Springer-Lehrbuch

Einführung in die Kryptographie

Bearbeitet von
Johannes Buchmann

6., überarb. Auflage 2016. Taschenbuch. XXXVi, 330 S. Softcover
ISBN 978 3 642 39774 5
Format (B x L): 16,8 x 24 cm
Gewicht: 603 g

Kongruenzen und Restklassenringe

2

In diesem Kapitel führen wir das Rechnen in Restklassenringen und in primen Restklassengruppen ein. Diese Techniken sind von zentraler Bedeutung in kryptographischen Verfahren. Einige der behandelten Sachverhalte gelten allgemeiner in Gruppen. Daher behandeln wir in diesem Kapitel auch endliche Gruppen und ihre Eigenschaften.

Im ganzen Kapitel ist m immer eine natürliche Zahl und kleine lateinische Buchstaben bezeichnen ganze Zahlen.

2.1 Kongruenzen

Definition 2.1 Wir sagen, a ist *kongruent* zu b modulo m und schreiben $a \equiv b \bmod m$, wenn m die Differenz $b - a$ teilt.

Beispiel 2.1 Es gilt $-2 \equiv 19 \bmod 21$, $10 \equiv 0 \bmod 2$.

Es ist leicht zu verifizieren, dass Kongruenz modulo m eine Äquivalenzrelation auf der Menge der ganzen Zahlen ist. Das bedeutet, dass

1. jede ganze Zahl zu sich selbst kongruent ist modulo m (Reflexivität),
2. aus $a \equiv b \bmod m$ folgt, dass auch $b \equiv a \bmod m$ gilt (Symmetrie),
3. aus $a \equiv b \bmod m$ und $b \equiv c \bmod m$ folgt, dass auch $a \equiv c \bmod m$ gilt (Transitivität).

Außerdem gilt folgende Charakterisierung:

Lemma 2.1 *Folgende Aussagen sind äquivalent.*

1. $a \equiv b \bmod m$.
2. $a = b + km$ *mit* $k \in \mathbb{Z}$.
3. a und b *lassen bei der Division durch* m *denselben Rest.*

J. Buchmann, *Einführung in die Kryptographie*, Springer-Lehrbuch,
DOI 10.1007/978-3-642-39775-2_2

Die *Äquivalenzklasse* von a besteht aus allen ganzen Zahlen, die sich aus a durch Addition ganzzahliger Vielfacher von m ergeben, sie ist also

$$\{b : b \equiv a \bmod m\} = a + m\mathbb{Z}.$$

Man nennt sie *Restklasse* von a mod m.

Beispiel 2.2 Die Restklasse von 1 mod 4 ist die Menge $\{1, 1\pm4, 1\pm2*4, 1\pm3*4, \ldots\} = \{1, -3, 5, -7, 9, -11, 13, \ldots\}$.

Die Restklasse von 0 mod 2 ist die Menge aller geraden ganzen Zahlen. Die Restklasse von 1 mod 2 ist die Menge aller ungeraden ganzen Zahlen.

Die Restklassen mod 4 sind $0 + 4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$, $3 + 4\mathbb{Z}$.

Die Menge aller Restklassen mod m wird mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet. Sie hat m Elemente, weil genau die Reste $0, 1, 2, \ldots, m-1$ bei der Division durch m auftreten. Ein *Vertretersystem* für diese Äquivalenzrelation ist eine Menge ganzer Zahlen, die aus jeder Restklasse mod m genau ein Element enthält. Jedes solche Vertretersystem heißt *volles Restsystem* mod m.

Beispiel 2.3 Ein volles Restsystem mod 3 enthält je ein Element aus den Restklassen $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, $2 + 3\mathbb{Z}$. Also sind folgende Mengen volle Restsysteme mod 3: $\{0, 1, 2\}, \{3, -2, 5\}, \{9, 16, 14\}$.

Ein volles Restsystem mod m ist z. B. die Menge $\{0, 1, \ldots, m-1\}$. Seine Elemente nennt man *kleinste nicht negative Reste* mod m. Wir bezeichnen dieses Vertretersystem mit $\mathbb{Z}_m$. Genauso ist die Menge $\{1, 2, \ldots, m\}$ ein volles Restsystem mod m. Seine Elemente heißen *kleinste positive Reste* mod m. Schließlich ist $\{n+1, n+2, \ldots, n+m\}$ mit $n = -\lceil m/2 \rceil$ ein vollständiges Restsystem mod m. Seine Elemente heißen *absolut kleinste Reste* mod m.

Beispiel 2.4 Es ist

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

die Menge der kleinsten nicht negativen Reste mod 13 und

$$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$$

ist die Menge der absolut kleinsten Reste mod 13.

Wir brauchen einige Rechenregeln für Kongruenzen. Die erlauben es uns später, eine Ringstruktur auf der Menge der Restklassen mod m zu definieren.

Theorem 2.1 *Aus* $a \equiv b \bmod m$ *und* $c \equiv d \bmod m$ *folgt* $-a \equiv -b \bmod m$, $a + c \equiv b + d \bmod m$ *und* $ac \equiv bd \bmod m$.

Beweis Weil m ein Teiler von $a - b$ ist, ist m auch ein Teiler von $-a + b$. Daher ist $-a \equiv -b \bmod m$. Weil m ein Teiler von $a - b$ und von $c - d$ ist, ist m auch ein Teiler von $a - b + c - d = (a + c) - (b + d)$. Daher ist $a + c \equiv b + d \bmod m$. Um zu zeigen, dass $ac \equiv bd \bmod m$ ist, schreiben wir $a = b + lm$ und $c = d + km$. Dann erhalten wir $ac = bd + m(ld + kb + lkm)$, wie behauptet. □

Beispiel 2.5 Wir wenden die Rechenregeln aus Theorem 2.1 an, um zu beweisen, dass die fünfte Fermat-Zahl $2^{2^5} + 1$ durch 641 teilbar ist. Zunächst gilt

$$641 = 640 + 1 = 5 * 2^7 + 1.$$

Dies zeigt

$$5 * 2^7 \equiv -1 \bmod 641.$$

Aus Theorem 2.1 folgt, dass diese Kongruenz bestehen bleibt, wenn man die rechte und linke Seite viermal mit sich selbst multipliziert, also zur vierten Potenz erhebt. Das machen wir und erhalten

$$5^4 * 2^{28} \equiv 1 \bmod 641. \tag{2.1}$$

Andererseits ist

$$641 = 625 + 16 = 5^4 + 2^4.$$

Daraus gewinnt man

$$5^4 \equiv -2^4 \bmod 641.$$

Wenn man diese Kongruenz in (2.1) benutzt, erhält man

$$-2^{32} \equiv 1 \bmod 641,$$

also

$$2^{32} + 1 \equiv 0 \bmod 641.$$

Dies beweist, dass 641 ein Teiler der fünften Fermat-Zahl ist.

Wir wollen zeigen, dass die Menge der Restklassen mod m einen Ring bildet. Wir wiederholen in den folgenden Abschnitten kurz einige Grundbegriffe.

2.2 Halbgruppen

Definition 2.2 Ist X eine Menge, so heißt eine Abbildung $\circ : X \times X \to X$, die jedem Paar (x_1, x_2) von Elementen aus X ein Element $x_1 \circ x_2$ zuordnet, eine *innere Verknüpfung* auf X.

Beispiel 2.6 Auf der Menge der reellen Zahlen kennen wir bereits die inneren Verknüpfungen Addition und Multiplikation.

Auf der Menge $\mathbb{Z}/m\mathbb{Z}$ aller Restklassen modulo m führen wir zwei innere Verknüpfungen ein, Addition und Multiplikation.

Definition 2.3 Die Summe der Restklassen $a + m\mathbb{Z}$ und $b + m\mathbb{Z}$ ist $(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}$. Das Produkt der Restklassen $a + m\mathbb{Z}$ und $b + m\mathbb{Z}$ ist $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}$.

Man beachte, dass Summe und Produkt von Restklassen modulo m unter Verwendung von Vertretern dieser Restklassen definiert sind. Aus Theorem 2.1 folgt aber, dass die Definition von den Vertretern unabhängig ist. In der Praxis werden Restklassen durch feste Vertreter dargestellt und die Rechnung wird mit diesen Vertretern durchgeführt. Man erhält auf diese Weise eine Addition und eine Multiplikation auf jedem Vertretersystem.

Beispiel 2.7 Wir verwenden zur Darstellung von Restklassen die kleinsten nicht negativen Reste. Es ist $(3 + 5\mathbb{Z}) + (2 + 5\mathbb{Z}) = (5 + 5\mathbb{Z}) = 5\mathbb{Z}$ und $(3 + 5\mathbb{Z})(2 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$. Diese Rechnungen kann man auch als $3 + 2 \equiv 0 \bmod 5$ und $3 * 2 \equiv 1 \bmod 5$ darstellen.

Definition 2.4 Sei $\circ$ eine innere Verknüpfung auf der Menge X. Sie heißt *assoziativ*, wenn $(a \circ b) \circ c = a \circ (b \circ c)$ gilt für alle $a, b, c \in X$. Sie heißt *kommutativ*, wenn $a \circ b = b \circ a$ gilt für alle $a, b \in X$.

Beispiel 2.8 Addition und Multiplikation auf der Menge der reellen Zahlen sind assoziative und kommutative Verknüpfungen. Dasselbe gilt für Addition und Multiplikation auf der Menge $\mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m.

Definition 2.5 Ein Paar $(H, \circ)$, bestehend aus einer nicht leeren Menge H und einer assoziativen inneren Verknüpfung $\circ$ auf H, heißt eine *Halbgruppe*. Die Halbgruppe heißt *kommutativ* oder *abelsch*, wenn die innere Verknüpfung $\circ$ kommutativ ist.

Beispiel 2.9 Kommutative Halbgruppen sind $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, \cdot)$.

Sei $(H, \circ)$ eine Halbgruppe und bezeichne $a^1 = a$ und $a^{n+1} = a \circ a^n$ für $a \in H$ und $n \in \mathbb{N}$, dann gelten die *Potenzgesetze*

$$a^n \circ a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad a \in H, n, m \in \mathbb{N}. \tag{2.2}$$

Sind $a, b \in H$ und gilt $a \circ b = b \circ a$, dann folgt

$$(a \circ b)^n = a^n \circ b^n. \tag{2.3}$$

Ist die Halbgruppe also kommutativ, so gilt (2.3) immer.

Definition 2.6 Ein *neutrales Element* der Halbgruppe $(H, \circ)$ ist ein Element $e \in H$, das $e \circ a = a \circ e = a$ erfüllt für alle $a \in H$. Enthält die Halbgruppe ein neutrales Element, so heißt sie *Monoid*.

Eine Halbgruppe hat höchstens ein neutrales Element. (siehe Übung 2.3).

Definition 2.7 Ist e das neutrale Element der Halbgruppe $(H, \circ)$ und ist $a \in H$, so heißt $b \in H$ *Inverses* von a, wenn $a \circ b = b \circ a = e$ gilt. Besitzt a ein Inverses, so heißt a *invertierbar* in der Halbgruppe.

In Monoiden besitzt jedes Element höchstens ein Inverses (siehe Übung 2.5).

Beispiel 2.10
1. Die Halbgruppe $(\mathbb{Z}, +)$ besitzt das neutrale Element 0. Das Inverse von a ist $-a$.
2. Die Halbgruppe $(\mathbb{Z}, \cdot)$ besitzt das neutrale Element 1. Die einzigen invertierbaren Elemente sind 1 und -1.
3. Die Halbgruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ besitzt das neutrale Element $m\mathbb{Z}$. Das Inverse von $a+m\mathbb{Z}$ ist $-a + m\mathbb{Z}$.
4. Die Halbgruppe $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ besitzt das neutrale Element $1 + m\mathbb{Z}$. Die invertierbaren Elemente werden später bestimmt.

2.3 Gruppen

Definition 2.8 Eine *Gruppe* ist eine Halbgruppe, die ein neutrales Element besitzt und in der jedes Element invertierbar ist. Die Gruppe heißt *kommutativ* oder *abelsch*, wenn die Halbgruppe kommutativ ist.

Beispiel 2.11
1. Die Halbgruppe $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.
2. Die Halbgruppe $(\mathbb{Z}, \cdot)$ ist keine Gruppe, weil nicht jedes Element ein Inverses besitzt.
3. Die Halbgruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ ist eine abelsche Gruppe.

Ist $(G, \cdot)$ eine multiplikativ geschriebene Gruppe, bezeichnet a^{-1} das Inverse eines Elementes a aus G und setzt man $a^{-n} = (a^{-1})^n$ für jede natürliche Zahl n, so gelten die Potenzgesetze (2.2) für alle ganzzahligen Exponenten. Ist die Gruppe abelsch, so gilt (2.3) für alle ganzen Zahlen n.

