \mathrm{ord}_p(a) = d\}|.$$

Es gilt, dass

$$\psi(d) = \varphi(d).$$

Beweis: Wir nehmen zuerst an, dass $\psi(d) > 0$. Es existiert nun eine Zahl $1 \leq a < p$ mit $\mathrm{ord}_p(a) = d$. Insbesondere sind die Zahlen $a, a^2, \ldots, a^d$ nicht kongruent modulo p (vergleichen Sie zum Beweis von Lemma 5.1.3). Außerdem gilt, dass

$$(a^i)^d \equiv (a^d)^i \equiv 1^i \equiv 1 \pmod{p}.$$

Also ist a^i eine Lösung der Kongruenz $x^d \equiv 1 \pmod{p}$ für $i = 1, \ldots, d$.

Satz 5.1.6 impliziert, dass die Kongruenz $x^d \equiv 1 \pmod{p}$ genau d Lösungen modulo p besitzt. Diese Lösungen sind daher $a, a^2, \ldots, a^d$. Lemma 5.1.4 impliziert, dass $\mathrm{ord}_p(a^i) = d$ genau dann gilt, wenn $\mathrm{ggT}(i, d) = 1$ ist, also wenn $i \in \mathbb{Z}/d\mathbb{Z}^*$ ist. Die Anzahl solcher i ist $\varphi(d)$. Wir haben daher gezeigt, dass falls $\psi(d) > 0$, so ist $\psi(d) = \varphi(d)$.

Wir zeigen nun noch, dass der Fall $\psi(d) = 0$ nicht eintreten kann. Wir wissen, dass die Ordnung $\mathrm{ord}_p(a)$ jeder Zahl $0 < a < p$ ein Teiler von $p-1$ ist. Daher gilt, dass

$$\sum_{d \mid (p-1)} \psi(d) = p - 1.$$

Außerdem gilt, dass

$$\sum_{d \mid (p-1)} \varphi(d) = p - 1,$$

nach Lemma 2.5.13. Für jedes d gilt, dass $\psi(d) \leq \varphi(d)$ ist: Falls $\psi(d) = 0$ ist, so ist dies offensichtlich, falls $\psi(d) > 0$ ist, so haben wir gezeigt, dass $\psi(d) = \varphi(d)$. Daher gilt, dass

$$p - 1 = \sum_{d \mid (p-1)} \psi(d) \leq \sum_{d \mid (p-1)} \varphi(d) = p - 1.$$

Aber dies ist nur möglich falls $\psi(d) = \varphi(d)$ für alle $d \mid (p-1)$. □

Korollar 5.1.8 *Sei p eine Primzahl. Es existiert eine Primitivwurzel modulo p.*

Beweis: Theorem 5.1.7 impliziert, dass die Anzahl der Primitivwurzeln modulo p gleich $\psi(p-1) = \varphi(p-1)$ ist. Satz 2.7.5 impliziert, dass $\varphi(p-1) \geq 1$ ist. □

Beispiel 5.1.9 In Beispiel 5.1.2 haben wir gesehen, dass zwei Primitivwurzeln modulo 7 existieren, nämlich 3 und 5. In der Tat gilt, dass $\varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2 = 2$.

Es gibt $\varphi(10) = 4$ Primitivwurzel modulo 11, nämlich $2, 6, 7$ und 8.

Es existieren viele Primitivwurzel modulo p: Die Anzahl ist $\varphi(p-1)$. Leider gibt uns Korollar 5.1.8 keine Methode eine Primitivwurzel zu finden. Um eine Primitivwurzel zu finden, bleibt uns nicht viel anderes übrig als die Ordnung modulo p von Elementen in $\mathbb{Z}/p\mathbb{Z}^*$ zu berechnen bis wir eine Primitivwurzel gefunden haben. So bald wir eine Primitivwurzel r modulo p gefunden haben, ist es leicht alle anderen zu finden: Der Beweis von Theorem 5.1.7 impliziert, dass die anderen Primitivwurzel r^i sind, wobei $\mathrm{ggT}(i, p-1) = 1$ ist.

5.2 Der diskrete Logarithmus

Sei p eine Primzahl. Wir betrachten $G = (\mathbb{Z}/p\mathbb{Z})^*$. Sei r eine Primitivwurzel modulo p. Diese existiert nach Korollar 5.1.8. Jedes Element von G lässt sich schreiben als Potenz von r:

$$G = \{r, r^2, r^3, \ldots, r^{p-1}\}, \tag{18}$$

(Lemma 5.1.3).

Wir definieren die *Exponentialfunktion* bezüglich der Primitivwurzel r durch

$$\exp_r : \mathbb{Z}/(p-1)\mathbb{Z} \to G, \qquad i \mapsto r^i.$$

Diese Abbildung heißt Exponentialfunktion, da $\exp_r(i+j) = \exp_r(i) \cdot \exp_r(j)$ gilt. Wir bemerken, dass $\exp_r$ wegen (18) eine Bijektion ist. Die Umkehrfunktion

$$\mathrm{dlog}_r : G \to \mathbb{Z}/(p-1)\mathbb{Z}, \qquad a = r^i \mapsto i \pmod{p-1}$$

heißt der *diskrete Logarithmus*. (Die Funktion heißt "diskreter" Logarithmus, da G endlich ist.) Wir bemerken, dass sowohl die Exponentialfunktion als auch der diskrete Logarithmus von der Wahl des Primitivwurzels r abhängt.

Beispiel 5.2.1 Sei $p = 7$ und $G = (\mathbb{Z}/7\mathbb{Z})^*$. Die Zahl $r = 5$ ist eine Primitivwurzel modulo 7. Wir berechnen $\mathrm{dlog}_r : G \to \mathbb{Z}/6\mathbb{Z}$:

a	1	2	3	4	5	6
$\mathrm{dlog}_r(a)$	0	4	5	2	1	3

Der diskrete Logarithmus ist, zum Beispiel, nützlich für das lösen von Gleichungen der Form

$$x^e \equiv a \pmod{p}. \tag{19}$$

Sei $i = \mathrm{dlog}_r(a)$ und $j = \mathrm{dlog}_r(x)$. Die Kongruenz (19) ist äquivalent zur linearen Kongruenz

$$ej \equiv i \pmod{p-1}.$$

Lineare Kongruenzen können wir mit Hilfe von Satz 2.1.5 lösen. Wir erläutern dies an Hand eines Beispiels.

Beispiel 5.2.2 Wir lösen die Kongruenz

$$x^5 \equiv 4 \pmod 7.$$

Hierzu bemerken wir, dass $\operatorname{dlog}_5(4) = 2$, da $5^2 \equiv 4 \bmod 7$ ist. Wir schreiben nun $j = \operatorname{dlog}_5(x)$ und bekommen die lineare Kongruenz

$$5j \equiv 2 \pmod 6.$$

Da 5 teilerfremd zu 6 ist, hat diese Kongruenz eine eindeutige Lösung modulo 6, nämlich

$$j \equiv \frac{2}{5} \equiv 4 \bmod 6.$$

Für die Berechnung der Exponentialfunktion $\exp_r$ ist effizient möglich mit Hilfe der schnellen Exponentiation (§ 2.6). Für die Berechnung des diskreten Logarithmus gibt es keine effiziente Algorithmen: Um $\operatorname{dlog}_r(a)$ zu berechnen, berechnen wir die Potenzen der Primitivwurzel r bis wir ein i gefunden haben mit $g^i \equiv a \pmod p$. Nun ist $i = \operatorname{dlog}_r(a)$. Falls p eine große Primzahl ist, dauert es im Schnitt sehr Lange $\operatorname{dlog}_r(a)$ zu berechnen, da man im Schnitt sehr viele Potenzen ausrechnen muss. In der Kryptographie nennt man $\exp_r$ daher eine *Einwegfunktion*. Auf dieser Idee basieren verschiedene Verfahren in der Kryptographie. Genauere Aussage und bessere Algorithmen zur Berechnung des diskreten Logarithmus finden Sie im Skript der Vorlesung Kryptologie [6].

Problem 5.2.3 (Das diskrete-Logarithmus-Problem) Sei $a \in \mathbb{Z}/p\mathbb{Z}^*$ gegeben und sei r eine Primitivwurzel modulo p. Berechne $i = \operatorname{dlog}_r(a)$.

Wir besprechen nun eine Anwendung des diskreten Logarithmus in der Kryptographie: Das *Diffie–Hellman-Schlüsselaustauschverfahren*. Alice und Bob wollen über eine unsichere Leitung vertrauliche Nachrichten austauschen. Dazu benutzen Sie ein symmetrisches Verschüsselungsverfahren. Sie müssen aber zuerst einen geheimen Schlüssel austauschen. Hierfür haben sie aber auch nur die unsichere Leitung zur Verfügung. Sie gehen nun wie folgt vor.

Algorithmus 5.2.4 (Diffie–Hellman) Schritt 1. Alice und Bob wählen eine Primzahl p und eine Primitivwurzel r modulo p. Dies ist der öffentliche Schlüssel.

Schritt 2. Bob wählt zufällig eine Zahl $i \in \{1, \ldots, p-1\}$ und berechnet $a = g^i \in G$. Er sendet die Zahl a an Alice.

Schritt 3. Alice wählt zufällig eine Zahl $j \in \{1, \ldots, p-1\}$ und berechnet $b = g^j \in G$. Sie sendet die Zahl b an Bob.

Schritt 4. Alice und Bob können nun beide das Element

$$k = a^j = g^{ij} = b^i \in G \tag{20}$$

berechnen. Dies ist nun der private Schlüssel den sowohl Alice als auch Bob kennen.

Eve hat den unsicheren Kanal abgehört. Sie kennt also p, r, a und b. Um den geheimen Schlüssel k zu berechnen muss Sie aber entweder i oder j kennen (20). Hierzu muss Sie das diskrete Logarithmusproblem lösen, da

$$i = \mathrm{dlog}_r(a), \qquad j = \mathrm{dlog}_r(b).$$

Falls die Primzahl p groß genug gewählt ist, kann Eve dieses Problem nicht lösen und daher auch nicht den geheimen Schlüssel k berechnen. Alice und Bob können ihre verschlüsselten Nachrichten sicher verschicken.

