

Zahlentheorie und Kryptographie

Prof. Dr. Caroline Lassueur
Leibniz Universität Hannover

Kurzschrift zur Vorlesung, WS 2024/25
Nach Vorlagen von apl. Prof. Dr. Thorsten Holm und Prof. Dr. Gunter Malle

Version: Januar 2025

Kapitel 1: Was ist Kryptographie?	6
Kapitel 2: Die ganzen Zahlen und Teilbarkeit	7
1 Die ganzen Zahlen	7
2 Teilbarkeit in \mathbb{Z}	8
3 Der größte gemeinsame Teiler	9
4 Aufgaben zu Kapitel 2	14
Kapitel 3: Modulare Arithmetik	16
5 Kongruenzen und Restklassenringe	16
6 Invertierbare Restklassen	20
7 Der Chinesische Restsatz	23
8 Die eulersche φ -Funktion	25
9 Aufgaben zu Kapitel 3	28
Kapitel 4: Das RSA-Verfahren	30
10 Das Prinzip	30
11 Das RSA-Verfahren: Mathematische Idee	30
12 Das RSA-Verfahren in der Praxis	31
13 Das RSA-Verfahren: Sicherheit und Sicherheitslücken	33
14 Aufgaben zu Kapitel 4	34
Kapitel 5: Das Rabin-Verfahren	36
15 Das Rabin-Verfahren	36
16 Das Rabin-Verfahren: Korrektheit und Sicherheit	38
17 Aufgaben zu Kapitel 5	39
Kapitel 6: Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ und Primitivwurzeln modulo n	40
18 Die Einheitengruppe $(\mathbb{Z}/2^a\mathbb{Z})^\times$	41
19 Die Einheitengruppe $(\mathbb{Z}/p^a\mathbb{Z})^\times$ für p ungerade	42
20 Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$	44
21 Aufgaben zu Kapitel 6	45

Kapitel 7: Kurze Einführung in die Kodierungstheorie	47
Kapitel 8: Das quadratische Reziprozitätsgesetz	48
22 Quadratische Reste	48
23 Eine Methode von Gauß	51
24 Das quadratische Reziprozitätsgesetz	53
25 Das Jacobi-Symbol	56
26 Aufgaben zu Kapitel 8	59

Kapitel 1: Was ist Kryptographie?

Siehe Folien!

Die Datei `Woche_2_Kapitel_1_Was_ist_Kryptographie.pdf` kann von Stud.IP heruntergeladen werden.

In diesem Kapitel stellen wir Ergebnisse aus der Algebra I zu den ganzen Zahlen zusammen, die im Folgenden wichtig sind.

Notation. Wir benutzen die üblichen Zahlenbereiche:

- **Natürliche Zahlen** (ohne Null): $\mathbb{N} = \{1, 2, 3, 4, 5, 6, \dots\}$
- **Natürliche Zahlen mit Null:** $\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, 6, \dots\}$
- **Ganze Zahlen:** $\mathbb{Z} = \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}$

1 Die ganzen Zahlen

Wiederholung 2.1 (Ringstruktur der ganzen Zahlen)

Auf \mathbb{Z} haben wir zwei natürliche Verknüpfungen:

- (1) die übliche Addition $+: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, (a, b) \mapsto a + b$, und
- (2) die übliche Multiplikation $\cdot: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, (a, b) \mapsto a \cdot b$.

Dann ist $(\mathbb{Z}, +, \cdot)$ ein **kommutativer Ring mit Eins** ($= 1$), d.h. die folgenden Axiome sind erfüllt:

- (R1) $(a + b) + c = a + (b + c) \quad \forall a, b, c \in \mathbb{Z}$ ($+$ ist assoziativ);
- (R2) $a + b = b + a \quad \forall a, b \in \mathbb{Z}$ ($+$ ist kommutativ);
- (R3) $\exists 0 \in \mathbb{Z}$ mit $a + 0 = a = 0 + a \quad \forall a \in \mathbb{Z}$ (0 ist das neutrale Element für $+$);
- (R4) $\forall a \in \mathbb{Z}$ existiert ein Element $-a \in \mathbb{Z}$ mit $a + (-a) = 0 = (-a) + a$ ($-a$ ist das inverse Element bzgl. $+$);
- (R5) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in \mathbb{Z}$ (\cdot ist assoziativ);

- (R6) $a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$ (\cdot ist kommutativ);
- (R7) $\exists 1 \in \mathbb{Z}$ mit $a \cdot 1 = a = 1 \cdot a \quad \forall a \in \mathbb{Z}$ (1 ist das neutrale Element für \cdot);
- (R8) $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = b \cdot c + b \cdot c \quad \forall a, b, c \in \mathbb{Z}$ (\cdot ist distributiv über $+$).

Aber $(\mathbb{Z}, +, \cdot)$ ist kein Körper! Die Elemente $a \in \mathbb{Z} \setminus \{0\}$ sind nicht invertierbar bzgl. Multiplikation.

2 Teilbarkeit in \mathbb{Z}

Definition 2.2 (Teilbarkeit in \mathbb{Z})

Für $a, b \in \mathbb{Z}$ sagt man a **teilt** b (oder a ist ein **Teiler** von b , oder b ist **durch** a **teilbar**), falls ein Element $c \in \mathbb{Z}$ mit $a \cdot c = b$ existiert.

Notation: Man schreibt $a \mid b$.

Definition 2.3 (Vielfaches)

Seien $a, b \in \mathbb{Z}$. Gilt $a \mid b$, so heißt b ein **Vielfaches** von a und $a\mathbb{Z} := \{a \cdot m \mid m \in \mathbb{Z}\}$ ist die Menge aller Vielfachen von a .

Bekannt aus der Vorlesung Algebra I: $a\mathbb{Z}$ ist ein Ideal von \mathbb{Z} .

Lemma 2.4 (Eigenschaften der Teilbarkeit in \mathbb{Z})

Seien $a, b, c \in \mathbb{Z}$. Dann gelten:

- (a) $a \mid a$, $\pm 1 \mid a$ und $a \mid 0$
aber: ist $a \neq 0$, so gilt $0 \nmid a$;
- (b) $a \mid b \implies a \mid -b$, $(-a) \mid b$ und $(-a) \mid (-b)$;
- (c) $a \mid b \implies a \mid bc$;
- (d) $(a \mid b \text{ und } b \mid c) \implies a \mid r \cdot b + s \cdot c \quad \forall r, s \in \mathbb{Z}$;
- (e) $a \mid b \implies (b = 0 \text{ oder } |a| \leq |b|)$;
- (f) $a \mid b \text{ und } b \mid a \implies a = b \text{ oder } a = -b$;
- (g) $a \mid b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$.

Beweis: (Übungsaufgabe bzw. bekannt aus der Algebra I.)

Als Muster beweisen wir (f):

- (1) $a \mid b \implies \exists c \in \mathbb{Z}$ mit $a \cdot c = b$, und
- (2) $b \mid a \implies \exists d \in \mathbb{Z}$ mit $b \cdot d = a$.

Somit ist $a = b \cdot d = (a \cdot c) \cdot d = acd$. Nun, im Fall $a = 0$ ist auch $b = ac = 0 \cdot c = 0$. Ist $a \neq 0$, so muss $cd = 1$ gelten und somit sind $c = \pm 1$ und $d = \pm 1$. Mit (2) folgt $a = bc = b \cdot (\pm 1) = \pm b$. ■

Satz 2.5 (Division mit Rest)

Sind $a, b \in \mathbb{Z}$ mit $b \neq 0$, so existieren eindeutig bestimmte Elemente $q, r \in \mathbb{Z}$, so dass

$$a = q \cdot b + r \quad \text{und} \quad a \leq r < |b|$$

Dabei heißt r der **Rest bei der Division von a durch b** .

Beweis: Wir zeigen die Existenz und die Eindeutigkeit separat.

- (1) Existenz: Wir betrachten die Menge $M := \{a - qb \in \mathbb{N}_0 \mid q \in \mathbb{Z}\} \subseteq \mathbb{N}_0$. Diese Menge ist nicht-leer, da $b \neq 0$. Sei also r das kleinste Element von M . (Jede nicht-leere Teilmenge von \mathbb{N}_0 besitzt ein kleinstes Element.) Dann gelten:

- $r \in M \implies \exists q \in \mathbb{Z}$ mit $r = a - qb$, d.h. $a = qb + r$;
- $r \in \mathbb{N}_0 \implies 0 \leq r$;
- $r < |b|$ (sonst $r - |b| \in M$ und dies ist ein Widerspruch zur Minimalität von r).

- (2) Eindeutigkeit: Angenommen $\exists q, q', r, r' \in \mathbb{Z}$ mit

$$\begin{aligned} a &= qb + r & \text{und} & \quad 0 \leq r < |b|, \\ a &= q'b + r' & \text{und} & \quad 0 \leq r' < |b| \end{aligned}$$

erhalten wir

$$q \cdot b + r = q' \cdot b + r' \implies (q - q')b = r' - r \implies |q - q'| \cdot |b| = |r' - r| < |b|,$$

da $0 \leq r, r' < |b|$. Die einzige Möglichkeit ist $|q - q'| = 0$, so dass $q = q'$ und $r = r'$ ist. ■

3 Der größte gemeinsame Teiler

Zunächst betrachten wir eine Verallgemeinerung des Begriffs eines *größten gemeinsamen Teilers* von zwei Elementen.

Definition 2.6 (größter gemeinsamer Teiler)

Seien $a_1, \dots, a_n \in \mathbb{Z}$ mit $n \in \mathbb{Z}_{\geq 2}$.

- Die Menge $\text{gT}(a_1, \dots, a_n) := \{d \in \mathbb{Z} \mid d \mid a_1, \dots, d \mid a_n\}$ ist die Menge aller gemeinsamen Teiler von a_1, \dots, a_n .
- Ein $d \in \text{gT}(a_1, \dots, a_n)$ heißt **größter gemeinsamer Teiler** (ggT) von a_1, \dots, a_n , wenn für jeden gemeinsamen Teiler $d' \in \text{gT}(a_1, \dots, a_n)$ gilt, dass $d' \mid d$.
- Die Zahlen $a_1, \dots, a_n \in \mathbb{Z}$ heißen **teilerfremd**, wenn 1 ein größter gemeinsamer Teiler von a_1, \dots, a_n ist.

Anmerkung 2.7

⚠ Größte gemeinsame Teiler sind nur bis auf Vorzeichen eindeutig!

Z.B.: Beide +5 und −5 sind größte gemeinsame Teiler von 15, 20 und 25.

Beweis: Falls $d, d' \in \mathbb{Z}$ größte gemeinsame Teiler von a_1, \dots, a_n , so gilt nach Definition $d \mid d'$ und

$d' \mid d$. Somit liefert Lemma 2.4(f), dass $d = \pm d'$ ist, wie behauptet.

Notation: Mit $\text{ggT}(a_1, \dots, a_n)$ bezeichnen wir stets den nicht-negativen größten gemeinsamen Teiler von a_1, \dots, a_n .

⚠ Es ist a priori nicht klar, dass größte gemeinsame Teiler existieren.

Der folgende Satz liefert ein Verfahren zur Berechnung eines größten gemeinsamen Teiler von zwei ganzen Zahlen. Insbesondere liefert dieses Verfahren die Existenz eines ggTs.

Satz 2.8 (Erweiterter Euklidischer Algorithmus)

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$.

Setze $r_0 := a$, $r_1 := b$, $s_0 := 1$, $t_0 := 0$, $s_1 := 0$, $t_1 := 1$ und betrachte die folgende Kette von Divisionen mit Rest:

$$\begin{array}{llll} a = q_1 \cdot b + r_2 & \text{mit} & 0 \leq r_2 < |b|; \\ b = q_2 \cdot r_2 + r_3 & \text{mit} & 0 \leq r_3 < r_2; \\ \vdots & & \vdots \\ r_{i-1} = q_i \cdot r_i + r_{i+1} & \text{mit} & 0 \leq r_{i+1} < r_i; \\ \vdots & & \vdots \\ r_{m-2} = q_{m-1} \cdot r_{m-1} + r_m & \text{mit} & 0 \leq r_m < r_{m-1}; \\ r_{m-1} = q_m \cdot r_m + 0. \end{array}$$

Außerdem setze

$$s_{i+1} := s_{i-1} - q_i \cdot s_i \quad \text{und} \quad t_{i+1} := t_{i-1} - q_i \cdot t_i \quad \forall i = 1, \dots, m-1.$$

Dann gelten:

- (a) Das Verfahren bricht nach endlich vielen Schritten ab, d.h. es gibt eine Zahl $m \in \mathbb{N}$ mit $r_{m-1} = q_m \cdot r_m$.
- (b) Es ist $\text{ggT}(a, b) = r_m$.
- (c) Für alle $i = 0, 1, \dots, m$ ist $r_i = s_i \cdot a + t_i \cdot b$.
Insbesondere existieren ganze Zahlen $s := s_m$ und $t := t_m$ mit

$$\text{ggT}(a, b) = s \cdot a + t \cdot b.$$

Die Zahlen $s, t \in \mathbb{Z}$ heißen **Bézout-Koeffizienten**.

Beweis:

- (a) 1. Fall: $b \mid a$. Das Verfahren bricht schon im ersten Schritt ab.

2. Fall: $b \nmid a$. In diesem Fall ist $r_2 > 0$ und wir erhalten eine echt absteigende Kette von Zahlen in \mathbb{N}_0 :

$$r_2 > r_3 > \dots > r_i > \dots > 0$$

Diese muss nach endlich vielen Schritten enden, da r_2 eine positive ganze Zahl ist.

(b) (1) Wir zeigen, dass $r_m \mid a$ und $r_m \mid b$.

Wir lesen die Gleichungen von unten nach oben. Wir erhalten:

$$\begin{aligned}
 r_{m-1} = q_m \cdot r_m &\implies r_m \mid r_{m-1} \\
 &\implies r_m \mid q_{m-1} \cdot r_{m-1} + r_m = r_{m-2} \\
 &\implies \dots \\
 &\implies r_m \mid q_2 \cdot r_2 + r_3 = b \\
 &\implies r_m \mid q_1 \cdot b + r_2 = a
 \end{aligned}$$

Somit ist $r_m \in \text{gT}(a, b)$.

(2) Wir zeigen: $d \in \text{gT}(a, b) \implies d \mid r_m$.

Wir lesen hier die Gleichungen von oben nach unten und wir erhalten:

$$\begin{aligned}
 d \mid a - q_1 \cdot b = r_2 &\implies d \mid b - q_2 \cdot r_2 = r_3 \\
 &\implies \dots \\
 &\implies d \mid r_{m-2} - q_{m-1} \cdot r_{m-1} = r_m
 \end{aligned}$$

Nach Definition gilt also $r_m = \text{ggT}(a, b)$.

(c) Per Induktion nach i :

- Induktionsanfang:
 $i = 0$ liefert $r_0 = a = 1 \cdot a + 0 \cdot b = s_0 \cdot a + t_0 \cdot b$, und
 $i = 1$ liefert $r_1 = b = 0 \cdot a + 1 \cdot b = s_1 \cdot a + t_1 \cdot b$, wie verlangt.
- Induktionsvoraussetzung (IV): Wir nehmen an, die Formel gelte bereits für r_{i-1} und r_i .
- Induktionsschritt: Wir zeigen, dass die Formel auch für r_{i+1} gilt. Wir berechnen:

$$\begin{aligned}
 r_{i+1} &= r_{i-1} - q_i \cdot r_i \\
 &\stackrel{(IV)}{=} s_{i-1} \cdot a + t_{i-1} \cdot b - q_i \cdot (s_i \cdot a + t_i \cdot b) \\
 &= (s_{i-1} - q_i s_i) \cdot a + (t_{i-1} - q_i t_i) \\
 &\stackrel{\text{Def.}}{=} s_i \cdot a + t_i \cdot b.
 \end{aligned}$$

Beispiel 2.9

Wir betrachten die ganzen Zahlen $a = 14351$ und $b = 12317$.

