Kapitel 1

Rechnen mit Restklassen

In diesem Kapitel wird an grundsätzliche Definitionen, wie die der Teilbarkeit, erinnert. Wir zeigen, dass es unendlich viele Primzahlen gibt. Außerdem zeigen wir den Kleinen Fermatschen Satz und die Existenz primitiver Wurzeln modulo p. All dies wird oft als „elementare Zahlentheorie“ bezeichnet.

1.1 Teilbarkeit

Im Zentrum des zahlentheoretischen Interesses stehen die natürlichen Zahlen

$$\mathbb{N} = \{\, 1, 2, 3, 4, \dots \}\,.$$

Natürliche Zahlen kann man stets addieren. Die Umkehroperation, die Subtraktion $n - m$, ist in $\mathbb{N}$ nur durchführbar, wenn m kleiner als n ist. Man befreit sich von dieser Einschränkung, indem man zu den ganzen Zahlen

$$\mathbb{Z} = \{\, \dots, -2, -1, 0, 1, 2, \dots \}$$

übergeht. Im Falle der Multiplikation ist das Hindernis für die Umkehrung die Teilbarkeitsrelation.

Definition 1.1.1. *Eine ganze Zahl a* **teilt** *eine ganze Zahl b (symbolisch: $a|b$), wenn eine ganze Zahl c mit $ac = b$ existiert. Man nennt dann a* **Teiler** *von b.*

Die Zahl 0 teilt offensichtlich nur die 0 (was nicht bedeutet, dass man dem Quotienten $0/0$ einen Sinn geben könnte), und jede Zahl teilt 0. Die Zahlen ± 1 teilen jede Zahl und spielen eine Sonderrolle. Man nennt sie *Einheiten*. Ist $a \neq 0$, so existiert der Quotient $c = b/a$ in $\mathbb{Z}$ genau dann, wenn $a|b$, und ist dann eindeutig bestimmt. Man befreit sich von dieser Einschränkung durch Übergang zu den rationalen Zahlen $\mathbb{Q}$. Dort ist die Division (außer durch 0) uneingeschränkt durchführbar. Die Teilbarkeitsrelation verliert durch diese Konstruktion jedoch nicht ihre Bedeutung. Wir werden zunächst einige Eigenschaften sammeln. Den Beweis des nächsten Lemmas überlassen wir dem Leser.

Lemma 1.1.2. *Für $a, b, c, m, n \in \mathbb{Z}$ gilt:*

(i) $a|b$ *und* $a|c \Longrightarrow a|(b+c)$,
(ii) $a|b \Longrightarrow a|bc$,
(iii) $a|n$ *und* $b|m \Longrightarrow ab|nm$.

Die Menge der Teiler einer von Null verschiedenen ganzen Zahl a ist nicht leer (sie enthält die 1) und endlich (wegen $d|a \Rightarrow |d| \leq |a|$). Daher ist die folgende Definition sinnvoll.

Definition 1.1.3. *Der* **größte gemeinsame Teiler** *zweier von Null verschiedener ganzer Zahlen a und b ist die größte natürliche Zahl d mit $d|a$ und $d|b$. Bezeichnung: $d = (a, b)$. Wir nennen a und b* **teilerfremd** *oder auch* **relativ prim**, *wenn $(a, b) = 1$ gilt. Außerdem setzen wir $(0, a) = (a, 0) = |a|$ für beliebiges ganzes a.*

Eine wichtige Eigenschaft des größten gemeinsamen Teilers ist seine lineare Kombinierbarkeit. Diese ist der Inhalt des folgenden Satzes.

Satz 1.1.4. *Sei $d = (a, b)$. Dann existieren ganze Zahlen x, y mit $d = ax + by$.*

Beweis. Für $a = 0$ oder $b = 0$ ist die Aussage trivial, also sei $ab \neq 0$. Wir können außerdem annehmen, dass a und b positiv sind, ansonsten ändern wir zum Schluss das Vorzeichen von x bzw. y. Des Weiteren sei o.B.d.A. $b \leq a$. Wir führen den **Euklidischen Algorithmus** aus, d.h. wir teilen sukzessive mit Rest:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < b \\ b &= r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, & r_n = 0. \end{aligned}$$

Die Folge $b > r_1 > r_2 > \cdots$ ist eine strikt fallende Folge nichtnegativer ganzer Zahlen. Daher bricht der Prozess ab, d.h. es gibt ein n mit $r_n = 0$. Nun gilt $r_{n-1} = d$. Das sieht man folgendermaßen. Von unten nach oben durch die Gleichungen gehend sehen wir, dass r_{n-1} sowohl a als auch b teilt. Also gilt $r_{n-1} \leq d$. Von oben nach unten gehend sehen wir, dass r_{n-1} durch d teilbar ist. Hieraus folgt $d = r_{n-1}$. Starten wir nun von der vorletzten Zeile $r_{n-3} = r_{n-2} q_{n-1} + d$ und setzen sukzessive ein, erhalten wir die gewünschte Darstellung $d = ax + by$. □

Hieraus folgern wir, dass der größte gemeinsame Teiler nicht nur bezüglich der Kleiner-Relation maximal ist, sondern auch im multiplikativen Sinne.

Korollar 1.1.5. $e|a$ *und* $e|b \Longrightarrow e|(a, b)$.

Beweis. Es existieren $x, y \in \mathbb{Z}$ mit $ax + by = (a, b)$. Also ist (a, b) durch e teilbar. □

Dies ist die wichtigste Eigenschaft des größten gemeinsamen Teilers. Später werden wir in Zahlbereichen arbeiten, in denen keine Kleiner-Relation definiert ist. Die in Korollar 1.1.5 formulierte Eigenschaft wird dort zur Definition des größten gemeinsamen Teilers. Man muss sich dann natürlich Rechenschaft ablegen, ob ein solcher überhaupt existiert (das ist nicht immer der Fall) und in welchem Sinne er eindeutig ist.

Wir beenden diesen Abschnitt mit zwei einfachen Korollaren aus dem eben Gesagten.

Korollar 1.1.6. *$a|bc$ und $(a,b)=1 \Longrightarrow a|c$.*

Beweis. Sei $bc = za$ und $ax+by=1$. Dann ist $c = cax+cby = a(cx+zy)$. □

Korollar 1.1.7. *$a|m$, $b|m$ und $(a,b)=1 \Longrightarrow ab|m$.*

Beweis. Wähle x, y mit $ax + by = 1$. Dann ist $m = max + mby$. Nun gilt $ab|max$ und $ab|mby$, also $ab|m$. □

Aufgabe 1. Man zeige: $(2,3,7)$ ist das einzige Tripel natürlicher Zahlen ≥ 2 mit der Eigenschaft „das Produkt zweier $+1$ ist durch die dritte teilbar“.