In einer Gruppe gelten folgende *Kürzungsregeln*, die man durch Multiplikation mit einem geeigneten Inversen beweist.

Theorem 2.2 *Sei $(G, \cdot)$ eine Gruppe und $a, b, c \in G$. Aus $ca = cb$ folgt $a = b$ und aus $ac = bc$ folgt $a = b$.*

Definition 2.9 Die *Ordnung* einer Gruppe oder Halbgruppe ist die Anzahl ihrer Elemente.

Beispiel 2.12 Die additive Gruppe $\mathbb{Z}$ hat unendliche Ordnung. Die additive Gruppe $\mathbb{Z}/m\mathbb{Z}$ hat die Ordnung m.

2.4 Restklassenringe

Definition 2.10 Ein *Ring* ist ein Tripel $(R, +, \cdot)$, für das $(R, +)$ eine abelsche Gruppe und $(R, \cdot)$ eine Halbgruppe ist, und für das zusätzlich die Distributivgesetze $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ und $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ für alle $x, y, z \in R$ gelten. Der Ring heißt *kommutativ*, wenn die Halbgruppe $(R, \cdot)$ kommutativ ist. Ein *Einselement* des Ringes ist ein neutrales Element der Halbgruppe $(R, \cdot)$.

Beispiel 2.13 Das Tripel $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement 1 und daraus leitet man ab, dass $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Einselement $1 + m\mathbb{Z}$ ist. Der letztere Ring heißt *Restklassenring* modulo m.

In der Definition wurde festgelegt, dass Ringe Tripel sind, dass also die Verknüpfungen immer miterwähnt werden müssen. Im allgemeinen ist aber klar, welche Verknüpfungen gemeint sind. Dann lassen wir sie einfach weg und sprechen zum Beispiel von dem Restklassenring $\mathbb{Z}/m\mathbb{Z}$.

Definition 2.11 Sei R ein Ring mit Einselement. Ein Element a von R heißt *invertierbar* oder *Einheit*, wenn es in der multiplikativen Halbgruppe von R invertierbar ist. Das Element a heißt *Nullteiler*, wenn es von Null verschieden ist und es ein von Null verschiedenes Element $b \in R$ gibt mit $ab = 0$ oder $ba = 0$. Enthält R keine Nullteiler, so heißt R *nullteilerfrei*.

In Übung 2.9 wird gezeigt, dass die invertierbaren Elemente eines kommutativen Rings R mit Einselement eine Gruppe bilden. Sie heißt *Einheitengruppe* des Rings und wird mit R^* bezeichnet.

Beispiel 2.14 Der Ring der ganzen Zahlen ist nullteilerfrei.

Die Nullteiler im Restklassenring $\mathbb{Z}/m\mathbb{Z}$ sind die Restklassen $a + m\mathbb{Z}$, für die $1 < \gcd(a, m) < m$ ist. Ist $a + m\mathbb{Z}$ nämlich ein Nullteiler von $\mathbb{Z}/m\mathbb{Z}$, dann muss es eine ganze Zahl b geben mit $ab \equiv 0 \bmod m$, aber es gilt weder $a \equiv 0 \bmod m$ noch $b \equiv 0 \bmod m$. Also ist m ein Teiler von ab, aber weder von a noch von b. Das bedeutet, dass $1 < \gcd(a, m) < m$ gelten muss. Ist umgekehrt $1 < \gcd(a, m) < m$ und $b = m/\gcd(a, m)$, so ist $a \not\equiv 0 \bmod m$, $ab \equiv 0 \bmod m$ und $b \not\equiv 0 \bmod m$. Also ist $a + m\mathbb{Z}$ ein Nullteiler von $\mathbb{Z}/m\mathbb{Z}$.

Ist m eine Primzahl, so besitzt $\mathbb{Z}/m\mathbb{Z}$ also keine Nullteiler.

2.5 Körper

Definition 2.12 Ein *Körper* ist ein kommutativer Ring mit Einselement, in dem jedes von Null verschiedene Element invertierbar ist.

Beispiel 2.15 Die Menge der ganzen Zahlen ist kein Körper, weil die einzigen invertierbaren ganzen Zahlen 1 und -1 sind. Sie ist aber im Körper der rationalen Zahlen enthalten. Auch die reellen und komplexen Zahlen bilden Körper. Wie wir unten sehen werden, ist der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper, wenn m eine Primzahl ist.

2.6 Division im Restklassenring

Teilbarkeit in Ringen ist definiert wie Teilbarkeit in $\mathbb{Z}$. Sei R ein Ring und seien $a, n \in R$.

Definition 2.13 Man sagt a *teilt* n, wenn es $b \in R$ gibt mit $n = ab$.

Wenn a das Ringelement n teilt, dann heißt a *Teiler* von n und n *Vielfaches* von a und man schreibt $a|n$. Man sagt auch, n ist durch a *teilbar*. Wenn a kein Teiler von n ist, dann schreibt man $a \nmid n$.

Wir untersuchen das Problem, durch welche Elemente des Restklassenrings mod m dividiert werden darf, welche Restklasse $a + m\mathbb{Z}$ also ein multiplikatives Inverses besitzt. Zuerst stellen wir fest, dass die Restklasse $a + m\mathbb{Z}$ genau dann in $\mathbb{Z}/m\mathbb{Z}$ invertierbar ist, wenn die Kongruenz

$$ax \equiv 1 \bmod m \tag{2.4}$$

lösbar ist. Wann das der Fall ist, wird im nächsten Satz ausgesagt.

Theorem 2.3 *Die Restklasse $a + m\mathbb{Z}$ ist genau dann in $\mathbb{Z}/m\mathbb{Z}$ invertierbar, d. h. die Kongruenz (2.4) ist genau dann lösbar, wenn $\gcd(a, m) = 1$ gilt. Ist $\gcd(a, m) = 1$, dann ist das Inverse von $a + m\mathbb{Z}$ eindeutig bestimmt, d. h. die Lösung x von (2.4) ist eindeutig bestimmt* mod m.

Beweis Sei $g = \gcd(a, m)$ und sei x eine Lösung von (2.4), dann ist g ein Teiler von m und damit ein Teiler von $ax - 1$. Aber g ist auch ein Teiler von a. Also ist g ein Teiler von 1, d. h. $g = 1$, weil g als ggT positiv ist. Sei umgekehrt $g = 1$. Dann gibt es nach Korollar 1.2 Zahlen x, y mit $ax + my = 1$, d. h. $ax - 1 = -my$. Dies zeigt, dass x eine Lösung der Kongruenz (2.4) ist, und dass $x + m\mathbb{Z}$ ein Inverses von $a + m\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$ ist.

Zum Beweis der Eindeutigkeit sei $v + m\mathbb{Z}$ ein weiteres Inverses von $a + m\mathbb{Z}$. Dann gilt $ax \equiv av \bmod m$. Also teilt m die Zahl $a(x - v)$. Weil $\gcd(a, m) = 1$ ist, folgt daraus, dass m ein Teiler von $x - v$ ist. Somit ist $x \equiv v \bmod m$. □

Eine Restklasse $a + m\mathbb{Z}$ mit $\gcd(a, m) = 1$ heißt *prime Restklasse* modulo m. Aus Theorem 2.3 folgt, dass eine Restklasse $a + m\mathbb{Z}$ mit $1 \leq a < m$ entweder ein Nullteiler oder eine prime Restklasse, d. h. eine Einheit des Restklassenrings mod m, ist.

Im Beweis von Theorem 2.3 wurde gezeigt, wie man die Kongruenz $ax \equiv 1 \bmod m$ mit dem erweiterten euklidischen Algorithmus (siehe Abschn. 1.6.3) löst. Man muss nur die Darstellung $1 = ax + my$ berechnen. Man braucht sogar nur den Koeffizienten x. Nach Theorem 1.13 kann die Lösung der Kongruenz also effizient berechnet werden.

Beispiel 2.16 Sei $m = 12$. Die Restklasse $a + 12\mathbb{Z}$ ist genau dann invertierbar in $\mathbb{Z}/12\mathbb{Z}$, wenn $\gcd(a, 12) = 1$. Die invertierbaren Restklassen mod 12 sind also $1 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 11 + 12\mathbb{Z}$. Um das Inverse von $5 + 12\mathbb{Z}$ zu finden, benutzen wir den erweiterten euklidischen Algorithmus. Wir erhalten $5 * 5 \equiv 1 \bmod 12$. Entsprechend gilt $7 * 7 \equiv 1 \bmod 12$, $11 * 11 \equiv 1 \bmod 12$.

Wir führen noch den Restklassenkörper modulo einer Primzahl ein, der in der Kryptographie sehr oft benutzt wird.

Theorem 2.4 *Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis Gemäß Theorem 2.3 ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper, wenn $\gcd(k, m) = 1$ gilt für alle k mit $1 \leq k < m$. Dies ist genau dann der Fall, wenn m eine Primzahl ist. □

2.7 Rechenzeit für die Operationen im Restklassenring

In allen Verfahren der Public-Key-Kryptographie wird intensiv in Restklassenringen gerechnet. Oft müssen diese Rechnungen auf Chipkarten ausgeführt werden. Daher ist es wichtig, zu wissen, wie effizient diese Rechnungen ausgeführt werden können. Das wird in diesem Abschnitt beschrieben.

Wir gehen davon aus, dass die Elemente des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ durch ihre kleinsten nicht negativen Vertreter $\{0, 1, 2, \ldots, m-1\}$ dargestellt werden. Unter dieser Voraussetzung schätzen wir den Aufwand der Operationen im Restklassenring ab.

Seien also $a, b \in \{0, 1, \ldots, m-1\}$.

Um $(a + m\mathbb{Z}) + (b + m\mathbb{Z})$ zu berechnen, müssen wir $(a + b) \bmod m$ berechnen. Wir bestimmen also zuerst $c = a + b$. Die gesuchte Summe ist $c + m\mathbb{Z}$, aber c ist vielleicht der falsche Vertreter. Es gilt nämlich $0 \leq c < 2m$. Ist $0 \leq c < m$, so ist c der richtige Vertreter. Ist $m \leq c < 2m$, so ist der richtige Vertreter $c - m$, weil $0 \leq c - m < m$ ist. In diesem Fall ersetzt man c durch $c - m$. Entsprechend berechnet man $(a + m\mathbb{Z}) - (b + m\mathbb{Z})$. Man bestimmt $c = a - b$. Dann ist $-m < c < m$. Gilt $0 \leq c < m$, so ist c der richtige Vertreter der Differenz. Ist $-m < c < 0$, so ist der richtige Vertreter $c + m$. Also muss c durch $c + m$ ersetzt werden. Aus den Ergebnissen von Abschn. 1.6.1 folgt also, dass

Summe und Differenz zweier Restklassen modulo m in Zeit $O(\text{size}\, m)$ berechnet werden können.

Nun wird $(a + m\mathbb{Z})(b + m\mathbb{Z})$ berechnet. Dazu wird $c = ab$ bestimmt. Dann ist $0 \leq c < m^2$. Wir dividieren c mit Rest durch m und ersetzen c durch den Rest dieser Division. Für den Quotienten q dieser Division gilt $0 \leq q < m$. Nach den Ergebnissen aus Abschn. 1.6.1 kann man die Multiplikation und die Division in Zeit $O((\text{size}\, m)^2)$ durchführen. Die Restklassen können also in Zeit $O((\text{size}\, m)^2)$ multipliziert werden.

Schließlich wird die Invertierung von $a+m\mathbb{Z}$ diskutiert. Man berechnet $g = \gcd(a, m)$ und x mit $ax \equiv g \bmod m$ und $0 \leq x < m$. Hierzu benutzt man den erweiterten euklidischen Algorithmus. Nach Korollar 1.6 gilt $|x| \leq m/(2g)$. Der Algorithmus liefert aber möglicherweise einen negativen Koeffizienten x, den man durch $x + m$ ersetzt. Gemäß Theorem 1.13 erfordert diese Berechnung Zeit $O((\text{size}\, m)^2)$. Die Restklasse $a + m\mathbb{Z}$ ist genau dann invertierbar, wenn $g = 1$ ist. In diesem Fall ist x der kleinste nicht negative Vertreter der inversen Klasse. Die gesamte Rechenzeit ist $O((\text{size}\, m)^2)$. Es folgt, dass auch die Division durch eine prime Restklasse mod m Zeit $O((\text{size}\, m)^2)$ kostet.