Wir berechnen mit der euklidische Algorithmus:

$$14351 = 1 \cdot 12317 + 2034$$

$$12317 = 6 \cdot 2034 + 113$$

$$2034 = 18 \cdot 113 + 0$$

Somit ist $\text{ggT}(527, 390) = 113$ und wir berechnen Bézout-Koeffizienten mithilfe des erweiterten Algorithmus:

i	r_i	q_i	s_i	t_i
0	14351	-	1	0
1	12317	1	0	1
2	2034	6	1	-1
3	113	18	-6	7
4	0	-	-	-

Der ggT und die Bézout-Koeffizienten lassen sich aus der vorletzten Zeile ablesen:

$$\text{ggT}(14351, 12317) = 113 = (-6) \cdot 14351 + 7 \cdot 12317$$

d.h. $s = -6$ und $t = 7$.

Lemma 2.10

Seien $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ mit $n \in \mathbb{Z}_{\geq 2}$. Dann gelten:

(a) Ist $n \geq 3$, so ist $\text{ggT}(a_1, \dots, a_n) = \text{ggT}(\text{ggT}(a_1, \dots, a_{n-1}), a_n)$.

(b) Es gilt die folgende Gleichheit von Idealen von \mathbb{Z} :

$$(\text{ggT}(a_1, \dots, a_n))_{\mathbb{Z}} = (a_1, \dots, a_n)_{\mathbb{Z}}.$$

(c) Es existieren Koeffizienten $b_1, \dots, b_n \in \mathbb{Z}$ mit $\text{ggT}(a_1, \dots, a_n) = b_1 a_1 + \dots + b_n a_n$.

(d) a_1, \dots, a_n sind genau dann teilerfremd, wenn $\text{ggT}(a_1, \dots, a_n) = 1$.

Beweis: (a) Sei $h := \text{ggT}(\text{ggT}(a_1, \dots, a_{n-1}), a_n)$. Nach Definition gilt $h \mid \text{ggT}(a_1, \dots, a_{n-1})$, $h \mid a_n$ und h ist maximal mit diesen Eigenschaften.

Nun: $h \mid \text{ggT}(a_1, \dots, a_{n-1}) \implies h \mid a_1, \dots, h \mid a_{n-1}$. Somit ist $h \in \text{gT}(a_1, \dots, a_n)$ und wir müssen nur noch zeigen, dass h maximal mit dieser Eigenschaft ist.

Nehmen wir also an, dass $h' \in \mathbb{Z}$ erfüllt

$$h' \mid a_1, \dots, h' \mid a_n.$$

Insbesondere: $h' \mid a_1, \dots, h' \mid a_{n-1} \implies h' \in \text{gT}(a_1, \dots, a_{n-1})$.

Zusammengefasst gelten nun: $h' \mid \text{ggT}(a_1, \dots, a_{n-1})$ and $h' \mid a_n$ und die Maximalität von h liefert $h' \mid h$. Wir haben also gezeigt, dass $h = \text{ggT}(a_1, \dots, a_n)$ ist.

(b) Setze $g := \text{ggT}(a_1, \dots, a_n)$.

\subseteq : ist klar! Es gilt $g \mid a_1, \dots, g \mid a_n$, sodass es $b_1, \dots, b_n \in \mathbb{Z}$ mit $a_1 = gb_1, \dots, a_n = gb_n$ existieren. Somit gilt

$$a_1 \in g\mathbb{Z} = (g)_{\mathbb{Z}}, \dots, a_n \in g\mathbb{Z} = (g)_{\mathbb{Z}}$$

und daraus folgt

$$(a_1, \dots, a_n)_{\mathbb{Z}} \subseteq (\text{ggT}(a_1, \dots, a_n))_{\mathbb{Z}}.$$

\supseteq : Induktion nach n :

I.A.: Für $n = 2$ existieren $s, t \in \mathbb{Z}$ mit $g = sa_1 + ta_2$ nach dem Euklidischen Algorithmus.
 $\implies g \in (a_1, a_2)_{\mathbb{Z}} \implies (g)_{\mathbb{Z}} \subseteq (a_1, a_2)_{\mathbb{Z}}$.

I.V.: Wir nehmen an, es gelte bereits $(\text{ggT}(a_1, \dots, a_{n-1}))_{\mathbb{Z}} \subseteq (a_1, \dots, a_{n-1})_{\mathbb{Z}}$. I.S.: Wir müssen zeigen, dass $(g)_{\mathbb{Z}} \subseteq (a_1, \dots, a_n)_{\mathbb{Z}}$.

Nach (a) gilt $g = \text{ggT}(\text{ggT}(a_1, \dots, a_{n-1}), a_n)$ und nach dem Euklidischen Algorithmus existieren $s, t \in \mathbb{Z}$ mit

$$g = s \cdot \text{ggT}(a_1, \dots, a_{n-1}) + t \cdot a_n.$$

Somit gilt mit der Induktionsvoraussetzung:

$$g \in (\text{ggT}(a_1, \dots, a_{n-1}), a_n)_{\mathbb{Z}} \subseteq (a_1, \dots, a_{n-1}, a_n)_{\mathbb{Z}}.$$

Die liefert

$$(g)_{\mathbb{Z}} \subseteq (a_1, \dots, a_{n-1}, a_n)_{\mathbb{Z}}.$$

(c) folgt direkt aus (b).

(d) Klar aus der Definition von teilerfremd und vom ggT. ■

Anmerkung 2.11

Die Elemente b_1, \dots, b_n und auch $\text{ggT}(z_1, \dots, z_n)$ können z.B. induktiv mit dem erweiterten euklidischen Algorithmus bestimmt werden.

⚠ Diese Darstellung hängt von der Reihenfolge der Operationen ab!

Beispiel 2.12

(a) Seien $a_1 = 24$, $a_2 = 18$, $a_3 = 10$. Mit dem euklidischen Algorithmus erhalten wir:

$$\text{ggT}(24, 18) = 6 = 1 \cdot 24 + (-1) \cdot 18, \text{ und } \text{ggT}(6, 10) = 2 = 2 \cdot 6 + (-1) \cdot 10$$

Also ist

$$\begin{aligned} \text{ggT}(24, 18, 10) &= \text{ggT}(\text{ggT}(24, 18), 10) = 2 \\ &= 2 \cdot 6 + (-1) \cdot 10 \\ &= 2 \cdot (1 \cdot 24 + (-1) \cdot 18) + (-1) \cdot 10 \\ &= 2 \cdot 24 + (-2) \cdot 18 + (-1) \cdot 10 \\ &= 2 \cdot a_1 + (-2) \cdot a_2 + (-1) \cdot a_3 \end{aligned}$$

d.h. $b_1 = 2$, $b_2 = -2$ und $b_3 = -1$.

Mit einer verschiedenen Reihenfolge der Operationen erhalten wir

$$\text{ggT}(18, 10) = 2 = (-1) \cdot 18 + 2 \cdot 10, \text{ und } \text{ggT}(24, 2) = 2 = 0 \cdot 24 + 1 \cdot 2.$$

Somit ist

$$\begin{aligned} \text{ggT}(24, 18, 10) &= \text{ggT}(24, \text{ggT}(18, 10)) = 2 \\ &= 0 \cdot 24 + 1 \cdot 2 \\ &= 0 \cdot 24 + 1 \cdot ((-1) \cdot 18 + 2 \cdot 10) \\ &= 0 \cdot 24 + (-1) \cdot 18 + 2 \cdot 10 \\ &= 0 \cdot a_1 + (-1) \cdot a_2 + 2 \cdot a_3. \end{aligned}$$

d.h. in diesem Fall sind $b_1 = 0$, $b_2 = -1$ und $b_3 = 2$.

(b) ⚠ Es kann sein, daß die Elemente a_1, \dots, a_n nicht paarweise teilerfremd sind, aber es gilt $\text{ggT}(a_1, \dots, a_n) = 1$.

Z.B. ist $\text{ggT}(10, 15, 21) = 1$ aber es gilt $\text{ggT}(10, 15) = 5$ und $\text{ggT}(15, 21) = 3$.

4 Aufgaben zu Kapitel 2

Aufgabe 1

- (1) Gilt $0 \mid 0$?
- (2) Geben Sie alle ganzzahligen Teiler von 20 an.

Aufgabe 2

Seien $a, b, c \in \mathbb{Z}$. Zeigen Sie:

- (1) Gilt $a \mid b$ und $b \mid c$, so gilt $a \mid (rb + sc)$ für alle $r, s \in \mathbb{Z}$;
- (2) a ist genau dann ein Teiler von b , wenn $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Aufgabe 3

Zeigen Sie, dass für alle $n \in \mathbb{N}$ die Zahl $n^2 + 3n + 2$ durch 2 teilbar ist.

Aufgabe 4

Sei $a \in \mathbb{Z}$ eine ungerade Zahl. Zeigen Sie, dass $a^2 + (a + 2)^2 + (a + 4)^2 + 1$ durch 12 teilbar ist.

Aufgabe 5

Bestimmen Sie alle $n \in \mathbb{N}$, für die $n \mid 2n + 3$ gilt.

Aufgabe 6

Bestimmen Sie mithilfe des erweiterten Euklidischen Algorithmus den größten gemeinsamen Teiler von 621 und 391 und Zahlen $s, t \in \mathbb{Z}$, so dass $\text{ggT}(621, 391) = s \cdot 621 + t \cdot 391$.

Geben Sie dabei alle Schritte an und erstellen Sie eine Tabelle wie im Beispiel nach Satz 2.7.

Aufgabe 7

Seien $a_1 = 24$, $a_2 = 18$ und $a_3 = 10$. Berechnen Sie mithilfe des erweiterten Euklidischen Algorithmus:

- (1) $\text{ggT}(24, 18, 10)$ als $\text{ggT}(\text{ggT}(24, 18), 10)$ und bestimmen Sie dabei Zahlen $b_1, b_2, b_3 \in \mathbb{Z}$, sodass $\text{ggT}(24, 18, 10) = b_1 \cdot a_1 + b_2 \cdot a_2 + b_3 \cdot a_3$;
- (2) $\text{ggT}(24, 18, 10)$ als $\text{ggT}(24, \text{ggT}(18, 10))$ und bestimmen Sie dabei Zahlen $b'_1, b'_2, b'_3 \in \mathbb{Z}$, sodass $\text{ggT}(24, 18, 10) = b'_1 \cdot a_1 + b'_2 \cdot a_2 + b'_3 \cdot a_3$.

Anmerkung: Aufgabe 2 zeigt, dass die Zahlen b_1, \dots, b_n aus den Eigenschaften 2.8(c) im Allgemeinen nicht eindeutig bestimmt sind.

Aufgabe 8

Betrachten Sie die Gleichung $aX + bY + cZ = d$ mit $a, b, c, d \in \mathbb{Z}$, wobei X, Y, Z Unbekannten sind. Ferner nehmen wir an, dass a, b, c nicht alle gleich Null sind. Zeigen Sie:

- (1) Sind x, y, z ganze Zahlen mit $ax + by + cz = d$, so gilt $\text{ggT}(a, b, c) \mid d$.

(2) Gilt $\text{ggT}(a, b, c) \mid d$, so existieren ganze Zahlen x, y, z mit $ax + by + cz = d$.

Gibt es ganze Zahlen x, y, z mit $24x + 18y + 10z = 3$?

[Hinweis: Verwenden Sie die Eigenschaften 2.8.]

Aufgabe 9

Man nennt $v \in \mathbb{Z}$ ein *gemeinsames Vielfaches* von $a_1, \dots, a_n \in \mathbb{Z}$, falls $a_i \mid v$ für alle $i = 1, \dots, n$ gilt. Ein gemeinsames Vielfaches $v \in \mathbb{N}_0$ heißt *kleinstes gemeinsames Vielfache*, falls v jedes gemeinsame Vielfache von a_1, \dots, a_n teilt. Wir schreiben dann $\text{kgV}(a_1, \dots, a_n) := v$.

Zeigen Sie:

(1) $\text{kgV}(a_1, \dots, a_n)$ ist nur bis auf Vorzeichen eindeutig bestimmt;

(2) $\text{kgV}(a_1, \dots, a_n) = \text{kgV}(a_1, \text{kgV}(a_2, \dots, a_n))$.

Aufgabe 10

Seien $c_0, c_1, c_2 \in \mathbb{Z}_{>0}$ mit $\text{ggT}(c_1, c_2) \mid c_0$ und $\text{ggT}(c_1, c_2) = a_1 \cdot c_1 + a_2 \cdot c_2$, wobei $a_1, a_2 \in \mathbb{Z}$ Bézout-Koeffizienten sind. Zeigen Sie: Genau dann ist $(x_1, x_2) \in \mathbb{Z}^2$ eine Lösung der linearen diophantischen Gleichung

$$c_1 \cdot X_1 + c_2 \cdot X_2 = c_0,$$

wenn es ein $k \in \mathbb{Z}$ existiert, so dass

$$x_1 = \frac{c_0 \cdot a_1}{\text{ggT}(c_1, c_2)} + \frac{c_2 \cdot k}{\text{ggT}(c_1, c_2)} \quad \text{und} \quad x_2 = \frac{c_0 \cdot a_2}{\text{ggT}(c_1, c_2)} - \frac{c_1 \cdot k}{\text{ggT}(c_1, c_2)}.$$

Aufgabe 11

Ein Straßenverkäufer verkauft Luftballons, kleine zu 98 Cent das Stück und große zu 1,58 Euro. Am Abend hat er 170,28 Euro in der Tasche und von den je 100 kleinen und großen Ballons, die er dabei hatte, ist ein großer Teil verkauft. Wie viele Ballons von welcher Größe hat er verkauft?

[Hinweis: Rechnen Sie mit Cents und verwenden Sie Aufgabe 1.]

Aufgabe 12

Sei $n \in \mathbb{N}$. Zeigen Sie:

(1) Sind a_1, \dots, a_n ganze Zahlen, so gilt $\text{kgV}(a_1, \dots, a_n)\mathbb{Z} = a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z}$.

(2) Sind a_1, \dots, a_n positive ganze Zahlen, so gilt

$$\text{kgV}(a_1, \dots, a_n) = \frac{A}{\text{ggT}(A_1, \dots, A_n)},$$

wobei $A := a_1 \cdot \dots \cdot a_n$ und $A_i := \frac{A}{a_i}$ für alle $1 \leq i \leq n$.

Insbesondere, für zwei positive ganzen Zahlen a, b gilt

$$\text{kgV}(a, b) = \frac{a \cdot b}{\text{ggT}(a, b)}.$$

(3) Gilt die Formel aus (2) auch für beliebige ganze Zahlen $a_1, \dots, a_n \in \mathbb{Z}$?

Die modulare Arithmetik ist ein Teilgebiet der Zahlentheorie und der Algebra, das man kurz als „Arithmetik mit Resten“ beschreiben könnte. In ihrer modernen Notation und dem heute bekannten Formalismus geht sie auf den Mathematiker Carl Friedrich Gauß zurück, der sie 1801 in seinen *Disquisitiones Arithmeticae* vorstellte.

5 Kongruenzen und Restklassenringe

Definition 3.1 (*Kongruenz modulo n*)

Sei $n \in \mathbb{N}$. Sind $a, b \in \mathbb{Z}$, so heißt a **kongruent zu b modulo n** , wenn $n \mid a - b$.

Notation: $a \equiv b \pmod{n}$.