Aufgabe 2. Für eine natürliche Zahl n bezeichnet man das Produkt $n \cdot (n-1) \cdots 1$ mit $n!$ (sprich: „n Fakultät“). Für $m, n \in \mathbb{N}$ zeige man $(m! \cdot n!) \,|\, (m+n)!$.

Aufgabe 3. Man zeige, dass für eine natürliche Zahl n die Zahlen $n(n+1)$ und $n(n+2)$ niemals Quadratzahlen sind.

Aufgabe 4. Man zeige, dass zu jeder natürlichen Zahl n eine natürliche Zahl m mit

$$(\sqrt{2}-1)^n = \sqrt{m+1} - \sqrt{m}$$

existiert.

Aufgabe 5. Für eine reelle Zahl x bezeichne $[x]$ die größte ganze Zahl kleiner gleich x. Man zeige für reelle Zahlen x, y die Ungleichung $[x]+[y] \leq [x+y]$.

1.2 Primzahlen

Beginnend mit der Zahl 1 lässt sich jede natürliche Zahl durch sukzessives Addieren der 1 gewinnen. Also ist 1 der Grundbaustein, aus dem sich durch Addition alle natürlichen Zahlen produzieren lassen. Bezüglich der Multiplikation ergibt sich ein anderes Bild. Hier sind die Primzahlen die Grundbausteine.

Definition 1.2.1. *Eine ganze Zahl $p > 1$ heißt* **Primzahl**, *wenn 1 und p die einzigen positiven Teiler von p sind.*

Man beachte, dass 1 *keine* Primzahl ist. Das sieht zunächst wie eine willkürliche Festlegung aus, hat aber einen tieferen Sinn: Die 1 teilt jede Zahl und ist für die Teilbarkeitslehre uninteressant. Dass man die negativen Zahlen -2, -3, -5, -7, ... nicht als Primzahlen bezeichnet, ist eine althergebrachte Konvention, die man auch anders festlegen könnte. Denn auch für diese Zahlen ist die folgende Aussage richtig.

Lemma 1.2.2. *Ist p eine Primzahl und gilt $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.*

Beweis. Angenommen $p \nmid a$. Dann ist $(a, p) = 1$ und nach Korollar 1.1.6 ist b durch p teilbar. □

Man kann sich leicht überlegen, dass eine natürliche Zahl $p > 1$ genau dann Primzahl ist, wenn die Aussage von Lemma 1.2.2 für p richtig ist. In allgemeineren Zahlbereichen wird diese Aussage zur definierenden Eigenschaft für *Primelemente*.

Den nächsten Satz kennt jeder aus der Schulzeit, hat aber typischerweise nie einen Beweis dafür gesehen.

Satz 1.2.3. *Jede natürliche Zahl n ist in, bis auf die Reihenfolge, eindeutiger Weise das Produkt von Primzahlen.*

Beweis. 1. Existenz der Zerlegung per Induktion: $n = 1$ ist das (leere) Produkt von 0 Primzahlen. Sei $n > 1$ und die Aussage sei für alle Zahlen m, $1 \leq m \leq n-1$ richtig. Ist n eine Primzahl, so sind wir fertig. Ansonsten lässt sich n in der Form $n = m_1 m_2$ mit $1 \leq m_1, m_2 \leq n-1$ schreiben. Da sich m_1 und m_2 als Produkt von Primzahlen schreiben lassen, ist dies auch für n der Fall.
2. Eindeutigkeit der Zerlegung: Für $n = 1$ ist dies klar und wir nutzen wieder Induktion. Sei $n > 1$ und

$$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_l.$$

Nach Lemma 1.2.2 teilt p_1 eines der q_i, $i = 1, \ldots, l$. Nach eventueller Umnummerierung können wir $p_1 | q_1$ annehmen. Weil q_1 eine Primzahl ist, folgt $p_1 = q_1$. Dann teilen wir beide Seiten durch p_1 und wenden die Induktionsvoraussetzung an. □

Typischerweise fasst man mehrfach vorkommende Primzahlen zusammen, so dass jede natürliche Zahl n eine bis auf Reihenfolge eindeutige Zerlegung der Form

$$n = p_1^{e_1} \cdots p_k^{e_k}, \quad e_i \geq 1,\ i = 1, \ldots, k\,,$$

mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_k$ hat.

Korollar 1.2.4. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, es gäbe nur endlich viele und P sei ihr Produkt. Dann wäre $P+1$ größer als 1 und durch keine Primzahl teilbar. Dies widerspräche der Aussage von Satz 1.2.3. Daher gibt es unendlich viele Primzahlen. □

Es ist wohlbekannt, dass die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

divergiert, d.h. die Partialsummen $\sum_{n=1}^{N} \frac{1}{n}$ übersteigen für hinreichend großes N jede gegebene Schranke. Das nächste Theorem sagt uns, dass es „sehr viele“ Primzahlen gibt, d.h. wenn man die Nichtprimzahlen aus dieser Reihe entfernt, divergiert sie immer noch. Der bekannten (und erstaunlichen) Formel

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

entnehmen wir, dass es in einem wohlbestimmten Sinne mehr Prim- als Quadratzahlen gibt.

Theorem 1.2.5 (Euler). *Die Reihe*

$$\sum_{p \text{ Primz.}} \frac{1}{p}$$

divergiert.

Beweis. Zunächst setzen wir als bekannt voraus, dass die Folge $(1+\frac{1}{n})^n$ von unten gegen die Eulersche Zahl e konvergiert. Also gilt $(1+\frac{1}{p-1})^{p-1} < e$ und somit $\log(1+\frac{1}{p-1}) < \frac{1}{p-1} = \frac{1}{p} + \frac{1}{p(p-1)}$. Unter Beachtung von $\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p-1}$ erhalten wir somit für jedes N

$$\log \prod_{p \le N} \frac{1}{1-\frac{1}{p}} = \sum_{p \le N} \log\big(1 + \frac{1}{p-1}\big) < \sum_{p \le N} \frac{1}{p} + \sum_{p \le N} \frac{1}{p(p-1)}.$$

Erinnern wir uns an die geometrische Reihe

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots$$

und bezeichnen mit $p_+(n)$ den größten Primteiler einer natürlichen Zahl n (Vereinbarung: $p_+(1) = 0$, $p_+(0) = \infty$), so erhalten wir andererseits durch Ausmultiplizieren

$$\prod_{p \le N} \frac{1}{1-\frac{1}{p}} = \prod_{p \le N} (1 + \frac{1}{p} + \frac{1}{p^2} + \cdots) = \sum_{p_+(n) \le N} \frac{1}{n} > \sum_{n \le N} \frac{1}{n}.$$

Zusammen ergibt dies

$$\log \sum_{n \le N} \frac{1}{n} < \sum_{p \le N} \frac{1}{p} + \sum_{p \le N} \frac{1}{p(p-1)}.$$

Würde nun $\sum_p \frac{1}{p}$ konvergieren, so auch $\sum_p \frac{1}{p(p-1)}$, d.h. die rechte Seite der Ungleichung bliebe bei $N \to \infty$ beschränkt. Die linke Seite wird aber beliebig groß, weil die Reihe $\sum \frac{1}{n}$ divergiert. Dieser Widerspruch zeigt, dass auch die Reihe $\sum_p \frac{1}{p}$ divergiert. □

Andererseits haben wir den

Satz 1.2.6. *In der Folge der natürlichen Zahlen gibt es beliebig große primzahlfreie Teilabschnitte.*

Beweis. Für jedes $n \geq 1$ ist unter den n aufeinanderfolgenden Zahlen

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$$

keine Primzahl, denn die erste Zahl ist durch 2 teilbar, die zweite durch 3, usw. □

Bemerkung: Die Anzahl $\pi(N)$ der Primzahlen kleiner gleich N verhält sich nach dem *Primzahlsatz* (siehe [FB], Kap.VII, Thm. 4.5) asymptotisch wie $\frac{N}{\log(N)}$, d.h.