In allen Algorithmen müssen nur konstant viele Zahlen der Größe $O(\text{size}\, m)$ gespeichert werden. Daher brauchen die Algorithmen auch nur Speicherplatz $O(\text{size}\, m)$. Wir merken an, dass es asymptotisch effizientere Algorithmen für die Multiplikation und Division von Restklassen gibt. Sie benötigen Zeit $O(\log m(\log\log m)^2)$ (siehe [3]). Für Zahlen der Größenordnung, um die es in der Kryptographie geht, sind diese Algorithmen aber langsamer als die hier analysierten. Die $O((\text{size}\, m)^2)$-Algorithmen lassen in vielen Situationen Optimierungen zu. Einen Überblick darüber findet man in [49].

Wir haben folgenden Satz bewiesen.

Theorem 2.5 *Angenommen, die Restklassen modulo m werden durch ihre kleinsten nicht negativen Vertreter dargestellt. Dann erfordert die Addition und Subtraktion zweier Restklassen Zeit* $O(\text{size}\, m)$ *und die Multiplikation und Division zweier Restklassen kostet Zeit* $O((\text{size}\, m)^2)$. *Alle Operationen brauchen Speicherplatz* $O(\text{size}\, m)$.

2.8 Prime Restklassengruppen

Von fundamentaler Bedeutung in der Kryptographie ist folgendes Ergebnis.

Theorem 2.6 *Die Menge aller primen Restklassen modulo m bildet eine endliche abelsche Gruppe bezüglich der Multiplikation.*

Beweis Nach Theorem 2.3 ist diese Menge die Einheitengruppe des Restklassenrings mod m. □

Die Gruppe der primen Restklassen modulo m heißt *prime Restklassengruppe* modulo m und wird mit $(\mathbb{Z}/m\mathbb{Z})^*$ bezeichnet. Ihre Ordnung bezeichnet man mit $\varphi(m)$.

Tab. 2.1 Werte der Eulerschen φ-Funktion

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Die Abbildung

$$\mathbb{N} \to \mathbb{N}, m \mapsto \varphi(m)$$

heißt *Eulersche φ-Funktion*. Man beachte, dass $\varphi(m)$ die Anzahl der Zahlen a in $\{1, 2, \ldots, m\}$ ist mit $\gcd(a, m) = 1$. Insbesondere ist $\varphi(1) = 1$.

Beispiel 2.17 Z. B. ist $(\mathbb{Z}/12\mathbb{Z})^* = \{1 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 11 + 12\mathbb{Z}\}$ die prime Restklassengruppe mod 12. Also ist $\varphi(12) = 4$.

Einige Werte der Eulerschen φ-Funktion findet man in Tab. 2.1.

Man sieht, dass in dieser Tabelle $\varphi(p) = p - 1$ für die Primzahlen p gilt. Dies ist auch allgemein richtig, weil für eine Primzahl p alle Zahlen a zwischen 1 und $p - 1$ zu p teilerfremd sind. Also gilt der folgende Satz:

Theorem 2.7 *Falls p eine Primzahl ist, gilt $\varphi(p) = p - 1$.*

Die Eulersche φ-Funktion hat folgende nützliche Eigenschaft:

Theorem 2.8

$$\sum_{d|m, d>0} \varphi(d) = m.$$

Beweis Es gilt

$$\sum_{d|m, d>0} \varphi(d) = \sum_{d|m, d>0} \varphi(m/d),$$

weil die Menge der positiven Teiler von m genau $\{m/d : d|m, d > 0\}$ ist. Nun ist $\varphi(m/d)$ die Anzahl der ganzen Zahlen a in der Menge $\{1, \ldots, m/d\}$ mit $\gcd(a, m/d) = 1$. Also ist $\varphi(m/d)$ die Anzahl der ganzen Zahlen b in $\{1, 2, \ldots, m\}$ mit $\gcd(b, m) = d$. Daher ist

$$\sum_{d|m, d>0} \varphi(d) = \sum_{d|m, d>0} |\{b : 1 \le b \le m \text{ mit } \gcd(b, m) = d\}|.$$

Es gilt aber

$$\{1, 2, \ldots, m\} = \cup_{d|m, d>0} \{b : 1 \le b \le m \text{ mit } \gcd(b, m) = d\}.$$

Da die Mengen auf der rechten Seite paarweise disjunkt sind, folgt daraus die Behauptung. □

2.9 Ordnung von Gruppenelementen

Als nächstes führen wir Elementordnungen und ihre Eigenschaften ein. Dazu sei G eine Gruppe, die multiplikativ geschrieben ist, mit neutralem Element 1.

Definition 2.14 Sei $g \in G$. Wenn es eine natürliche Zahl e gibt mit $g^e = 1$, dann heißt die kleinste solche Zahl *Ordnung* von g in G. Andernfalls sagt man, dass die Ordnung von g in G unendlich ist. Die Ordnung von g in G wird mit $\operatorname{order}_G g$ bezeichnet. Wenn es klar ist, um welche Gruppe es sich handelt, schreibt man auch $\operatorname{order} g$.

Theorem 2.9 *Sei $g \in G$ und $e \in \mathbb{Z}$. Dann gilt $g^e = 1$ genau dann, wenn e durch die Ordnung von g in G teilbar ist.*

Beweis Sei $n = \operatorname{order} g$. Wenn $e = kn$ ist, dann folgt

$$g^e = g^{kn} = (g^n)^k = 1^k = 1.$$

Sei umgekehrt $g^e = 1$. Sei $e = qn + r$ mit $0 \leq r < n$. Dann folgt

$$g^r = g^{e-qn} = g^e (g^n)^{-q} = 1.$$

Weil n die kleinste natürliche Zahl ist mit $g^n = 1$, und weil $0 \leq r < n$ ist, muss $r = 0$ und damit $e = qn$ sein. Also ist n ein Teiler von e, wie behauptet. □

Korollar 2.1 *Sei $g \in G$ und seien k, l ganze Zahlen. Dann gilt $g^l = g^k$ genau dann, wenn $l \equiv k \bmod \operatorname{order} g$ ist.*

Beweis Setze $e = l - k$ und wende Theorem 2.9 an. □

Beispiel 2.18 Wir bestimmen die Ordnung von $2 + 13\mathbb{Z}$ in $(\mathbb{Z}/13\mathbb{Z})^*$. Wir ziehen dazu folgende Tabelle heran.

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \bmod 13$	1	2	4	8	3	6	12	11	9	5	10	7	1

Man sieht, dass die Ordnung von $2 + 13\mathbb{Z}$ den Wert 12 hat. Diese Ordnung ist gleich der Gruppenordnung von $(\mathbb{Z}/13\mathbb{Z})^*$. Dies stimmt aber nicht für jedes Gruppenelement. Zum Beispiel hat $4 + 13\mathbb{Z}$ die Ordnung 6.

Wir bestimmen noch die Ordnung von Potenzen.

Theorem 2.10 *Ist $g \in G$ von endlicher Ordnung e und ist n eine ganze Zahl, so ist* $\operatorname{order} g^n = e / \gcd(e, n)$.

Beweis Es gilt

$$(g^n)^{e/\gcd(e,n)} = (g^e)^{n/\gcd(e,n)} = 1.$$

Nach Theorem 2.9 ist also $e/\gcd(e,n)$ ein Vielfaches der Ordnung von g^n. Gelte

$$1 = (g^n)^k = g^{nk},$$

dann folgt aus Theorem 2.9, dass e ein Teiler von nk ist. Daher ist $e/\gcd(e,n)$ ein Teiler von k, woraus die Behauptung folgt. □

2.10 Untergruppen

Wir führen Untergruppen ein. Mit G bezeichnen wir eine Gruppe.

Definition 2.15 Eine Teilmenge U von G heißt *Untergruppe* von G, wenn U mit der Verknüpfung von G selbst eine Gruppe ist.

Beispiel 2.19 Für jedes $g \in G$ bildet die Menge $\{g^k : k \in \mathbb{Z}\}$ eine Untergruppe von G. Sie heißt die von g *erzeugte Untergruppe* und wir schreiben $\langle g \rangle$ für diese Untergruppe.

Hat g endliche Ordnung e, dann ist $\langle g \rangle = \{g^k : 0 \le k < e\}$. Ist nämlich x eine ganze Zahl, dann gilt $g^x = g^{x \bmod e}$ nach Korollar 2.1. Aus Korollar 2.1 folgt ebenfalls, dass in diesem Fall e die Ordnung von $\langle g \rangle$ ist.

Beispiel 2.20 Die von $2 + 13\mathbb{Z}$ erzeugte Untergruppe von $(\mathbb{Z}/13\mathbb{Z})^*$ ist gemäß Beispiel 2.18 die ganze Gruppe $(\mathbb{Z}/13\mathbb{Z})^*$. Die von $4 + 13\mathbb{Z}$ erzeugte Untergruppe hat die Ordnung 6. Sie ist $\{k + 13\mathbb{Z} : k = 1, 4, 3, 12, 9, 10\}$.

Definition 2.16 Wenn $G = \langle g \rangle$ für ein $g \in G$ ist, so heißt G *zyklisch* und g heißt *Erzeuger* von G. Die Gruppe G ist dann die von g erzeugte Gruppe.

Beispiel 2.21 Die additive Gruppe $\mathbb{Z}$ ist zyklisch. Sie hat zwei Erzeuger, nämlich 1 und -1.

Theorem 2.11 *Ist G endlich und zyklisch, so hat G genau $\varphi(|G|)$ Erzeuger, und die haben alle die Ordnung $|G|$.*

Beweis Sei $g \in G$ ein Element der Ordnung e. Dann hat die von g erzeugte Gruppe die Ordnung e. Also ist ein Element von G genau dann ein Erzeuger von G, wenn es die Ordnung $|G|$ hat. Wir bestimmen die Anzahl der Elemente der Ordnung $|G|$ von G. Sei g ein Erzeuger von G. Dann ist $G = \{g^k : 0 \le k < |G|\}$. Nach Theorem 2.10 hat ein Element dieser Menge genau dann die Ordnung $|G|$, wenn $\gcd(k, |G|) = 1$ ist. Das bedeutet, dass die Anzahl der Erzeuger von G genau $\varphi(|G|)$ ist. □

Beispiel 2.22 Weil $2 + 13\mathbb{Z}$ in $(\mathbb{Z}/13\mathbb{Z})^*$ die Ordnung 12 hat, ist $(\mathbb{Z}/13\mathbb{Z})^*$ zyklisch. Unten werden wir beweisen, dass $(\mathbb{Z}/p\mathbb{Z})^*$ immer zyklisch ist, wenn p eine Primzahl ist. Nach Beispiel 2.18 sind die Erzeuger dieser Gruppe die Restklassen $a + 13\mathbb{Z}$ mit $a \in \{2, 6, 7, 11\}$.

Um das nächste Resultat zu beweisen, brauchen wir ein paar Begriffe. Eine Abbildung $f : X \to Y$ heißt *injektiv*, falls aus $f(x) = f(y)$ immer $x = y$ folgt. Zwei verschiedene Elemente aus X können also nie die gleichen Funktionswerte haben. Die Abbildung heißt *surjektiv*, wenn es für jedes Element $y \in Y$ ein Element $x \in X$ gibt mit $f(x) = y$. Die Abbildung heißt *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist. Eine bijektive Abbildung heißt auch *Bijektion*. Wenn es eine bijektive Abbildung zwischen zwei endlichen Mengen gibt, so haben beide Mengen dieselbe Anzahl von Elementen.

Beispiel 2.23 Betrachte die Abbildung $f : \mathbb{N} \to \mathbb{N}, n \mapsto f(n) = n$. Diese Abbildung ist offensichtlich bijektiv.

Betrachte die Abbildung $f : \mathbb{N} \to \mathbb{N}, n \mapsto f(n) = n^2$. Da natürliche Zahlen paarweise verschiedene Quadrate haben, ist die Abbildung injektiv. Da z. B. 3 kein Quadrat einer natürlichen Zahl ist, ist die Abbildung nicht surjektiv.

Betrachte die Abbildung $f : \{1, 2, 3, 4, 5, 6\} \to \{0, 1, 2, 3, 4, 5\}, n \mapsto f(n) = n \bmod 6$. Da die Urbildmenge ein volles Restsystem modulo 6 ist, ist die Abbildung bijektiv.

Wir beweisen den Satz von Lagrange.

Theorem 2.12 *Ist G eine endliche Gruppe, so teilt die Ordnung jeder Untergruppe die Ordnung von G.*

Beweis Sei H eine Untergruppe von G. Wir sagen, dass zwei Elemente a und b aus G äquivalent sind, wenn $a/b = ab^{-1}$ zu H gehört. Dies ist eine Äquivalenzrelation. Es ist nämlich $a/a = 1 \in H$, daher ist die Relation reflexiv. Außerdem folgt aus $a/b \in H$, dass auch das Inverse b/a zu H gehört, weil H eine Gruppe ist. Daher ist die Relation symmetrisch. Ist schließlich $a/b \in H$ und $b/c \in H$, so ist auch $a/c = (a/b)(b/c) \in H$. Also ist die Relation transitiv.