5.3 Das ElGamal-Kryptoverfahren

In diesem Abschnitt besprechen wir das ElGamal-Kryptoverfahren. Dies wurde im Jahre 1984 von Taher ElGamal erfunden. Das ElGamal-Verfahren ist eine Weiterentwicklung des Diffie–Hellman-Schlüsselaustauschverfahren. Es benutzt die Idee des Diffie–Hellman-Verfahren zum ver- und entschlüßeln von Nachrichten statt zum Schlüsselaustausch.

Wie in § 5.2, sind eine Primzahl p und eine Primitivwurzel r modulo p vorgegeben: Diese Zahlen sind Teil des öffentlichen Schlüssels. Wir gehen davon aus, dass die Nachricht aus Blöcke B_i mit $0 \leq B_i < p$ besteht.

Vorbereitung: Alice möchte Bob eine geheime Nachricht schicken. Sie benutzt hierzu Bobs öffentlichen Schlüssel (p, r, a). Hierbei ist $a = r^i$ die Zahl die Bob im Schritt 2 des Diffie–Hellman-Verfahrens berechnet hat. Alice wählt wieder eine Zahl $j \in \mathbb{Z}/p\mathbb{Z}$, berechnet $b = r^j \in \mathbb{Z}/p\mathbb{Z}$ und schickt Bob diese Zahl. Wie im Diffie–Hellman-Verfahren kann Alice die Zahl

$$k \equiv a^j \pmod{p}$$

berechnen. Dies ist wieder der private Schlüssel.

Verschlüsseln: Zum verschlüsseln eines Blocks B des Klartextes, berechnet Alice

$$C \equiv k \cdot B \pmod{p}.$$

Entschlüsseln: Bob hat von Alice den Geheimtext C zusammen mit der Zahl b empfangen.

Um die Nachricht zu entschlüsseln muss Bob die Zahl $k^{-1} \pmod{p}$ berechnen, da

$$B \equiv k^{-1}C \pmod{p}$$

ist.

Bob kennt die Zahl i, weil er diese selber gewählt hat. Außerdem kennt er die Zahl $b = r^j$ die er von Alice bekommen hat. Daher kann er

$$k^{-1} \equiv r^{-ij} \equiv b^{-i} \pmod{p}$$

berechnen und damit den Geheimtext entschlüsseln.

Eve versucht den Geheimtext zu entschlüsseln. Sie kennt Bobs öffentliche Schlüssel (p, r, a). Außerdem hat sie über die unsichere Leitung die Zahl b und den Geheimtext C abgefangen. Um den Geheimtext zu entschlüsseln muss Sie die Zahl $k^{-1} \pmod p$ berechnen. Wie in § 5.2 muss sie dazu entweder $i = \mathrm{dlog}_r(a)$ oder $j = \mathrm{dlog}_r(b)$ berechnen, also das diskrete Logarithmusproblem lösen. Die Sicherheit des ElGamal-Verfahrens beruht darauf, dass Eve dies nicht kann.

6 Das quadratische Reziprozitätsgesetz

In diesem Abschnitt betrachten wir die Lösbarkeit von Kongruenzen von der Form

$$x^2 \equiv a \pmod m.$$

6.1 Das Legendre-Symbol

Definition 6.1.1 Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ teilerfremd zu p. Die Zahl a heißt *quadratischer Rest* $\pmod p$, falls die Kongruenz $x^2 \equiv a \pmod p$ eine Lösung besitzt. Sonst heißt a *quadratischer Nichtrest* $\pmod p$.

Beispiel 6.1.2 Die quadratische Resten $\pmod{13}$ sind $a = 1, 4, 9, 3, 12, 10$. Die quadratische Nichtreste $\pmod{13}$ sind $a = 2, 5, 6, 7, 8$.

Definition 6.1.3 Sei p eine ungerade Primzahl. Das *Legendre-Symbol* ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ ein quadratischer Rest} \pmod p \text{ ist,} \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest} \pmod p \text{ ist,} \\ 0 & \text{falls } p \mid a. \end{cases}$$

Lemma 6.1.4 *Sei p eine ungerade Primzahl.*

(a) Es existieren genau $(p-1)/2$ quadratische Reste $\pmod p$ und $(p-1)/2$ quadratische Nichtreste $\pmod p$.

(b) Es gilt

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

Beweis: (a) Die Restklassen $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ sind offensichtlich quadratische Reste $\pmod p$. Da $a^2 \equiv (-a)^2 \pmod p$, sind dies alle quadratische Reste $\pmod p$. Sei nun $a^2 \equiv b^2 \pmod p$. Da p eine Primzahl ist, impliziert Lemma 1.2.3, dass $a \equiv \pm b \pmod p$. Wir schließen, dass für $1 \leq a, b \leq (p-1)/2$ mit $a \neq b$ die Restklassen a^2 und b^2 nicht kongruent $\pmod p$ sind. Also ist die Anzahl der quadratische Reste $\pmod p$ gleich $(p-1)/2$.

(b) Falls $a \equiv 0 \pmod{p}$, so ist die Aussage offensichtlich. Wir nehmen daher an, dass $a \not\equiv 0 \pmod{p}$ ist. Der kleine Satz von Fermat (Korollar 2.5.8) impliziert, dass

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \pmod{p}.$$

Also folgt aus Lemma 1.2.3, dass $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ ist.

Sei a ein quadratischer Rest $\pmod{p}$. Es existiert ein $b \in \mathbb{Z}/p\mathbb{Z}$, sodass $b^2 \equiv a \pmod{p}$. Daher gilt, dass

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p} = \left(\frac{a}{p}\right).$$

Da $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Körper ist, besitzt die Kongruenz

$$x^{(p-1)/2} - 1 \equiv 0 \pmod{p} \tag{21}$$

höchtens $(p-1)/2$ Lösungen (Satz 4.2.10). Aber die $(p-1)/2$ quadratische Reste $\pmod{p}$ sind Lösungen der Kongruenz (21). Also besitzt (21) keine weitere Lösungen. Falls a ein quadratischer Nichtrest ist, ist a daher keine Lösung von (21). Wir schließen, dass

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

ist. □

Sei g eine Primitivwurzel $\pmod{p}$ (Korollar 5.1.8). Lemma 6.1.4 kann man auch beweisen in dem man bemerkt, dass $a \in \mathbb{Z}/p\mathbb{Z}^*$ genau dann ein quadratischer Rest $\pmod{p}$ ist, wenn $a \equiv g^{2i}$ eine gerade Potenz der Primitivwurzel ist.

Der folgende Satz gibt einige Rechenregel für das Legendre-Symbol.

Satz 6.1.5 *Sei p eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Es gilt*

(a)

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

(b) $a \equiv b \pmod{p}$ *impliziert, dass* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(c) ist $\mathrm{ggT}(a, p) = 1$, *so gilt*

$$\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right).$$

Beweis: Die Aussage (a) ist offensichtlich, falls $p \mid ab$. Falls $p \nmid ab$, folgt aus Lemma 6.1.4.(b), dass

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

Die Teilen (b) und (c) sind klar. □

Korollar 6.1.6 *Sei p eine ungerade Primzahl. Es gilt*

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

Beweis: Lemma 6.1.4.(b) impliziert, dass

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

Man überprüft leicht, dass $(p-1)/2$ genau dann gerade ist, wenn $p \equiv 1 \pmod 4$ ist. Die zweite Gleichung folgt. □

6.2 Der Beweis des quadratischen Reziprozitätsgesetz

In diesem Abschnitt formulieren und beweisen wir das quadratische Reziprozitätsgesetz. Das quadratische Reziprozitätsgesetz wurde vermutet von Euler und Legendre und bewiesen von Gauss. Wir werden sehen, wie man diese Aussagen benutzen kann, um das Legendre-Symbol effizient zu berechnen.

Definition 6.2.1 Sei p eine ungerade Primzahl. Für $x \in \mathbb{Z}$ teilerfremd zu p bezeichnen wir mit $\langle x \rangle$ die eindeutig bestimmte Zahl mit $-(p-1)/2 \leq \langle x \rangle \leq (p-1)/2$ und $\langle x \rangle \equiv x \pmod p$. Die Restklassen $-(p-1)/2 \leq \langle x \rangle < 0$ nennen wir *negative Reste*. Die Restklassen $0 < \langle x \rangle \leq (p-1)/2$ nennen wir *positive Reste*.

Für $r \in \mathbb{Q}$ schreiben wir $[r]$ für die größte ganze Zahl kleiner gleich r.

Satz 6.2.2 (Lemma von Gauß) *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ teilerfremd zu p. Sei*

$$\mathcal{S} = \{1 \leq i \leq (p-1)/2 \mid \langle ia \rangle \text{ ist ein negativer Rest}\}$$

und sei s die Kardinalität von $\mathcal{S}$. Es gilt

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Beweis: Seien a und p wie in der Aussage des Lemmas. Wir schreiben $\{\langle ia \rangle \mid 1 \leq i \leq (p-1)/2, i \in \mathcal{S}\} = \{u_1, \ldots, u_s\}$ für die negative Resten und $\{\langle ia \rangle \mid 1 \leq i \leq (p-1)/2, i \notin \mathcal{S}\} = \{v_1, \ldots, v_t\}$ für die überige Reste. Der Kürzungssatz (Satz 2.1.5) impliziert, dass die u_i und v_j paarweise verschieden sind. Wir schließen, dass

$$u_1 \cdots u_s v_1 \cdots v_t \equiv \prod_{i=1}^{(p-1)/2} (ai) \equiv a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p \qquad (22)$$

Wir behaupten, dass $-u_i \not\equiv v_j \pmod p$ für alle i und j. Sei nämlich $-u_i \equiv v_j \pmod p$. Schreibe $u_i \equiv \langle ka \rangle$ und $v_j \equiv \langle \ell a \rangle$ mit $1 \leq k, \ell \leq (p-1)/2$. Es folgt,

dass $-k \equiv \ell \pmod{p}$. Aber dies widerspricht der Annahme $1 \leq k, \ell \leq (p-1)/2$. Die Behauptung folgt.