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

Unter Annahme der *Riemannschen Vermutung* kann eine noch feinere Aussage getroffen werden.

Aufgabe 1. Sei p eine Primzahl und n eine natürliche Zahl. Sei p^k, $k \geq 0$, die höchste p-Potenz, die in $n!$ aufgeht. Man zeige

$$k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \quad .$$

Aufgabe 2. Man zeige

$$(m,n) = 1 \Longrightarrow \frac{(m+n-1)!}{m!\cdot n!} \in \mathbb{Z}.$$

Man gebe ein Gegenbeispiel im Fall $(m,n) \neq 1$ an.

Eine Funktion $f : \mathbb{N} \longrightarrow \mathbb{C}$ heißt zahlentheoretische Funktion. Man nennt f multiplikativ, wenn für $(m,n) = 1$ stets $f(mn) = f(m)f(n)$ gilt.

Aufgabe 3. Man zeige, dass die Funktion

$$\tau(n) = \text{Anzahl der positiven Teiler von } n$$

multiplikativ ist.

Aufgabe 4. Man zeige, dass die Funktion

$$\sigma(n) = \text{Summe der positiven Teiler von } n$$

multiplikativ ist.

Aufgabe 5. Man zeige, dass die Möbius-Funktion

$$\mu(n) = \begin{cases} 1, & n = 1, \\ 0, & n \text{ ist durch eine Quadratzahl} > 1 \text{ teilbar}, \\ (-1)^k, & n \text{ ist Produkt von } k \text{ paarweise verschiedenen Primzahlen}, \end{cases}$$

multiplikativ ist.

Aufgabe 6. Man zeige, dass für eine natürliche Zahl n die Zahl $n(n+1)(n+2)$ niemals eine Quadratzahl ist.

Aufgabe 7. Es seien $a, n \geq 2$ natürliche Zahlen. Man zeige: Ist $a^n - 1$ eine Primzahl, so gilt $a = 2$ und n ist eine Primzahl.

1.3 Kongruenzen

In diesem Abschnitt wird das Rechnen mit Restklassen modulo einer natürlichen Zahl eingeführt. Im „wirklichen“ Leben machen wir das oft intuitiv, so betrachten wir Wochentage modulo 7, Monate modulo 12, Uhrzeiten modulo 12 oder 24, usw.

Sei $m > 1$ eine fixierte natürliche Zahl.

Definition 1.3.1. *Zwei ganze Zahlen a und b heißen* **kongruent modulo m** *(symbolisch: $a \equiv b \bmod m$), wenn $m|(a-b)$.*

Bei gegebenem m wollen wir ganze Zahlen, die kongruent modulo m sind, als gleich ansehen. Der formale Weg, dies zu tun, ist der Übergang zu Äquivalenzklassen bezüglich einer Äquivalenzrelation. Wir erinnern an die relevanten Definitionen. Eine **Relation** R auf einer Menge M ist eine Teilmenge $R \subset M \times M$ der Menge der geordneten Paare (x, x') von Elementen aus M. Man schreibt $x \sim x'$ genau dann, wenn $(x, x') \in R$, und bezeichnet die Relation suggestiv auch mit $\sim$.

Eine Relation $\sim$ heißt **Äquivalenzrelation**, wenn die folgenden drei Bedingungen erfüllt sind:

Reflexivität: Es gilt $x \sim x$ für alle $x \in M$.

Symmetrie: Es gilt $x \sim x'$ genau dann, wenn $x' \sim x$.

Transitivität: Aus $x \sim x'$ und $x' \sim x''$ folgt $x \sim x''$.

Sei auf M die Äquivalenzrelation $\sim$ gegeben. Für jedes $x \in M$ heißt die Teilmenge

$$\{x' \in M \mid x \sim x'\} \subset M$$

die **Äquivalenzklasse** von x bzgl. $\sim$. Insbesondere ist das Element x selbst in seiner Äquivalenzklasse enthalten, und man sagt, x sei ein **Repräsentant** oder auch **Vertreter** seiner Äquivalenzklasse. Man sieht leicht ein, dass zwei Äquivalenzklassen entweder disjunkt oder gleich sind. Daher zerfällt die Menge M in die disjunkte Vereinigung der Äquivalenzklassen. Will man nun Elemente aus M, die die $\sim$-Relation miteinander eingehen, als gleich betrachten,

so geht man von M zur Menge der Äquivalenzklassen bzgl. $\sim$ über. Das machen wir nun mit der Menge $\mathbb{Z}$ der ganzen Zahlen und der Relation ‚kongruent modulo m'.

Lemma 1.3.2. *Die Relation $a \sim b \iff a \equiv b \bmod m$ ist eine Äquivalenzrelation auf $\mathbb{Z}$.*

Beweis. Wir haben die folgenden Eigenschaften nachzuweisen:

Reflexivität: $a \equiv a \bmod m$ für jedes $a \in \mathbb{Z}$.
Symmetrie: $a \equiv b \bmod m \Longrightarrow b \equiv a \bmod m$.
Transitivität: ($a \equiv b \bmod m$ und $b \equiv c \bmod m$) $\Longrightarrow a \equiv c \bmod m$.

Das ist ganz einfach und sei dem Leser überlassen. □

Definition 1.3.3. *Die Äquivalenzklassen bezüglich der Relation $a \sim b \iff a \equiv b \bmod m$ heißen* **Restklassen** *modulo m. Bei fixiertem m wird die Restklasse einer ganzen Zahl a mit $\bar{a}$ bezeichnet. Die Menge aller Restklassen modulo m wird mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet.*

Die Restklasse $\bar{a}$ modulo m einer ganzen Zahl a besteht genau aus der Menge

$$a + m\mathbb{Z} = \{a + mb \mid b \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Es gibt genau m Restklassen modulo m. Diese werden durch die ganzen Zahlen $0, 1, \ldots, m-1$ vertreten. Man kann sich natürlich auch andere Vertreter wählen.