Wir zeigen, dass die Äquivalenzklassen alle die gleiche Anzahl von Elementen haben. Die Äquivalenzklasse von $a \in G$ ist $\{ha : h \in H\}$. Seien a, b zwei Elemente aus G. Betrachte die Abbildung

$$\{ha : h \in H\} \to \{hb : h \in H\}, ha \mapsto hb.$$

Die Abbildung ist injektiv, weil in G die Kürzungsregel gilt. Die Abbildung ist außerdem offensichtlich surjektiv. Daher haben beide Äquivalenzklassen gleich viele Elemente. Es ist damit gezeigt, dass alle Äquivalenzklassen die gleiche Anzahl von Elementen haben. Eine solche Äquivalenzklasse ist aber die Äquivalenzklasse von 1 und die ist H. Die Anzahl der Elemente in den Äquivalenzklassen ist somit $|H|$. Weil G aber die disjunkte Vereinigung aller Äquivalenzklassen ist, ist $|G|$ ein Vielfaches von $|H|$. □

Definition 2.17 Ist H eine Untergruppe von G, so heißt die natürliche Zahl $|G|/|H|$ der *Index* von H in G.

2.11 Der kleine Satz von Fermat

Wir formulieren den berühmten kleinen Satz von Fermat.

Theorem 2.13 *Wenn* $\gcd(a, m) = 1$ *ist, dann folgt* $a^{\varphi(m)} \equiv 1 \bmod m$.

Dieses Theorem eröffnet zum Beispiel eine neue Methode, prime Restklassen zu invertieren. Es impliziert nämlich, dass aus $\gcd(a, m) = 1$ die Kongruenz

$$a^{\varphi(m)-1} \cdot a \equiv 1 \bmod m$$

folgt. Das bedeutet, dass $a^{\varphi(m)-1} + m\mathbb{Z}$ die inverse Restklasse von $a + m\mathbb{Z}$ ist.

Wir beweisen den kleinen Satz von Fermat in einem allgemeineren Kontext. Dazu sei G eine endliche Gruppe der Ordnung $|G|$, die multiplikativ geschrieben ist, mit neutralem Element 1.

Theorem 2.14 *Die Ordnung eines Gruppenelementes teilt die Gruppenordnung.*

Beweis Die Ordnung eines Gruppenelementes g ist die Ordnung der von g erzeugten Untergruppe. Also folgt die Behauptung aus Theorem 2.12. □

Aus diesem Resultat folgern wir eine allgemeine Version des kleinen Satzes von Fermat.

Korollar 2.2 *Es gilt* $g^{|G|} = 1$ *für jedes* $g \in G$.

Beweis Die Behauptung folgt aus Theorem 2.14 und Theorem 2.9. □

Da $(\mathbb{Z}/m\mathbb{Z})^*$ eine endliche abelsche Gruppe der Ordnung $\varphi(m)$ ist, folgt Theorem 2.13 aus Korollar 2.2.

2.12 Schnelle Exponentiation

Theorem 2.13 zeigt, dass eine ganze Zahl x mit $x \equiv a^{\varphi(m)-1} \bmod m$ die Kongruenz (2.4) löst. Es ist also nicht nötig, diese Kongruenz durch Anwendung des erweiterten euklidischen Algorithmus zu lösen. Man kann z. B. $x = a^{\varphi(m)-1} \bmod m$ setzen. Soll die neue Methode effizient sein, dann muss man die Potenz schnell berechnen können.

Wir beschreiben jetzt ein Verfahren zur schnellen Berechnung von Potenzen in einem Monoid G. Dieses Verfahren und Varianten davon sind zentral in vielen kryptographi-

schen Algorithmen. Sei $g \in G$ und e eine natürliche Zahl. Sei

$$e = \sum_{i=0}^{k} e_i 2^i.$$

die Binärentwicklung von e. Man beachte, dass die Koeffizienten e_i entweder 0 oder 1 sind. Dann gilt

$$g^e = g^{\sum_{i=0}^{k} e_i 2^i} = \prod_{i=0}^{k} (g^{2^i})^{e_i} = \prod_{0 \le i \le k, e_i = 1} g^{2^i}.$$

Aus dieser Formel gewinnt man die folgende Idee:

1. Berechne die sukzessiven Quadrate g^{2^i}, $0 \le i \le k$.
2. Bestimme g^e als Produkt derjenigen g^{2^i}, für die $e_i = 1$ ist.

Beachte dabei

$$g^{2^{i+1}} = (g^{2^i})^2.$$

Daher kann $g^{2^{i+1}}$ aus g^{2^i} mittels einer Quadrierung berechnet werden. Bevor wir das Verfahren präzise beschreiben und analysieren, erläutern wir es an einem Beispiel. Es zeigt sich, dass der Algorithmus viel effizienter ist als die naive Multiplikationsmethode.

Beispiel 2.24 Wir wollen 6^{73} mod 100 berechnen. Wir schreiben die Binärentwicklung des Exponenten auf:

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

Dann bestimmen wir die sukzessiven Quadrate 6, $6^2 = 36$, $6^{2^2} = 36^2 \equiv -4 \bmod 100$, $6^{2^3} \equiv 16 \bmod 100$, $6^{2^4} \equiv 16^2 \equiv 56 \bmod 100$, $6^{2^5} \equiv 56^2 \equiv 36 \bmod 100$, $6^{2^6} \equiv -4 \bmod 100$. Also ist $6^{73} \equiv 6 * 6^{2^3} * 6^{2^6} \equiv 6 * 16 * (-4) \equiv 16 \bmod 100$. Wir haben nur 6 Quadrierungen und zwei Multiplikationen in $\mathbb{Z}/m\mathbb{Z}$ verwendet, um das Resultat zu berechnen. Hätten wir 6^{73} mod 100 nur durch Multiplikation berechnet, dann hätten wir dazu 72 Multiplikationen modulo 100 gebraucht.

Algorithmus 2.1 ist eine Implementierung der schnellen Exponentiation.

Algorithmus 2.1 (fastExponentiation(g, e))

$r \leftarrow 1$
$b \leftarrow g$
while $e > 0$ **do**
  if e is odd **then**
    $r \leftarrow rb, e \leftarrow e - 1$
  end if

$b \leftarrow b^2$
$e \leftarrow e/2$
end while
return r

Die Implementierung arbeitet so: In der Variablen `result` ist das Resultat gespeichert, soweit es bisher bestimmt ist. In der Variablen `base` sind die sukzessiven Quadrate gespeichert. Die Quadrate werden eins nach dem anderen ausgerechnet und mit dem Resultat multipliziert, wenn das entsprechende Bit 1 ist.

Die Komplexität des Algorithmus gibt folgender Satz an, der leicht verifiziert werden kann.

Theorem 2.15 `fastExponentiation` *berechnet* g^e *und benötigt dazu höchstens* $\lfloor \log_2 e \rfloor$ *Quadrierungen und Multiplikationen. Der Algorithmus muss nur eine konstante Anzahl von Gruppenelementen speichern.*

Aus Theorem 2.15 und Theorem 2.5 erhalten wir eine Abschätzung für die Zeit, die die Berechnung von Potenzen in der primen Restklassengruppe mod m benötigt.

Korollar 2.3 *Ist* e *eine ganze Zahl und* $a \in \{0, \ldots, m-1\}$, *so erfordert die Berechnung von* $a^e \bmod m$ *Zeit* $O((\operatorname{size} e)(\operatorname{size} m)^2)$ *und Platz* $O(\operatorname{size} e + \operatorname{size} m)$.

Exponentiation in der primen Restklassengruppe ist also in polynomieller Zeit möglich. Es gibt Varianten des schnellen Exponentiationsalgorithmus, die in [33] und [53] beschrieben sind. Sie sind in unterschiedlichen Situationen effizienter als die Basisvariante.

2.13 Schnelle Auswertung von Potenzprodukten

Angenommen, G ist eine endliche abelsche Gruppe, $g_1, \ldots, g_k$ sind Elemente von G und $e_1, \ldots, e_k$ sind nicht negative ganze Zahlen. Wir wollen das Potenzprodukt

$$A = \prod_{i=1}^{k} g_i^{e_i}$$

berechnen. Dazu brauchen wir die Binärentwicklung der Exponenten e_i. Sie werden auf gleiche Länge normiert. Die Binärentwicklung von e_i sei

$$b_{i,n-1} b_{i,n-2} \ldots b_{i,0}, \quad 1 \le i \le k.$$

Für wenigstens ein i sei $b_{i,n-1}$ ungleich Null. Für $1 \le i \le k$ und $0 \le j < n$ sei $e_{i,j}$ die ganze Zahl mit Binärentwicklung $b_{i,n-1} b_{i,n-2} \ldots b_{i,j}$. Ferner sei $e_{i,n} = 0$ für $1 \le i \le k$.

Dann ist $e_i = e_{i,0}$ für $1 \leq i \leq k$. Zuletzt setze

$$A_j = \prod_{i=1}^{k} g_i^{e_{i,j}}.$$

Dann ist $A_0 = A$ das gewünschte Potenzprodukt. Wir berechnen iterativ $A_n, A_{n-1}, \ldots, A_0 = A$. Dazu beachten wir, dass

$$e_{i,j} = 2 * e_{i,j+1} + b_{i,j}, \quad 1 \leq i \leq k, 0 \leq j < n$$

ist. Daher ist

$$A_j = A_{j+1}^2 \prod_{i=1}^{k} g_i^{b_{i,j}}, \quad 0 \leq j < n.$$

Für alle $\vec{b} = (b_1, \ldots, b_k) \in \{0,1\}^k$ wird

$$G_{\vec{b}} = \prod_{i=1}^{k} g_i^{b_i}$$

bestimmt. Dann gilt

$$A_j = A_{j+1}^2 G_{(b_{1,j},\ldots,b_{k,j})}, \quad 0 \leq j < n.$$

Wir analysieren dieses Verfahren. Die Berechnung aller $G_{\vec{b}}, \vec{b} \in \{0,1\}^k$ erfordert $2^k - 2$ Multiplikationen in G. Sind diese ausgeführt, so werden noch $n-1$ Quadrierungen und Multiplikationen in G benötigt, um A zu berechnen. Damit ist folgendes Resultat bewiesen:

Theorem 2.16 *Sei $k \in \mathbb{N}$, $g_i \in G$, $e_i \in \mathbb{Z}_{\geq 0}$, $1 \leq i \leq k$ und sei n die maximale binäre Länge der e_i. Dann kann man das Potenzprodukt $\prod_{i=1}^{k} g_i^{e_i}$ mittels $2^k + n - 3$ Multiplikationen und $n-1$ Quadrierungen bestimmen.*

Das beschriebene Verfahren ist für den Fall $k = 1$ eine andere Methode der schnellen Exponentiation. Während in der Methode aus Abschn. 2.12 die Binärentwicklung des Exponenten von rechts nach links abgearbeitet wird, geht man in dieser Methode die Binärentwicklung von links nach rechts durch.

2.14 Berechnung von Elementordnungen

In kryptographischen Anwendungen braucht man häufig Gruppenelemente großer Ordnung. Wir diskutieren das Problem, die Ordnung eines Elementes g einer endlichen Gruppe G zu berechnen bzw. zu überprüfen, ob eine vorgelegte natürliche Zahl die Ordnung von g ist.

Der folgende Satz zeigt, wie die Ordnung von g berechnet werden kann, wenn die Primfaktorzerlegung

$$|G| = \prod_{p||G|} p^{e(p)}$$

der Ordnung von G bekannt ist. Wenn diese Primfaktorzerlegung unbekannt ist, kann man die Ordnung nicht so leicht finden. In der Public-Key-Kryptographie kennt man aber die Gruppenordnung und ihre Faktorisierung oft.

Theorem 2.17 *Für jeden Primteiler p von $|G|$ sei $f(p)$ die größte ganze Zahl derart, dass $g^{|G|/p^{f(p)}} = 1$ ist. Dann ist*

$$\operatorname{order} g = \prod_{p||G|} p^{e(p)-f(p)}. \tag{2.5}$$

Beweis Übung 2.22. □

Theorem 2.17 kann man unmittelbar in einen Algorithmus verwandeln, der die Ordnung eines Elementes g berechnet.