Anmerkung 3.2

- (1) $a \equiv b \pmod{n}$ bedeutet, dass a und b denselben Rest bei Division mit Rest durch n haben.

(Die Division mit Rest liefert die Existenz von $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, so dass

$$a = q_1 \cdot n + r_1 \quad \text{mit } 0 \leq r_1 < n,$$

$$b = q_2 \cdot n + r_2 \quad \text{mit } 0 \leq r_2 < n$$

gelten. Somit ist $a - b = (q_1 - q_2)n + (r_1 - r_2)$ und es gilt

$$n \mid a - b \iff n \mid r_1 - r_2 \iff r_1 - r_2 = 0 \iff r_1 = r_2,$$

da $0 \leq r_1, r_2 < n$.)

- (2) Kongruenz modulo n ist eine Äquivalenzrelation auf \mathbb{Z} . [Beweis: Übung! Zu zeigen: diese Relation ist reflexiv, symmetrisch und transitiv.]

Wir dürfen also die Äquivalenzklassen dieser Relation betrachten. Dies liefert die folgende Definition:

Definition 3.3 (*Restklasse modulo n*)

Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$.

(a) Die Restklasse von a modulo n ist die Menge

$$\begin{aligned} [a]_n &:= \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} \\ &= \{b \in \mathbb{Z} \mid n \mid b - a\} \\ &= \{b \in \mathbb{Z} \mid \exists t \in \mathbb{Z} \text{ mit } n \mid b - a\} =: a + n\mathbb{Z} \end{aligned}$$

(b) Die Menge aller Restklassen modulo n bezeichnen wir mit $\mathbb{Z}/n\mathbb{Z}$. D.h.

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}.$$

Anmerkung 3.4

(1) Manche Bücher schreiben \mathbb{Z}_n statt $\mathbb{Z}/n\mathbb{Z}$.

(2) **Warnung:** $[a]_n$ ist eine Menge! Keine Zahl!

Es gilt

$$\begin{aligned} [a]_n &= [a + n]_n = [a + 2n]_n = \dots \\ &= [a - n]_n = [a - 2n]_n = \dots \end{aligned}$$

Z.B. für $n = 3$ gelten:

$$\begin{aligned} [0]_3 &= [3]_3 = [6]_3 = [9]_3 = \dots \\ &= [-3]_3 = [-6]_3 = [-9]_3 = \dots \end{aligned}$$

$$\begin{aligned} [1]_3 &= [4]_3 = [7]_3 = [10]_3 = \dots \\ &= [-2]_3 = [-5]_3 = [-8]_3 = \dots \end{aligned}$$

$$\begin{aligned} [2]_3 &= [5]_3 = [8]_3 = [11]_3 = \dots \\ &= [-1]_3 = [-4]_3 = [-7]_3 = \dots \end{aligned}$$

Auf $\mathbb{Z}/n\mathbb{Z}$ erhalten wir wohldefinierte Verknüpfungen. Eine Addition

$$\begin{aligned} +: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ ([a]_n, [b]_n) &\mapsto [a]_n + [b]_n := [a + b]_n \end{aligned}$$

und eine Multiplikation

$$\begin{aligned} \cdot: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ ([a]_n, [b]_n) &\mapsto [a]_n \cdot [b]_n := [a \cdot b]_n, \end{aligned}$$

sodass $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Eins ist. Genauer ist $[1]_n$ das neutrale Element für die Multiplikation.

- (3) **Alternative Schreibweise:** $n\mathbb{Z} \subseteq \mathbb{Z}$ ist ein Ideal, sodass $\mathbb{Z}/n\mathbb{Z}$ als Faktorring verstanden werden kann (d.h. wie in der Algebra I), wobei die Elemente von $\mathbb{Z}/n\mathbb{Z}$ als $a + n\mathbb{Z}$ geschrieben werden. (Vgl. Definition 3.3.)

Beispiel 3.5 (*Rechnen modulo n*)

Das Rechnen modulo n erlaubt es uns z.B. die folgenden Fragen bzw. Behauptungen durch einfache Methoden zu beantworten bzw. beweisen.

- (1) **Welcher Rest bleibt bei der Division mit Rest von 17^{341} durch 5?**

Da $17 \equiv 2 \pmod{5}$ und $341 = 2 \cdot 170 + 1$ gelten, liefert das Rechnen modulo 5, dass

$$17^{341} \equiv 2^{341} \equiv (2^2)^{170} \cdot 2^1 \pmod{5}.$$

Aber $2^2 = 4 \equiv -1 \pmod{5}$ und 170 ist gerade. Somit gilt

$$17^{341} \equiv (2^2)^{170} \cdot 2^1 \equiv (-1)^{170} \cdot 2 \equiv 2 \pmod{5}$$

und der gesuchte Rest ist 2.

- (2) **Welcher Rest bleibt bei der Division mit Rest von 3^{3719} durch 8?**

Es gilt $3719 = 2 \cdot 1859 + 1$. Somit ist $3^{3719} = (3^2)^{1859} \cdot 3 = 9^{1859} \cdot 3$. Rechnen modulo 8 liefert

$$3^{3719} = 9^{1859} \cdot 3 \equiv 1^{1859} \cdot 3 \equiv 3 \pmod{8}$$

und der gesuchte Rest ist 3.

- (3) **Behauptung:** Für jede natürliche Zahl $n \in \mathbb{N}$ ist $2^{5n+1} + 5^{n+2}$ durch 27 teilbar. Beweis: Sei $n \in \mathbb{N}$. Hier rechnen wir modulo 27. Zunächst beobachten wir, dass

$$2^{5n+1} = (2^5)^n \cdot 2 = (32)^n \cdot 2 \equiv 5^n \cdot 2 \pmod{27}.$$

Daraus folgt, dass

$$2^{5n+1} + 5^{n+2} \equiv 5^n \cdot 2 + 5^{n+2} \equiv 5^n \cdot (2 + 5^2) \equiv 5^n \cdot 27 \equiv 5^n \cdot 0 \equiv 0 \pmod{27}$$

und somit gilt $27 \mid 2^{5n+1} + 5^{n+2}$.

- (4) Sei $a \in \mathbb{N}$ eine natürliche Zahl. Die Dezimaldarstellung von a ist

$$a = a_r a_{r-1} \cdots a_1 a_0 \quad (r \in \mathbb{N}_0)$$

mit Ziffern $a_0, \dots, a_r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und $a_r \neq 0$. Dies bedeutet, dass

$$a = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_1 \cdot 10^1 + a_0.$$

Behauptung: Die letzte Ziffer von a^4 ist in $\{0, 1, 5, 6\}$.

Beweis: Wir müssen modulo 10 rechnen. Es gilt

$$a = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_1 \cdot 10^1 + a_0 \equiv a_0 \pmod{10}$$

und somit ist $a^4 \equiv a_0^4 \pmod{10}$. Die Möglichkeiten für a_0^4 sind also:

a_0	0	1	2	3	4	5	6	7	8	9
$a_0^4 \pmod{10}$	0	1	6	1	6	5	6	1	6	1

Wir haben wie folgt gerechnet:

- $0^4 = 0 \equiv 0 \pmod{10}$;
- $1^4 = 1 \equiv 1 \pmod{10}$;
- $2^4 = 16 \equiv 6 \pmod{10}$;
- $3^4 = 9^2 \equiv (-1)^2 \equiv 1 \pmod{10}$;
- $4^4 = (2^2)^4 = (2^4)^2 \equiv (16)^2 \equiv 6^2 \equiv 36 \equiv 6 \pmod{10}$;
- $5^4 = 25^2 \equiv 5^2 \equiv 25 \equiv 5 \pmod{10}$;
- für $a \in \{6, 7, 8, 9\}$ ist $a \equiv a - 10 \pmod{10}$, wobei $a - 10 \in \{-1, -2, -3, -4\}$. Wir erhalten also

$$a^4 \equiv (-(a - 10))^4,$$

wobei $-(a - 10) \in \{1, 2, 3, 4\}$.

Z.B.: $6 \equiv -4 \pmod{10} \implies 6^4 \equiv (-4)^4 \equiv 4^4 \equiv 6 \pmod{10}$, da wir 4^4 modulo 10 schon kennen!

Als Anwendung erhalten wir wohlbekannte Teilbarkeitsregeln.

Anwendung 3.6 (Teilbarkeitsregeln)

Wir betrachten erneut eine natürliche Zahl a mit Dezimaldarstellung

$$a = a_r a_{r-1} \cdots a_1 a_0 \quad (r \in \mathbb{N}_0)$$

mit Ziffern $a_0, \dots, a_r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und $a_r \neq 0$, sodass

$$a = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_1 \cdot 10^1 + a_0$$

gilt.

(1) **Teilbarkeit durch 3 und 9.** Es gilt $10 \equiv 1 \pmod{3}$ bzw. $\pmod{9}$. Daraus folgt

$$10^k \equiv 1^k \equiv 1 \pmod{3} \text{ bzw. } \pmod{9}$$

und wir erhalten, dass

$$\begin{aligned} a &= a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_1 \cdot 10^1 + a_0 \\ &\equiv a_r \cdot 1 + a_{r-1} \cdot 1 + \dots + a_1 \cdot 1 + a_0 \\ &\equiv a_r + a_{r-1} + \dots + a_1 + a_0 \pmod{3} \text{ bzw. } \pmod{9}. \end{aligned}$$

Die Summe $a_r + a_{r-1} + \dots + a_1 + a_0 = \sum_{k=0}^r a_k$ nennt man **Quersumme** von a und somit gelten die folgenden Teilbarkeitsregeln:

$3 \mid a \iff$ Quersumme von a kongruent zu 0 modulo 3 \iff Quersumme von a durch 3 teilbar.
--

und

$9 \mid a \iff$ Quersumme von a kongruent zu 0 modulo 9 \iff Quersumme von a durch 9 teilbar.
--

(2) **Teilbarkeit durch 11.** Es gilt $10 \equiv -1 \pmod{11}$. Daraus folgt

$$10^k \equiv (-1)^k \equiv \begin{cases} 1 \pmod{11} & \text{für } k \text{ gerade,} \\ -1 \pmod{11} & \text{für } k \text{ ungerade.} \end{cases}$$

Wir erhalten also, dass

$$a = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_1 \cdot 10^1 + a_0 \equiv \sum_{k=0}^r (-1)^k \cdot a_k \pmod{11}.$$

Die Summe $\sum_{k=0}^r (-1)^k \cdot a_k$ nennt man **alternierende Quersumme** von a und somit gilt

$11 \mid a \iff \text{alternierende Quersumme von } a \text{ durch 11 teilbar.}$
--

6 Invertierbare Restklassen

ZENTRALE FRAGE in ZAHLBEREICHE: Welche Elemente sind invertierbar bzgl. Multiplikation?

\mathbb{N}	$\{1\}$
\mathbb{Z}	$\{\pm 1\}$
\mathbb{Q}	$\mathbb{Q} \setminus \{0\}$
\mathbb{R}	$\mathbb{R} \setminus \{0\}$
$\mathbb{Z}/n\mathbb{Z}$??

Anmerkung 3.7 (Einfache Beobachtungen)

(1) **Wiederholung:** Ein Element $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann **invertierbar**, wenn es $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ mit

$$[1]_n = [a]_n \cdot [b]_n$$

existiert. Dann ist auch $[b]_n$ invertierbar und heißt **inverse Element** zu $[a]_n$. Invertierbare Elemente werden auch **Einheiten** genannt.

(2) Es ist klar, dass $[1]_n$ und $[-1]_n$ invertierbar in $\mathbb{Z}/n\mathbb{Z}$ sind, da

$$[1]_n \cdot [1]_n = [1]_n \quad \text{und} \quad [-1]_n \cdot [-1]_n = [1]_n.$$

(3) Für $n \geq 2$ ist $[0]_n$ NIE invertierbar in $\mathbb{Z}/n\mathbb{Z}$, da $[0]_n \cdot [a]_n = [0]_n \neq [1]_n$ für alle $[a]_n \in \mathbb{Z}/n\mathbb{Z}$.

(4) ⚠ Der Fall $n = 1$ ist komplizierter: Hier gilt $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\}$ und das ist der Nullring. Nichtsdestotrotz gilt $[0]_1 = [1]_1$ (neutrales Element bzgl. Addition = neutrales Element bzgl. Multiplikation), sodass $[0]_1$ invertierbar ist. Es ist also besser zu schreiben, dass $\mathbb{Z}/1\mathbb{Z} = \{[1]_1\}$.

Beispiel 3.8 (Invertierbare Elemente von $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/5\mathbb{Z}$)

- (1) Für $n = 3$ ist $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$ und nach Anmerkung 3.7(2),(4) sind die Invertierbare Elemente von $\mathbb{Z}/3\mathbb{Z}$ genau $[1]_3$ und $[2]_3 = [-1]_3$.
- (2) Für $n = 4$ ist $\mathbb{Z}/4\mathbb{Z} = \{[0]_4, [1]_4, [2]_4, [3]_4\}$.
Die Invertierbare Elemente von $\mathbb{Z}/4\mathbb{Z}$ sind genau $[1]_4$ und $[3]_4 = [-1]_4$.
Hier ist $[2]_4$ nicht invertierbar, da es kein Element $[b]_4 \in \mathbb{Z}/4\mathbb{Z}$ mit $[2]_4 \cdot [b]_4 = [1]_4$ gibt!
($[2]_4 \cdot [0]_4 = [0]_4$, $[2]_4 \cdot [1]_4 = [2]_4$, $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$ und $[2]_4 \cdot [3]_4 = [6]_4 = [2]_4$)
- (3) Für $n = 5$ sind $[1]_5$ und $[-1]_5 = [4]_5$ invertierbar in $\mathbb{Z}/5\mathbb{Z}$ nach (*).
Zudem gilt $[2]_5 \cdot [3]_5 = [6]_5 = [1]_5$, sodass $[2]_5$ und $[3]_5$ auch invertierbar in $\mathbb{Z}/5\mathbb{Z}$ sind.

Definition 3.9

Sei $n \in \mathbb{N}_{\geq 2}$.

- (a) Wir bezeichnen die Menge aller invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ mit $(\mathbb{Z}/n\mathbb{Z})^\times$.
- (b) Ein Element von $(\mathbb{Z}/n\mathbb{Z})^\times$ heisst **prime Restklasse modulo n** (oder **Einheit** von $\mathbb{Z}/n\mathbb{Z}$).
- (c) Das inverse Element zu $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ wird mit $[a]_n^{-1}$ bezeichnet. (Klar: $[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$.)

Anmerkung 3.10

Die Menge $(\mathbb{Z}/n\mathbb{Z})^\times$ zusammen mit der Multiplikation der Restklassen bildet eigentlich eine Gruppe, die **Einheitengruppe** von $\mathbb{Z}/n\mathbb{Z}$ heisst.

Satz 3.11

Seien $n \in \mathbb{N}_{\geq 2}$ und $a \in \mathbb{Z}$. Dann gilt:

$$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \text{ggT}(a, n) = 1.$$

Anders formuliert ist

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(a, n) = 1\}.$$

Beweis:

\Rightarrow : Sei $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Dann existiert $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ mit

$$[1]_n = [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Somit gilt $n \mid 1 - ab$ und daher existiert $s \in \mathbb{Z}$ mit $n \cdot s = 1 - a \cdot b$.

Nun, ist $d \in \mathbb{Z}$ ein gemeinsamer Teiler von a und n , so gilt $d \mid a \cdot b + n \cdot s = 1$, d.h. $\text{ggT}(a, n) = 1$.