Wir wollen nun mit Restklassen modulo m *rechnen*. Dass dies möglich ist, zeigt das nächste Lemma, dessen elementarer Beweis dem Leser überlassen sei.

Lemma 1.3.4. *Gilt $a \equiv b \bmod m$ und $c \equiv d \bmod m$, so gelten die Kongruenzen $a + c \equiv b + d \bmod m$, $a - c \equiv b - d \bmod m$ und $ac \equiv bd \bmod m$.*

Daher kann man Restklassen modulo m addieren, subtrahieren und multiplizieren, indem man beliebige Vertreter addiert, subtrahiert bzw. multipliziert und dann wieder zur Restklasse übergeht. Eine Division von Restklassen ist im Allgemeinen nicht möglich.

Bemerkung: Die Menge $\mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m wird mit diesen Operationen ein kommutativer Ring mit 1 (siehe Abschnitt 4.1).

Kongruenzen modulo dem Produkt paarweise teilerfremder Zahlen kann man simultan lösen. Dies ist der Inhalt des Chinesischen Restklassensatzes:

Satz 1.3.5 (Chinesischer Restklassensatz). *Seien $r_1, \ldots, r_k \in \mathbb{Z}$ und seien $m_1, \ldots, m_k$ paarweise teilerfremde natürliche Zahlen größer als 1. Dann hat das System von Kongruenzen*

$$\begin{aligned} x &\equiv r_1 \mod m_1 \\ x &\equiv r_2 \mod m_2 \\ &\vdots \qquad\quad \vdots \\ x &\equiv r_k \mod m_k \end{aligned}$$

eine Lösung $x \in \mathbb{Z}$ und x ist eindeutig bestimmt modulo $m_1 m_2 \cdots m_k$.

Beweis. Der Fall $k = 1$ ist offensichtlich. Betrachten wir zunächst den Fall $k = 2$. Wegen $(m_1, m_2) = 1$ existieren $a, b \in \mathbb{Z}$ mit $am_1 + bm_2 = 1$. Für die Zahl

$$x = r_2 a m_1 + r_1 b m_2$$

gilt nun $x \equiv r_1 b m_2 \bmod m_1$. Aber $bm_2 = 1 - am_1 \equiv 1 \bmod m_1$, also $x \equiv r_1 \bmod m_1$. Analog erhält man $x \equiv r_2 a m_1 \equiv r_2(1 - bm_2) \equiv r_2 \bmod m_2$. Dies zeigt die Existenz von x im Fall $k = 2$.

Wir fahren per Induktion über k fort. Ist $k > 2$ und der Satz für $2, \ldots, k-1$ schon bewiesen, so wenden wir die Induktionsvoraussetzung für $k - 1$ an und erhalten ein $y \in \mathbb{Z}$ mit

$$\begin{aligned} y &\equiv\ r_1 \mod m_1 \\ y &\equiv\ r_2 \mod m_2 \\ &\vdots \\ y &\equiv r_{k-1} \mod m_{k-1}. \end{aligned}$$

Dann wenden wir die Induktionsvoraussetzung für $k = 2$ an und erhalten ein $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv\ y \mod m_1 \cdots m_{k-1} \\ x &\equiv r_k \mod m_k. \end{aligned}$$

Dieses x erfüllt die gewünschte Bedingung. Es bleibt die Eindeutigkeit modulo $m_1 \cdots m_k$ zu zeigen. Erfüllen x_1 und x_2 beide die gegebenen Kongruenzen, so gilt

$$x_1 \equiv x_2 \mod m_i \quad \text{für } i = 1, \ldots, k.$$

Daher gilt $m_i | (x_1 - x_2)$ für $i = 1, \ldots, k$. Da die m_i paarweise teilerfremd sind, ergibt eine induktive Anwendung von Korollar 1.1.7 die Teilbarkeitsrelation $m_1 \cdots m_k \,|\, (x_1 - x_2)$, d.h. $x_1 \equiv x_2 \bmod m_1 \cdots m_k$. □

Bemerkung: Eine äquivalente Formulierung des Chinesischen Restklassensatzes ist die folgende: Für paarweise teilerfremde $m_1, \ldots, m_k$ ist die natürliche Abbildung

$$\begin{aligned} \varphi\colon\ \mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z} &\longrightarrow (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z}) \\ a \bmod m_1 \cdots m_k &\longmapsto (a \bmod m_1, \ldots, a \bmod m_k) \end{aligned}$$

bijektiv. Sie ist außerdem mit Addition und Multiplikation verträglich, d.h. ein Ringisomorphismus (siehe Abschnitt 4.1).

Definition 1.3.6. *Die Menge $(\mathbb{Z}/m\mathbb{Z})^\times$ der* **primen Restklassen** *modulo m ist die Teilmenge der Restklassen in $\mathbb{Z}/m\mathbb{Z}$, die bezüglich Multiplikation ein Inverses haben. D.h. für eine Klasse $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ gilt genau dann $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$, wenn eine Klasse $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$ mit $\bar{a}\bar{b} = \bar{1}$ existiert.*

Die inverse Klasse einer primen Restklasse $\bar{a}$ ist eine eindeutig bestimmte prime Restklasse. Dies ist ein Standardargument: Sind $\bar{b}_1, \bar{b}_2$ zwei Inverse zu $\bar{a}$, so gilt $\bar{b}_1 = \bar{b}_1(\bar{a}\bar{b}_2) = (\bar{b}_1\bar{a})\bar{b}_2 = \bar{b}_2$. Üblicherweise bezeichnet man das Inverse zu $\bar{a}$ mit $\bar{a}^{-1}$.

Lemma 1.3.7. *Die Menge $(\mathbb{Z}/m\mathbb{Z})^\times$ der primen Restklassen modulo m ist unter Multiplikation abgeschlossen.*

Beweis. Es seien $\bar{a}, \bar{b}$ prime Restklassen und $\bar{c}, \bar{d}$ Restklassen mit $\bar{a}\bar{c} = \bar{1} = \bar{b}\bar{d}$. Dann gilt $(\bar{a}\bar{b})(\bar{c}\bar{d}) = \bar{1}$, d.h. $\bar{a}\bar{b}$ ist auch eine prime Restklasse. □

Bemerkung: Mit der Multiplikation als Operation wird $(\mathbb{Z}/m\mathbb{Z})^\times$ zu einer abelschen Gruppe (siehe Abschnitt 4.1).

Korollar 1.3.8. *Ist $ab \equiv 0 \bmod m$, so ist $\bar{a}$ oder $\bar{b}$ eine nicht-prime Restklasse.*

Beweis. Ansonsten wäre $\bar{0} = \bar{a}\bar{b}$ auch eine prime Restklasse, was niemals der Fall ist. □

Nun fragt man sich, wann Gleichungen Lösungen modulo m haben. Dieses Problem wird uns im weiteren Verlauf noch oft beschäftigen. Den einfachsten Fall einer linearen Gleichung in einer Unbestimmten können wir sofort lösen.