Die Definition von u_i und v_j impliziert, dass $-u_i, v_j \in \{1, \ldots, (p-1)/2\}$ sind. Da $-u_1, \ldots, -u_s, v_1, \ldots, v_t$ genau $s + t = (p-1)/2$ verschiedene Zahlen (mod p) sind, gilt, dass

$$\{-u_1, \ldots, -u_s, v_1, \ldots, v_t\} = \{1, \ldots, (p-1)/2\}. \tag{23}$$

Daher folgt, dass

$$(-u_1) \cdots (-u_s) v_1 \cdots v_t = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)!$$

ist. Wir schließen, dass

$$(-1)^s u_1 \cdots u_s v_1 \cdot v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p} \tag{24}$$

ist. Die Gleichungen (22) und (24) implizieren daher, dass

$$(-1)^s a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

ist. Aus Lemma 6.1.4.(b) und Satz 2.1.5 folgt nun, dass

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \equiv (-1)^s \pmod{p}.$$

□

Korollar 6.2.3 *Sei p eine ungerade Primzahl. Es gilt*

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

Beweis: Das Lemma von Gauß (Satz 6.2.2) impliziert, dass

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

wobei s die Anzahl der Elemente der Menge $\mathcal{S} = \{1 \leq i \leq (p-1)/2 \mid \langle 2i \rangle < 0\}$ ist. Wir müssen zeigen, dass $s = (p^2-1)/8$ ist.

Für $1 \leq j \leq (p-1)/2$ gilt $2 \leq 2j \leq p-1$. Daher ist $\langle 2j \rangle \leq (p-1)/2$ genau dann, wenn $j \leq [(p-1)/4]$ ist. Es gilt also, dass $s = (p-1)/2 - [(p-1)/4]$ ist.

Wir schreiben $p = \alpha + 8k$ mit $\alpha \in \mathbb{Z}/8\mathbb{Z}^* = \{1, 3, 5, 7\}$. Wir betrachten nur den Fall, dass $p = 1 + 8k$ ist. Die andere Fälle sind ähnlich. In diesem Fall gilt, dass $s = (p-1)/2 - [(p-1)/4] = 4k - 2k = 2k$ gerade ist. Außerdem gilt, dass $(p^2-1)/8 = (1 + 2 \cdot 8k + 8^2k^2)/8 = 2k + 8k^2$ auch gerade ist. Wir schließen, dass

$$(-1)^s = (-1)^{(p^2-1)/8}.$$

□

Theorem 6.2.4 (Quadratische Reziprozitätsgesetz) *Seien p und q zwei verschiedene ungerade Primzahlen. Es gilt*

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

Bemerkung 6.2.5 Seien p und q wie in Theorem 6.2.4. Man kann die Aussage des quadratische Reziprozitätsgesetz auch wie folgt formulieren:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{falls } p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right) & \text{falls } p \equiv 3 \pmod 4 \text{ und } q \equiv 3 \pmod 4. \end{cases}$$

Der Beweis des quadratische Reziprozitätsgesetz benutzt folgendes Lemma.

Lemma 6.2.6 *Sei p eine ungerade Primzahl und a eine ungerade Zahl teilerfremd zu p. Es gilt*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)},$$

wobei

$$T(a,p) = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$$

ist.

Beweis: Wir benutzen die gleiche Bezeichnung wie im Lemma von Gauß (Satz 6.2.2).

Für $j = 1, \ldots, (p-1)/2$ schreiben wir

$$ja = \left[\frac{ja}{p}\right] \cdot p + \rho_j,$$

wobei $\rho_j \in \{p+u_1, \ldots, p+u_s\}$, falls ρ_j ein negativer Rest und $\rho_j \in \{v_1, \ldots, v_t\}$, falls ρ_j ein positiver Rest ist.

Es gilt, dass

$$\begin{aligned} \sum_{j=1}^{(p-1)/2} ja &= p \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] + \sum_{j=1}^{(p-1)/2} \rho_j \\ &= p \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] + ps + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_i. \end{aligned} \tag{25}$$

Aus (23) folgt, dass

$$\sum_{j=1}^{(p-1)/2} j = -\sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{26}$$

Aus (25) und (26) folgt nun, dass

$$(a-1)\sum_{j=1}^{(p-1)/2} j = p\sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] + ps + 2\sum_{j=1}^{s} u_j \equiv p(T(a,p)+s) \pmod 2,$$

da a ungerade ist. Da p ungerade ist, schließen wir, dass $T(a,p) \equiv s \pmod 2$ ist. Das Lemma von Gauß (Satz 6.2.2) impliziert nun, dass

$$\left(\frac{a}{p}\right) = (-1)^s = (-1)^{T(a,p)}.$$

□

Beweis von Theorem 6.2.4: Seien p und q zwei verschiedene, ungerade Primzahlen. Lemma 6.2.6 impliziert, dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(p,q)+T(q,p)} \tag{27}$$

ist, wobei

$$T(p,q) = \sum_{j=1}^{(q-1)/2}\left[\frac{jp}{q}\right], \quad T(q,p) = \sum_{j=1}^{(p-1)/2}\left[\frac{jq}{p}\right]$$

ist. Zu zeigen ist, dass $T(p,q)+T(q,p) \equiv (p-1)(q-1)/4 \pmod 2$ ist.

Wir betrachten dazu die Menge

$$\mathcal{G} = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} \mid 1 \le x \le (p-1)/2, 1 \le y \le (q-1)/2\}.$$

Wir definieren folgende Teilmengen von $\mathcal{G}$:

$$\mathcal{G}_1 = \{(x,y) \in \mathcal{G} \mid qx > py\}, \qquad \mathcal{G}_2 = \{(x,y) \in \mathcal{G} \mid qx < py\}.$$

Da $p \neq q$, sind p und q teilerfremd. Dies impliziert, dass kein Paar $(x,y) \in \mathcal{G}$ mit $qx = py$ existiert. Daher ist $\mathcal{G}$ die disjunkte Vereinigung von $\mathcal{G}_1$ und $\mathcal{G}_2$. Wir schließen, dass $|\mathcal{G}_1| + |\mathcal{G}_2| = |\mathcal{G}| = (p-1)(q-1)/4$. Die Anzahl der Gitterpunkte in $\mathcal{G}$ unterhalb der Gerade $qx = py$ ist

$$|\mathcal{G}_1| = \sum_{x=1}^{(p-1)/2}\left[\frac{qx}{p}\right] = T(q,p).$$

Ebenso gilt, dass die Anzahl der Gitterpunkte in $\mathcal{G}$ oberhalb der Gerade $qx = py$

$$|\mathcal{G}_2| = \sum_{y=1}^{(q-1)/2}\left[\frac{py}{q}\right] = T(p,q)$$

ist. Also folgt, dass

$$T(p,q) + T(q,p) = |\mathcal{G}_1| + |\mathcal{G}_2| = \frac{(p-1)(q-1)}{4}.$$

Das quadratische Reziprozitätsgesetz folgt daher aus (27). □

Beispiel 6.2.7 (a) Wir erläutern wie man mit Hilfe der Rechnenregeln (Satz 6.1.5) und das quadratische Reziprozitätsgesetz (Theorem 6.2.4, Korollar 6.1.6 und Korollar 6.2.3) Legendre-Symbole berechnen kann. Wir bestimmen ob 7 ein quadratischer Rest (mod 19) ist. Da $7 \equiv 19 \equiv 3 \pmod 4$, gilt

$$\left(\frac{7}{19}\right) \overset{\text{QR}}{=} -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) \overset{\text{QR}}{=} -\left(\frac{2}{5}\right) = 1.$$

(b) Wir bestimmen ob 713 ein quadratischer Rest (mod 1009) ist. Bemerke, dass 1009 eine Primzahl ist. Dies überprüft man zum Beispiel mit Hilfe der Probedivision (§ 1.3). Die Primfaktorzerlegung von 713 ist $23 \cdot 31$. Wir berechnen

$$\begin{aligned}\left(\frac{23}{1009}\right) &\overset{\text{QR}}{=} +\left(\frac{1009}{23}\right) \overset{\text{(b)}}{=} \left(\frac{2^2 \cdot 5}{23}\right) \overset{\text{(c)}}{=} \left(\frac{5}{23}\right) \overset{\text{QR}}{=} +\left(\frac{23}{5}\right) \\ &\overset{\text{(b)}}{=} \left(\frac{3}{5}\right) \overset{\text{QR}}{=} +\left(\frac{2}{3}\right) = -1.\end{aligned}$$

Hierbei ist QR die Abkürzung für das quadratische Reziprozitätsgesetz und (a)-(c) beziehen sich auf die Teile von Satz 6.1.5. Ebenso folgt, dass

$$\left(\frac{31}{1009}\right) \overset{\text{QR}}{=} \left(\frac{17}{31}\right) \overset{\text{QR}}{=} \left(\frac{14}{17}\right) \overset{(a)}{=} \left(\frac{2}{17}\right) \cdot \left(\frac{7}{17}\right) \overset{\text{QR}}{=} +1 \left(\frac{3}{7}\right) \overset{\text{QR}}{=} -\left(\frac{1}{3}\right) = -1.$$

Wir schließen, dass

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right) \cdot \left(\frac{31}{1009}\right) = (-1)(-1) = 1.$$

Also ist 713 ein quadratischer Rest (mod 1009).

(c) Wir fragen uns ob die Kongruenz $x^2 \equiv 13 \pmod{76}$ lösbar ist. Da $76 = 4 \cdot 19$ sagt der chinesische Restsatz (Theorem 2.7), dass die Kongruenz äquivalent ist zu

$$\begin{cases} x^2 \equiv 13 \equiv 1 \pmod 4, \\ x^2 \equiv 13 \pmod{19}. \end{cases} \tag{28}$$

Um zu bestimmen ob die zweite Kongruenz lösbar ist, berechnen wir

$$\left(\frac{13}{19}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -\left(\frac{1}{3}\right) = -1.$$

Wir schließen, dass die zweite Kongruenz von (28) nicht lösbar ist, und also auch die ursprüngliche Kongruenz nicht.

6.3 Das Jacobi-Symbol

In Beispiel 6.2.7 haben wir gesehen, dass wir die Zahl 713 faktorisieren müssen um das Legendre-Symbol $(\frac{713}{1009})$ zu berechnen. Für kleine Zahlen wie 713 ist dies kein Problem, aber für sehr große Zahlen ist dies unpraktisch (siehe § 3.4). In diesem Abschnitt besprechen wir eine Verallgemeinerung des Legendre-Symbols welches uns erlaubt, das Legendre-Symbol von großen Zahlen zu berechnen, ohne in jedem Schritt die Primfaktorzerlegung zu berechnen.

Definition 6.3.1 Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd zu n. Sei $n = p_1 \cdot p_2 \cdots p_r$ die Primfaktorzerlegung von n. Das *Jacobi-Symbol* $(\frac{a}{n})$ ist definiert als

$$(\frac{a}{n}) = \prod_{i=1}^{r} (\frac{a}{p_i}),$$

wobei $(\frac{a}{p_i})$ das Legendre-Symbol ist.