\Leftarrow : Wir nehmen nun an, dass $\text{ggT}(a, n) = 1$ ist. Nach dem Euklidischen Algorithmus existieren Bézout-Koeffizienten $r, s \in \mathbb{Z}$ mit

$$1 = \text{ggT}(a, n) = s \cdot a + r \cdot n.$$

Somit ist $1 - s \cdot a = r \cdot n$ und $n \mid 1 - s \cdot a$. Daher ist

$$[1]_n = [s \cdot a]_n = [s]_n \cdot [a]_n$$

und $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. ■

Satz 3.12

Ist $n \in \mathbb{N}_{\geq 2}$, so gilt:

$$\mathbb{Z}/n\mathbb{Z} \text{ ist ein Körper} \iff n \text{ ist eine Primzahl.}$$

Beweis: Wir wissen bereits, dass $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring ist. Somit gilt:

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \text{ Körper} &\iff [a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \forall [a]_n \in \mathbb{Z}/n\mathbb{Z} \setminus \{[0]_n\} \\ &\stackrel{(3.11)}{\iff} \text{ggT}(a, n) = 1 \forall a = 1, \dots, n-1 \\ &\iff n \text{ Primzahl.} \end{aligned}$$

■

Anmerkung 3.13

Der Beweis von Satz 3.11 liefert, dass die inverse Restklasse durch Bézout-Koeffizienten bestimmt sind. D.h.: Diese können mit dem erweiterten Euklidischen Algorithmus berechnet werden.

Beispiel 3.14

Wir möchten nachprüfen, dass $[390]_{527}$ invertierbar in $\mathbb{Z}/527\mathbb{Z}$ ist und $[390]_{527}^{-1}$ berechnen.

Der Euklidische Algorithmus liefert:

$$\begin{aligned} 527 &= 1 \cdot 390 + 137 \\ 390 &= 2 \cdot 137 + 116 \\ 137 &= 1 \cdot 116 + 21 \\ 116 &= 5 \cdot 21 + 11 \\ 21 &= 1 \cdot 11 + 10 \\ 11 &= 1 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 + 0 \end{aligned}$$

Somit ist $\text{ggT}(527, 390) = 1$ und $[390]_{527} \in (\mathbb{Z}/527\mathbb{Z})^\times$ nach Satz 3.11.

Als Nächstes berechnen wir Bézout-Koeffizienten mithilfe des erweiterten Algorithmus:

i	r_i	q_i	s_i	t_i
0	527	–	1	0
1	390	1	0	1
2	137	2	1	-1
3	116	1	-2	3
4	21	5	3	-4
5	11	1	-17	23
6	10	1	20	-27
7	1	10	-37	50
8	0	–	–	–

Somit gilt $1 = \text{ggT}(527, 390) = (-37) \cdot 527 + 50 \cdot 390$

$$\implies [1]_{527} = [-37]_{527} \cdot [527]_{527} + [50]_{527} \cdot [390]_{527} = [50]_{527} \cdot [390]_{527} \quad \text{in } \mathbb{Z}/527\mathbb{Z}$$

und die inverse Restklasse ist also $[390]_{527}^{-1} = [50]_{527}$.

7 Der Chinesische Restsatz

Ziel: Beschreibung aller Lösungen eines Systems von $k \in \mathbb{N}$ Kongruenzgleichungen der Form

$$\begin{cases} x \equiv b_1 & (\text{mod } n_1) \\ x \equiv b_2 & (\text{mod } n_2) \\ \vdots \\ x \equiv b_k & (\text{mod } n_k) \end{cases}$$

mit $b_1, \dots, b_k \in \mathbb{Z}$ und mit $n_1, \dots, n_k \in \mathbb{N}_{\geq 2}$ paarweise teilerfremd.

Satz 3.15 (*Chinesische Restsatz — Kongruenzgleichungen-Version*)

Sei $k \in \mathbb{N}$ und seien $n_1, \dots, n_k \in \mathbb{N}_{\geq 2}$ paarweise teilerfremd.
Sind $b_1, \dots, b_k \in \mathbb{Z}$, so besitzt das System von Kongruenzgleichungen

$$\begin{cases} x \equiv b_1 & (\text{mod } n_1) \\ x \equiv b_2 & (\text{mod } n_2) \\ \vdots \\ x \equiv b_k & (\text{mod } n_k) \end{cases}$$

eine Lösung $x \in \mathbb{Z}$. Diese Lösung ist eindeutig bestimmt modulo $N := \prod_{i=1}^k n_i$ und die Menge aller Lösungen ist $[x]_N = x + N\mathbb{Z}$.

Satz 3.16 (*Chinesische Restsatz — Ring-Version*)

Seien k, n_1, \dots, n_k, N wie in Satz 3.15. Dann ist die Abbildung

$$\begin{aligned} \Psi: \mathbb{Z}/N\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ [a]_N &\mapsto ([a]_{n_1}, \dots, [a]_{n_k}) \end{aligned}$$

ist ein Isomorphismus von Ringen.

Folgerung 3.17

Die Einschränkung

$$\begin{aligned} \Psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}: (\mathbb{Z}/N\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/n_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/n_k\mathbb{Z})^\times \\ [a]_N &\mapsto ([a]_{n_1}, \dots, [a]_{n_k}) \end{aligned}$$

der Abbildung Ψ aus Satz 3.16 auf die Einheitengruppe von $\mathbb{Z}/N\mathbb{Z}$ ist ein Isomorphismus von Gruppen.

Beweis von 3.15, 3.16 und 3.17: Wir beweisen die drei Aussagen zusammen.

(3.15): Eindeutigkeit: Seien $x, y \in \mathbb{Z}$ zwei Lösungen vom System. Somit gilt

$$n_j \mid x - b_j \text{ und } n_j \mid y - b_j \quad \forall 1 \leq j \leq k,$$

sodass

$$n_j \mid (x - b_j) - (y - b_j) = x - y \quad \forall 1 \leq j \leq k$$

und es gilt $N = \prod_{j=1}^k n_j \mid x - y$, d.h. $x \equiv y \pmod{N}$.

Existenz: Wir geben hier ein konkretes Verfahren zur Berechnung einer Lösung an.

Für $j = 1, \dots, k$ setze $n'_j := \frac{N}{n_j} \implies \text{ggT}(n'_j, n_j) = 1$ für alle $j = 1, \dots, k$. Somit existieren Bézout-Koeffizienten r'_j, r_j mit

$$1 = \text{ggT}(n'_j, n_j) = r_j n_j + r'_j n'_j \quad \forall 1 \leq j \leq k$$

und $[r'_j]_{n_j} = [n'_j]_{n_j}^{-1}$ in $\mathbb{Z}/n_j\mathbb{Z}$.

Wir behaupten, dass

$$x := \sum_{j=1}^k b_j r'_j n'_j$$

eine Lösung vom System ist.

Sei also $\ell \in \{1, \dots, k\}$ fest. Für all $1 \leq j \neq \ell \leq k$ gilt $b_j r'_j n'_j \equiv 0 \pmod{n_\ell}$, da $n_\ell \mid n'_j$. Damit hat die Summe $x = \sum_{j=1}^k b_j r'_j n'_j$ modulo n_ℓ nur einen Summanden ungleich Null. Genauer ist $x \equiv b_\ell r'_\ell n'_\ell \pmod{n_\ell}$. Aber

$$x \equiv b_\ell r'_\ell n'_\ell = b_\ell(1 - r_\ell n_\ell) \equiv b_\ell \pmod{n_\ell}.$$

(3.16): (1) Zunächst ist es klar, dass Ψ ein Homomorphismus von Ringen ist, da das direkte Produkt von Ringen komponentenweise Addition und Multiplikation hat.

(2) Ψ ist wohldefiniert: Seien $a, a' \in \mathbb{Z}$. Dann:

$$\begin{aligned} [a]_N = [a']_N &\implies N \mid a - a' \implies n_j \mid a - a' \quad \forall 1 \leq j \leq k \\ &\implies [a]_{n_j} = [a']_{n_j} \quad \forall 1 \leq j \leq k \\ &\implies \Psi([a]_N) = \Psi([a']_N). \end{aligned}$$

(3) Ψ ist surjektiv: Sei $([b_1]_{n_1}, \dots, [b_k]_{n_k}) \in \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ ein beliebiges Element. Nach Satz 3.15 existiert $x \in \mathbb{Z}$ mit

$$x \equiv b_1 \pmod{n_1}, \dots, x \equiv b_k \pmod{n_k}$$

und somit gilt $\Psi([x]_N) = ([b_1]_{n_1}, \dots, [b_k]_{n_k})$.

(4) Ψ ist injektiv: Die Injektivität folgt aus der Surjektivität, weil die Mengen $\mathbb{Z}/N\mathbb{Z}$ und $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ endlich mit derselben Anzahl von Elementen sind:

$$|\mathbb{Z}/N\mathbb{Z}| = N = \prod_{j=1}^k n_j = \prod_{j=1}^k |\mathbb{Z}/n_j\mathbb{Z}| = |\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}|.$$

(3.17): Zunächst behaupten wir, dass das Bild von $\Psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}$ genau $(\mathbb{Z}/n_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/n_k\mathbb{Z})^\times$ ist. Dies ist klar:

$$\begin{aligned} [a]_N \in (\mathbb{Z}/N\mathbb{Z})^\times &\stackrel{(3.11)}{\iff} \text{ggT}(a, N) = 1 \\ &\iff \text{ggT}(a, n_i) = 1 \quad \forall 1 \leq i \leq k \\ &\stackrel{(3.11)}{\iff} [a]_{n_i} \in (\mathbb{Z}/n_i\mathbb{Z})^\times \quad \forall 1 \leq i \leq k. \end{aligned}$$

Somit ist $\Psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}$ surjektiv und $\Psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}$ ist auch injektiv, da Ψ injektiv ist. Außerdem ist $\Psi|_{(\mathbb{Z}/N\mathbb{Z})^\times}$ ein Homomorphismus von Gruppen, da Ψ ein Homomorphismus von Ringen ist und somit wird die Multiplikation respektiert. ■

8 Die eulersche φ -Funktion

Die eulersche φ -Funktion beantwortet die Frage „Wie viele invertierbare Elemente gibt es in $\mathbb{Z}/n\mathbb{Z}$?“

Definition 3.18 (eulersche φ -Funktion)

Die eulersche φ -Funktion ist die arithmetische Funktion

$$\begin{aligned}\varphi: \mathbb{N} &\longrightarrow \mathbb{N} \\ m &\longmapsto \#\{d \in \mathbb{Z} \mid 1 \leq d \leq m \text{ und } \text{ggT}(d, m) = 1\}.\end{aligned}$$

Beispiel 3.19

Zum Beispiel nimmt die eulersche φ -Funktion für $1 \leq m \leq 12$ die folgenden Werte an:

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

Satz 3.20 (Eigenschaften der Eulerschen φ -Funktion)

- (a) Ist $m \in \mathbb{N}$, so ist $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$.
- (b) Die eulersche φ -Funktion ist multiplikativ, d.h. $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2) \quad \forall m_1, m_2 \in \mathbb{N}$ mit $\text{ggT}(m_1, m_2) = 1$.
- (c) Ist p eine Primzahl und $n \in \mathbb{N}$, so gilt $\varphi(p^n) = p^n - p^{n-1}$.
- (d) Für $m \in \mathbb{N}_{\geq 2}$ mit Primfaktorzerlegung $m = \prod_{i=1}^k p_i^{n_i}$ gilt

$$\varphi(m) = \prod_{i=1}^k (p_i^{n_i} - p_i^{n_i-1}) = \prod_{i=1}^k p_i^{n_i-1} \cdot (p_i - 1).$$

Beweis:

- (a) Für $m \geq 2$ ist die Behauptung es klar aus der Definition von φ und Satz 3.11.
Für $m \geq 1$ ist $(\mathbb{Z}/1\mathbb{Z})^\times = \{[1]_1\}$ nach Anmerkung 3.7(4) und somit gilt $\varphi(1) := |(\mathbb{Z}/1\mathbb{Z})^\times|$.
- (b) Die Folgerung zum Chinesischen Restsatz liefert einen Gruppenisomorphismus

$$(\mathbb{Z}/(m_1 m_2)\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times.$$

Damit folgt aus (a), dass

$$\varphi(m_1 m_2) = |(\mathbb{Z}/(m_1 m_2)\mathbb{Z})^\times| = |(\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times| = |(\mathbb{Z}/m_1\mathbb{Z})^\times| \cdot |(\mathbb{Z}/m_2\mathbb{Z})^\times| = \varphi(m_1) \cdot \varphi(m_2).$$

- (c) Wir betrachten den Gruppenhomomorphismus $f: (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times: [a]_{p^n} \mapsto [a]_p$. Dieser ist offensichtlich surjektiv mit Kern $\ker(f) = \{(1 + px) + p^n\mathbb{Z} \mid 0 \leq x < p^{n-1}\}$. Nun folgt aus dem Homomorphiesatz, dass

$$\varphi(p^n) \stackrel{(a)}{=} |(\mathbb{Z}/p^n\mathbb{Z})^\times| = |\ker(f)| \cdot |\text{Im}(f)| = p^{n-1} \cdot (p - 1) = p^n - p^{n-1}$$

ist.

(d) Es gilt:

$$\varphi(m) = \varphi\left(\prod_{i=1}^k p_i^{n_i}\right) \stackrel{(b)}{=} \prod_{i=1}^k \varphi(p_i^{n_i}) \stackrel{(c)}{=} \prod_{i=1}^k (p_i^{n_i} - p_i^{n_i-1}).$$

Beispiel 3.21

Eine Anwendung von Satz 3.20 liefert z. B.:

(a) Für $n = 12 = 3 \cdot 4$ ist $\varphi(12) = \varphi(3)\varphi(4) = (3^1 - 3^0) \cdot (2^2 - 2^1) = 2 \cdot 2 = 4$.

(b) Für $n = 30 = 2 \cdot 3 \cdot 5$ ist $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = (2^1 - 2^0) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0) = 1 \cdot 2 \cdot 4 = 8$.
In der Tat sind genau folgende acht Zahlen zwischen 1 und 30 prim zu 30:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Satz 3.22 (Satz von Euler)

Für alle $a, n \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$ gilt

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

Der Beweis des Satzes von Euler ist eine Anwendung des Satzes von Lagrange.

Beweis: Wegen $\text{ggT}(a, n) = 1$ ist also $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ (d.h. invertierbar). Nach Satz ??(a) ist $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ und aus dem Satz von Lagrange folgt

$$[1] = [a]^{|(\mathbb{Z}/n\mathbb{Z})^\times|} = [a]^{\varphi(n)} = [a^{\varphi(n)}] \in (\mathbb{Z}/n\mathbb{Z})^\times,$$

d.h.

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

Beispiel 3.23

Wir überlegen uns nun, wie lineare Kongruenzen mit dem Satz von Euler gelöst werden können. Sei dazu $ax \equiv b \pmod{n}$ mit $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ und $\text{ggT}(a, n) = 1$ gegeben. Damit ist $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ und es gilt

$$[x] = [b] \cdot [a]^{-1} = [b] \cdot [1] \cdot [a]^{-1} = [b] \cdot [a]^{\varphi(n)} \cdot [a]^{-1} = [b] \cdot [a]^{\varphi(n)-1} \in \mathbb{Z}/n\mathbb{Z}$$

nach dem Satz von Euler, da $a^{\varphi(n)} \equiv 1 \pmod{n}$. Somit ist $x = ba^{\varphi(n)-1}$ eine Lösung der Kongruenz $ax \equiv b \pmod{n}$.