Satz 1.3.9. *Es seien $a, b \in \mathbb{Z}$ gegeben. Die Kongruenz*

$$ax \equiv b \mod m$$

ist genau dann in $\mathbb{Z}$ lösbar, wenn $(a, m) \mid b$ gilt.

Beweis. Sei $ax \equiv b \bmod m$ mit $x \in \mathbb{Z}$. Dann gibt es ein $y \in \mathbb{Z}$ mit $ax = b + ym$. Also teilt (a, m) die Zahl $b = ax - ym$. Gelte nun umgekehrt $(a, m) | b$. Nach Satz 1.1.4 finden wir ganze Zahlen c, d mit $ac + md = (a, m)$. Dann gilt

$$ac\frac{b}{(a,m)} + md\frac{b}{(a,m)} = b$$

und folglich ist

$$x = c\frac{b}{(a,m)}$$

eine Lösung der Kongruenz. □

Korollar 1.3.10. *Die Restklasse modulo m einer ganzen Zahl a ist genau dann prim, wenn a teilerfremd zu m ist, d.h. $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \iff (a, m) = 1$.*

Beweis. Offenbar ist $\bar{a}$ genau dann prime Restklasse, wenn die Kongruenz $ax \equiv 1 \bmod m$ eine ganzzahlige Lösung hat. Nach Satz 1.3.9 ist dies äquivalent zu $(a, m)|1$, d.h. zu $(a, m) = 1$. □

Ist $m = p$ eine Primzahl, so ist $(a, p) = 1$ äquivalent zu $p \nmid a$ und wir erhalten das

Korollar 1.3.11. *Ist p eine Primzahl, so gibt es genau $p-1$ prime Restklassen modulo p und genau eine (die $\bar{0}$) nicht-prime Restklasse.*

Eine ganze Zahl $a \neq 0$ definiert eine prime Restklasse modulo fast aller Primzahlen.

Korollar 1.3.12. *Ist $m = p$ eine Primzahl, so folgt aus $\bar{a}\bar{b} = \bar{0}$, dass $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$ ist.*

Dies ist eine direkte Konsequenz aus Korollar 1.3.8. Man beachte, dass die Primzahlvoraussetzung notwendig ist, z.B. gilt modulo 15 die Gleichung $\bar{3} \cdot \bar{5} = \bar{0}$.

Definition 1.3.13. *Für $m > 1$ sei $\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times$ die Anzahl der primen Restklassen modulo m. Man setzt $\varphi(1) = 1$. Die Funktion $n \mapsto \varphi(n)$ heißt* **Eulersche φ-Funktion**.

Satz 1.3.14. *Die Eulersche φ-Funktion ist eine* **multiplikative zahlentheoretische Funktion**, *d.h. für $n, m \in \mathbb{N}$ mit $(n, m) = 1$ gilt*

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

Beweis. Nach dem Chinesischen Restklassensatz ist eine Restklasse modulo nm durch ihre Reste modulo n und modulo m eindeutig gegeben und umgekehrt. Ist nun a eine ganze Zahl, so erhalten wir nach Korollar 1.3.10 die Äquivalenzen $\bar{a} \in (\mathbb{Z}/nm\mathbb{Z})^\times \Leftrightarrow (a, nm) = 1 \Leftrightarrow (a, n) = 1$ und $(a, m) = 1 \Leftrightarrow \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$. □

Wegen ihrer Multiplikativität müssen wir, um die Eulersche φ-Funktion zu berechnen, nur noch ihre Werte auf Primzahlpotenzen bestimmen.

Lemma 1.3.15. *Sei p eine Primzahl und e eine natürliche Zahl. Dann gilt*

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

Beweis. Die Restklassen modulo p^e werden durch die p^e natürlichen Zahlen $1, \ldots, p^e$ repräsentiert. Nach Korollar 1.3.10 werden die primen Restklassen genau durch die nicht durch p teilbaren Zahlen unter diesen repräsentiert. Unter den Zahlen $1, \ldots, p^e$ gibt es genau p^{e-1} durch p teilbare. Daher gilt $\varphi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$. □

Satz 1.3.16. *Ist $n = p_1^{e_1} \cdots p_k^{e_k}$, mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_k$ und natürlichen Zahlen $e_1, \ldots, e_k$, so gilt*

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}.$$

Wir haben nun die Eulersche φ-Funktion berechnet. Allerdings ist diese Berechnung rein theoretischer Natur. Beim praktischen Rechnen scheitert man daran, eine gegebene große natürliche Zahl in ihre Primfaktoren zu zerlegen. Die Schwierigkeit, diese Zerlegung zu finden, hat aber auch ihr Gutes: Ein weitverbreitetes kryptographisches Verfahren (RSA) basiert darauf. Bemerkenswerterweise ist es hier die Unfähigkeit, ein Problem zu lösen, die zur praktischen Anwendung führt.

Wir beenden diesen Abschnitt mit der folgenden Aussage.

Satz 1.3.17. *Für jede natürliche Zahl m gilt die Gleichung*

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

wobei sich die Summation über die positiven Teiler d von m erstreckt.

Beweis. Wir führen den Beweis per Induktion über die Anzahl der verschiedenen Primteiler von m. Für $m = 1$ ist die Aussage ist trivial. Sei nun $m = np^e$, $(n, p) = 1$ und für n sei alles schon bewiesen. Jeder Teiler von np^e hat eine eindeutige Darstellung der Form dp^i mit $d|n$ und $0 \leq i \leq e$. Daher erhalten wir

$$\begin{aligned}
\textstyle\sum_{d|np^e} \varphi(d) &= \textstyle\sum_{d|n} \varphi(d) + \sum_{d|n} \varphi(dp) + \cdots + \sum_{d|n} \varphi(dp^e) \\
&= n + n\varphi(p) + \cdots n\varphi(p^e) \\
&= n(1 + \varphi(p) + \cdots + \varphi(p^e)) \\
&= n(1 + (p-1)p^0 + \cdots + (p-1)(p^{e-1})) \\
&= np^e = m.
\end{aligned}$$

□

Aufgabe 1. Die Folge (a_n) ganzer Zahlen sei rekursiv durch die Regel

$$a_1 = 2, \quad a_{n+1} = a_n^2 - a_n + 3$$

gegeben. Man zeige, dass keines der Folgenglieder durch 19 teilbar ist.

Aufgabe 2. (Bruchrechnung modulo m) Für $a \in \mathbb{Z}/m\mathbb{Z}$ und $b \in (\mathbb{Z}/m\mathbb{Z})^\times$ bezeichne $\frac{a}{b}$ die eindeutig bestimmte Restklasse c modulo m mit $bc = a$. Unter der Voraussetzung, dass alle Nenner in $(\mathbb{Z}/m\mathbb{Z})^\times$ sind, verifiziere man die folgenden Rechenregeln:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

1.4 Der Kleine Fermatsche Satz

Der folgende Satz bietet ein (vom numerischen Standpunkt unbrauchbares) Kriterium, um zu entscheiden, ob eine gegebene natürliche Zahl Primzahl ist.