Bemerkung 6.3.2 Falls $(\frac{a}{n}) = -1$, so ist die Kongruenz $x^2 \equiv a \pmod{n}$ nicht lösbar, da mindestens eine der Legendre-Symbole $(\frac{a}{p_i}) = -1$ ist. Falls $(\frac{a}{n}) = +1$, können wir nur schließen, dass die Anzahl der Primzahlen p_i mit $(\frac{a}{p_i}) = -1$ gerade ist. Wir können daher nicht schließen, dass a eine quadratische Rest $\pmod{n}$ ist.

Das Jacobi-Symbol erfüllt die gleichen Rechenregeln wie das Legendre-Symbol.

Satz 6.3.3 *Seien n und n' ungerade, natürliche Zahlen.*

(a) Falls $a \equiv a' \pmod{n}$, so ist $(\frac{a}{n}) = (\frac{a'}{n})$.

(b) Es gilt $(\frac{a}{n})(\frac{a}{n'}) = (\frac{a}{nn'})$ und $(\frac{a}{n})(\frac{a'}{n}) = (\frac{aa'}{n})$.

Beweis: Dies folgt direkt aus der Definition des Jacobi-Symbols. □

Folgendes Theorem ist das quadratische Reziprozitätsgesetz für Jacobi-Symbole.

Theorem 6.3.4 *Seien n und m ungerade natürliche Zahlen, welche teilerfemd sind. Es gilt:*

(a) $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$,

(b) $(\frac{-1}{n}) = (-1)^{(n-1)/2}$,

(c) $(\frac{m}{n})(\frac{n}{m}) = (-1)^{(m-1)(n-1)/4}$.

Beweis: (a) Sei $n = p_1 \cdots p_r$ die Primfaktorzerlegung von n. Laut Definition des Jacobi-Symbols und Korollar 6.2.3 gilt, dass

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{r} \left(\frac{2}{p_i}\right) = (-1)^{\sum_{i=1}^{r}(p_i^2-1)/8}.$$

Für ungerade Zahlen a und b zeigt man, dass

$$(a^2b^2 - 1) - (a^2 - 1) - (b^2 - 1) = (a^2 - 1)(b^2 - 1).$$

Da $a \equiv b \equiv 1 \pmod{2}$, folgt, dass $a^2 - 1 \equiv b^2 - 1 \equiv 0 \pmod{4}$, also $(a^2b^2 - 1) \equiv (a^2 - 1) + (b^2 - 1) \pmod{16}$. Hieraus folgt mit Induktion, dass

$$p_1^2 \cdots p_r^2 - 1 \equiv \sum_{i=1}^{r} (p_i^2 - 1) \pmod{16}. \tag{29}$$

Wir schließen, dass

$$\left(\frac{2}{n}\right) = (-1)^{\sum_{i=1}^{r}(p_i^2-1)/8} = (-1)^{(n^2-1)/8}.$$

Teil (b) folgt ähnlich wie (a) aus

$$p_1 \cdots p_r - 1 \equiv \sum_{i=1}^{r}(p_i - 1) \pmod 4. \tag{30}$$

(c) Schreibe $m = \prod_{j=1}^{t} q_j$ und $n = \prod_{i=1}^{r} p_i$. Satz 6.3.3.(b) und Theorem 6.2.4 implizieren, dass

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{j=1}^{t}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}}.$$

Wir schreiben $\sum_{i=1}^{r}(p_i-1) = p_1\cdots p_r - 1 + 4A$ und $\sum_{j=1}^{t}(q_j-1) = q_1\cdots q_t - 1 + 4B$ (Kongruenz (30)). Da n und m ungerade sind, folgt, dass

$$\begin{aligned}\sum_{i,j}(p_i-1)(q_j-1) &= [\sum_{i=1}^{r}(p_i-1)]\cdot[\sum_{j=1}^{t}(q_j-1)] \\ &= [p_1\cdots p_r - 1 + 4A][q_1\cdots q_t - 1 + 4B] \\ &= (n-1)(m-1) + 4[A(m-1) + B(n-1)] + 16AB \\ &\equiv (n-1)(m-1) \pmod 8.\end{aligned}$$

Dies impliziert (c). □

Beispiel 6.3.5 Mit Hilfe des Jacobi-Symbol kann man nun schnell das Legendre-Symbol berechnen:

$$\begin{aligned}\left(\frac{383}{443}\right) &= -\left(\frac{443}{383}\right) = -\left(\frac{2^2\cdot 15}{383}\right) = -\left(\frac{15}{383}\right) = \left(\frac{383}{15}\right) \\ &= \left(\frac{2^3}{15}\right) = \left(\frac{2}{15}\right) = 1\end{aligned}$$

Da 443 eine Primzahl ist, schließen wir, dass 383 ein quadratischer Rest (mod 443) ist. Der Vorteil gegenüber der Methode von § 6.2 ist, dass wir die Primfaktorzerlegung der Zwischenschritte nur unvolständig Berechnung müssen: Wir brauchen nur die Faktoren 2.

7 Diophantische Gleichungen

In diesem Abschnitt betrachten wir einige Beispiele von diophantische Gleichungen. Eine *diophantische Gleichung* ist eine Gleichung $f(x_1, x_2, \ldots, x_n) = 0$,

wobei $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ ein Polynom mit ganzzahligen Koeffizienten ist. Ziel ist es ganzzahlige Lösungen $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ der Gleichung zu finden. Diophantische Gleichungen sind benannt nach dem griechischen Mathematiker Diophant von Alexandrien. Er lebte rund 250 n. Chr. Mehr Information finden Sie auf der MacTutor-Webseite:
`http://www-groups.dcs.st-and.ac.uk/ history/Biographies/Diophantus.html`.

Die berühmteste diophantische Gleichung ist $x^n + y^n = z^n$. Der letzte Satz von Fermat besagt, dass diese Gleichung keine Lösung besitzt für $x, y, z \in \mathbb{N}$ und $n > 3$. Der Satz ist benannt nach Pierre de Fermat, einem französischen Mathematiker der rund 1630 in einer Übersetzung von Diophants' Arithmetica schrieb, dass er ein wahrhaft wunderbaren Beweis gefunden habe, für den aber auf dem Rand nicht genug Platz sei. Der Satz wurde letztendlich 1994 von Wiles und Taylor–Wiles bewiesen. Hier finden Sie mehr Information:
`http://www-history.mcs.st-andrews.ac.uk/HistTopics/Fermat's_last_theorem.html`

7.1 Pythagoräische Tripel

Der Satz des Pythagoras ist der vieleicht bekannteste Satz der Mathematik. Er besagt, dass in einem rechtwinkligen Dreieck die Summe der Flächeninhalte der Kathetenquadrate gleich den Flächeninhalt des Hypotenusenquadrates ist. In Formel:

$$a^2 + b^2 = c^2, \tag{31}$$

wobei c die Länge der Hypotenuse eines rechtwinkligen Dreiecks ist, und a und b die Länge der überigen Seiten sind. In diesem Abschnitt betrachten wir Lösungen von (31) wobei a, b, c natürliche Zahlen sind.

Definition 7.1.1 (a) Ein Tripel $(a, b, c) \in \mathbb{N}^3$ heißt *pythagoräisches Tripel*, falls $a^2 + b^2 = c^2$.

(b) Ein pytagoräisches Tripel heißt *primitiv*, falls $\mathrm{ggT}(a, b, c) = 1$.

Beispiel 7.1.2 Beispiele von primitive pythagoräische Tripeln sind

$$3^2 + 4^2 = 5^2, \qquad 5^2 + 12^2 = 13^2.$$

Falls (a, b, c) ein primitives pythagoräisches Tripel ist, so ist $(\alpha a, \alpha b, \alpha c)$ auch ein pythagoräisches Tripel, für jedes $\alpha \in \mathbb{N}$. Um alle pythagoräischen Tripeln zu bestimmen, reicht es also die primitiven Tripel zu bestimmen.

Bemerkung 7.1.3 Sei (a, b, c) ein primitives pythagoräisches Tripel. Die Zahlen a und b sind nicht beide ungerade. Falls nämlich $a \equiv b \equiv 1 \pmod 2$, gilt $c^2 = a^2 + b^2 \equiv 2 \pmod 2$. Aber 2 ist ein quadratischer Nichtrest (modulo 4).

Theorem 7.1.4 *Sei $a, b, c \in \mathbb{N}$ mit b gerade und $\mathrm{ggT}(a, b, c) = 1$. Nun ist (a, b, c) genau dann ein primitives pythagoräisches Tripel, wenn $r, s \in \mathbb{N}$ mit $r > s$ und $r \not\equiv s \pmod 2$ und $\mathrm{ggT}(r, s) = 1$, sodass*

$$a = r^2 - s^2, \qquad b = 2rs, \qquad c = r^2 + s^2 \tag{32}$$

existieren.

Beweis: Sei r, s wie in (32). Es gilt

$$a^2 + b^2 = (r^2 - s^2)^2 + (2rs)^2 = (r^2 + s^2)^2 = c^2.$$

Außerdem gilt, dass $\mathrm{ggT}(a, b, c) = 1$. Also ist (a, b, c) ein primitives pythagoräisches Tripel.

Sei (a, b, c) ein primitives pythagoräisches Tripel. Ohne Einschränkung dürfen wir annehmen, dass b gerade ist (Bemerkung 7.1.3). Es gilt $b^2 = c^2 - a^2 = (c+a)(c-a)$. Da $b \equiv 0 \bmod 2$, gilt also, dass $a \equiv c \pmod 2$. Da $\mathrm{ggT}(a, b, c) = 1$, sind a und c beide ungerade. Also finden wir, dass

$$\left(\frac{b}{2}\right)^2 = \left(\frac{c-a}{2}\right)\left(\frac{c+a}{2}\right). \tag{33}$$

Wir behaupten, dass $d := \mathrm{ggT}(a, c) = 1$. Es gilt, dass $d \mid (c-a)$ und $d \mid (c+a)$. Also impliziert (33), dass $d^2 \mid b^2$. Da $\mathrm{ggT}(a, b, c) = 1$ ist, folgt also, dass $d = 1$.