Beispiel 2.25 Sei G die prime Restklassengruppe modulo 101. Ihre Ordnung ist $100 = 2^2 * 5^2$. Also ist

$$e(2) = e(5) = 2.$$

Wir berechnen die Ordnung von $2 + 101\mathbb{Z}$. Dazu berechnen wir zuerst die Zahlen $f(p)$ aus Theorem 2.17. Es ist

$$2^{2*5^2} \equiv 2^{50} \equiv -1 \bmod 101.$$

Also ist $f(2) = 0$. Weiter ist

$$2^{2^2*5} \equiv 2^{20} \equiv -6 \bmod 101.$$

Also ist $f(5) = 0$. Insgesamt ist also 100 die Ordnung von $2 + 101\mathbb{Z}$. Das bedeutet, dass $\mathbb{Z}/101\mathbb{Z}$ zyklisch ist und $2 + 101\mathbb{Z}$ ein Erzeuger dieser Gruppe ist.

Der Algorithmus bestimmt die Zahlen $f(p)$ für alle Primteiler p von $|G|$. Daraus wird dann die Elementordnung berechnet. Die Implementierung wird dem Leser überlassen.

Als nächstes stellen wir das Problem, zu verifizieren, dass eine vorgelegte Zahl die Ordnung eines Elementes g ist. Das braucht man zum Beispiel, wenn man beweisen will, dass ein vorgelegtes Element die Gruppe erzeugt. Folgendes Resultat ist die Grundlage des Algorithmus. Es ist eine unmittelbare Folge von Theorem 2.17.

Korollar 2.4 *Sei $n \in \mathbb{N}$, und gelte $g^n = 1$ und $g^{n/p} \neq 1$ für jeden Primteiler p von n. Dann ist n die Ordnung von g.*

Ist die Faktorisierung der Ordnung der Gruppe oder sogar der Elementordnung bekannt, so kann man die Elementordnung in Polynomzeit finden bzw. verifizieren. Ist aber

keine dieser Faktorisierungen bekannt, so sind diese Aufgaben im Allgemeinen wesentlich schwieriger.

Beispiel 2.26 Wir behaupten, dass 25 die Ordnung der Restklasse $5+101\mathbb{Z}$ in der primen Restklassengruppe modulo 101 ist. Tatsächlich ist $5^{25} \equiv 1 \bmod 101$ und $5^5 \equiv -6 \bmod 101$. Also folgt die Behauptung aus Korollar 2.4.

2.15 Der Chinesische Restsatz

Seien $m_1, \ldots, m_n$ natürliche Zahlen, die paarweise teilerfremd sind, und seien $a_1, \ldots, a_n$ ganze Zahlen. Wir erläutern eine Lösungsmethode für folgende *simultane Kongruenz*

$$x \equiv a_1 \bmod m_1, \quad x \equiv a_2 \bmod m_2, \quad \ldots, \quad x \equiv a_n \bmod m_n. \tag{2.6}$$

Setze

$$m = \prod_{i=1}^{n} m_i, \quad M_i = m/m_i, \quad 1 \le i \le n.$$

Wir werden sehen, dass die Lösung der Kongruenz (2.6) modulo m eindeutig ist. Es gilt

$$\gcd(m_i, M_i) = 1, \quad 1 \le i \le n,$$

weil die m_i paarweise teilerfremd sind. Wir benutzen den erweiterten euklidischen Algorithmus, um Zahlen $y_i \in \mathbb{Z}$, $1 \le i \le n$, zu berechnen mit

$$y_i M_i \equiv 1 \bmod m_i, \quad 1 \le i \le n. \tag{2.7}$$

Dann setzen wir

$$x = \left(\sum_{i=1}^{n} a_i y_i M_i \right) \bmod m. \tag{2.8}$$

Wir zeigen, dass x eine Lösung der simultanen Kongruenz (2.6) ist. Aus (2.7) folgt

$$a_i y_i M_i \equiv a_i \bmod m_i, \quad 1 \le i \le n, \tag{2.9}$$

und weil für $j \ne i$ die Zahl m_i ein Teiler von M_j ist, gilt

$$a_j y_j M_j \equiv 0 \bmod m_i, \quad 1 \le i, j \le n, i \ne j. \tag{2.10}$$

Aus (2.8), (2.9) und (2.10) folgt

$$x \equiv a_i y_i M_i + \sum_{j=1, j \ne i}^{n} a_j y_j M_j \equiv a_i \bmod m_i, \quad 1 \le i \le n.$$

Also löst x die Kongruenz (2.6).

Beispiel 2.27 Wir wollen die simultane Kongruenz

$$x \equiv 2 \bmod 4, \quad x \equiv 1 \bmod 3, \quad x \equiv 0 \bmod 5$$

lösen. Also ist $m_1 = 4$, $m_2 = 3$, $m_3 = 5$, $a_1 = 2$, $a_2 = 1$, $a_3 = 0$. Dann ist $m = 60$, $M_1 = 60/4 = 15$, $M_2 = 60/3 = 20$, $M_3 = 60/5 = 12$. Wir lösen $y_1 M_1 \equiv 1 \bmod m_1$, d. h. $-y_1 \equiv 1 \bmod 4$. Die absolut kleinste Lösung ist $y_1 = -1$. Wir lösen $y_2 M_2 \equiv 1 \bmod m_2$, d. h. $-y_2 \equiv 1 \bmod 3$. Die absolut kleinste Lösung ist $y_2 = -1$. Schließlich lösen wir $y_3 M_3 \equiv 1 \bmod m_3$, d. h. $2y_3 \equiv 1 \bmod 5$. Die kleinste nicht negative Lösung ist $y_3 = 3$. Daher erhalten wir $x \equiv -2 * 15 - 20 \equiv 10 \bmod 60$. Eine Lösung der simultanen Kongruenz ist $x = 10$.

Man beachte, dass in dem beschriebenen Algorithmus die Zahlen y_i und M_i nicht von den Zahlen a_i abhängen. Sind also die Werte y_i und M_i berechnet, dann kann man (2.8) benutzen, um (2.6) für jede Auswahl von Werten a_i zu lösen. Eine Implementierung findet man im Algorithmus 2.2, der die Vorberechnung macht und im Algorithmus 2.15.

Algorithmus 2.2 (CRTPrecomputation($m[\,], n$))

$M[0] \leftarrow 1$
for $i = 1, \ldots, n$ **do**
  $M[0] \leftarrow M[0]m[i]$
end for
for $i = 1, \ldots, n$ **do**
  $M[i] \leftarrow M[0]/m[i]$
  $(g, x, y[i]) \leftarrow \text{xEuclid}(M[i], m[i])$
end for
return $y[\,], M[\,]$

Algorithmus 2.3 (CRT($m[\,], a[\,], y[\,], M[\,], n$))

$x \leftarrow 1$
for $i = 1, \ldots, n$ **do**
  $x \leftarrow (r + a[i] \cdot y[i] \cdot M[i]) \bmod M[0]$
end for
return x

Jetzt wird der *Chinesische Restsatz* formuliert.

Theorem 2.18 *Seien $m_1, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen und seien $a_1, \ldots, a_n$ ganze Zahlen. Dann hat die simultane Kongruenz (2.6) eine Lösung x, die eindeutig ist* mod $m = \prod_{i=1}^{n} m_i$.

Beweis Die Existenz wurde schon bewiesen. Also muss noch die Eindeutigkeit gezeigt werden. Zu diesem Zweck seien x und x' zwei solche Lösungen. Dann gilt $x \equiv x' \bmod m_i$, $1 \leq i \leq n$. Weil die Zahlen m_i paarweise teilerfremd sind, folgt $x \equiv x' \bmod m$. □

Der folgende Satz schätzt den Aufwand zur Konstruktion einer Lösung einer simultanen Kongruenz ab.

Theorem 2.19 *Das Verfahren zur Lösung der simultanen Kongruenz (2.6) kostet Zeit $O((\text{size}\, m)^2)$ und Platz $O(\text{size}\, m)$.*

Beweis Die Berechnung von m erfordert nach den Ergebnissen aus Abschn. 1.6.1 Zeit $O(\text{size}\, m \sum_{i=1}^{n} \text{size}\, m_i) = O((\text{size}\, m)^2)$. Die Berechnung aller M_i und y_i und des Wertes x kostet dieselbe Zeit. Das folgt ebenfalls aus den Ergebnissen von Abschn. 1.6.1 und aus Theorem 1.13. Die Platzschranke ist leicht zu verifizieren. □

2.16 Zerlegung des Restklassenrings

Wir benutzen den Chinesischen Restsatz, um den Restklassenring $\mathbb{Z}/m\mathbb{Z}$ zu zerlegen. Diese Zerlegung erlaubt es, anstatt in einem großen Restklassenring $\mathbb{Z}/m\mathbb{Z}$ in vielen kleinen Restklassenringen $\mathbb{Z}/m_i\mathbb{Z}$ zu rechnen. Das ist oft effizienter. Man kann diese Methode zum Beispiel verwenden, um die Entschlüsselung im RSA-Verfahren zu beschleunigen.

Wir definieren das *direkte Produkt von Ringen*.

Definition 2.18 Seien $R_1, R_2, \ldots, R_n$ Ringe. Dann ist ihr *direktes Produkt* $\prod_{i=1}^{n} R_i$ definiert als die Menge aller Tupel $(r_1, r_2, \ldots, r_n) \in R_1 \times \cdots \times R_n$ zusammen mit komponentenweiser Addition und Multiplikation.

Man kann leicht verifizieren, dass $R = \prod_{i=1}^{n} R_i$ aus Definition 2.18 ein Ring ist. Wenn die R_i kommutative Ringe mit Einselementen e_i, $1 \leq i \leq n$, sind, dann ist R ein kommutativer Ring mit Einselement $(e_1, \ldots, e_n)$.

Das direkte Produkt von Gruppen ist entsprechend definiert.

Beispiel 2.28 Sei $R_1 = \mathbb{Z}/2\mathbb{Z}$ und $R_2 = \mathbb{Z}/9\mathbb{Z}$. Dann besteht $R = R_1 \times R_2$ aus allen Paaren $(a + 2\mathbb{Z}, b + 9\mathbb{Z})$, $0 \leq a < 2, 0 \leq b < 9$. Also hat $R = R_1 \times R_2$ genau 18 Elemente. Das Einselement in R ist $(1 + 2\mathbb{Z}, 1 + 9\mathbb{Z})$.

Wir brauchen auch noch den Begriff des Homomorphismus und des Isomorphismus.

Definition 2.19 Seien $(X, \perp_1, \ldots, \perp_n)$ und $(Y, \top_1, \ldots, \top_n)$ Mengen mit jeweils n inneren Verknüpfungen. Eine Abbildung $f : X \to Y$ heißt *Homomorphismus* dieser Strukturen, wenn $f(a \perp_i b) = f(a) \top_i f(b)$ gilt für alle $a, b \in X$ und $1 \leq i \leq n$. Ist die Abbildung bijektiv, so heißt sie *Isomorphismus* dieser Strukturen.

Wenn man einen Isomorphismus zwischen zwei Ringen kennt, den man in beiden Richtungen leicht berechnen kann, dann lassen sich alle Aufgaben in dem einen Ring auch in dem anderen Ring lösen. Dies bringt oft Effizienzvorteile.

Beispiel 2.29 Ist m eine natürliche Zahl, so ist die Abbildung $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto a + m\mathbb{Z}$ ein Ringhomomorphismus.

Ist G eine zyklische Gruppe der Ordnung n mit Erzeuger g, so ist $\mathbb{Z}/n\mathbb{Z} \to G, e + n\mathbb{Z} \mapsto g^e$ ein Isomorphismus von Gruppen (siehe Übung 2.24).

Theorem 2.20 *Seien $m_1, \ldots, m_n$ paarweise teilerfremde ganze Zahlen und sei $m = m_1 m_2 \cdots m_n$. Dann ist die Abbildung*

$$\mathbb{Z}/m\mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}, \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z}) \tag{2.11}$$

ein Isomorphismus von Ringen.

Beweis Beachte zuerst, dass (2.11) wohldefiniert ist. Ist nämlich $a \equiv b \bmod m$, dann folgt $a \equiv b \bmod m_i$ für $1 \leq i \leq n$. Es ist auch leicht, zu verifizieren, dass (2.11) ein Homomorphismus von Ringen ist. Um die Surjektivität zu beweisen, sei $(a_1 + m_1\mathbb{Z}, \ldots, a_n + m_n\mathbb{Z}) \in \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$. Dann folgt aus Theorem 2.18, dass dieses Tupel ein Urbild unter (2.11) hat. Die Injektivität folgt aus der Eindeutigkeit in Theorem 2.18. □

Theorem 2.20 zeigt, dass man Berechnungen in $\mathbb{Z}/m\mathbb{Z}$ auf Berechnungen in $\prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ zurückführen kann. Man verwandelt dazu eine Restklasse mod m in ein Tupel von Restklassen mod m_i, führt die Berechnung auf dem Tupel aus und benutzt den chinesischen Restsatz, um das Ergebnis wieder in eine Restklasse mod m zu verwandeln. Dies ist z. B. effizienter, wenn die Berechnung mod m_i unter Benutzung von Maschinenzahlen ausgeführt werden kann, während die Berechnungen mod m die Verwendung einer Multiprecision-Arithmetik erfordern würden.