Z.B.: Löse $5x \equiv 4 \pmod{12}$. Hier ist $\varphi(12) = 4$ und damit ist

$$x = 4 \cdot 5^3 = 4 \cdot 125 = 500$$

eine Lösung. Wegen $500 = 41 \cdot 12 + 8 \equiv 8 \pmod{12}$ ist auch $x = 8$ eine Lösung:

$$5 \cdot 8 = 40 \equiv 4 \pmod{12}.$$

Folgerung 3.24 (kleiner Satz von Fermat)

Sei $k \in \mathbb{Z}_{>0}$ eine positive ganze Zahl.

(1) Ist $p \in \mathbb{P}$ und $p \nmid k$, so gilt $k^{p-1} \equiv 1 \pmod{p}$.

(2) Ist $p \in \mathbb{P}$ und $p \mid k$, so gilt $k^p \equiv 0 \equiv k \pmod{p}$.

Zusammengefasst: für alle $k \in \mathbb{Z}_{>0}$ und alle Primzahlen $p \in \mathbb{P}$ gilt:

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

Beweis:

(2) ist klar.

(1) ist ein Spezialfall des Satzes von Euler, weil $\text{ggT}(k, p) = 1$. Es gilt also

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

und multiplizieren mit k liefert

$$k^p \equiv k \pmod{p}.$$

■

Anmerkung 3.25

Das vorstehende Resultat liefert also eine notwendige Bedingung dafür, dass eine positive Zahl p prim ist. Dies führt zu folgendem einfachen **Primzahltest**:

Für $n \in \mathbb{Z}_{>0}$ teste, ob $k^{n-1} \equiv 1 \pmod{n}$ für alle $k < n$.

· Falls dies nicht der Fall ist, so ist n keine Primzahl.

· Falls doch, so ist n entweder eine Primzahl oder eine sogenannte Carmichael-Zahl:

Eine zusammengesetzte natürliche Zahl n heißt **Carmichael-Zahl**, falls für alle zu n teilerfremden Zahlen a gilt: $a^{n-1} \equiv 1 \pmod{n}$.

Beispiel 3.26

Wir können z.B. den Satz von Euler, wie folgt anwenden:

(1) **Was ist der Rest bei Division mit Rest von 3^{4010} durch 2500?**

Zuerst berechnen wir

$$\varphi(2500) = \varphi(2^2 \cdot 5^4) = 2^{2-1}(2-1) \cdot 5^{4-1}(5-1) = 2 \cdot 1 \cdot 5^3 \cdot 4 = 1000$$

und der Satz von Euler liefert $3^{1000} = 3^{\varphi(2500)} \equiv 1 \pmod{2500}$. Somit gilt

$$3^{4010} = (3^{1000})^4 \cdot 3^{10} \equiv 1^4 \cdot 3^{10} = 3^5 \cdot 3^5 \equiv 243 \cdot 243 = 59049 \equiv 1549 \pmod{2500}.$$

(2) **Was sind die beiden letzten Ziffern der Dezimaldarstellung von 7^{22} ?**

Wir müssen hier modulo 100 rechnen. Zunächst gilt

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^{2-1}(2-1) \cdot 5^{2-1}(5-1) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$$

und somit liefert der Satz von Euler, dass $7^{40} = 7^{\varphi(100)} \equiv 1 \pmod{100}$. Wir berechnen damit:

$$7^{222} = (7^4)^5 \cdot 7^2 \equiv 1^5 \cdot 7^2 = (7^4)^5 \cdot 7^2 = 2401^5 \cdot 49 \equiv 1 \cdot 49 \pmod{100}$$

und die Antwort lautet 49.

9 Aufgaben zu Kapitel 3

Aufgabe 13

Beantworten Sie die folgenden Fragen mithilfe der modularen Arithmetik.

- (1) Welcher Rest bleibt bei Division mit Rest von $(16^{123} + 5^{2422}) \cdot 11^{4533}$ durch 12?
- (2) Welcher Rest bleibt bei Division mit Rest von $5^7 \cdot 7^3 + 4^4$ durch 9?

Aufgabe 14

Zeigen Sie mithilfe der modularen Arithmetik:

- (1) für jede natürliche Zahl n ist die Zahl $2^{n+4} + 3^{3n+2}$ durch 25 teilbar.
- (2) für jede natürliche Zahl n ist $n^2 + 5n + 8$ gerade.

Aufgabe 15

Beantworten Sie die folgenden Fragen mithilfe der modularen Arithmetik.

- (1) Kann die Dezimaldarstellung des Quadrats einer natürlichen Zahl auf 2 enden? Und auf 8?
- (2) Sei $a \in \mathbb{N}$ eine natürliche Zahl. Auf welche natürlichen Zahlen kann die Dezimaldarstellung der Zahl $a^2 - 2a$ enden?

Aufgabe 16

Sei $a \in \mathbb{N}$ eine natürliche Zahl mit Dezimaldarstellung $a = a_r a_{r-1} \dots a_1 a_0$ (d.h. mit $r \in \mathbb{N}_0$, mit $a_0, a_1, \dots, a_r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ und mit $a_r \neq 0$). Dann heißt

$$Q_2(a) := \begin{cases} (a_1 a_0) + (a_3 a_2) + \dots + (a_r a_{r-1}) & \text{für } r \text{ ungerade,} \\ (a_1 a_0) + (a_3 a_2) + \dots + (0 a_r) & \text{für } r \text{ gerade,} \end{cases}$$

die **Quersumme zweiter Stufe** von a . Finden Sie Teilbarkeitsregeln für die Teilbarkeit durch 99 mithilfe von Q_2 . Finden Sie Teilbarkeitsregeln für die Teilbarkeit durch 101.

Aufgabe 17

- (1) Entscheiden Sie, ob die Restklasse $[91]_{143}$ in $\mathbb{Z}/143\mathbb{Z}$ invertierbar ist.
- (2) Berechnen Sie mithilfe des erweiterten Euklidischen Algorithmus die inverse Restklasse von $[19]_{35}$ in $\mathbb{Z}/35\mathbb{Z}$.

Aufgabe 18

Finden Sie alle invertierbare Elemente vom Ring $\mathbb{Z}/20\mathbb{Z}$ mithilfe des Chinesischen Restsatzes.

Aufgabe 19

Finden Sie alle Lösungen vom folgenden System von Kongruenzgleichungen:

$$\begin{cases} x \equiv 23 \pmod{6} \\ x \equiv 7 \pmod{5} \\ x \equiv 9 \pmod{7} \end{cases}$$

Aufgabe 20

- (1) Bestimmen Sie $\varphi(999)$.
- (2) Zeigen Sie: Für alle $n \in \mathbb{N}$ gilt $\varphi(10^n) = 4 \cdot 10^{n-1}$.
- (3) Bestimmen Sie die letzten vier Ziffern der Dezimaldarstellung von 3^{24008} mithilfe des Satzes von Euler.
- (4) Sei p eine Primzahl. Zeigen Sie:
 $2p + 1$ ist genau dann eine Primzahl, wenn es eine natürliche Zahl $n \in \mathbb{N}$ mit $\varphi(n) = 2p$ existiert.

Aufgabe 21

Entscheiden Sie, ob die folgenden Aussagen wahr oder falsch sind? Begründen Sie Ihre Antworten mit einem Gegenbeispiel oder mit einem Beweis.

- (i) Für alle $n \geq 3$ ist $\varphi(n)$ gerade.
- (ii) Es gibt eine Zahl $n \in \mathbb{N}$ mit $\varphi(n) = 14$.
- (iii) Sind $m, n \in \mathbb{N}$ mit $m \mid n$, so gilt $\varphi(m) \mid \varphi(n)$.

Die Eulersche φ -Funktion bildet die Grundlage für eines der bekanntesten und meistbenutzten Kryptosysteme: das **RSA-Verfahren**. Es wurde 1977/78 von R. Rivest, A. Shamir und L. Adleman am MIT entwickelt.

10 Das Prinzip

Wir betrachten das folgende Problem:

Problem 4.1

Bob (der Sender) will Alice (der Empfänger) eine Nachricht schicken, ohne dass ein Abfänger diese lesen oder unbemerkt verändern kann, falls er die Nachricht abfängt.

Die Lösung ist, die Nachricht zu verschlüsseln. Genauer: im RSA-Verfahren besteht die Verschlüsselung aus zwei Schlüsseln:

- einem öffentlichen, und
- einem privaten Schlüssel.

Mit dem öffentlichen Schlüssel kann man Nachrichten verschlüsseln, aber nicht entschlüsseln. Deshalb wird dieser Schlüssel öffentlich zur Verfügung gestellt, z. B. im Internet. Hier kann den Schlüssel dann jeder benutzen, um Nachrichten zu verschlüsseln, die aber nur der Empfänger (= derjenige, der den öffentlichen Schlüssel anbietet) wieder entschlüsseln kann. Zum Entschlüsseln braucht man den privaten Schlüssel, und den kennt nur der Empfänger.

11 Das RSA-Verfahren: Mathematische Idee

Das RSA-Verfahren basiert auf der folgenden mathematischen Aussage:

Satz 4.2

Seien $p, q \in \mathbb{P}$ zwei verschiedene Primzahlen und setze $N := p \cdot q$. Ferner seien $e, d \in \mathbb{Z}$ mit $0 < e, d < N$, $\text{ggT}(e, \varphi(N)) = 1$ und $d \cdot e \equiv 1 \pmod{\varphi(N)}$. Dann gilt für jedes $m \in \mathbb{Z}$ mit $0 < m < N$, dass

$$(m^e)^d \equiv m \pmod{N}$$

ist.

Beweis: Zunächst folgt aus $d \cdot e \equiv 1 \pmod{\varphi(N)}$, dass es $k \in \mathbb{Z}$ mit $1 = de + k\varphi(N)$ existiert. Somit ist

$$(m^e)^d = m^{1-k\varphi(N)} = m \cdot (m^{\varphi(N)})^{-k}.$$

Wegen $m < N = p \cdot q$ gilt $\text{ggT}(m, N) \in \{1, p, q\}$, sodass wir drei Fälle unterscheiden können.

1. Fall: $\text{ggT}(m, N) = 1$.

Wegen $\text{ggT}(m, N) = 1$ folgt aus dem Satz von Euler, dass

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

Also ist

$$(m^e)^d = m \cdot (m^{\varphi(N)})^{-k} \equiv m \cdot 1^{-k} = m \cdot 1 = m \pmod{N}.$$

2. Fall: $\text{ggT}(m, N) = p$. Wir benutzen hier den Chinesischen Restsatz. Zunächst impliziert $m \equiv 0 \pmod{p}$, dass

$$m^{ed} \equiv 0 \equiv m \pmod{p}$$

ist. Wegen $\text{ggT}(m, N) = p$ gilt $q \nmid m$ und es folgt aus dem Satz von Euler, dass

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

ist. Aus $\varphi(N) = (p-1)(q-1)$ folgt dann

$$m^{ed} = m \cdot (m^{\varphi(N)})^{-k} = m \cdot (m^{(q-1)})^{-k(p-1)} \equiv m \cdot 1 = m \pmod{q}.$$

Mit dem Chinesischen Restsatz erhalten wir also $m^{ed} \equiv m \pmod{p \cdot q}$, d.h. modulo N , wie behauptet.

3. Fall: $\text{ggT}(m, N) = q$. Analog zum 2. Fall! ■

12 Das RSA-Verfahren in der Praxis

Das RSA-Verfahren.

1. Schritt: Erzeugung des öffentlichen Schlüssels. (Alice)

1a. Eine Schranke N ermitteln:

Wähle $p \neq q \in \mathbb{P}$ zwei (sehr große) Primzahlen;

Setze $N := p \cdot q$.

1b. Eine Zahl e ermitteln:

Berechne $\varphi(N) = (p-1) \cdot (q-1)$;

Wähle eine beliebige Zahl $1 < e < \varphi(N)$ mit $\text{ggT}(e, \varphi(N)) = 1$.

Der **öffentliche Schlüssel** ist dann das 2-Tupel (e, N) . Dieser wird (von Alice) veröffentlicht (z.B. im Internet). (⚠ Die Primzahlen p und q müssen geheim bleiben.)

2. Schritt: Erzeugung des privaten Schlüssels (Alice)

2a. Berechne mit Hilfe des euklidischen Algorithmus eine Zahl d mit

$$e \cdot d \equiv 1 \pmod{\varphi(N)}.$$

Der **private Schlüssel** ist dann das 2-Tupel (d, N) . Dieser muss geheim bleiben.

3. Schritt: Nachricht verschlüsseln. (Bob mit dem öffentlichen Schlüssel (e, N))

3a. Die Nachricht $1 < m < N$ wird mit ihrer Restklasse $[m] \in \mathbb{Z}/N\mathbb{Z}$ identifiziert.

3b. Die Nachricht wird durch

$$s := m^e \pmod{N}$$

verschlüsselt.

Dieses s schickt Bob dann an Alice.

4. Schritt: Nachricht entschlüsseln. (Alice mit dem privaten Schlüssel (d, N))

4a. Die Nachricht wird nach Konstruktion von d durch

$$m := s^d \pmod{N}$$

entschlüsselt.

Beispiel 4.3

Sei $p = 47$ und $q = 71$. Somit ist $N = p \cdot q = 3337$ und $\varphi(N) = (p - 1)(q - 1) = 46 \cdot 70 = 3220$. Abhängig von $\varphi(N)$ wird eine zufällige Zahl e mit $\varphi(N) > e > 1$ gewählt, wobei $\text{ggT}(e, \varphi(N)) = 1$ sein muss. Wir wählen zum Beispiel

$$e = 79.$$

Aus e und $\varphi(N)$ können wir nun d mit dem euklidischen Algorithmus ausrechnen:

$$de \equiv 1 \pmod{\varphi(N)} \iff [d]_{3220} = [e]_{3220} = [79]_{3220} \iff d \equiv 1019 \pmod{3220}.$$

Somit haben wir die beiden Schlüssel:

Der öffentliche Schlüssel $= (e, N) = (79, 3337)$; und

der private Schlüssel $= (d, N) = (1019, 3337)$.

Bob kann nun seine Nachricht

$$m = 688$$

verschlüsseln und Alice schicken:

$$s = m^e = 688^{79} \equiv 1570 \pmod{3337}.$$

Alice kann dann dieses Chiffretext entschlüsseln. Dafür verwendet sie den privaten Schlüssel und sie bekommt:

$$m \equiv s^d \pmod{N} \equiv 1570^{1019} \pmod{3337} \equiv 688 \pmod{3337}$$

Anmerkung 4.4

(a) Das RSA-Verfahren verschlüsselt und entschlüsselt nur Zahlen in Zahlen, daher muss erst der Klartext mit einem öffentlich bekannten Alphabet in eine Zahlenfolge (numerical Encoding) übersetzt werden.

(b) **Beispiele von Anwendungsgebieten:**

- Internet- und Telefonie-Infrastruktur: X.509-Zertifikate
- E-Mail-Verschlüsselung: OpenPGP, S/MIME
- Authentifizierung SIM-Karten
- Kartenzahlung: EMV
- RFID Chip auf dem deutschen Reisepass
- Electronic Banking: HBCI
- Übertragungs-Protokolle: IPsec, TLS, SSH, WASTE

13 Das RSA-Verfahren: Sicherheit und Sicherheitslücken

Die Sicherheit des RSA-Verfahrens beruht auf dem Problem, Zahlen der Form $N = pq$ mit $p, q \in \mathbb{P}$ zu faktorisieren. Bisher hat es noch keiner geschafft, diese Zahlen effektiv und schnell zu zerlegen. Deswegen ist es wichtig *große* Primzahlen $p, q \in \mathbb{P}$ zu wählen. Selbst mit einem Computer braucht man in der Praxis bis zu einem Jahr, falls $pq \lesssim 10^{150}$ gilt. Für $pq \simeq 10^{300}$ würde ein Abfänger viele tausend Jahre und viele tausend Computer benötigen, um die Faktorisierung zu erreichen.