Wir haben gezeigt, dass $\mathrm{ggT}(a, c) = 1$. Hieraus folgt auch, dass $\mathrm{ggT}((c-a)/2, (a+c)/2) = 1$. Daher impliziert (33), dass $(c-a)/2$ und $(c+a)/2$ Quadrate sind. Wir schreiben

$$\left(\frac{c+a}{2}\right) = r^2, \qquad \left(\frac{c-a}{2}\right) = s^2,$$

also

$$c = r^2 + s^2, \qquad a = r^2 - s^2, \qquad b = 2rs.$$

Außerdem gilt $\mathrm{ggT}(r, s) = \mathrm{ggT}((c-a)/2, (a+c)/2) = 1$. Da

$$r^2 = \left(\frac{c+a}{2}\right) = \left(\frac{c-a}{2}\right) + a = s^2 + a \equiv s^2 + 1 \pmod 2,$$

gilt $r \not\equiv s \pmod 2$. □

Der geometrische Beweis.
Wir geben einen zweiten geometrischen Beweis von Theorem 7.1.4. Sei (a, b, c) ein primitives pythagoräisches Tripel. Wir erlauben jetzt $a, b, c \in \mathbb{Z}$. Sei $P = (a/c, b/c) =: (p, q) \in \mathbb{Q} \times \mathbb{Q}$. Es gilt $p^2 + q^2 = 1$, also ist P einen Punkt auf dem Einheitskreis $x^2 + y^2 = 1$.

Sei nun $P = (p, q) \neq (1, 0)$ einen Punkt auf dem Einheitskreis mit $p, q \in \mathbb{Q}$. Wir betrachten die Gerade L durch P und $(1, 0)$. Die Gerade L ist gegeben durch die Gleichung

$$y = t(1 - x), \qquad \text{mit } t = \frac{q}{1-p}.$$

Lemma 7.1.5 *Sei* $\mathcal{S} = \{(p,q) \in \mathbb{Q} \times \mathbb{Q} \,|\, p^2 + q^2 = 1\} \setminus \{(1,0)\}$. *So ist*

$$F : \mathcal{S} \to \mathbb{Q}\backslash, \qquad (p,q) \mapsto t = \frac{q}{1-p}$$

eine Bijektion.

Beweis: Sei $(p,q) \in \mathcal{S}$. Da $(p,q) \neq (1,0)$, ist $p \neq 1$. Also ist $t = q/(1-p) \in \mathbb{Q}$.

Sei nun $t \in \mathbb{Q}$. Wir betrachten die Gerade L_t durch $(1,0)$ mit Steigung t. Die Gleichung der Gerade L_t ist $y = t(1-x)$. Wir berechnen die Schnittpunkte von L_t mit dem Einheitskreis. Wir finden

$$\begin{aligned} 1 &= x^2 + [t(1-x)]^2, \\ 0 &= x^2(1+t^2) - 2t^2 x + t^2 - 1, \\ x &= \frac{2t^2}{2(1+t^2)} \pm \frac{1}{2(1+t^2)} \sqrt{4t^4 - 4t^4 + 4}. \end{aligned}$$

Also gilt

$$(x,y) = (1,0), \qquad \text{oder} \qquad (x,y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1} \right).$$

Beide Punkte haben rationale Koordinaten.

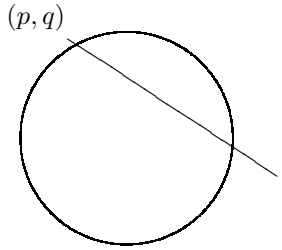
Wir sehen, dass L_t 2 Schnittpunkte mit der Einheitskreis hat: Der Punkt $(1,0)$ und ein Punkt $P = P_t \in \mathcal{S}$. Wir überlassen es den Leser zu überprüfen, dass die Abbildung $t \mapsto P_t$ eine Umkehrabbildung zu F definiert. Wir schließen, dass F eine Bijektion ist. □

Theorem 7.1.6 *Die Gleichung* $x^4 + y^4 = z^2$ *hat keine Lösungen mit* $x, y, z \in \mathbb{N}$.

Aus Theorem 7.1.6 folgt der letzte Satz von Fermat für $n = 4$.

Korollar 7.1.7 *Die Gleichung* $x^4 + y^4 = z^4$ *hat keine Lösungen mit* $x, y, z \in \mathbb{N}$.

Beweis: Sei $(x,y,z) \in \mathbb{N}^3$ mit $x^4 + y^4 = z^4$, so ist (x,y,z^2) eine Lösung zu der Gleichung von Theorem 7.1.6. Dies liefert einen Widerspruch. □



Beweis des Theorems: Wir nehmen an, dass die Gleichung $x^4 + y^4 = z^2$ eine Lösung hat. Sei $x_0, y_0, z_0 \in \mathbb{N}$ eine Lösung mit z_0 minimal. Insbesondere gilt, dass $\text{ggT}(x_0, y_0) = 1$ ist.

Sei $x_0 \equiv y_0 \equiv 1 \pmod 2$. Es gilt, dass $x_0^4 \equiv y_0^4 \equiv 1 \pmod 8$. Aber 2 ist ein quadratischer Nichtrest modulo 8. Also sind x_0 und y_0 nicht beide ungerade. Wir dürfen also annehmen, dass y_0 gerade ist.

Nun ist (x_0^2, y_0^2, z_0) ein primitives pythagoräisches Tripel. Theorem 7.1.4 impliziert daher, dass $r, s \in \mathbb{N}$ existieren, sodass

$$x_0^2 = r^2 - s^2, \quad y_0^2 = 2rs, \quad z_0 = r^2 + s^2, \qquad \text{ggT}(r, s) = 1.$$

Da $x_0^2 + s^2 = r^2$ und $\text{ggT}(x_0, r, s) = 1$ folgt, dass (x_0, s, r) ein primitives pythagoräisches Tripel ist.

Wir wenden Theorem 7.1.4 nun auf (x_0, s, r) an und finden, dass $\rho, \sigma \in \mathbb{N}$ existieren, sodass

$$x_0 = \rho^2 - \sigma^2, \quad s = 2\rho\sigma, \quad r = \rho^2 + \sigma^2, \qquad \text{ggT}(\rho, \sigma) = 1.$$

Da $y_0^2 = 2rs$, finden wir

$$\left(\frac{y_0}{2}\right)^2 = \rho\sigma(\rho^2 + \sigma^2).$$

Da $\rho, \sigma, \rho^2 + \sigma^2$ paarweise teilerfremd sind und das Produkt dieser 3 Elementen einen Quadratzahl ist, existieren $u, v, w \in \mathbb{Z}$, sodass

$$\rho = u^2, \quad \sigma = v^2, \quad \rho^2 + \sigma^2 = w^2.$$

Wir finden nun, dass

$$w^2 = \rho^2 + \sigma^2 = u^4 + v^4.$$

Also ist (u, v, w) eine Lösung der Gleichung $u^4 + v^4 = w^2$. Aber

$$|w| = \sqrt{\rho^2 + \sigma^2} = \sqrt{r} < r^2 + s^2 = z_0.$$

Dies widerspricht der Wahl der Lösung (x_0, y_0, z_0). Also hat die Gleichung keine Lösungen. □

7.2 Welche Zahlen sind die Summe von zwei Quadraten?

In diesem Abschnitt fragen wir uns, welche natürliche Zahlen man als Summe von zwei Quadraten schreiben kann. Um zu überprüfen ob eine Zahl n sich schreiben lässt als Summe von zwei Quadraten, überprüfen wir ob $n - a^2$ eine Quadratzahl ist, wobei es reicht die Zahlen a kleiner gleich $\sqrt{n/2}$ zu überprüfen. Dies sieht man wie folgt: Sei $n = a^2 + b^2$ mit $a \leq b$. Es folgt, dass $n \geq 2a^2$, also $a \leq \sqrt{n/2}$.

Zuerst gucken wir uns eine kleine Tabelle an und fragen uns ob wir ein Muster erkennen können.

$1 = 0^2 + 1^2$	11 Nein	21 Nein
$2 = 1^2 + 1^2$	12 Nein	22 Nein
3 Nein	$13 = 2^2 + 3^3$	23 Nein
$4 = 0^2 + 2^2$	14 Nein	24 Nein
$5 = 1^2 + 2^2$	15 Nein	$25 = 0^2 + 5^2 = 3^2 + 4^2$
6 Nein	$16 = 0^2 + 4^2$	$26 = 1^2 + 5^2$
7 Nein	$17 = 1^2 + 4^2$	27 Nein
$8 = 2^2 + 2^2$	$18 = 3^2 + 3^2$	28 Nein
$9 = 0^2 + 3^2$	19 Nein	$29 = 2^2 + 5^2$
10 Nein	$20 = 2^2 + 4^2$	30 Nein

Auf den ersten Blick ist es nicht einfach ein Muster zu erkennen. Einfacher wird es, wenn wir uns die Primzahlen angucken: Die Primzahlen kleiner 30 die sich als Summe von zwei Quadraten schreiben lassen sind: $2, 5, 13, 17, 29$. Die übrigen Primzahlen $3, 11, 19, 23$ sind keine Summe von zwei Quadraten. Wir vermuten nun, dass eine Primzahl p genau dann die Summe von zwei Quadraten ist, wenn $p = 2$ oder $p \equiv 1 \pmod 4$ ist. Wir werden sehen, dass dies tatsächlich stimmt (Theorem 7.2.3). Folgendes Lemma zeigt eine Richtung der Aussage.

Lemma 7.2.1 *Sei $n = a^2 + b^2$, so gilt, dass $n \not\equiv 3 \pmod 4$ ist.*

Beweis: Die quadratische Reste (mod 4) sind $0, 1$. Falls $n = a^2 + b^2$ gilt daher, dass n kongruent zu $0 + 0 = 0,\ 0 + 1 \equiv 1 + 0 \equiv 1$ oder $1 + 1 \equiv 2 \pmod 4$ ist. □

Bemerkung 7.2.2 Falls p eine ungerade Primzahl ist, können wir auch einen alternativen Beweis von Lemma 7.2.1 geben mit Hilfe des Legendre-Symbols. Wir nehmen an, dass $p = a^2 + b^2$. Da p eine Primzahl ist, folgt, dass a und b teilerfemd zu p sind. Also gilt $a^2 \equiv -b^2 \pmod p$. Die Rechenregeln für das Legendre-Symbol (Satz 6.1.5) implizieren, dass

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

Aus Korollar 6.1.6 folgt, dass $(\frac{-1}{p}) = 1$ genau dann, wenn $p \equiv 1 \pmod 4$ ist.