2.17 Bestimmung der Eulerschen φ-Funktion

Jetzt leiten wir eine Formel für die Eulersche φ-Funktion her.

Theorem 2.21 *Seien $m_1, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen und $m = \prod_{i=1}^{n} m_i$. Dann gilt $\varphi(m) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_n)$.*

Beweis Es folgt aus Theorem 2.20, dass die Abbildung

$$(\mathbb{Z}/m\mathbb{Z})^* \to \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})^*, a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z}) \tag{2.12}$$

ein Isomorphismus von Gruppen ist. Insbesondere ist die Abbildung bijektiv. Daher ist die Anzahl $\varphi(m)$ der Elemente von $(\mathbb{Z}/m\mathbb{Z})^*$ gleich der Anzahl $\prod_{i=1}^{n} \varphi(m_i)$ der Elemente von $\prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})^*$. □

Theorem 2.22 *Sei m eine natürliche Zahl und $m = \prod_{p|m} p^{e(p)}$ ihre Primfaktorzerlegung. Dann gilt*

$$\varphi(m) = \prod_{p|m} (p-1)p^{e(p)-1} = m \prod_{p|m} \frac{p-1}{p}.$$

Beweis Nach Theorem 2.21 gilt

$$\varphi(m) = \prod_{p|m} \varphi(p^{e(p)}).$$

Also braucht nur $\varphi(p^e)$ berechnet zu werden, und zwar für eine Primzahl p und eine natürliche Zahl e. Nach Theorem 1.3 hat jedes a in der Menge $\{0, 1, 2, \ldots, p^e - 1\}$ eine eindeutige Darstellung

$$a = a_e + a_{e-1}p + a_{e-2}p^2 + \ldots + a_1 p^{e-1}$$

mit $a_i \in \{0, 1, \ldots, p-1\}$, $1 \leq i \leq e$. Außerdem gilt genau dann $\gcd(a, p^e) = 1$, wenn $a_e \neq 0$ ist. Dies impliziert, dass

$$\varphi(p^e) = (p-1)p^{e-1} = p^e \left(1 - \frac{1}{p}\right).$$

Also ist die Behauptung bewiesen. □

Beispiel 2.30 Es gilt $\varphi(2^m) = 2^{m-1}$, $\varphi(100) = \varphi(2^2 * 5^2) = 2 * 4 * 5 = 40$.

Wenn die Faktorisierung von m bekannt ist, kann $\varphi(m)$ gemäß Theorem 2.22 in Zeit $O((\text{size}\, m)^2)$ berechnet werden.

2.18 Polynome

Wir wollen in diesem Kapitel noch beweisen, dass für jede Primzahl p die prime Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch von der Ordnung $p - 1$ ist. Dazu brauchen wir Polynome, die wir in diesem Abschnitt kurz einführen. Polynome brauchen wir später auch noch, um endliche Körper einzuführen.

Es sei R ein kommutativer Ring mit Einselement $1 \neq 0$. Ein *Polynom* in einer Variablen über R ist ein Ausdruck

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

wobei x die Variable ist und die *Koeffizienten* $a_0, \ldots, a_n$ zu R gehören. Die Menge aller Polynome über R in der Variablen x wird mit $R[x]$ bezeichnet.

Sei $a_n \neq 0$. Dann heißt n der *Grad* des Polynoms. Man schreibt $n = \deg f$ und setzt $\deg(0) = -\infty$. Außerdem heißt a_n der *Leitkoeffizient* oder *führender Koeffizient* von f. Sind alle Koeffizienten außer dem führenden Koeffizienten 0, so heißt f *Monom*.

Beispiel 2.31 Die Polynome $2x^3 + x + 1$, x, 1 liegen in $\mathbb{Z}[x]$. Das erste Polynom hat den Grad 3, das zweite den Grad 1 und das dritte den Grad 0.

Ist $r \in R$, so heißt

$$f(r) = a_n r^n + \cdots + a_0$$

der *Wert* von f an der Stelle r. Ist $f(r) = 0$, so heißt r *Nullstelle* von f.

Beispiel 2.32 Der Wert des Polynoms $2x^3 + x + 1 \in \mathbb{Z}[x]$ an der Stelle -1 ist -2.

Beispiel 2.33 Bezeichne die Elemente von $\mathbb{Z}/2\mathbb{Z}$ mit 0 und 1. Dann ist $x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$. Dieses Polynom hat die Nullstelle 1.

Sei

$$g(x) = b_m x^m + \cdots + b_0$$

ein anderes Polynom über R und gelte $n \geq m$. Indem man die fehlenden Koeffizienten auf Null setzt, kann man

$$g(x) = b_n x^n + \cdots + b_0$$

schreiben. Die *Summe* der Polynome f und g ist

$$(f + g)(x) = (a_n + b_n)x^n + \cdots + (a_0 + b_0).$$

Dies ist wieder ein Polynom.

Beispiel 2.34 Ist $g(x) = x^2 + x + 1 \in \mathbb{Z}[x]$ und $f(x) = x^3 + 2x^2 + x + 2 \in \mathbb{Z}[x]$, so ist $(f + g)(x) = x^3 + 3x^2 + 2x + 3$.

Die Addition von f und g benötigt $O(\max\{\deg f, \deg g\} + 1)$ Additionen in R.

Das *Produkt* der Polynome f und g ist

$$(fg)(x) = c_{n+m} x^{n+m} + \cdots + c_0$$

wobei

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad 0 \le k \le n+m$$

ist. Auch hierin sind die nicht definierten Koeffizienten a_i und b_i auf 0 gesetzt.

Beispiel 2.35 Sei $f(x) = x^2 + x + 1 \in \mathbb{Z}[x]$ und $g(x) = x^3 + 2x^2 + x + 2 \in \mathbb{Z}[x]$. Dann ist $(fg)(x) = (x^2 + x + 1)(x^3 + 2x^2 + x + 2) = x^5 + (2+1)x^4 + (1+2+1)x^3 + (2+1+2)x^2 + (2+1)x + 2 = x^5 + 3x^4 + 4x^3 + 5x^2 + 3x + 2$.

Wir schätzen die Anzahl der Operationen ab, die zur Multiplikation von f und g verwandt werden. Es werden alle Produkte $a_i b_j$, $0 \le i \le \deg f$, $0 \le j \le \deg g$ gebildet. Dies sind $(\deg f + 1)(\deg g + 1)$ Multiplikationen. Dann werden diejenigen Produkte $a_i b_j$ addiert, für die $i + j$ den gleichen Wert hat. Diese Summe bildet den Koeffizienten von x^{i+j}. Da jedes Produkt in genau einer Summe vorkommt, sind dies höchstens $(\deg f + 1)(\deg g + 1)$ Additionen. Insgesamt braucht man also zur Multiplikation von f und g $O((\deg f + 1)(\deg g + 1))$ Additionen und Multiplikationen in R. Schnellere Polynomoperationen mit Hilfe der schnellen Fouriertransformation werden in [3] beschrieben. Siehe auch [39].

Man sieht leicht ein, dass $(R[x], +, \cdot)$ ein kommutativer Ring mit Einselement 1 ist.

2.19 Polynome über Körpern

Sei K ein Körper. Dann ist der Polynomring $K[x]$ nullteilerfrei. Folgende Regel kann man leicht verifizieren.

Lemma 2.2 *Sind* $f, g \in K[x]$, $f, g \neq 0$, *dann gilt* $\deg(fg) = \deg f + \deg g$.

Wie im Ring der ganzen Zahlen ist im Polynomring $K[x]$ die Division mit Rest möglich.

Theorem 2.23 *Seien* $f, g \in K[x]$, $g \neq 0$. *Dann gibt es eindeutig bestimmte Polynome* $q, r \in K[x]$ *mit* $f = qg + r$ *und* $r = 0$ *oder* $\deg r < \deg g$.

Beweis Ist $f = 0$, so setze $q = r = 0$. Sei also $f \neq 0$. Ist $\deg g > \deg f$, so setze $q = 0$ und $r = f$. Wir nehmen also weiter an, dass $\deg g \le \deg f$ ist.

Wir beweisen die Existenz von q und r durch Induktion über den Grad von f.

Ist $\deg f = 0$, dann ist $\deg g = 0$. Also sind $f, g \in K$ und man kann $q = f/g$ und $r = 0$ setzen.

Sei $\deg f = n > 0$, $\deg g = m$, $n \ge m$ und

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0.$$

Setze

$$f_1 = f - a_n/b_m x^{n-m} g.$$

Entweder ist $f_1 = 0$ oder $\deg f_1 < \deg f$. Nach Induktionsvoraussetzung gibt es Polynome q_1 und r mit $f_1 = q_1 g + r$ und $r = 0$ oder $\deg r < \deg g$. Daraus folgt

$$f = (a_n/b_m x^{n-m} + q_1)g + r.$$

Die Polynome $q = a_n/b_m x^{n-m} + q_1$ und r von oben erfüllen die Behauptung.

Jetzt beweisen wir noch die Eindeutigkeit. Seien $f = qg + r = q'g + r'$ zwei Darstellungen wie im Satz. Dann ist $(q - q')g = r' - r$. Ist $r = r'$, so ist $q = q'$, weil $g \neq 0$ und $K[x]$ nullteilerfrei ist. Ist $r \neq r'$, so ist $q - q' \neq 0$ und wegen $\deg g > \deg r$ und $\deg g > \deg r'$ gilt nach Lemma 2.2 auch $\deg(q - q')g > \deg(r' - r)$. Dies kann aber nicht sein, weil $(q - q')g = r' - r$ ist. □

In der Situation von Theorem 2.23 nennt man q den *Quotienten* und r den *Rest* der Division von f durch g und man schreibt $r = f \bmod g$.

Aus dem Beweis von Theorem 2.23 erhält man einen Algorithmus, der es ermöglicht, ein Polynom f durch ein anderes Polynom g mit Rest zu dividieren. Man setzt zuerst $r = f$ und $q = 0$. Solange $r \neq 0$ und $\deg r \geq \deg g$ ist, setzt man $h(x) = (a/b)x^{\deg r - \deg g}$, wobei a der höchste Koeffizient von r und b der höchste Koeffizient von g ist. Dann ersetzt man r durch $r - hg$ und q durch $q + h$. Sobald $r = 0$ oder $\deg r < \deg g$ ist, gibt man den Quotienten q und den Rest r aus. Dies wird im folgenden Beispiel illustriert.

Beispiel 2.36 Sei $K = \mathbb{Z}/2\mathbb{Z}$ der Restklassenring mod 2. Dieser Ring ist ein Körper. Die Elemente werden durch ihre kleinsten nicht negativen Vertreter dargestellt. Wir schreiben also $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

Sei

$$f(x) = x^3 + x + 1, \quad g(x) = x^2 + x.$$

Wir dividieren f mit Rest durch g. Wir setzen also zuerst $r = f$ und $q = 0$. Dann eliminieren wir x^3 in r. Wir setzen $h(x) = x$ und ersetzen r durch $r - hg = x^3 + x + 1 - x(x^2 + x) = x^2 + x + 1$ und q durch $q + h = x$. Danach ist $\deg r = \deg g$. Der Algorithmus benötigt also noch eine Iteration. Wieder eliminieren wir den höchsten Koeffizienten in r. Dazu setzen wir $h(x) = 1$ und ersetzen r durch $r - hg = 1$ und q durch $q + h = x + 1$. Da nun $0 = \deg r < \deg g = 2$ ist, sind wir fertig und haben den Quotienten $q = x + 1$ und den Rest $r = 1$ berechnet.

Wir schätzen die Anzahl der Operationen in K ab, die man für die Division mit Rest von f durch g braucht. Die Berechnung eines Monoms h erfordert eine Operation in K. Die Anzahl der Monome h ist höchstens $\deg q + 1$, weil deren Grade streng monoton fallen und ihre Summe gerade q ist. Jedesmal, wenn h berechnet ist, muss man $r - hg$ berechnen. Die Berechnung von hg erfordert $\deg g + 1$ Multiplikationen in K. Der Grad der Polynome r und hg ist derselbe und die Anzahl der von Null verschiedenen Koeffizienten in hg ist höchstens $\deg g + 1$. Daher erfordert die Berechnung von $r - hg$

höchstens $\deg g + 1$ Additionen in K. Insgesamt erfordert die Division mit Rest höchstens $O((\deg g + 1)(\deg q + 1))$ Operationen in K.