Problem/Nachteil: Es ist aber auch nicht bewiesen, dass es sich bei der Primfaktorzerlegung von $N = pq$ um ein prinzipiell schwieriges Problem handelt!

Satz 4.5 (Sicherheit des RSA-Verfahrens)

Seien $p, q \in \mathbb{P}$ zwei verschiedene Primzahlen und setze $N := p \cdot q$. Dann sind die folgenden Aussagen äquivalent:

- (i) N und $\varphi(N)$ sind bekannt; und
- (ii) p und q sind bekannt.

Beweis:

(i) \Rightarrow (ii): Es gilt

$$\varphi(N) = (p-1) \cdot (q-1) = p \cdot q - (p+q) + 1 = (N+1) - (p+q).$$

Somit ist $(p+q) = N+1-\varphi(N)$ bekannt, da N und $\varphi(N)$ bekannt sind. Daher ist auch das Polynom $X^2 - (p+q)X + N \in \mathbb{Z}[X]$ bekannt. Aber p und q sind die Nullstellen von diesem Polynom, da

$$X^2 - (p+q)X + N = (X-p) \cdot (X-q)$$

ist. Diese lassen sich leicht berechnen! D.h. mit den üblichen Formeln.

(ii) \Rightarrow (i): Wenn p und q bekannt sind, so sind offensichtlich auch $N = p \cdot q$ und $\varphi(N) = (p-1) \cdot (q-1)$. ■

Anmerkung 4.6

Der folgende Algorithmus zeigt, dass es extrem wichtig ist, dass die Zahl d geheim bleibt. Wenn ein Abfänger die Zahl d besitzt, so kann er N faktorisieren und Nachrichten entschlüsseln bzw. verändern. (Siehe Aufgabe 1 auf Blatt 7.)

Algorithmus 1 Faktorisierung des Modulus N unter Benutzung von e und d

```

1: Input: Modulus  $N$ , privater Schlüssel  $(d, N)$ , öffentlicher Schlüssel  $(e, N)$ .
2: Output: Primzahlen  $p$  und  $q$  mit  $N = pq$ .
3: Berechne  $k := ed - 1$ .
4: Entferne gerade Faktoren:  $k = 2^s \cdot t$  mit  $t$  ungerade.
5: Setze  $a := 2$ .
6: while true do
7:    $b = a^t \bmod N$ 
8:   for  $\ell$  in  $0 : s$  do
9:     Berechne  $p = \text{ggT}(b^{2^\ell}, N)$ 
10:    if  $1 < p$  und  $p$  ist prim then
11:      return  $p$  und  $q = N/p$ 
12:    else
13:      Wähle neues  $a \in \mathbb{Z}/N\mathbb{Z}$  zufällig.
14:    end if
15:  end for
16: end while
```

14 Aufgaben zu Kapitel 4

Aufgabe 22

Sei $m \in \mathbb{N}$ eine Nachricht. Wir benutzen RSA, um m mehrmals unabhängig zu verschlüsseln mit jeweils verschiedenen öffentlichen Schlüsseln. Wir verschlüsseln m einmal mit $(e_1, N_1) = (3, 391)$ und erhalten 208. Des Weiteren verschlüsseln wir m mit $(e_2, N_2) = (3, 55)$ und bekommen 38 und schließlich einmal mit $(e_3, N_3) = (3, 87)$ mit dem Ergebnis 32. Berechnen Sie die Nachricht, ohne zu faktorisieren.

Aufgabe 23

Was passiert, wenn wir das RSA-Verfahren mit drei statt zwei Primfaktoren durchführen, d.h. $N = pqr$ mit paarweise verschiedenen Primzahlen p, q und r . Beschreiben Sie, ob und wie sich folgende Schritte dadurch verändern:

- Generierung des öffentlichen Schlüssels,
- Generierung des privaten Schlüssels,
- Verschlüsselung der Nachricht,
- Entschlüsselung einer empfangenen Nachricht.

Ist es vorteilhaft, drei Primfaktoren zu verwenden?

Das Rabin-Kryptosystem ist ein weiteres Verfahren der Public-Key-Kryptographie, das Ähnlichkeiten mit dem RSA-Verfahren hat. Die Vorteile und Nachteile sind die folgenden.

VORTEILE:

Es lässt sich beweisen, dass das Brechen des Verfahrens äquivalent zur Faktorisierung ist großer Zahlen $N = p \cdot q$ ist.

NACHTEILE: Die Entschlüsselung ist nicht eindeutig!! (Bis 4 Möglichkeiten!) Es gibt kaum Anwendungen in der Praxis.

15 Das Rabin-Verfahren

1. Schritt: Erzeugung der Schlüssel. (Alice)

- 1a. Alice wählt $p \neq q \in \mathbb{P}$ zwei (sehr große) Primzahlen mit $p \equiv q \equiv 1 \pmod{4}$ und setzt $N := p \cdot q$.
- 1b. Der öffentliche Schlüssel ist die Zahl N .
- 1c. Der private Schlüssel ist das Paar $N := (p, q)$. Dieser muss geheim bleiben.

2. Schritt: Nachricht verschlüsseln. (Bob mit dem öffentlichen Schlüssel N)

- 2a. Bob verschlüsselt seine Nachricht $[m]_N \in \mathbb{Z}/N\mathbb{Z}$ (mit $[m]_N \neq [0]_N$) durch Verwendung der Abbildung

$$e : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}, [m]_N \mapsto e([m]_N) := [m]_N^2$$

$[m] \in \mathbb{Z}/N\mathbb{Z}$ identifiziert.

- 2b. Bob schickt $e([m]_N)$ an Alice.

3. Schritt: Nachricht entschlüsseln. (Alice mit dem privaten Schlüssel (p, q))

- 3a. Alice empfängt die Nachricht $e([m]_N) \in \mathbb{Z}/N\mathbb{Z}$. Sie setzt $[y]_N := e([m]_N)$ mit $1 \leq y \leq N$. Die Nachricht wird durch

$$\left([y]_p^{\frac{p+1}{4}}, [y]_q^{\frac{p+1}{4}} \right) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$$

entschlüsselt. Dies ist eine der **höchstens vier Quadratwurzeln** von der empfangenen Nachricht $[y]_N$.

Wir müssen also die Quadratwurzeln der Elemente aus $\mathbb{Z}/N\mathbb{Z}$ verstehen.

Anmerkung 5.1

(a) Schreibe

$$\begin{aligned}\Psi: \mathbb{Z}/N\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ [a]_N &\mapsto ([a]_p, [a]_q)\end{aligned}$$

für den Ring-Isomorphismus aus dem chinesischen Restsatz.

Da p, q ungerade Primzahlen sind, so sind $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/q\mathbb{Z}$ Körper und es gibt genau zwei Quadratwurzeln von $[1]_p$ bzw. $[1]_q$ in $\mathbb{Z}/p\mathbb{Z}$ bzw. $\mathbb{Z}/q\mathbb{Z}$, d.h. $[\pm 1]_p$ bzw. $[\pm 1]_q$. (Es sind die Nullstellen vom Polynom $X^2 - [1]_p$ bzw. $X^2 - [1]_q$.)

Somit hat $1_{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}} = ([1]_p, [1]_q)$ genau **vier** Quadratwurzeln in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$:

$$([1]_p, [1]_q), ([-1]_p, [1]_q), ([1]_p, [-1]_q), \text{ und } ([-1]_p, [-1]_q).$$

In $\mathbb{Z}/N\mathbb{Z}$ gibt es also auch genau **vier** Quadratwurzeln von $[1]_N$, nämlich die Urbilder der oben angegebenen Elemente:

$$\begin{aligned}\Psi^{-1}([1]_p, [1]_q) &= [1]_N \\ \Psi^{-1}([-1]_p, [-1]_q) &= [-1]_N \\ \Psi^{-1}([-1]_p, [1]_q) &=: [\omega]_N \\ \Psi^{-1}([1]_p, [-1]_q) &= [-\omega]_N\end{aligned}$$

(b) Sei nun $[y]_N \in \mathbb{Z}/N\mathbb{Z}$ beliebig.

(c) Die Quadratwurzeln von $[y]_N$ in $\mathbb{Z}/N\mathbb{Z}$ entsprechen die Quadratwurzeln von

$$\Psi([y]_N) = ([y]_p, [y]_q) \text{ in } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z},$$

d.h. die Paare $([m]_p, [m]_q) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ mit $[m]_p^2 = [y]_p$ und $[m]_q^2 = [y]_q$. Nun hat das Polynom $X^2 - [y]_p$ bzw. $X^2 - [y]_q$ höchstens zwei Nullstellen in $\mathbb{Z}/p\mathbb{Z}$ bzw. $\mathbb{Z}/q\mathbb{Z}$, so dass es höchstens vier Quadratwurzeln von $[y]_N$ in $\mathbb{Z}/N\mathbb{Z}$ existieren kann.

Nun, ist $[m]_N$ eine Quadratwurzel von $[y]_N$ in $\mathbb{Z}/N\mathbb{Z}$, so sind die anderen Quadratwurzeln von $[y]_N$ gegeben durch

$$-[m]_N, [\omega]_N \cdot [m]_N, \text{ und } -[\omega]_N \cdot [m]_N,$$

$$\text{da } (-[m]_N)^2 = ([\omega]_N \cdot [m]_N)^2 = (-[\omega]_N \cdot [m]_N)^2 = [m]_N^2 = [y]_N.$$

⚠ Wiederholungen in dieser Liste sind möglich!

(d) **Folgerung:** Die Verschlüsselungsfunktion $e: \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}, [m]_N \mapsto [m]_N^2$ ist nicht injektiv! Daher ist die Entschlüsselung von Nachrichten nicht eindeutig! Es kann in der Tat bis vier Elemente aus $\mathbb{Z}/N\mathbb{Z}$ geben, die auf $[m]_N^2$ abgebildet werden. Siehe Aufgabe 1 auf Blatt 7 für ein Beispiel mit $N = 15$.

16 Das Rabin-Verfahren: Korrektheit und Sicherheit

Lemma 5.2 (Korrektheit des Rabin-Verfahrens)

Sei $[y]_N := e([m]_N) = [m]_N^2$ mit $0 < y < N$ die empfangene Nachricht. Dann gilt

$$\left([y]_p^{\frac{p+1}{4}}, [y]_q^{\frac{q+1}{4}} \right)^2 = ([y]_p, [y]_q) \quad \text{in } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}.$$

Beweis: Der kleine Satz von Fermat liefert $[m]_p^p = [m]_p$ in $\mathbb{Z}/p\mathbb{Z}$ und $[m]_q^q = [m]_q$ in $\mathbb{Z}/q\mathbb{Z}$. Somit gilt

$$\begin{aligned} \left([y]_p^{\frac{p+1}{4}}, [y]_q^{\frac{q+1}{4}} \right)^2 &= \left(([y]_p^{\frac{p+1}{4}})^2, ([y]_q^{\frac{q+1}{4}})^2 \right) \\ &= \left([y]_p^{\frac{p+1}{2}}, [y]_q^{\frac{q+1}{2}} \right) \\ &= \left(([m]_p^2)^{\frac{p+1}{2}}, ([m]_q^2)^{\frac{q+1}{2}} \right) \\ &= ([m]_p^{p+1}, [m]_q^{q+1}) \\ &= ([m]_p^p \cdot [m]_p, [m]_q^q \cdot [m]_q) \\ &= ([m]_p \cdot [m]_p, [m]_q \cdot [m]_q) \\ &= ([m]_p^2, [m]_q^2) \\ &= ([y]_p, [y]_q). \end{aligned}$$

■

Anmerkung 5.3 (Sicherheit des Rabin-Verfahrens)

- (a) Zunächst ist es klar, dass ein Einbrecher das Rabin-Verfahren brechen kann, wenn er die Faktorisierung $N = p \cdot q$ kennt.
- (b) Anders als beim RSA-Verfahren, gilt auch die Umkehrung! Angenommen, ein Angreifer das Verfahren brechen kann, d.h. er kann zu jedem Quadrat in $\mathbb{Z}/N\mathbb{Z}$ eine Quadratwurzel berechnen (und als Folgerung alle andere Quadratwurzeln auch), so kann er N als $N = p \cdot q$ mit $p, q \in \mathbb{P}$ faktorisieren.

(1.) Er wählt zufällig eine natürliche Zahl x mit $1 < x < N$.

Falls $\text{ggT}(N, x) \neq 1$, so hat er ein echter Primteiler gefunden. O.B.d.A. $x = p$ und $q = N/x$.

(2.) Er kann also annehmen, dass $\text{ggT}(N, x) = 1$. Er berechnet dann $x^2 \pmod{N}$ und eine Quadratwurzel $[m]_N$ von $[x^2]_N$.

Wir haben gesehen, dass es höchstens vier Quadratwurzeln gibt und diese sind die Lösungen von den folgenden Gleichungssystemen:

- (i) $m \equiv x \pmod{p}$ und $m \equiv x \pmod{1}$;
- (ii) $m \equiv x \pmod{p}$ und $m \equiv -x \pmod{1}$;
- (iii) $m \equiv -x \pmod{p}$ und $m \equiv x \pmod{1}$; und
- (iv) $m \equiv -x \pmod{p}$ und $m \equiv -x \pmod{1}$.

(3.) Er beobachtet:

Kapitel 6: Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ und Primitivwurzeln modulo n

In diesem Kapitel haben wir zwei Ziele:

Ziel 1

Multiplikative Struktur der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ von $\mathbb{Z}/n\mathbb{Z}$ für eine beliebige positive Zahl $n \in \mathbb{Z}_{>0}$.

Ziel 2

Existenz von Primitivwurzeln modulo n entweder beweisen oder widerlegen.

Definition 6.1 (*Primitivwurzel modulo n*)

Eine natürliche Zahl $a \in \mathbb{N}$ heißt **Primitivwurzel modulo $n \in \mathbb{N}$** , wenn

$$(\mathbb{Z}/n\mathbb{Z})^\times = \langle [a]_n \rangle = \{[a]_n, \dots, [a]_n^{\varphi(n)}\},$$

d.h. die Ordnung von $[a]_n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ ist $\varphi(n)$.

Beispiel 6.2

Durch Probieren erhalten wir modulo 7:

Für $[2]_7$ gilt: $[2]_7^2 = [4]_7$, $[2]_7^3 = [1]_7$, also ist 2 keine Primitivwurzel modulo 7, da $\varphi(7) = 6$ ist.

Aber 3 ist eine Primitivwurzel modulo 7, denn

$$\{[3]_7^1, \dots, [3]_7^6\} = \{[3]_7^6, [3]_7^2, [3]_7^1, [3]_7^4, [3]_7^5, [3]_7^3\} = \{[3]_7, [2]_7, [6]_7, [4]_7, [5]_7, [1]_7\} = (\mathbb{Z}/7\mathbb{Z})^\times.$$

Anmerkung 6.3

Sei $n = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorzerlegung von $n \in \mathbb{Z}_{>0}$ (mit ungeraden paarweise verschiedenen Primzahlen p_1, \dots, p_r , $\alpha \in \mathbb{N}_0, \alpha_1, \dots, \alpha_r \in \mathbb{N}$). Dann liefert den Chinesischen Restsatz einen Gruppenisomorphismus

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

Ziel 2 werden wir als Konsequenz von Ziel 1 erreichen. Zu Ziel 1 benötigen wir zuerst die Struktur der Gruppe $(\mathbb{Z}/q^r\mathbb{Z})^\times$ für eine beliebige Primzahl q und $r \in \mathbb{N}$.