Bemerkung 7.2.2 stellt eine Beziehung her zwischen dem Legendre-Symbol und der Frage welche Zahlen die Summe von zwei Quadraten sind. Diese Idee benutzen wir im Beweis von Theorem 7.2.3.

Theorem 7.2.3 *Eine Primzahl p ist genau dann die Summe von zwei Quadraten, wenn $p = 2$ oder $p \equiv 1 \pmod 4$.*

Beweis: Falls $p = a^2 + b^2$ die Summe von zwei Quadraten ist, so folgt aus Lemma 7.2.1, dass $p = 2$ oder $p \equiv 1 \pmod 4$ ist. Wir haben schon gesehen, dass $p = 2$ die Summe von zwei Quadraten ist.

Sei $p \equiv 1 \pmod 4$ eine Primzahl. Wir zeigen, dass $p = a^2 + b^2$ die Summe von zwei Quadraten ist. Die Beweismethode heißt *Fermats Abstiegargument*.

Aus Bemerkung 7.2.2 folgt, dass $(\frac{-1}{p}) = 1$. Also existiert eine Zahl $0 \leq A < p$ mit $A^2 \equiv -1 \pmod p$. Wähle m mit $A^2 + 1 = m \cdot p$. Da $m = (A^2 + 1)/p$, gilt

$$m \leq \frac{(p-1)^2 + 1^2}{p} = p - \frac{2(p-1)}{p} < p.$$

Falls $m = 1$, sind wir fertig. Wir nehmen daher an, dass $m > 1$ ist, und setzen $a_0 = A, b_0 = 1$ und $m_0 = m$. Ziel der Methode ist es neue Zahlen (a_1, b_1, m_1) zu finden mit $a_1^2 + b_1^2 = m_1 \cdot p$ und $m_1 < m_0$. Wir wiederholen dies so Lange bis $m_r = 1$. Dann haben wir $p = m_r \cdot p = a_r^2 + b_r^2$ geschrieben als Summe von zwei Quadraten.

Das Verfahren beruht auf folgender Formel, welche man leicht überprüft:

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2. \tag{34}$$

Fermats Abstiegargument: Gegeben sind Zahlen (a_i, b_i, m_i) mit $1 < m_i < p$ und $a_i^2 + b_i^2 = m_i \cdot p$. Wir suchen Zahlen $(a_{i+1}, b_{i+1}, m_{i+1})$ mit $1 < m_{i+1} < m_i$ und $a_{i+1}^2 + b_{i+1}^2 = m_{i+1} \cdot p$.

Wähle $-m_i/2 \leq u_i, v_i \leq m_i/2$, sodass $u_i \equiv a_i \pmod{m_i}$ und $v_i \equiv b_i \pmod{m_i}$. Es gilt, dass

$$0 \equiv a_i^2 + b_i^2 \equiv u_i^2 + v_i^2 \pmod{m_i}.$$

Wir schreiben $u_i^2 + v_i^2 = m_i \cdot r_i$.

Wir behaupten, dass

(a) $1 \leq r_i < m_i$,

(b) $m_i \mid (u_i a_i + v_i b_i)$,

(c) $m_i \mid (v_i a_i - u_i b_i)$.

Behauptung (b) und (c) folgen direkt aus der Definition von u_i und v_i. Für (a), bemerken wir, dass

$$r_i = \frac{u_i^2 + v_i^2}{m_i} \leq \frac{(m_i/2)^2 + (m_i/2)^2}{m_i} = \frac{1}{2}\frac{m_i^2}{m_i} = \frac{1}{2}m_i < m_i.$$

Offensichtlich gilt, dass $r_i \geq 0$. Wir nehmen an, dass $r_i = 0$. Es folgt, dass $u_i^2 + v_i^2 = 0$ ist, also gilt $u_i = v_i = 0$. Dies impliziert, dass $a_i \equiv b_i \equiv 0 \pmod{m_i}$ ist. Also gilt, dass m_i^2 ein Teiler von $a_i^2 + b_i^2 = m_i \cdot p$ ist. Hieraus folgt, dass $m_i = 1$ ist, aber dies hatten wir ausgeschlossen. Wir schließen, dass $r_i \geq 1$ ist. Dies beweist Behauptung (a).

Mit Hilfe von (34), schreiben wir nun

$$m_i^2 r_i p = (u_i^2 + v_i^2)(a_i^2 + b_i^2) = (u_i a_i + v_i b_i)^2 + (v_i a_i - u_i b_i)^2. \qquad (35)$$

Wir definieren

$$a_{i+1} = \frac{u_i a_i + v_i b_i}{m_i}, \quad b_{i+1} = \frac{v_i a_i - u_i b_i}{m_i}, \quad m_{i+1} = r_i.$$

Aus (34) folgt, dass

$$a_{i+1}^2 + b_{i+1}^2 = m_{i+1} p, \qquad \text{mit } 1 \leq m_{i+1} < m_i.$$

Wie oben erklärt, folgt die Aussage des Theorems mittels Induktion. □

Beispiel 7.2.4 Wir schreiben $p = 881$ als Summe von zwei Quadraten mit Hilfe des Abstiegsarguments.

Wir bemerken, dass $p = 881 \equiv 1 \pmod 4$. Wir suchen zuerst eine Lösung der Kongruenz $x^2 \equiv -1 \pmod p$. Hier ist eine Methode so eine Lösung zu finden. Wähle $0 < a < p$ beliebig und setze $x = a^{(p-1)/4}$. Bemerke, dass $(p-1)/4$ eine ganze Zahl ist, da $p \equiv 1 \pmod 4$. Lemma 6.1.4 sagt, dass $(\frac{a}{p}) = a^{(p-1)/2} = x^2$ ist. Also ist $x^2 \equiv -1 \pmod p$ genau dann, wenn a ein quadratischer Nichtrest ist.

Wir finden, dass $2^{(p-1)/2} \equiv 1 \pmod p$ und $3^{(p-1)/2} \equiv -1 \pmod p$, also ist 2 ein quadratischer Rest (mod p) und 3 ein quadratischer Nichtrest (mod p). Wir schließen, dass $x \equiv 3^{(p-1)/4} \equiv 387$ eine Lösung der Kongruenz $x^2 \equiv -1 \pmod p$ ist.

Folgende Tabelle gibt die Werte der Variablen a_i, b_i, m_i, u_i, v_i und r_i für jedes i an.

i	a_i	b_i	m_i	u_i	v_i	r_i
0	387	1	170	47	1	13
1	107	2	13	3	2	1
2	25	16	1	−	−	−.

Wir finden daher als Lösung $881 = 25^2 + 16^2$. Da 881 eine relativ kleine Zahl ist, hätte man dies auch einfach durch ausprobieren lösen können.

Als Nächstes möchten wir besprechen welche zusammengesetzte Zahlen man als Summe von zwei Quadraten schreiben kann. Wir werden sehen, dass die Antwort für n sich auf der Antwort für die Primfaktoren von n zurückführen lässt.

Theorem 7.2.5 *Sei n eine natürliche Zahl mit Primfaktorzerlegung $n = \prod_i p_i^{e_i}$, wobei $p_i \neq p_j$ für $i \neq j$ ist. Die Zahl n kann man schreiben als Summe von zwei Quadraten genau dann, wenn für jedes i mindestens eine der folgenden Bedingungen erfüllt ist:*

- $p_i = 2$,

- $p_i \equiv 1 \pmod 4$,
- e_i *gerade.*

Beweis: Der Beweis folgt aus einem wiederholten Anwenden der Formel (34). Wir überlassen dies dem Leser/der Leserin. □

Beispiel 7.2.6 Wir betrachten die Zahl $n = 585 = 3^2 \cdot 5 \cdot 13$. Da $5 \equiv 13 \equiv 1 \pmod 4$, lässt n sich schreiben als Summe von zwei Quadraten. Da $5 = 1^2 + 2^2$ und $13 = 2^2 + 3^2$, finden wir mit Hilfe von (34), dass

$$n = 3^2(1^2+2^2)(2^2+3^2) = 3^2[(1\cdot 2+2\cdot 3)^2+(2\cdot 2-1\cdot 3)^2] = (3\cdot 8)^2+(3\cdot 1)^2 = 24^2+3^2.$$

7.3 Die gaußsche Zahlen

In diesem Abschnitt geben wir einen alternativen Beweis von Theorem 7.2.5 mit Hilfe der Primfaktorzerlegung in dem Ring der gaußschen Zahlen. Hierzu betrachten wir die Zerlegung $n = a^2 + b^2 = (a + bi)(a - bi)$, wobei $i^2 = -1$ ist. Als Hilfmittel für diesen Beweis müssen wir zuerst die Begriffe Primzahl, Primfaktorzerlegung und euklidischer Algorithmus auf dem Ring der gaußschen Zahlen verallgemeinern.

Definition 7.3.1 Sei $\mathbb{Z}[i] = \{a + bi \mid a, b, \in \mathbb{Z}\}$ der Ring der ganzen gaußschen Zahlen. Addition und Multiplikation sind definiert durch:

$$(a+bi)+(c+di) = (a+c)+(b+d)i, \qquad (a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i.$$

Insbesondere ist $i^2 = -1$.

Die *Norm* einer ganzen gaußschen Zahl $z = a + bi$ ist definiert als $N(z) = a^2 + b^2 \in \mathbb{Z}_{\geq 0}$.

Wir bemerken, dass jede ganze gaußsche Zahl $z = a+bi$ auch eine komplexe Zahl ist. Sei $|z|$ der komplexe Betrag, so gilt $N(z) = |z|^2 = z \cdot \bar{z}$, wobei $\bar{z} = a-bi$ die Konjugierte von z ist. Hieraus folgt die Relation $N(z)N(w) = N(z \cdot w)$. Außerdem gilt, dass $N(z) = 0$ ist genau dann, wenn $z = 0$. Für alle $z \neq 0$ ist $N(z) \geq 1$.

Definition 7.3.2 (a) Seien z, w ganze gaußsche Zahlen. Wir sagen, dass z ein Teiler von w ist, falls eine ganze gaußsche Zahl $v \neq 0$ mit $z \cdot v = w$ existiert. Wir schreiben: $z \mid w$.

(b) Eine ganze gaußsche Zahl z heißt *Einheit*, falls z ein Teiler von 1 ist, oder äquivalent, falls $z^{-1} \in \mathbb{Z}[i]$ ist.