Theorem 2.24 *Sind $f, g \in K[x]$ mit $g \neq 0$, so kann man f mit Rest durch g unter Verwendung von $O((\deg g + 1)(\deg q + 1))$ Operationen in K dividieren, wobei q der Quotient der Division ist.*

Aus Theorem 2.23 erhält man folgende Konsequenzen.

Korollar 2.5 *Ist f ein von Null verschiedenes Polynom in $K[x]$ und ist a eine Nullstelle von f, dann ist $f = (x - a)q$ mit $q \in K[x]$, d. h. f ist durch das Polynom $x - a$ teilbar.*

Beweis Nach Theorem 2.23 gibt es Polynome $q, r \in K[x]$ mit $f = (x - a)q + r$ und $r = 0$ oder $\deg r < 1$. Daraus folgt $0 = f(a) = r$, also $f = (x - a)q$. □

Beispiel 2.37 Das Polynom $x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ hat die Nullstelle 1 und es gilt $x^2 + 1 = (x - 1)^2$.

Korollar 2.6 *Ein Polynom $f \in K[x]$, $f \neq 0$, hat höchstens $\deg f$ viele Nullstellen.*

Beweis Wir beweisen die Behauptung durch Induktion über $n = \deg f$. Für $n = 0$ ist die Behauptung wahr, weil $f \in K$ und $f \neq 0$ ist. Sei $n > 0$. Wenn f keine Nullstelle hat, dann ist die Behauptung wahr. Wenn f aber eine Nullstelle a hat, dann gilt nach Korollar 2.5 $f = (x - a)q$ und $\deg q = n - 1$. Nach Induktionsvoraussetzung hat q höchstens $n - 1$ Nullstellen. Weil K keine Nullteiler enthält, hat f also höchstens n Nullstellen. □

Wir zeigen in folgendem Beispiel, dass Korollar 2.6 wirklich nur eine obere Schranke liefert, die keineswegs immer angenommen wird.

Beispiel 2.38 Das Polynom $x^2 + x \in (\mathbb{Z}/2\mathbb{Z})[x]$ hat die Nullstellen 0 und 1 in $\mathbb{Z}/2\mathbb{Z}$. Mehr Nullstellen kann es auch nach Korollar 2.6 nicht haben.

Das Polynom $x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ hat die einzige Nullstelle 1 in $\mathbb{Z}/2\mathbb{Z}$. Nach Korollar 2.6 könnte es aber 2 Nullstellen haben.

Das Polynom $x^2+x+1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ hat keine Nullstellen in $\mathbb{Z}/2\mathbb{Z}$. Nach Korollar 2.6 könnte es aber 2 Nullstellen haben.

2.20 Konstruktion endlicher Körper

In diesem Abschnitt beschreiben wir, wie man zu jeder Primzahl p und jeder natürlichen Zahl n einen endlichen Körper mit p^n Elementen konstruieren kann. Dieser Körper ist bis auf Isomorphie eindeutig bestimmt und wird mit $\mathrm{GF}(p^n)$ bezeichnet. Die Abkürzung GF steht für *galois field*. Das ist die englische Bezeichnung für endliche Körper. Aus

Theorem 2.4 wissen wir bereits, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen ist. Er wird mit $\mathrm{GF}(p)$ bezeichnet. Die Primzahl p heißt *Charakteristik* des Körpers $\mathrm{GF}(p^n)$. Der Körper $\mathrm{GF}(p)$ heißt *Primkörper*. Die Konstruktion ist mit der Konstruktion des Körpers $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p eng verwandt. Wir werden die Konstruktion nur skizzieren. Details und Beweise findet man z. B. in [52].

Sei p eine Primzahl, sei n eine natürliche Zahl und sei f ein Polynom mit Koeffizienten in $\mathbb{Z}/p\mathbb{Z}$ vom Grad n. Das Polynom muss *irreduzibel* sein, d. h. es darf nicht als Produkt $f = gh$ geschrieben werden können, wobei g und h Polynome in $(\mathbb{Z}/p\mathbb{Z})[X]$ sind, deren Grad größer als Null ist. Polynome, die nicht irreduzibel sind heißen *reduzibel*.

Beispiel 2.39 Sei $p = 2$.

Das Polynom $f(X) = X^2 + X + 1$ ist irreduzibel in $(\mathbb{Z}/2\mathbb{Z})[X]$. Wäre f reduzibel, müsste f nach Lemma 2.2 Produkt von zwei Polynomen vom Grad eins aus $(\mathbb{Z}/2\mathbb{Z})[X]$ sein. Dann hätte f also eine Nullstelle in $\mathbb{Z}/2\mathbb{Z}$. Es ist aber $f(0) \equiv f(1) \equiv 1 \bmod 2$. Also ist f irreduzibel.

Das Polynom $f(X) = X^2 + 1$ ist reduzibel in $(\mathbb{Z}/2\mathbb{Z})[X]$, denn es gilt $X^2 + 1 \equiv (X + 1)^2 \bmod 2$.

Die Elemente des endlichen Körpers, der nun konstruiert wird, sind Restklassen mod f. Die Konstruktion dieser Restklassen entspricht der Konstruktion von Restklassen in $\mathbb{Z}$. Die Restklasse des Polynoms $g \in (\mathbb{Z}/p\mathbb{Z})[X]$ besteht aus allen Polynomen h in $(\mathbb{Z}/p\mathbb{Z})[X]$, die sich von g nur durch ein Vielfaches von f unterscheiden, für die also $g - h$ durch f teilbar ist. Wir schreiben $g + f(\mathbb{Z}/p\mathbb{Z})[X]$ für diese Restklasse, denn es gilt

$$g + f(\mathbb{Z}/p\mathbb{Z})[X] = \{g + hf : h \in (\mathbb{Z}/p\mathbb{Z})[X]\}.$$

Nach Theorem 2.23 gibt es in jeder Restklasse mod f einen eindeutig bestimmten Vertreter, der entweder Null ist oder dessen Grad kleiner als der Grad von f ist. Diesen Vertreter kann man durch Division mit Rest bestimmen. Will man also feststellen, ob die Restklassen zweier Polynome gleich sind, so kann man jeweils diesen Vertreter berechnen und vergleichen. Sind sie gleich, so sind die Restklassen gleich. Sind sie verschieden, so sind die Restklassen verschieden.

Die Anzahl der verschiedenen Restklassen mod f ist p^n. Das liegt daran, dass die Restklassen aller Polynome, deren Grad kleiner n ist, paarweise verschieden sind und dass jede Restklasse mod f einen Vertreter enthält, dessen Grad kleiner als n ist.

Beispiel 2.40 Die Restklassen in $(\mathbb{Z}/2\mathbb{Z})[X]$ mod $f(X) = X^2 + X + 1$ sind $f(\mathbb{Z}/2\mathbb{Z})$, $1 + f(\mathbb{Z}/2\mathbb{Z})$, $X + f(\mathbb{Z}/2\mathbb{Z})$, $X + 1 + f(\mathbb{Z}/2\mathbb{Z})$.

Sind $g, h \in (\mathbb{Z}/p\mathbb{Z})[X]$, dann ist die Summe der Restklassen von g und h mod f definiert als die Restklasse von $g + h$. Das Produkt der Restklassen von g und h ist die Restklasse des Produkts von g und h. Mit dieser Addition und Multiplikation ist die Menge der Restklassen mod f ein kommutativer Ring mit Einselement $1 + f(\mathbb{Z}/p\mathbb{Z})[X]$.

Tab. 2.2 Addition in GF(4)

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Tab. 2.3 Multiplikation in GF(4)

$*$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

Beispiel 2.41 Sei $p=2$ und $f(X)=X^2+X+1$.

Die Restklassen mod f sind die Restklassen der Polynome 0, 1, X und $X+1$ mod f. In Tab. 2.2 und Tab. 2.3 geben wir die Additions- und Multiplikationstabelle dieser Restklassen an. Dabei bezeichnet α die Restklasse $X+f(\mathbb{Z}/2\mathbb{Z})[X]$. Man beachte, dass α eine Nullstelle von f in GF(4) ist, also $\alpha^2+\alpha+1=0$ gilt.

Weil f irreduzibel ist, ist der Restklassenring mod f sogar ein Körper. In Beispiel 2.41 sieht man, dass alle von Null verschiedenen Restklassen mod f ein multiplikatives Inverses besitzen. Das ist auch allgemein richtig. Soll die Restklasse eines Polynoms $g\in(\mathbb{Z}/p\mathbb{Z})[X]$ invertiert werden, verwendet man ein Analogon des erweiterten euklidischen Algorithmus, um ein Polynom $r\in(\mathbb{Z}/p\mathbb{Z})[X]$ zu bestimmen, das $gr+fs=1$ für ein Polynom $s\in(\mathbb{Z}/p\mathbb{Z})[X]$ erfüllt. Dann ist die Restklasse von r das Inverse der Restklasse von g. Das geht also genauso, wie Invertieren in $\mathbb{Z}/p\mathbb{Z}$. Ist f nicht irreduzibel, so kann man nicht alle von Null verschiedenen Restklassen invertieren. Man erhält dann durch die beschriebene Konstruktion einen Ring, der im Allgemeinen nicht nullteilerfrei ist.

Beispiel 2.42 Sei $p=2$ und sei $f(X)=x^8+x^4+x^3+x+1$. Dieses Polynom ist irreduzibel in $(\mathbb{Z}/2\mathbb{Z})[X]$ (siehe Übung 2.26). Sei α die Restklasse von X mod f. Wir bestimmen das Inverse von $\alpha+1$. Hierzu wenden wir den erweiterten euklidischen Algorithmus an. Es gilt

$$f(X)=(X+1)q(X)+1$$

mit

$$q(X)=X^7+X^6+X^5+X^4+X^2+X.$$

Wie in Beispiel 1.33 bekommt man folgende Tabelle

k	0	1	2	3
r_k	f	$X+1$	1	0
q_k		$q(X)$	$X+1$	
x_k	1	0	1	$X^8+X^4+X^3$
y_k	0	1	$q(X)$	$X\cdot q(X)$

Es gilt also

$$f(X) - q(X)(X+1) = 1.$$

Daher ist die Restklasse von $q(X)$, also $\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$, das Inverse von $\alpha + 1$.

Konstruiert man auf diese Weise Körper für verschiedene Polynome vom Grad n, so sind diese Körper isomorph, also nicht wirklich verschieden.

Da es für jede natürliche Zahl n ein irreduzibles Polynom in $(\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad n gibt, existiert auch der Körper $\mathrm{GF}(p^n)$ für alle p und n.

2.21 Struktur der Einheitengruppe endlicher Körper

Wir untersuchen jetzt die Einheitengruppe K^* eines endlichen Körpers K, also eines Körpers mit endlich vielen Elementen. Wir beweisen, dass diese Gruppe immer zyklisch ist. Daher ist sie für die Kryptographie besonders interessant, weil dort Gruppen mit Elementen hoher Ordnung benötigt werden. Wir kennen bereits die endlichen Körper $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p. Ihre Einheitengruppe hat die Ordnung $p-1$. Später werden wir noch andere endliche Körper kennenlernen.

Allgemein hat die Einheitengruppe K^* eines Körpers K mit q Elementen die Ordnung $q-1$, weil alle Elemente außer der Null Einheiten sind.

Theorem 2.25 *Sei K ein endlicher Körper mit q Elementen. Dann gibt es für jeden Teiler d von $q-1$ genau $\varphi(d)$ Elemente der Ordnung d in der Einheitengruppe K^*.*

Beweis Sei d ein Teiler von $q-1$. Bezeichne mit $\psi(d)$ die Anzahl der Elemente der Ordnung d in K^*.

Angenommen, $\psi(d) > 0$. Wir zeigen, dass unter dieser Voraussetzung $\psi(d) = \varphi(d)$ gilt. Später beweisen wir dann, dass tatsächlich $\psi(d) > 0$ gilt. Sei a ein Element der Ordnung d in K^*. Die Potenzen a^e, $0 \le e < d$, sind paarweise verschieden und alle Nullstellen des Polynoms $x^d - 1$. Im Körper K gibt es nach Korollar 2.6 höchstens d Nullstellen dieses Polynoms. Das Polynom besitzt also genau d Nullstellen und sie sind die Potenzen von a. Nun ist aber jedes Element von K der Ordnung d eine Nullstelle von $x^d - 1$ und daher eine Potenz von a. Aus Theorem 2.10 folgt, dass a^e genau dann die Ordnung d hat, wenn $\gcd(d, e) = 1$ ist. Also haben wir bewiesen, dass aus $\psi(d) > 0$ folgt, dass $\psi(d) = \varphi(d)$ ist.