18 Die Einheitengruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$

Als ersten Schritt untersuchen wir die Einheitengruppe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ für 2-Potenzen 2^α . In diesem Abschnitt ist stets $\alpha \in \mathbb{N}$. Für kleine α beobachten wir Folgendes:

Beispiel 6.4

- Für $\alpha = 1$ ist $(\mathbb{Z}/2\mathbb{Z})^\times = \{[1]_2\} = \langle [1]_2 \rangle$ zyklisch der Ordnung 1.
- Für $\alpha = 2$ ist $(\mathbb{Z}/4\mathbb{Z})^\times = \{[1]_2, [3]_2\} = \langle [3]_2 \rangle$ zyklisch der Ordnung 2.
- Für $\alpha = 3$ gilt

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$$

wobei $[3]_8^2 = [1]_8$, $[5]_8^2 = [1]_8$, $[7]_8^2 = [1]_8$. Also haben $[3]_8, [5]_8, [7]_8$ Ordnung 2, und $(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch. Es ist die kleinsche Viergruppe.

Bemerkung 6.5

Sind $a \in \mathbb{N}$ ungerade und $\alpha \in \mathbb{N}_{\geq 3}$, so gilt

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Beweis: Per Induktion nach α .

Für $\alpha = 3$ behaupten wir, dass $a^2 \equiv 1 \pmod{8}$ für alle ungeraden a ist. Dies gilt nach obigem Beispiel.

Sei die Behauptung nun für $\alpha - 1$ bewiesen. Dann ist demnach

$$a^{2^{\alpha-3}} \equiv 1 \pmod{2^{\alpha-1}},$$

d.h., es existiert ein $t \in \mathbb{N}$ mit

$$a^{2^{\alpha-3}} = 1 + 2^{\alpha-1}t.$$

Quadrieren liefert

$$a^{2^{\alpha-2}} = (1 + 2^{\alpha-1}t)^2 = 1 + 2^\alpha t + 2^{2\alpha-2}t^2 \equiv 1 \pmod{2^\alpha}.$$

■

Anmerkung 6.6

Da gerade $a \in \mathbb{N}$ nicht invertierbar modulo 2^α sind, besagt Bemerkung 6.5, dass alle Elemente $[a]_{2^\alpha} \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ für $\alpha \geq 3$ höchstens Ordnung $2^{\alpha-2}$ haben. Aber

$$|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times| = \varphi(2^\alpha) = 2^{\alpha-1},$$

also ist $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ nicht zyklisch für $\alpha \geq 3$. Es gibt also **keine** Primitivwurzel modulo 2^α für $\alpha \geq 3$.

Satz 6.7

Ist $\alpha \in \mathbb{N}_{\geq 3}$, so gilt $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Beweis:

- (1) Nach Voraussetzung, ist $[-1]_{2^\alpha} \neq [1]_{2^\alpha}$ da $\alpha \geq 3$. Zudem gilt $[-1]_{2^\alpha}^2 = [1]_{2^\alpha}$, sodass die Ordnung von $[-1]_{2^\alpha}$ in $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ gleich 2 ist. Somit ist $\langle [-1]_{2^\alpha} \rangle$ eine zyklische Gruppe der Ordnung 2, d.h.

$$\langle [-1]_{2^\alpha} \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

- (2) Übung auf Blatt 8: Zeigen Sie, dass $\langle [5]_{2^\alpha} \rangle \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

- (3) Wegen $5^x \equiv 1 \pmod{4}$ für alle $x \in \mathbb{N}$ ist $[-1]_{2^\alpha} \notin \langle [5]_{2^\alpha} \rangle$. Aus $\langle [-1]_{2^\alpha} \rangle = \{[1]_{2^\alpha}, [-1]_{2^\alpha}\}$ folgt $\langle [-1]_{2^\alpha} \rangle \cap \langle [5]_{2^\alpha} \rangle = \{[1]_{2^\alpha}\}$. Somit haben wir ein direktes Produkt $\langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle$, das eine Untergruppe von $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ ist.

- (4) Nach (1) und (2) hat direktes Produkt $\langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle$ die Ordnung $2 \cdot 2^{\alpha-2}$. Es muss also die ganze Gruppe sein, d.h.

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \langle [-1]_{2^\alpha} \rangle \times \langle [5]_{2^\alpha} \rangle$$

und die Behauptung folgt. ■

19 Die Einheitengruppe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ für p ungerade

Wir wollen zunächst den Primzahlfall behandeln. Dazu benötigen wir das folgende Ergebnis aus der elementaren Gruppentheorie (Algebra I):

Bemerkung 6.8 (Ohne Beweis)

Sei G eine endliche Gruppe der Ordnung $n \in \mathbb{Z}_{>0}$.

- (a) Hat G für jeden positiven Teiler $d \mid n$ höchstens $\varphi(d)$ Elemente der Ordnung d , so ist G zyklisch.
- (b) Ist umgekehrt G zyklisch, so existieren für alle positiven Teiler $d \mid n$ genau $\varphi(d)$ Elemente der Ordnung d in G .

Bemerkung 6.9

Eine endliche Untergruppe (G, \cdot) der multiplikativen Gruppe (K^\times, \cdot) eines Körpers $(K, +, \cdot)$ ist zyklisch.

Beweis: Setze $|G| =: n \in \mathbb{Z}_{>0}$. Ist $g \in G$ ein Element der Ordnung d , so gilt $g^d = 1$, und somit ist g eine Nullstelle des Polynoms $X^d - 1 \in K[X]$. Da K ein Körper ist, hat $X^d - 1$ höchstens d Nullstellen. Also gibt es höchstens d Elemente der Ordnung d in G , nämlich g, \dots, g^{d-1} . Dabei gilt: g^k hat genau dann Ordnung d , wenn $\text{ggT}(d, k) = 1$. Also gibt es genau $\varphi(d)$ Elemente der Ordnung d . Aus Bemerkung 6.8 folgt nun, dass G zyklisch ist. ■

Satz 6.10

Sei $p \in \mathbb{P}$ eine Primzahl. Dann ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch der Ordnung $\varphi(p) = p - 1$.

Beweis: Der Ring $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Aus Bemerkung 6.9 folgt, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist. ■

Satz 6.10 besagt demnach: Es existieren Primitivwurzeln modulo p , falls p eine Primzahl ist. Aber wie findet man solche Zahlen?

Unser nächstes Ziel ist nun zu zeigen, dass $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ für ungerade Primzahlen p zyklisch ist. Wir nehmen also nun an, dass p stets eine ungerade Primzahl ist, und $\alpha \in \mathbb{N}$.

Lemma 6.11

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl und sei $a \in \mathbb{N}$ eine Primitivwurzel modulo p^α . Dann entweder

- (i) a ist Primitivwurzel modulo $p^{\alpha+1}$, oder
- (ii) $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^{\alpha+1}}$.

Beweis: Sei m die Ordnung von $[a]$ in $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times$. Es gilt

$$m \mid |(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times| = \varphi(p^{\alpha+1}).$$

Andererseits ist $a^m \equiv 1 \pmod{p^{\alpha+1}}$, also ist $a^m \equiv 1 \pmod{p^\alpha}$ und somit $\varphi(p^\alpha) \mid m$, also

$$(p-1)p^{\alpha-1} = \varphi(p^\alpha) \mid m \mid \varphi(p^{\alpha+1}) = (p-1)p^\alpha.$$

Demnach gibt es nur zwei Möglichkeiten:

- (i) $m = \varphi(p^{\alpha+1})$, dann ist a Primitivwurzel in $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\times$, also modulo $p^{\alpha+1}$.
- (ii) $m = \varphi(p^\alpha)$, dann ist $a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^{\alpha+1}}$. ■

Satz 6.12

Sei $a \in \mathbb{Z}_{>0}$ eine Primitivwurzel modulo p mit $a^{p-1} = 1 + mp$ für ein $m \in \mathbb{Z}$ mit $p \nmid m$. Dann ist a eine Primitivwurzel modulo p^α für alle $\alpha \geq 1$.

Beweis: Wir zeigen, dass $a^{\varphi(p^\alpha)} = 1 + m_\alpha p^\alpha$ für $p \nmid m_\alpha$ für alle $\alpha \in \mathbb{Z}_{>0}$ ist. Dann gilt $a^{\varphi(p^\alpha)} \not\equiv 1 \pmod{p^{\alpha+1}}$ und die Aussage folgt aus Lemma 6.11.

Per Induktion nach α . Für $\alpha = 1$ ist $a^{\varphi(p)} = a^{p-1} = 1 + m_1 p$ mit $m_1 := m$ nach Voraussetzung. Sei die Behauptung jetzt für α gezeigt. Potenzieren mit p liefert nach Induktionsvoraussetzung

$$\begin{aligned} a^{\varphi(p^{\alpha+1})} &= a^{p\varphi(p^\alpha)} = (1 + m_\alpha p^\alpha)^p = 1 + \binom{p}{1} m_\alpha p^\alpha + \binom{p}{2} m_\alpha^2 p^{2\alpha} + \dots \\ &\equiv 1 + m_\alpha p^{\alpha+1} \pmod{p^{\alpha+2}}. \end{aligned}$$

Daher existiert $k \in \mathbb{Z}$ mit

$$a^{\varphi(p^{\alpha+1})} = 1 + m_\alpha p^{\alpha+1} + kp^{\alpha+2} = 1 + \underbrace{(m_\alpha + kp)}_{=: m_{\alpha+1}} p^{\alpha+1}. \quad \blacksquare$$

Anmerkung 6.13

Um eine Primitivwurzeln modulo p^α zu finden, reicht es also eine Primitivwurzel modulo p zu bestimmen, welche die Voraussetzung aus Satz 6.12 erfüllt.

Beispiel 6.14

$p = 3$: $a = 2$ ist eine Primitivwurzel modulo 3 und $2^{3-1} = 2^2 = 4 = 1 + 1 \cdot 3$. Somit folgt aus Satz 6.12, dass 2 eine Primitivwurzel modulo aller 3^α ist.

$p = 5$: $a = 2$ ist eine Primitivwurzel modulo 5 und $2^{5-1} = 16 = 1 + 3 \cdot 5$. Nach Satz 6.12 ist 2 eine Primitivwurzel modulo aller 5^α .

$p = 5$: $a = 7$ ist eine Primitivwurzel modulo 5, aber $7^4 = 49^2 \equiv (-1)^2 \equiv 1 \pmod{25}$. Daher tritt Fall (ii) von Lemma 6.11 ein und die Voraussetzung von Satz 6.12 ist nicht erfüllt. Tatsächlich hat 7 nur Ordnung $4 < \varphi(25) = 20$ modulo 25 und ist damit keine Primitivwurzel modulo 25.

Lemma 6.15

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Dann existiert eine Primitivwurzel a modulo p mit

$$a^{p-1} = 1 + mp \text{ für ein } m \in \mathbb{Z} \text{ mit } p \nmid m.$$

Beweis: Sei a eine Primitivwurzel modulo p (Satz 6.10). Gilt $a^{p-1} = 1 + mp$ mit $p \nmid m$, so sind wir fertig. Sonst gilt $a^{p-1} = 1 + mp$ mit $p \mid m$. Mit a ist auch $a' := a + p \equiv a \pmod{p}$ eine Primitivwurzel modulo p . Aber alle Terme der binomischen Entwicklung von $(a')^{p-1} = (a + p)^{p-1}$ ab dem dritten Grad sind durch p^2 teilbar, existiert also ein $t \in \mathbb{Z}$ mit

$$\begin{aligned} (a')^{p-1} &= (a + p)^{p-1} = a^{p-1} + \binom{p-1}{1} a^{p-2} p + tp^2 \\ &= 1 + mp + (p-1)pa^{p-2} + tp^2 = 1 + m'p, \end{aligned}$$

wobei

$$m' = m + (p-1)a^{p-2} + tp.$$

Aber a ist Primitivwurzel modulo p , also $p \nmid a$ und somit $p \nmid a^{p-2}$ und daher $p \nmid m'$, d.h. a' hat die geforderte Eigenschaft. ■

Satz 6.16

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Dann sind die Einheitengruppen $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ und $(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ zyklisch für alle $\alpha \geq 1$.

Beweis: Nach Satz 6.12 zusammen mit Lemma 6.15 existiert eine Primitivwurzel a modulo p^α . Somit ist $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ nach Definition 6.1 zyklisch. Da $(\mathbb{Z}/2\mathbb{Z})^\times$ die triviale Gruppe ist, erhalten wir

$$(\mathbb{Z}/2p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$$

nach dem Chinesischen Restsatz. ■

20 Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$

Bevor wir die Frage beantworten können, wann $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist, benötigen wir folgendes einfaches gruppentheoretisches Lemma:

Lemma 6.17

Sind G, H endliche zyklische Gruppen, so gilt:

$$G \times H \text{ ist genau dann zyklisch, wenn } \text{ggT}(|G|, |H|) = 1.$$

Folgerung 6.18

Sei $n \in \mathbb{Z}_{\geq 2}$. Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist genau dann zyklisch, wenn

$$n \in \{2, 4, p^\alpha, 2p^\alpha\},$$

wobei $p \in \mathbb{P} \setminus \{2\}$ und $\alpha \in \mathbb{Z}_{\geq 1}$.

Beweis: Verwende Lemma 6.17 induktiv zusammen mit Anmerkung 6.3, Satz 6.10, Satz 6.7 und Satz 6.16. ■

Zum Abschluss wollen wir eine weitere schon lange offene Frage erwähnen:

Anmerkung 6.19 (Die Vermutung von Artin)

Ist 2 Primitivwurzel modulo unendlich vieler Primzahlen?

21 Aufgaben zu Kapitel 6

Aufgabe 25

Sei $\alpha \in \mathbb{N}_{\geq 3}$.

(1) Zeigen Sie: Ist $5^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$, so gilt $\langle [5]_{2^\alpha} \rangle \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

(2) Zeigen Sie per Induktion, dass $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$ gilt. Geben Sie dabei deutlich an:

- den Induktionsanfang (IA),
- die Induktionsvoraussetzung (IV), und
- den Induktionsschritt (IS).

(3) Schlussfolgern Sie, dass der Isomorphismus $\langle [5]_{2^\alpha} \rangle \cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ gilt.

Aufgabe 26

Beweisen Sie Lemma 6.17.

Aufgabe 27

(1) Welche der Gruppen $(\mathbb{Z}/16\mathbb{Z})^\times$, $(\mathbb{Z}/20\mathbb{Z})^\times$ und $(\mathbb{Z}/24\mathbb{Z})^\times$ sind isomorph zueinander?

(2) Wahr oder falsch? Wenn die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist, dann hat sie genau $\varphi(\varphi(n))$ viele erzeugende Elemente.

Aufgabe 28

Bestimmen Sie alle erzeugenden Elemente der Gruppe $(\mathbb{Z}/23\mathbb{Z})^\times$.

[Hinweis: Zeigen Sie zuerst, dass die Anzahl der erzeugenden Elemente 10 ist. Berechnen Sie, die Potenzen von $[2]_23$ und beobachten Sie, dass $o([2]_23) = 11$ ist. Damit sind die Potenzen von $[2]_23$ keine Erzeuger und es gibt also $22 - 11 = 11$ Möglichkeiten übrig. Schließen Sie eine dieser Restklassen mit einem kurzen Argument aus!]

Aufgabe 29

Wahr oder falsch? Sei p eine ungerade Primzahl. Für alle erzeugenden Elemente $[a]_p$ der zyklischen Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ gilt $[a]_p^{\frac{p-1}{2}} = [-1]_p$.

Aufgabe 30

Sei $p > 3$ eine Primzahl. Zeigen Sie, dass das Produkt aller erzeugenden Elemente der zyklischen Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ gleich $[1]_p$ ist.

[Hinweis: Ist $[a]_p$ erzeugendes Element, so auch $[a]_p^{-1}$.)]