Sei $z = a + bi \neq 0$. Die Zahl z^{-1} berechnet man, wie für komplexe Zahlen:

$$\frac{1}{z} = \frac{1}{a+bi}\frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2} = \frac{\bar{z}}{N(z)}. \tag{36}$$

Folgendes Lemma bestimmt die Einheiten in $\mathbb{Z}[i]$.

Lemma 7.3.3 *Die Einheiten in $\mathbb{Z}[i]$ sind genau die Zahlen mit $N(\alpha) = 1$. Dies sind $\pm 1, \pm i$.*

Beweis: Sei $z = a + bi \in \mathbb{Z}[i]$ eine Einheit. Also existiert $w = z^{-1} \in \mathbb{Z}[i]$ mit $z \cdot w = 1$. Nun gilt, dass $N(z)N(w) = N(1) = 1$. Da $N(z) \in \mathbb{N}$ ist, folgt, dass $N(z) = 1$. Also gilt $a^2 + b^2 = 1$. Hieraus folgt, dass $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ ist. Also ist $z \in \{\pm 1, \pm i\}$. □

Der folgende Satz erklärt wie Division mit Rest in $\mathbb{Z}[i]$ funktioniert. Dies ist die Grundlage für dem euklidischen Algorithmus in $\mathbb{Z}[i]$ (Beispiel 7.3.5). Ein kommutativer Ring R mit einem euklidischen Algorithmus heißt *euklidischer Ring*. Aus technischen Gründen müssen wir auch fordern, dass R keine Nullteiler besitzt. (Dies sind Zahlen $z \neq 0$ mit $z \mid 0$.) Beispiele von euklidischen Ringen sind $\mathbb{Z}$, $\mathbb{Z}[i]$ und $k[x]$, wobei k ein Körper ist.

Satz 7.3.4 (Division mit Rest) *Seien $\alpha = a + bi, \beta = c + di \neq 0 \in \mathbb{Z}[i]$. Es existieren $q, r \in \mathbb{Z}[i]$, sodass*

$$\alpha = q \cdot \beta + r, \qquad \text{mit } 0 \leq N(r) < N(\beta).$$

Beweis: Wir betrachten die komplexe Zahl $z = \alpha/\beta = x + yi \in \mathbb{C}$. Aus (36) folgt, dass $x, y \in \mathbb{Q}$ sind. Sei nun $q = m + ni$ die ganze gaußsche Zahl der so nah wie möglich an z ist, also mit $N(z - q)$ minimal. Diese Zahl muss nicht eindeutig sein.

Nun gilt, dass $|x - m| \leq 1/2$ und $|y - n| \leq 1/2$. Also gilt

$$N(z - q) = (x - m)^2 + (y - n)^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2} < 1.$$

Setze $r = (z - q)\beta$. Aus der Definition von z folgt, dass $r = \alpha - q\beta \in \mathbb{Z}[i]$ ist. Außerdem gilt, dass

$$N(r) = N(z - q)N(\beta) < N(\beta).$$

□

Beispiel 7.3.5 Sei $\alpha = 19 + 10i$ und $\beta = 2 - 3i$. Es ist

$$z = \frac{\alpha}{\beta} = \frac{19 + 10i}{2 - 3i} \frac{2 + 3i}{2 + 3i} = \frac{8 + 77i}{13} = \frac{8}{13} + \frac{77}{13} i.$$

Wir wählen $q = 1 + 6i$. Die Zahl $r = \alpha - q\beta = -1 + i$ erfüllt $N(r) = 2 < N(\beta) = 13$.

Wir wenden den euklidischen Algorithmus auf α und β an und benutzen die gleiche Bezeichnung wie in § 1.1.

n	r_n	q_n
-1	$19 + 10i$	$-$
0	$2 - 3i$	$-$
1	$-1 + i$	$1 + 6i$
2	1	$-2 + i$

Was der euklidische Algorithmus für $\mathbb{Z}[i]$ genau berechnet, ist zunächst nicht ganz klar: Wir müssen uns davon überzeugen, dass der Begriff *größte gemeinsame Teiler* in $\mathbb{Z}[i]$ Sinn macht. Wir werden sehen, dass dies in der Tat der Fall ist. Der folgende Satz ist das Analogon für $\mathbb{Z}[i]$ von Lemma 1.1.9. Es gilt nicht nur für $\mathbb{Z}[i]$ sondern für jeden euklidischen Ring. Für $R = k[x]$ haben wir dies schon gesehen in Lemma 4.2.4. Vergleichen Sie diese drei Beweisen um festzustellen, dass sie alle drei Spezialfälle eines gemeinsamen Beweises sind!

Satz 7.3.6 *Seien $\alpha, \beta \in \mathbb{Z}[i]$ mit $\alpha, \beta \neq 0$.*

(a) Es existiert ein gemeinsamer Teiler d von α und β.

(b) Jeder gemeinsame Teiler von α und β ist auch ein Teiler von d.

Beweis: Wir betrachten die Menge $S = \{x\alpha+y\beta \mid x, y \in \mathbb{Z}[i]\}$. Sei $d = x_0\alpha+y_0\beta \in S \setminus \{0\}$ mit $N(d)$ minimal. Wir behaupten, dass d jedes $a = x\alpha + y\beta \in S$ teilt. Nämlich, sei $a \in S$ und sei $a = qd+r$ die Division mit Rest. Falls $r \neq 0$, so gilt, dass $r = a - qd = (x - qx_0)\alpha + (y - qy_0)\beta \in S$ ist. Aber $0 \neq N(r) < N(d)$. Die widerspricht den Wahl von d. Also ist $r = 0$ und d ein Teiler von a.

Aus der Darstellung $d = x\alpha + y\beta$ folgt, dass jeder gemeinsame Teiler von α und β auch d teilt. □

Satz 7.3.6 impliziert, dass $\alpha, \beta \in \mathbb{Z}[i]$ nicht beide Null einen *größten gemeinsamen Teiler* besitzen: Dies ist die Zahl d aus Satz 7.3.6.(a). Man sollte beachten, dass der ggT nur bis auf Einheiten eindeutig definiert ist, da die Einheiten Norm 1 haben (Lemma 7.3.3).

Wie für ganze Zahlen und Polynome können wir die ganzen gaußschen Zahlen x, y mit $d = x\alpha + y\beta$ mit Hilfe des erweiterten euklidischen Algorithmus ausrechnen.

Beispiel 7.3.7 Sei $\alpha = 19+10i$ und $\beta = 2-3i$ wie in Beispiel 7.3.5. Wir wenden den erweiterten euklidischen Algorithmus mit der üblichen Bezeichnung an.

n	r_n	q_n	x_n	y_n
-1	$19+10i$	$-$	1	0
0	$2-3i$	$-$	0	1
1	$-1+i$	$1+6i$	1	$-1-6i$
2	1	$-2+i$	$2-i$	$-7-11i.$

Wir schließen also, dass $\mathrm{ggT}(19+10i, 2-3i) = 1 = (2-i)(19+10i) + (-7-11i)(2-3i)$.

Maple kann auch mit gaußschen Zahlen rechnen. Sie benutzen hierzu das Paket `GaussInt`. Achten Sie darauf, dass die komplexe Einheit i in Maple als I eingegeben werden muss. Um obiges Beispiel mit Maple zu berechnen, typt man:

```
with(GaussInt):
GIgcd(19+10*I, 2-3*I);
```

Eine alternative Methode um $\mathrm{ggT}(\alpha, \beta)$ zu berechnen ist mit Hilfe der Norm. Wir bemerken, dass $N(19 + 10i) = 461$ und $N(2 - 3i) = 13$. Da 461 und 13 teilerfremd in $\mathbb{Z}$ sind, folgt, dass auch α und β in $\mathbb{Z}[i]$ teilerfremd sind.

Als Nächstes möchten wir definieren was "Primzahlen" in $\mathbb{Z}[i]$ sind. Es gibt zwei mögliche Verallgemeinerungen des Begriffs Primzahl in $\mathbb{Z}$: Wir können sowohl Definition 1.2.1 als auch die Behauptung von Lemma 1.2.3 als Definition einer Gauß -Primzahl nehmen. Für $\mathbb{Z}$ sind beide Definitionen äquivalent. Diese Aussage war der wichtigste Schritt im Beweis des Fundamentalsatzes der Arithmetik (Theorem 1.2.4). Wir werden sehen (Satz 7.3.9), dass dies für $\mathbb{Z}[i]$ auch gilt. (Allgemeiner, gilt dies in jedem beliebigen euklidischen Ring.)

Definition 7.3.8 (a) Eine Zahl $0 \neq \alpha \in \mathbb{Z}[i]$ heißt *irreduzibel* (oder unzerlegbar), falls α keine Einheit ist und $\alpha = \alpha_1 \cdot \alpha_2$ mit $\alpha_j \in \mathbb{Z}[i]$ impliziert, dass entweder α_1 oder α_2 eine Einheit ist.

(b) Eine Zahl $0 \neq \alpha \in \mathbb{Z}[i]$ heißt *Primelement*, falls α keine Einheit ist und $\alpha \mid \beta\gamma$ impliziert, dass α entweder β oder γ teilt.

Satz 7.3.9 *Sei $\alpha \in \mathbb{Z}[i]$. Die Zahl α ist genau dann irreduzibel, wenn α ein Primelement ist.*

Beweis: Sei $\alpha \in \mathbb{Z}[i]$ irreduzibel. Wir nehmen an, dass $\alpha \mid \beta \cdot \gamma$ mit $\beta, \gamma \in \mathbb{Z}[i]$ und $\alpha \nmid \beta$. Da α irreduzibel ist, folgt, dass $\mathrm{ggT}(\alpha, \beta) = 1$. Also existieren $x, y \in \mathbb{Z}[i]$ mit $1 = x\alpha + y\beta$ (Satz 7.3.6). Es folgt, dass $\gamma = x\alpha\gamma + y\beta\gamma$ ist. Da α ein Teiler von $\beta\gamma$ ist, schließen wir, dass $\alpha \mid \gamma$. Dies zeigt, dass α ein Primelement ist.