Satz 1.4.1 (Satz von Wilson). *Eine natürliche Zahl p ist genau dann eine Primzahl, wenn*

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

Beweis. Sei n keine Primzahl und sei $n = p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung. Ist $k \geq 2$, so sind die Zahlen $p_i^{e_i}$ paarweise verschieden und kleiner als n. Also ist $(n-1)!$ durch n teilbar. Ist $k = 1, e_1 \geq 2$, so ist $p_1 < n$ und also $(n-1)!$ durch p_1 teilbar. Also ist $(n-1)!$ keine prime Restklasse modulo n. Dies zeigt die Notwendigkeit. Sei nun p eine Primzahl. Dann werden die primen Restklassen modulo p durch die natürlichen Zahlen $1, 2, \ldots, p-1$ repräsentiert. Es gibt zu jeder primen Restklasse $\bar{a}$ eine eindeutig bestimmte inverse Restklasse $\bar{a}^{-1}$, die selbst wieder prim ist. Es gilt $\bar{a} = \bar{b} \Leftrightarrow \bar{a}^{-1} = \bar{b}^{-1}$. Außerdem ist für $\bar{a} \neq \pm\bar{1}$ auch $\bar{a}^{-1} \neq \bar{a}$, weil aus $\bar{a}^{-1} = \bar{a}$ sofort $\bar{a}^2 = \bar{1}$ und also $p|(a^2-1) = (a+1)(a-1)$ folgt. Also heben sich im Produkt

$$\prod_{\bar{r} \in (\mathbb{Z}/p\mathbb{Z})^\times} \bar{r}$$

alle Faktoren bis auf $\pm\bar{1}$ auf, und wir erhalten $(p-1)! \equiv -1 \bmod p$. □

Erhebt man eine prime Restklasse modulo m in die $\varphi(m)$-te Potenz, so erhält man $\bar{1}$. Dies ist der Inhalt des folgenden klassischen Satzes.

Satz 1.4.2 (Kleiner Fermatscher Satz). *Für $(a, m) = 1$ gilt*

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

Zum Beweis benötigen wir das folgende

Lemma 1.4.3. *Ist $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$, so induziert die $\bar{a}$-Multiplikation $\bar{b} \mapsto \bar{a}\bar{b}$ eine bijektive Abbildung*

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\bar{a}\cdot} (\mathbb{Z}/m\mathbb{Z})^\times.$$

Beweis. Injektivität: $\bar{a}\bar{b}_1 = \bar{a}\bar{b}_2 \Rightarrow \bar{b}_1 = \bar{a}^{-1}\bar{a}\bar{b}_1 = \bar{a}^{-1}\bar{a}\bar{b}_2 = \bar{b}_2$.
Surjektivität: $\bar{b} = \bar{a}(\bar{a}^{-1}\bar{b})$. □

Beweis von Satz 1.4.2. Nach Lemma 1.4.3 erhalten wir

$$\prod_{\bar{r} \in (\mathbb{Z}/m\mathbb{Z})^\times} \bar{r} = \prod_{\bar{r} \in (\mathbb{Z}/m\mathbb{Z})^\times} (\bar{a}\bar{r}) = \bar{a}^{\varphi(m)} \cdot \prod_{\bar{r} \in (\mathbb{Z}/m\mathbb{Z})^\times} \bar{r} \quad .$$

Multiplizieren wir beide Seiten mit dem Inversen der primen Restklasse $\prod_{\bar{r} \in (\mathbb{Z}/m\mathbb{Z})^\times} \bar{r}$, erhalten wir

$$\bar{a}^{\varphi(m)} = \bar{1}.$$

Gilt nun $(a, m) = 1$ für ein $a \in \mathbb{Z}$, so liegt nach Korollar 1.3.10 die Restklasse $\bar{a}$ von a modulo m in $(\mathbb{Z}/m\mathbb{Z})^\times$. Aus $\bar{a}^{\varphi(m)} = \bar{1}$ folgt $a^{\varphi(m)} \equiv 1 \bmod m$. □

Korollar 1.4.4. *Ist p eine Primzahl, so gilt für jedes $a \in \mathbb{Z}$*

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

Beweis. Ist a nicht durch p teilbar, so gilt $a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p$. Multiplizieren wir diese Kongruenz mit a, erhalten wir das Gewünschte. Ist a durch p teilbar, so gilt $a \equiv 0 \equiv a^p \mod p$. □

Aufgabe: Sei p eine Primzahl. Man zeige die Kongruenz

$$(a+b)^p \equiv a^p + b^p \mod p$$

und nutze diese, um für $m = p$ einen alternativen Beweis des Kleinen Fermatschen Satzes mit Hilfe von vollständiger Induktion nach a zu geben.

1.5 Primzahlen mit vorgegebener Restklasse I

Wir haben gelernt, dass es unendlich viele Primzahlen gibt. Für $m > 2$ ist es interessant zu fragen, ob prime Restklassen modulo m durch unendlich viele Primzahlen repräsentiert werden. Wir werden diese Frage im Verlauf des Buches immer wieder aufgreifen und entsprechend dem jeweiligen Kenntnisstand unser Wissen erweitern. Im Moment haben wir noch nichts Tiefliegendes zur Verfügung, können aber in wenigen Fällen den Beweis dafür, dass unendlich viele Primzahlen existieren, geeignet modifizieren, um genauere Aussagen zu erhalten.

Satz 1.5.1. *Es gibt unendlich viele Primzahlen kongruent -1 modulo 3.*

Beweis. Wir nehmen an, dass es nur endlich viele Primzahlen kongruent -1 modulo 3 gibt und führen diese Annahme zum Widerspruch. Sei P das Produkt dieser endlich vielen Primzahlen. Dann gilt $3P - 1 \equiv -1 \mod 3$. Andererseits ist $3P - 1$ weder durch 3 noch durch eine Primzahl kongruent -1 modulo 3 teilbar, hat also ausschließlich Primteiler kongruent 1 modulo 3 und wäre daher selbst kongruent 1 modulo 3. Dieser Widerspruch widerlegt die Annahme. □

Satz 1.5.2. *Es gibt unendlich viele Primzahlen kongruent -1 modulo 4.*

Beweis. Wir nehmen an, es gäbe nur endlich viele solche Primzahlen. Sei P ihr Produkt. Dann gilt $4P - 1 \equiv -1 \mod 4$. Andererseits ist $4P - 1$ ungerade und durch keine Primzahl kongruent -1 modulo 4 teilbar. Also sind alle Primteiler von $4P - 1$ kongruent 1 modulo 4, und folglich $4P - 1 \equiv 1 \mod 4$. Dieser Widerspruch widerlegt die Annahme. □

Aufgabe: Man zeige, dass es unendlich viele Primzahlen $p \equiv \pm 3 \mod 8$ gibt.