Wir zeigen nun, dass $\psi(d) > 0$ ist. Angenommen, $\psi(d) = 0$ für einen Teiler d von $q-1$. Dann gilt

$$q - 1 = \sum_{d \mid q-1} \psi(d) < \sum_{d \mid q-1} \varphi(d).$$

Dies widerspricht Theorem 2.8. □

Beispiel 2.43 Betrachte den Körper $\mathbb{Z}/13\mathbb{Z}$. Seine Einheitengruppe hat die Ordnung 12. In dieser Gruppe gibt es ein Element der Ordnung 1, ein Element der Ordnung 2, zwei Elemente der Ordnung 3, zwei Elemente der Ordnung 4, zwei Elemente der Ordnung 6 und vier Elemente der Ordnung 12. Insbesondere ist diese Gruppe also zyklisch und hat vier Erzeuger.

Ist K ein endlicher Körper mit q Elementen, so gibt es nach Theorem 2.25 genau $\varphi(q-1)$ Elemente der Ordnung $q-1$. Daraus ergibt sich folgendes:

Korollar 2.7 *Ist K ein endlicher Körper mit q Elementen, so ist die Einheitengruppe K^* zyklisch von der Ordnung $q-1$. Sie hat genau $\varphi(q-1)$ Erzeuger.*

2.22 Struktur der primen Restklassengruppe nach einer Primzahl

Sei p eine Primzahl. In Korollar 2.7 haben wir folgendes Resultat bewiesen:

Korollar 2.8 *Die prime Restklassengruppe* mod p *ist zyklisch von der Ordnung $p-1$.*

Eine ganze Zahl a, für die die Restklasse $a + p\mathbb{Z}$ die prime Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^*$ erzeugt, heißt *Primitivwurzel* mod p.

Beispiel 2.44 Für $p = 13$ ist $p-1 = 12$. Aus Theorem 2.22 folgt, dass $\varphi(12) = 4$. Also gibt es vier Primitivwurzeln mod 13, nämlich 2, 6, 7 und 11.

Wir diskutieren die Berechnung von Primitivwurzeln modulo einer Primzahl p. Wir haben in Theorem 2.7 gesehen, dass es $\varphi(p-1)$ Primitivwurzeln mod p gibt. Nun gilt

$$\varphi(n) \geq n/(6 \ln \ln n)$$

für jede natürliche Zahl $n \geq 5$ (siehe [62]). Der Beweis dieser Ungleichung sprengt den Rahmen dieses Buches. Also ist die Anzahl der Erzeuger einer zyklischen Gruppe der Ordnung n wenigstens $\lceil n/(6 \ln \ln n) \rceil$. Wenn $n = 2 * q$ mit einer Primzahl q ist, dann ist die Anzahl der Erzeuger sogar $q-1$. Fast die Hälfte aller Gruppenelemente erzeugen also die Gruppe. Wenn man also zufällig eine natürliche Zahl g mit $1 \leq g \leq p-1$ wählt, hat man eine gute Chance, eine Primitivwurzel mod p zu finden. Das Problem ist nur, zu verifizieren, dass man tatsächlich eine solche Primitivwurzel gefunden hat. Aus Korollar 2.4 kennen wir ein effizientes Verfahren, um zu überprüfen, ob g eine Primitivwurzel mod p ist, wenn wir $p-1$ faktorisieren können. In dem besonders einfachen Fall $p-1 = 2q$ mit einer Primzahl q brauchen wir nur zu testen, ob $g^2 \equiv 1 \bmod p$ oder $g^q \equiv 1 \bmod p$ ist. Wenn diese beiden Kongruenzen nicht erfüllt sind, ist g eine Primitivwurzel mod p.

Beispiel 2.45 Sei $p = 23$. Dann ist $p - 1 = 22 = 11 * 2$. Um zu prüfen, ob eine ganze Zahl g eine Primitivwurzel modulo 23 ist, muss man verifizieren, dass $g^2 \bmod 23 \neq 1$ ist und dass $g^{11} \bmod 23 \neq 1$ ist. Hier ist eine Tabelle mit den entsprechenden Resten für die Primzahlen zwischen 2 und 17.

g	2	3	5	7	11	13	17
$g^2 \bmod 23$	4	9	2	3	6	8	13
$g^{11} \bmod 23$	1	1	-1	-1	-1	1	-1

Es zeigt sich, dass 5, 7, 11, 17 Primitivwurzeln mod 23 sind und dass 2, 3, 13 keine Primitivwurzeln mod 23 sind.

2.23 Quadratische Reste

In diesem Abschnitt sei p eine Primzahl. Wir definieren quadratische Reste.

Definition 2.20 Ein *quadratischer Rest* modulo p ist eine zu p teilerfremde ganze Zahl, für die die Kongruenz $a \equiv x^2 \bmod p$ eine Lösung $x \in \mathbb{Z}$ hat. Eine zu p teilerfremde ganze Zahl, die kein quadratischer Rest modulo p ist, heißt *quadratischer Nichtrest* modulo p.

Wir definieren auch noch das Legendre-Symbol.

Definition 2.21 Für jede ganze Zahl a ist das Legendre-Symbol $\left(\frac{a}{p}\right)$ folgendermaßen definiert:

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

Als nächstes beweisen wir das *Eulersche Kriterium* dafür, dass eine zu p teilerfremde Zahl ein quadratischer Rest modulo p ist.

Theorem 2.26 *Sei a eine zu p teilerfremde Zahl. Dann ist* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.

Beweis Sei a ein quadratischer Rest modulo p, also $a \equiv x^2 \bmod p$ für eine ganze Zahl x. Dann ist x ebenfalls teilerfremd zu p und es gilt nach Satz 2.13, dass $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \bmod p$.

Sei a ein quadratischer Nichtrest modulo p und sei g eine Primitivwurzel modulo p. Dann ist a eine ungerade Potenz von g modulo p, also $a \equiv g^{2k+1} \bmod p$ für eine natürliche Zahl k. Also gilt $a^{(p-1)/2} \equiv g^{k(p-1)} g^{(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \bmod p$. □

Das Euler-Kriterium führt auch zu einen Algorithmus, der effizient prüft, ob eine zu p teilerfremde Zahl a ein quadratischer Rest modulo p ist oder nicht. Man muss nur mit schneller Exponentiation ausrechnen, ob $a^{(p-1)/2} \equiv 1 \bmod p$ ist. Nutzt man das quadratische Reziprozitätsgesetz aus (siehe [4]), kann das Legendre-Symbol noch schneller berechnet werden.

Wir geben auch die Anzahl der quadratischen Reste modulo p an.

Theorem 2.27 *Die Anzahl der quadratischen Reste modulo p in $\mathbb{Z}_p$ ist $(p-1)/2$.*

Beweis Sei g eine Primitivwurzel modulo p. Dann sind die primen Reste modulo p die Zahlen $g^k \bmod p$, $0 \leq k \leq p-2$. Eine solche Potenz ist genau dann ein quadratischer Rest, wenn der Exponent k gerade ist. Da es im Intervall $[0, p-2]$ genau $(p-1)/2$ gerade Zahlen gibt, folgt die Behauptung. □

Beispiel 2.46 Wir betrachten die prime Restklassengruppe modulo 7. Die folgende Tabelle zeigt, dass $1, 2, 4$ die quadratischen Reste modulo 7 in $\mathbb{Z}_7$ sind. Das sind genau drei, wie von Theorem 2.27 vorhergesagt.

a	1	2	3	4	5	6
$a^{(p-1)/2} \bmod p$	1	1	-1	1	-1	-1
$a^2 \bmod 7$	1	4	2	2	4	1

2.24 Übungen

Übung 2.1 Beweisen Sie die Potenzgesetze für Halbgruppen und Gruppen.

Übung 2.2 Bestimmen Sie alle Halbgruppen, die man durch Definition einer Operation auf $\{0, 1\}$ erhält.

Übung 2.3 Zeigen Sie, dass es in einer Halbgruppe höchstens ein neutrales Element geben kann.

Übung 2.4 Welche der Halbgruppen aus Übung 2.2 sind Monoide? Welche sind Gruppen?

Übung 2.5 Zeigen Sie, dass in einem Monoid jedes Element höchstens ein Inverses haben kann.

Übung 2.6 Sei n ein positiver Teiler einer positiven Zahl m. Beweisen Sie, dass die Abbildung $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a + m\mathbb{Z} \mapsto a + n\mathbb{Z}$ ein surjektiver Ringhomomorphismus ist.

Übung 2.7 Zeigen Sie an einem Beispiel, dass die Kürzungsregel in der Halbgruppe $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ im Allgemeinen nicht gilt.

Übung 2.8 Bestimmen Sie die Einheitengruppe und die Nullteiler des Rings $\mathbb{Z}/16\mathbb{Z}$.

Übung 2.9 Zeigen Sie, dass die invertierbaren Elemente eines kommutativen Rings mit Einselement eine Gruppe bilden.

Übung 2.10 Lösen Sie $122x \equiv 1 \bmod 343$.

Übung 2.11 Beweisen Sie, dass die Kongruenz $ax \equiv b \bmod m$ genau dann lösbar ist, wenn $\gcd(a, m)$ ein Teiler von b ist. Im Falle der Lösbarkeit bestimmen Sie alle Lösungen.

Übung 2.12 Sei $d_1 d_2 \ldots d_k$ die Dezimalentwicklung einer positiven ganzen Zahl d. Beweisen Sie, dass d genau dann durch 11 teilbar ist, wenn $\sum_{i=1}^{k} (-1)^{k-i}$ durch 11 teilbar ist.

Übung 2.13 Bestimmen Sie alle invertierbaren Restklassen modulo 25 und berechnen Sie alle Inverse.

Übung 2.14 Das kleinste gemeinsame Vielfache zweier von Null verschiedener ganzer Zahlen a, b ist die kleinste natürliche Zahl k, die sowohl ein Vielfaches von a als auch ein Vielfaches von b ist. Es wird mit $\operatorname{lcm}(a, b)$ bezeichnet. Dabei steht lcm für least common multiple.

1. Beweisen Sie Existenz und Eindeutigkeit von $\operatorname{lcm}(a, b)$.
2. Wie kann $\operatorname{lcm}(a, b)$ mit dem euklidischen Algorithmus berechnet werden?

Übung 2.15 Seien X und Y endliche Mengen und $f : X \to Y$ eine Bijektion. Zeigen Sie, dass X und Y gleich viele Elemente besitzen.

Übung 2.16 Berechnen Sie die von $2 + 17\mathbb{Z}$ in $(\mathbb{Z}/17\mathbb{Z})^*$ erzeugte Untergruppe.

Übung 2.17 Berechnen Sie die Ordnung von 2 mod 1237.

Übung 2.18 Bestimmen Sie die Ordnung aller Elemente in $(\mathbb{Z}/15\mathbb{Z})^*$.

Übung 2.19 Berechnen Sie $2^{20} \bmod 7$.

Übung 2.20 Sei G eine endliche zyklische Gruppe. Zeigen Sie, dass es für jeden Teiler d von $|G|$ genau eine Untergruppe von G der Ordnung d gibt.

Übung 2.21 Sei p eine Primzahl, $p \equiv 3 \bmod 4$. Sei a eine ganze Zahl, die ein Quadrat mod p ist (d. h., die Kongruenz $a \equiv b^2 \bmod p$ hat eine Lösung). Zeigen Sie, dass $a^{(p+1)/4}$ eine Quadratwurzel von a mod p ist.

Übung 2.22 Beweisen Sie Theorem 2.17.

Übung 2.23 Konstruieren Sie ein Element der Ordnung 103 in der primen Restklassengruppe mod 1237.

Übung 2.24 Sei G eine zyklische Gruppe der Ordnung n mit Erzeuger g. Zeigen Sie, dass $\mathbb{Z}/n\mathbb{Z} \to G, e + n\mathbb{Z} \mapsto g^e$ ein Isomorphismus von Gruppen ist.

Übung 2.25 Lösen Sie die simultane Kongruenz $x \equiv 1 \bmod p$ für alle $p \in \{2, 3, 5, 7\}$.

Übung 2.26 Zeigen Sie, dass das Polynom $f(X) = x^8 + x^4 + x^3 + x + 1$ in $(\mathbb{Z}/2\mathbb{Z})[X]$ irreduzibel ist.

Übung 2.27 Bestimmen Sie für $g = 2, 3, 5, 7, 11$ jeweils eine Primzahl $p > g$ mit der Eigenschaft, dass g eine Primitivwurzel mod p ist.

Übung 2.28 Finden Sie alle primen Restklassengruppen mit vier Elementen.

http://www.springer.com/978-3-642-39774-5

Einführung in die Kryptographie
Buchmann, J.
2016, XXVI, 330 S. 13 Abb., Softcover
ISBN: 978-3-642-39774-5