Wir nehmen an, dass $\alpha \in \mathbb{Z}[i]$ ein Primelement ist. Sei $\alpha = \alpha_1\alpha_2$ mit $\alpha_j \in \mathbb{Z}[i]$. Da $\alpha \mid \alpha = \alpha_1\alpha_2$, so teilt α entweder α_1 oder α_2. Wir dürfen annehmen, dass $\alpha \mid \alpha_1$ und schreiben $\alpha_1 = \beta\alpha$ mit $\beta \in \mathbb{Z}[i]$. Da $\alpha \neq 0$ ist, folgt $\beta\alpha_2 = 1$, also ist α_2 eine Einheit. Dies zeigt, dass α irreduzibel ist. □

Bemerkung 7.3.10 Der Beweis von Satz 7.3.9 zeigt sogar etwas Allgemeineres. Für jeden kommutativen Ring ohne Nullteiler gilt, dass die Primelemente auch irreduzibel sind. Die andere Implikation gilt für jeden euklidischen Ring.

Ein Beispiel von einem Ring wo beide Begriffe nicht äquivalent sind, ist $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Ähnlich wie für die gaußschen Zahlen, definiert man den Norm durch $N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$. In R gilt, dass

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{37}$$

Man berechnet, dass $N(2) = 4$, $N(3) = 9$ und $N(1 \pm \sqrt{-5}) = 6$. Außerdem überprüft man leicht, dass keine Elementen in R mit Norm 2 und 3 existieren. Dies impliziert, dass 2 und 3 in $\mathbb{Z}[\sqrt{-5}]$ irreduzibel sind.

Offensichtlich gilt, dass $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Da $N(2) = 4 \nmid N(1 \pm \sqrt{-5}) = 6$ folgt, dass $2 \nmid (1 \pm \sqrt{-5})$. Wir schließen, dass 2 kein Primelement ist. Das gleiche Argument zeigt, dass 3 kein Primelement ist.

Das folgende Lemma gibt ein einfaches Kriterium um zu überprüfen ob $\alpha \in \mathbb{Z}[i]$ irreduzibel ist.

Lemma 7.3.11 *Sei $\alpha \in \mathbb{Z}[i]$ ein Element mit $N(\alpha) = p$ eine Primzahl, so ist α irreduzibel.*

Beweis: Sei α wie in der Aussage des Lemmas. Wir schreiben $\alpha = \beta\gamma$ mit $\beta, \gamma \in \mathbb{Z}[i]$. Es folgt, dass $p = N(\alpha) = N(\beta)N(\gamma)$. Da $N(x) \in \mathbb{Z}_{\geq 0}$ ist, ist entweder $N(\beta)$ oder $N(\gamma)$ gleich 1. Lemma 7.3.3 impliziert, dass entweder β oder γ eine Einheit ist. Also ist α irreduzibel. □

Das folgende Theorem ist das Analogon des Fundamentalsatzes der Arithmetik (Theorem 1.2.4) für die gaußschen Zahlen. Wir wissen, dass irreduzible Elementen auch Primelementen sind. Daher können wir den Beweis von Theorem 1.2.4 in dieser Situation übertragen. (Überprüfen Sie dies!)

Theorem 7.3.12 *(a) Jedes $\alpha \in \mathbb{Z}[i]$, das nicht Null oder eine Einheit ist lässt sich schreiben als Produkt von Primelementen.*

(b) Die Primfaktorzerlegung aus (a) ist eindeutig bis auf Einheiten und Reihenfolge.

Bemerkung 7.3.13 Ein kommutativer Ring ohne Nullteiler mit eindeutiger Primfaktorzerlegung heißt *faktoriell*. Die Ergebnisse aus diesem Abschnitt zeigen auch, dass jede euklidischer Ring faktoriell ist. Ein Beispiel für ein nicht faktorieller Ring ist $\mathbb{Z}[\sqrt{-5}]$: Dies folgt aus (37).

Das letzte Ziel dieses Kapitels ist die Bestimmung der Primelementen in $\mathbb{Z}[i]$. Wir nennen diese Zahlen auch die *Gauß-Primzahlen*.

Lemma 7.3.14 *Sei $p \in \mathbb{Z}$ eine Primzahl, so ist p entweder eine Gauß-Primzahl oder es existiert ein irreduzibles Element $\pi \in \mathbb{Z}[i]$ mit $p = \pi \cdot \bar{\pi}$.*

Beweis: Sei $p \in \mathbb{Z}$ eine Primzahl, so ist $p \in \mathbb{Z}[i]$ keine Einheit (Lemma 7.3.3). Also existiert ein irreduzibeles Element $\pi = a + bi \in \mathbb{Z}[i]$, das p teilt. Es folgt, dass $N(\pi) \mid N(p) = p^2$, also ist $N(\pi)$ entweder p oder p^2.

Falls $N(\pi) = p^2$ ist, existiert eine Einheit ϵ mit $p = \epsilon\pi$. Wir schließen, dass p irreduzibel ist.

Falls $N(\pi) = p$ ist, ist π ein echter Teiler von p und es gilt, dass $\pi \cdot \bar{\pi} = N(\pi) = p$ ist. □

Lemma 7.3.15 *Sei $\pi \in \mathbb{Z}[i]$ eine Gauß-Primzahl, so ist $N(\pi) = \pi \cdot \bar{\pi}$ entweder p oder p^2, wobei $p \in \mathbb{Z}$ eine Primzahl ist.*

Beweis: Sei $\pi \in \mathbb{Z}[i]$ eine Gauß-Primzahl und sei $n = N(\pi) \in \mathbb{N}$. Sei $n = p_1 \cdot p_2 \cdots p_r$ die Primfaktorzerlegung von n in $\mathbb{Z}$. Dies ist auch eine Zerlegung in $\mathbb{Z}[i]$, aber die p_js sind nicht notwendigerweise Gauß-Primzahlen. Da π eine Gauß-Primzahl ist, teilt π mindestens eine der p_j. Wie im Beweis von Lemma

7.3.14 folgt, dass $N(\pi) = \pi \cdot \bar{\pi} \mid N(p_j) = p_j^2$. Also ist $N(\pi)$ entweder p_j oder p_j^2. □

Lemma 7.3.16 *Sei $p \in \mathbb{Z}$ eine Primzahl. Die folgende Aussagen sind äquivalent:*

(a) $p = \pi \cdot \bar{\pi}$, *wobei π eine Gauß-Primzahl ist,*

(b) es existieren $a, b \in \mathbb{Z}$ *mit* $p = a^2 + b^2$,

(c) $p = 2$ *oder* $p \equiv 1 \pmod 4$.

Beweis: (a) ⇒ (b): Sei $p = \pi \cdot \bar{\pi}$, wobei π eine Gauß-Primzahl ist. Schreibe $\pi = a + bi$. Nun gilt $p = \pi \cdot \bar{\pi} = a^2 + b^2$.

(b) ⇒ (a): Sei $p = a^2 + b^2$ und $\pi = a + bi$. Es gilt $N(\pi) = \pi \cdot \bar{\pi} = a^2 + b^2 = p$. Insbesondere ist π irreduzibel (Lemma 7.3.11).

(b) ⇒ (c): Dies folgt aus Lemma 7.2.1.

(c) ⇒ (b): Dies folgt aus Theorem 7.2.3. Alternativ kann man dies auch wie folgt direkt beweisen.

Falls $p = 2$, so gilt $2 = (1 + i)(1 - i)$, wobei $1 \pm i$ irreduzibel sind (Lemma 7.3.11. Sei nun $p \equiv 1 \pmod 4$. Also ist $(\frac{-1}{p}) = 1$ (Korollar 6.1.6) und es existiert ein $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod p$. Daher gilt, dass $p \mid (x^2 + 1) = (x - i)(x + i)$. Da $x \pm i$ keine Einheit ist, folgt, dass p keine Gauß-Primzahl ist. Lemma 7.3.14 impliziert daher, dass eine Gauß-Primzahl $\pi = a + bi$ mit $p = \pi \cdot \bar{\pi} = a^2 + b^2$ existiert. □

Der folgende Satz beschreibt die Gauß-Primzahlen. Der Satz folgt direkt aus den Lemata 7.3.14–7.3.16.

Satz 7.3.17 (Die Gauß-Primzahlen) *Es gibt 3 Typen von Gauß-Primzahlen:*

(a) $1 + i$,

(b) die Primzahlen p mit $p \equiv 3 \pmod 4$,

(c) falls p eine Primzahl mit $p \equiv 1 \pmod 4$ *ist, so existieren* $a, b \in \mathbb{Z}$ *mit* $p = a^2 + b^2$. *Nun ist $\pi = a + bi$ eine Gauß-Primzahl.*

Alle Gauß-Primzahlen sind vom obigen Typ (bis auf eine Einheit).

Beispiel 7.3.18 Wir berechnen die Primfaktorzerlegung von einigen ganzen gaußschen Zahlen.

(a) Sei $n = 143 = 11 \cdot 13$. Da $11 \equiv 3 \pmod 4$, also ist 11 eine Gauß-Primzahl. Die Zahl $13 \equiv 1 \pmod 4$ lässt sich schreiben als $13 = 2^2 + 3^2 = (2 + 3i)(2 - 3i)$. Die Primfaktorzerlegung von n is daher $n = 11(2 + 3i)(2 - 3i)$.

(b) Sei $\alpha = 9 + 5i$. Es gilt $N(\alpha) = 9^2 + 5^2 = 106 = 2 \cdot 53$. Für jeden irreduziblen Teiler π von α gilt $N(\pi) \mid N(\alpha)$, also $N(\pi) \in \{2, 53\}$. Wir bemerken, dass $53 = 2^2 + 7^2 = (2 + 7i)(2 - 7i)$. Bis auf Multiplikation mit einer Einheit ist $\pi \in \{1 + i, 2 + 7i, 2 - 7i\}$. Wir berechnen $(9 + 5i)/(1 + i) = 7 - 2i = i(2 + 7i)$. Also ist $\alpha = (1 + i)(7 - 2i)$ die Primfaktorzerlegung von α.

Literatur

[1] F. Beukers, *Elementary number theory*, Skript Universität Utrecht.

[2] I.I. Bouw, *Algebra*, Skript Universität Ulm, 2009.

[3] H. Maier, *Elementare Zahlentheorie*, Skript Universität Ulm, 2006.

[4] K.H. Rosen, *Elementary number theory and its applications*, fourth edition, Addison–Wesley, Reading, MA, 1999.

[5] H. Scheid, A. Frommer, *Zahlentheorie*, 4. Auflage, Spektrum, München, 2007.

[6] U. Schöning, *Kryptologie-Kompendium*, Skript Universität Ulm, 2008.

[7] J.H. Silverman, *A friendly introduction to modern number theory*, third edition, Pearson International Edition, Upper Saddle River, NJ, 2006.