1.6 Polynomkongruenzen

Nachdem wir Restklassen ganzer Zahlen betrachtet haben, betrachten wir nun Restklassen von Polynomen. Wir betrachten Polynome in $\mathbb{Z}[X]$, d.h. Ausdrücke der Form

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

mit ganzen Zahlen $a_0, a_1, \ldots, a_n$, die man die **Koeffizienten** von f nennt. Die ganze Zahl $grad(f) := \max(i \mid a_i \neq 0)$ heißt der **Grad** von f. Dem Nullpolynom wird der Grad $-\infty$ zugeordnet. Polynome werden entsprechend den Regeln

$$\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i$$
$$\sum_i a_i X^i \cdot \sum_i b_i X^i = \sum_i \sum_{j+k=i} (a_j \cdot b_k) X^i$$

addiert und multipliziert. Setzt man für die Variable X eine Zahl a ein, erhält man eine Zahl $f(a)$, den **Wert** von f in a. Wie zuvor sei $m > 1$ eine fixierte natürliche Zahl.

Definition 1.6.1. *Zwei Polynome $f, g \in \mathbb{Z}[X]$ heißen* **kongruent modulo m** *(symbolisch: $f \equiv g \bmod m$), falls alle Koeffizienten des Polynoms $f - g$ durch m teilbar sind.*

Den Beweis des folgenden Lemmas überlassen wir dem Leser.

Lemma 1.6.2. *Gilt $f_1 \equiv f_2 \bmod m$ und $g_1 \equiv g_2 \bmod m$, so gilt*

$$\begin{aligned} f_1 + g_1 &\equiv f_2 + g_2 \mod m, \\ f_1 - g_1 &\equiv f_2 - g_2 \mod m, \\ f_1 g_1 &\equiv f_2 g_2 \mod m. \end{aligned}$$

Mit anderen Worten: Polynomkongruenzen können addiert, subtrahiert und multipliziert werden.

Es ist wohlbekannt, dass man Nullstellen von Polynomen als Linearfaktoren abspalten kann. Gleiches gilt auch für Nullstellen modulo m.

Satz 1.6.3. *Es sei $f \in \mathbb{Z}[X]$ ein Polynom vom Grad n. Ist $a \in \mathbb{Z}$ eine Nullstelle von f modulo m, d.h.*

$$f(a) \equiv 0 \mod m,$$

so existiert ein Polynom $f_1 \in \mathbb{Z}[X]$ vom Grad $n-1$ mit

$$f \equiv f_1 \cdot (X - a) \mod m.$$

Beweis. Sei $f = a_n X^n + \cdots + a_0$. Wir setzen $h_1 = a_n X^{n-1}$ und erhalten eine Gleichung

$$f = h_1 \cdot (X - a) + g_1,$$

wobei $g_1 \in \mathbb{Z}[X]$ einen kleineren Grad als f hat. Es gilt $g_1(a) \equiv 0 \mod m$. Wir führen den Prozess mit g_1 fort und erhalten eine Gleichung

$$g_1 = h_2 \cdot (X - a) + g_2.$$

In jedem Schritt fällt der Grad um mindestens 1, weshalb dieser Prozess abbricht. Folglich gibt es ein n, so dass

$$g_n = h_{n+1} \cdot (X - a) + g_{n+1},$$

wobei g_{n+1} ein konstantes Polynom, d.h. eine ganze Zahl b ist. Nun ist $g_{n+1}(a) \equiv 0 \bmod m$, d.h. $m|b$, und wir erhalten mit $f_1 = h_1 + \cdots + h_{n+1}$ die Kongruenz

$$\begin{aligned} f &= (h_1 + \cdots + h_{n+1})(X - a) + b \\ &\equiv f_1 \cdot (X - a) \mod m. \end{aligned}$$

Das beendet den Beweis. □

Ist a eine Nullstelle von f modulo m, dann ist jedes $b \equiv a \bmod m$ auch Nullstelle von f modulo m. Daher fasst man die Nullstellen von $f \bmod m$ als Elemente in $\mathbb{Z}/m\mathbb{Z}$ auf. Die Anzahl der Nullstellen modulo m eines Polynoms f kann im Allgemeinen den Grad von f übersteigen. Z.B. hat das quadratische Polynom $f = X^2 - 1$ modulo 8 die vier verschiedenen Nullstellen $\bar{1}, \bar{3}, \bar{5}, \bar{7}$. Einfacher ist die Situation, wenn m eine Primzahl ist:

Satz 1.6.4. *Sei p eine Primzahl und $f \in \mathbb{Z}[X]$ ein Polynom vom Grad n, dessen Koeffizienten nicht alle durch p teilbar sind. Dann hat f höchstens n verschiedene Nullstellen modulo p.*

Beweis. Angenommen, das Polynom f hätte die $n+1$ verschiedenen Nullstellen $\bar{b}_1, \ldots, \bar{b}_{n+1}$ modulo p. Nach Satz 1.6.3 können wir Linearfaktoren abspalten und finden also ein Polynom f_1 vom Grad $n-1$ mit

$$f \equiv f_1 \cdot (X - b_1) \mod p.$$

Wegen $\bar{b}_i \neq \bar{b}_1$ für $i > 1$ sind nach Korollar 1.3.12 die Zahlen $b_2, \ldots, b_{n+1}$ Nullstellen modulo p von f_1. Führen wir diesen Prozess fort, erhalten wir eine ganze Zahl c (ein Polynom vom Grad 0) mit

$$f \equiv c \cdot (X - b_1) \cdots (X - b_n) \mod p.$$

Dann ist

$$0 \equiv f(b_{n+1}) \equiv c \cdot (b_{n+1} - b_1) \cdots (b_{n+1} - b_n) \mod p.$$

Für $i = 1, \ldots, n$ gilt nach Voraussetzung $(b_{n+1} - b_i) \not\equiv 0 \bmod p$, weshalb c nach Korollar 1.3.12 durch p teilbar ist. Aber dann sind alle Koeffizienten von f durch p teilbar, was ausgeschlossen war. Dieser Widerspruch zeigt, dass f höchstens n Nullstellen modulo p hat. □

Aufgabe 1. Es sei p eine Primzahl. Man finde ein Polynom $f \in \mathbb{Z}[X]$, so dass $f \not\equiv 0 \bmod p$, aber $f(a) \equiv 0 \bmod p$ für alle $a \in \mathbb{Z}$ gilt.

Aufgabe 2. Sei p eine Primzahl und n eine p-Potenz. Man zeige die Polynomkongruenz

$$(X+1)^n \equiv X^n + 1 \mod p.$$

Aufgabe 3. Sei p eine Primzahl. Man zeige: Gilt die Polynomkongruenz

$$(X+1)^n \equiv X^n + 1 \mod p,$$

so ist n eine p-Potenz.

Hinweis: Sei $n = p^k m$, $(m,p) = 1$. Dann gilt

$$(X+1)^n \equiv (X+1)^{p^k m} \equiv (X^{p^k}+1)^m \equiv X^n + mX^{p^k(m-1)} + \cdots \mod p.$$

1.7 Primitive Wurzeln

Additiv bauen sich die Restklassen modulo m auf die denkbar einfachste Art auf: Man erhält alle Restklassen, indem man die Klasse $\bar{1}$ hinreichend oft zu sich selbst addiert. Multiplikativ stellt sich diese Frage für die primen Restklassen und wird im Primzahlfall $m = p$ in diesem Abschnitt beantwortet. Wir führen zunächst den Begriff der Ordnung einer Restklasse ein.

Definition 1.7.1. *Sei p eine Primzahl und sei $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ eine prime Restklasse. Die* **Ordnung** *von $\bar{a}$ (symbolisch: $ord(\bar{a})$) ist die kleinste natürliche Zahl mit*

$$\bar{a}^{ord(\bar{a})} = \bar{1}.$$

Der Kleine Fermatsche Satz impliziert $ord(\bar{a}) \leq \varphi(p) = p - 1$, insbesondere ist die Ordnung wohldefiniert. Als Nächstes zeigen wir, dass die auftretenden Ordnungen sogar Teiler von $p-1$ sein müssen.

Satz 1.7.2. *Sei $\bar{a}$ eine prime Restklasse modulo p. Dann gilt für $r \in \mathbb{N}$*

$$\bar{a}^r = \bar{1} \iff ord(\bar{a}) | r.$$

Insbesondere gilt: $ord(\bar{a}) | (p-1)$.

Beweis. Die Richtung $\Leftarrow$ ist trivial. Sei nun r eine natürliche Zahl mit $\bar{a}^r = \bar{1}$. Wir setzen $d = (r, ord(\bar{a}))$ und wählen gemäß Satz 1.1.4 ganze Zahlen x, y mit $rx + ord(\bar{a})y = d$. Dann gilt

$$\bar{a}^d = \bar{a}^{rx + ord(\bar{a})y} = (\bar{a}^r)^x (\bar{a}^{ord(\bar{a})})^y = \bar{1}.$$

Folglich gilt $ord(\bar{a}) \leq d$, also $ord(\bar{a}) = d$ und $ord(\bar{a}) | r$. Dies zeigt die Implikation $\Rightarrow$. Schließlich gilt nach dem Kleinen Fermatschen Satz $\bar{a}^{p-1} = \bar{1}$, also $ord(\bar{a}) | (p-1)$. □

Lemma 1.7.3. *Sei d ein positiver Teiler von $p-1$. Dann gibt es entweder keine oder genau $\varphi(d)$ verschiedene prime Restklassen modulo p der Ordnung d.*

Beweis. Angenommen es existiert ein $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ der Ordnung d. Dann ist $\bar{a}$ Nullstelle modulo p des Polynoms

$$f = X^d - 1.$$

Die Restklassen $\bar{a}, \bar{a}^2, \ldots, \bar{a}^d$ sind wegen der Minimalität von d paarweise verschieden. Außerdem sind sie sämtlich Nullstellen von f mod p. Nach Satz 1.6.4 ist daher $\{\bar{a}, \bar{a}^2, \ldots, \bar{a}^d\}$ die genaue Nullstellenmenge von f modulo p. Jede Restklasse der Ordnung d ist Nullstelle von f und somit von der Form $\bar{a}^i$, $1 \leq i \leq d$. Genau die Potenzen $\bar{a}^i$ mit $(i,d) = 1$ haben die Ordnung d. Das sieht man folgendermaßen ein: Ist $(i,d) > 1$, so ist $(\bar{a}^i)^{\frac{d}{(i,d)}} = \bar{a}^{\frac{i}{(i,d)}d} = (\bar{a}^d)^{\frac{i}{(i,d)}} = \bar{1}$, also $ord(\bar{a}^i) < d$. Gilt andererseits $(i,d) = 1$ und ist $(\bar{a}^i)^r = \bar{1}$, so ist $\bar{a}^{ir} = \bar{1}$, also $d \,|\, ir$ und folglich $d \,|\, r$. □

Definition 1.7.4. *Eine Restklasse $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ heißt* **primitive Wurzel modulo p**, *wenn $\bar{a}$ die (maximal mögliche) Ordnung $p-1$ hat.*

Satz 1.7.5 (Gauß). *Sei d ein positiver Teiler von $p-1$. Dann gibt es genau $\varphi(d)$ verschiedene prime Restklassen modulo p der Ordnung d. Insbesondere gibt es genau $\varphi(p-1)$ verschiedene primitive Wurzeln modulo p.*

Beweis. Für $d \,|\, (p-1)$ bezeichne $A(d)$ die Anzahl der primen Restklassen modulo p der Ordnung d. Jede prime Restklasse hat eine Ordnung, also gilt

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

Unter Ausnutzung von Lemma 1.7.3 und Satz 1.3.17 erhalten wir

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

Also ist $A(d) = \varphi(d)$ für alle $d \,|\, (p-1)$. Insbesondere gilt $A(p-1) = \varphi(p-1)$, d.h. es gibt genau $\varphi(p-1)$ verschiedene primitive Wurzeln modulo p. □

Korollar 1.7.6. *Sei $\bar{a}$ eine primitive Wurzel modulo p. Dann durchläuft die Menge der Potenzen*

$$\bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1}$$

alle primen Restklassen modulo p. Mit anderen Worten: Jede prime Restklasse modulo p ist von der Form $\bar{a}^n$ für ein eindeutig bestimmtes n, $1 \leq n \leq p-1$.

Beweis. Die primen Restklassen

$$\bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1}$$

sind paarweise verschieden: Ansonsten würde man durch Dividieren ein j, $1 \leq j \leq p-2$, mit $\bar{a}^j = \bar{1}$ erhalten, was im Widerspruch dazu stünde, dass a primitive Wurzel ist. Es gibt aber nur $p-1$ prime Restklassen und daher sind die angegebenen Restklassen bereits alle. □

Aufgabe 1. Sei p eine Primzahl. Wie viele verschiedene Funktionen

$$f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \{0, +1, -1\}$$

mit der Eigenschaft $f(\bar{a}\bar{b}) = f(\bar{a})f(\bar{b})$ für alle a, b gibt es?

Aufgabe 2. Sei p eine Primzahl. Man zeige: Hat $\bar{a}$ in $\mathbb{Z}/p\mathbb{Z}$ die Ordnung 3, so hat $\overline{a+1}$ die Ordnung 6.

Hinweis: Man zeige zuerst die Kongruenz $(a+1)^2 \equiv a \bmod p$.

http://www.springer.com/978-3-540-45973-6

Einführung in die algebraische Zahlentheorie
Schmidt, A.
2007, XII, 215 S., Softcover
ISBN: 978-3-540-45973-6