Kapitel 7: Kurze Einführung in die Kodierungstheorie

Siehe Folien!

Die Datei `Woche_10_Einfuehrung_Kodierungstheorie.pdf` kann von Stud.IP heruntergeladen werden.

Kapitel 8: Das quadratische Reziprozitätsgesetz

Ziel dieses Kapitels: Untersuchung der Lösbarkeit der Kongruenzgleichung

$$X^2 \equiv a \pmod{p},$$

also die Frage, ob die ganze Zahl $a \in \mathbb{Z}$ eine Quadratwurzel modulo $p \in \mathbb{P}$ besitzt.

In Kapitel 6 hatten wir bereits ein erstes Kriterium für die Lösbarkeit bewiesen:

Ist $p \in \mathbb{P}$ ungerade, $g \in \mathbb{Z}_{>0}$ Primitivwurzel modulo p und $a \equiv g^d \pmod{p}$, so ist $X^2 \equiv a \pmod{p}$ genau dann lösbar, wenn d gerade ist.

Wie finden wir aber g und d ? In der Praxis benötigen wir ein besseres Kriterium. Dies wird uns das **quadratische Reziprozitätsgesetz** liefern.

22 Quadratische Reste

Definition 8.1 (quadratischer Rest, quadratischer Nichtrest)

Sei $n \in \mathbb{N}$. Eine ganze Zahl $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ heißt ein **quadratischer Rest modulo n** , falls die Kongruenz $x^2 \equiv a \pmod{n}$ eine Lösung hat, sonst heißt a **quadratischer Nichtrest modulo n** .

Bemerkung 8.2

Sei $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Eine ganze Zahl $a \in \mathbb{Z}_{>0}$ ist genau dann ein quadratischer Rest modulo p , wenn $\frac{p-1}{\text{ord}([a]_p)}$ gerade ist (wobei $[a]_p$ die Restklasse von a in $(\mathbb{Z}/p\mathbb{Z})^\times$ ist).

Beweis:

' \Rightarrow ' Ist a ein quadratischer Rest modulo p , dann existiert ein $b \in \mathbb{Z}_{>0}$ mit $b^2 \equiv a \pmod{p}$. Also gilt

$$[a]_p^{\frac{\varphi(p)}{2}} = [b]_p^{2\frac{\varphi(p)}{2}} = [1] \in \mathbb{Z}/p\mathbb{Z}$$

nach dem kleinen Satz von Fermat (Folgerung 3.24), somit

$$\text{ord}([a]_p) \mid \frac{\varphi(p)}{2} = \frac{p-1}{2}.$$

Dies bedeutet, dass $\frac{p-1}{\text{ord}([a]_p)}$ gerade sein muss.

' \Leftarrow ' Wir nehmen nun an, dass $\frac{p-1}{\text{ord}([a]_p)}$ gerade ist. Sei $g \in \mathbb{Z}_{>0}$ eine Primitivwurzel modulo p , d.h.

$$\langle [g]_p \rangle = (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{und} \quad \text{ord}([g]_p) = p-1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$$

und es gibt $m \in \mathbb{Z}_{>0}$, so dass $[a]_p = [g]_p^m$ ist. Dann ist

$$[1] = [a]_p^{\text{ord}([a]_p)} = [g]_p^{m \cdot \text{ord}([a]_p)}.$$

Also ist $p-1$ ein Teiler von $m \cdot \text{ord}([a]_p)$ und es gilt

$$\frac{p-1}{\text{ord}([a]_p)} \mid m.$$

Damit ist m als Vielfaches von $\frac{p-1}{\text{ord}([a]_p)}$ gerade. Setze also $b := g^{\frac{m}{2}}$, so dass $[b]_p^2 = [g]_p^m = [a]_p$ ist, und deshalb ist a ein quadratischer Rest modulo p . ■

Satz 8.3

Sei $p \in \mathbb{P} \setminus \{2\}$ ungerade. Die Menge

$$\begin{aligned} \mathcal{R}_p &:= \{[a]_p \in \mathbb{Z}/p\mathbb{Z} \mid a \in \mathbb{Z} \text{ quadratischer Rest modulo } p\} \\ &= \{[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \exists [x]_p \in \mathbb{Z}/p\mathbb{Z} \text{ mit } [a]_p = [x]_p^2\} \end{aligned}$$

ist eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$ der Ordnung

$$\frac{\varphi(p)}{2} = \frac{p-1}{2}.$$

Beweis: Zunächst ist es klar nach Definition, dass $\mathcal{R}_p \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$. Nun sind $[a]_p, [b]_p \in \mathcal{R}_p$, so existieren $[x]_p, [y]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit

$$[x]_p^2 = [a]_p, \quad \text{und} \quad [y]_p^2 = [b]_p.$$

Damit ist

$$[a]_p \cdot [b]_p^{-1} = [x]_p^2 \cdot [y]_p^{-2} = ([x]_p \cdot [y]_p^{-1})^2$$

ebenfalls ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ und \mathcal{R}_p ist eine Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$.

Weiter gilt $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, und die Elemente $x, -x \in \mathbb{Z}$ haben jeweils dasselbe Quadrat, also gibt es $\frac{p-1}{2}$ Quadrate und somit gilt $|\mathcal{R}_p| = \frac{p-1}{2}$. ■

Definition 8.4 (Legendre Symbol)

Seien $p \in \mathbb{P} \setminus \{2\}$ ungerade und $a \in \mathbb{Z}$. Das **Legendre-Symbol** ist definiert als

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

Man spricht dies „ a über p “ aus.

Anmerkung 8.5

Anders gesagt gibt $\left(\frac{a}{p}\right)$ Antwort auf die Frage: Ist a ein quadratischer Rest modulo p ?

Beispiel 8.6

Sei $p = 7$. Nach Satz 8.3 gibt es

$$\frac{p-1}{2} = \frac{7-1}{2} = 3$$

quadratische Reste modulo 7. Es gilt

$$1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 2 \pmod{7}.$$

Damit ist

$$\mathcal{R}_7 = \{[1]_7, [2]_7, [4]_7\},$$

also

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1, \quad \left(\frac{0}{7}\right) = 0.$$

Bemerkung 8.7 (Rechenregeln)

Seien $p \in \mathbb{P} \setminus \{2\}$, $a, b \in \mathbb{Z}$. Dann gelten:

- (a) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, falls $a \equiv b \pmod{p}$;
- (b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; und
- (c) $\left(\frac{a^2}{p}\right) = 1$, falls $p \nmid a$.

Beweis:

- (a) Nach Definition hängt das Legendre-Symbol $\left(\frac{a}{p}\right)$ nur von der Restklasse von a modulo p ab.
- (b) 1. Fall: Gilt $p \mid ab$, dann $p \mid a$ oder $p \mid b$. Damit ist $\left(\frac{ab}{p}\right) = 0$ genau dann, wenn $\left(\frac{a}{p}\right) = 0$ oder $\left(\frac{b}{p}\right) = 0$ ist.
2. Fall: Sei jetzt $\text{ggT}(a, p) = \text{ggT}(b, p) = 1$ und $\left(\frac{a}{p}\right) = 1$. Dann ist $[a]_p \in \mathcal{R}_p$ und daher $[b]_p \in \mathcal{R}_p$ genau dann, wenn $[a]_p[b]_p \in \mathcal{R}_p$ (nach Satz 8.3) und ebenso falls $\left(\frac{b}{p}\right) = 1$.
3. Fall: $\text{ggT}(a, p) = \text{ggT}(b, p) = 1$ und $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Somit sind $[a]_p, [b]_p \notin \mathcal{R}_p$. In diesem Fall müssen wir also zeigen, dass $[a]_p[b]_p \in \mathcal{R}_p$ ist, und somit ist $\left(\frac{ab}{p}\right) = 1$. Da $[a]_p$ invertierbar ist, ist die Multiplikation mit $[a]_p$

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ [c]_p & \mapsto & [a]_p \cdot [c]_p, \end{array}$$

ist eine bijektive Abbildung. Falls $[c]_p \in \mathcal{R}_p$, dann ist $[a]_p[c]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$, also wird \mathcal{R}_p nach $(\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$ abgebildet: $[a]_p \mathcal{R}_p = (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$. Daher gilt

$$[a]_p((\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p) = [a]_p^2 \mathcal{R}_p = \mathcal{R}_p$$

und damit $[a]_p[b]_p \in \mathcal{R}_p$.

- (c) Dies ist der Spezialfall $b = a$ von Teil (b). ■

Aber wie berechnen wir $\left(\frac{a}{p}\right)$? Eine erste, jedoch recht aufwendige Methode, wird gegeben durch:

Satz 8.8 (Euler)

Für alle ungeraden $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ gilt: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Beweis: Für $p \mid a$ sind beide Seiten Null. Sei nun $\text{ggT}(a, p) = 1$. Nach dem Satz von Fermat (Folgerung 3.24) gilt

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

d.h., $[a]_p^{\frac{p-1}{2}}$ ist eine Nullstelle von $X^2 - [1]_p$, also

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

Ist $a \equiv b^2 \pmod{p}$ einer der $\frac{p-1}{2}$ quadratischen Reste modulo p (Satz 8.3), so ist

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p},$$

und damit ist $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ wie behauptet. Insbesondere sind die Restklassen modulo p der $\frac{p-1}{2}$ quadratischen Reste modulo p Nullstellen von $X^{\frac{p-1}{2}} - [1]_p$. Dies sind sämtliche Nullstellen von $X^{\frac{p-1}{2}} - [1]_p$ in $\mathbb{Z}/p\mathbb{Z}$ (da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist und Polynome über Körpern höchstens so viele Nullstellen haben wie ihr Grad angibt). Die Restklassen der quadratischen Nichtreste modulo p sind also *keine* Nullstellen von $X^{\frac{p-1}{2}} - [1]_p$, also $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ für $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathcal{R}_p$. Somit ist für diese Zahl a wie verlangt

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

■

Beispiel 8.9

Wann ist -1 ein quadratischer Rest modulo p ? Dazu müssen wir $\left(\frac{-1}{p}\right)$ berechnen.

Nach Satz 8.8 gilt $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Aber $(-1)^{\frac{p-1}{2}} \in \{-1, 1\}$ und

$$\begin{cases} (-1)^{\frac{p-1}{2}} = 1 & \Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \\ (-1)^{\frac{p-1}{2}} = -1 & \Leftrightarrow (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \end{cases}$$

Somit gilt

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

23 Eine Methode von Gauß

Das Hauptresultat dieses Kapitels ist eine überraschende und wichtige Beziehung zwischen den Legendre-Symbolen $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$. Um diese im nächsten Abschnitt herleiten zu können, benötigen wir einige technische Vorbereitungen.

Lemma 8.10 (Gauß)

Seien $p \in \mathbb{P} \setminus \{2\}$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, p) = 1$. Für $1 \leq j \leq \frac{p-1}{2}$ sei a_j der betragsmäßig kleinste Rest von $a \cdot j$ modulo p , also

$$a \cdot j \equiv a_j \pmod{p} \quad \text{und} \quad -\frac{p-1}{2} \leq a_j \leq \frac{p-1}{2}.$$

Setze $\nu := \left| \{j \in \mathbb{Z}_{>0} \mid 1 \leq j \leq \frac{p-1}{2}, a_j < 0\} \right|$.

Dann gelten:

(a) die Beträge $|a_j|$ sind paarweise verschieden für alle $1 \leq j \leq \frac{p-1}{2}$, und daher ist

$$\{|a_j| \mid 1 \leq j \leq \frac{p-1}{2}\} = \{1, 2, \dots, \frac{p-1}{2}\};$$

(b) $(-1)^\nu \cdot \left(\frac{p-1}{2}\right)! = a_1 \cdots a_{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$.

Insbesondere ist

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

Beispiel 8.11

Für $p = 7$ und $a = 3$ gelten

$$a \cdot 1 = 3 \cdot 1 = 3, \quad a \cdot 2 = 3 \cdot 2 = 6, \quad a \cdot 3 = 3 \cdot 3 = 9$$

und somit sind $a_1 = 3, a_2 = -1$, und $a_3 = 2$. Deshalb ist $\nu = 1$ und somit $\left(\frac{3}{7}\right) = -1$ (vergleiche mit dem vorigen Beispiel).

Für $a = 4$ ist

$$a \cdot 1 = 4 \cdot 1 = 4, \quad a \cdot 2 = 4 \cdot 2 = 8, \quad a \cdot 3 = 4 \cdot 3 = 12$$

und somit $a_1 = -3, a_2 = 1, a_3 = -2$. Hier gilt also $\nu = 2$ und somit $\left(\frac{4}{7}\right) = (-1)^2 = 1$.

Beweis:

(a) Angenommen $|a_i| = |a_j|$, also $ia \equiv a_i \equiv \pm a_j \equiv \pm ja \pmod{p}$, dann folgt $(i \pm j)a \equiv 0 \pmod{p}$, also $p \mid a(i \pm j)$, also $p \mid (i \pm j)$ wegen $\text{ggT}(a, p) = 1$. Aber $1 \leq i, j \leq \frac{p-1}{2}$ und daher $|i \pm j| \leq p-1$, damit muss $i \pm j = 0$ sein, also $i = j$. Die $|a_i|$ sind daher sämtlich verschieden und es gilt

$$\{|a_j| \mid 1 \leq j \leq \frac{p-1}{2}\} = \{1, 2, \dots, \frac{p-1}{2}\}.$$

(b) Nach Teil (a) gilt

$$a_1 \cdots a_{\frac{p-1}{2}} = (-1)^\nu \cdot 1 \cdot 2 \cdots \frac{p-1}{2} = (-1)^\nu \cdot \left(\frac{p-1}{2}\right)!.$$

Aber nach Definition ist auch

$$a_1 \cdots a_{\frac{p-1}{2}} \equiv (1 \cdot a) \cdots \left(\frac{p-1}{2} \cdot a\right) \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Wegen $p \nmid \left(\frac{p-1}{2}\right)!$ ist $\left(\frac{p-1}{2}\right)!$ invertierbar modulo p . Deshalb gilt

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

nach Satz 8.8. Da sowohl $(-1)^v$ als auch $\left(\frac{a}{p}\right)$ nur Werte in $\{\pm 1\}$ annehmen und p ungerade ist, folgt sogar

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

■

Als Übung kann man mit diesem Lemma von Gauß zeigen:

Folgerung 8.12 (Aufgabe 2, Blatt 11)

Ist $p \in \mathbb{P} \setminus \{2\}$, so gilt

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

Notation: Für $x \in \mathbb{R}$ ist $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$ das größte Ganze.

Wir brauchen noch das folgende technische Lemma:

Lemma 8.13

Seien $0 < j \leq k$ und $a \in \mathbb{Z}_{>0}$. Dann ist $\lfloor \frac{k}{a} \rfloor - \lfloor \frac{j}{a} \rfloor$ die Anzahl der positiven ganzzahligen Vielfachen m von a mit $j < m \leq k$.

Beweis: Division mit Rest von k durch a liefert $k = qa + r$, mit $0 \leq r < a$. Damit sind $a, 2a, \dots, qa \leq k$, also ist $q = \lfloor \frac{k}{a} \rfloor$ die Anzahl der i mit $ia \leq k$. Genauso ist $\lfloor \frac{j}{a} \rfloor$ die Anzahl der i mit $ia \leq j$, somit ist $\lfloor \frac{k}{a} \rfloor - \lfloor \frac{j}{a} \rfloor$ die gesuchte Zahl. ■

24 Das quadratische Reziprozitätsgesetz

Damit können wir das Hauptresultat dieses Kapitels beweisen.

Satz 8.14 (Gaußsches Quadratisches Reziprozitätsgesetz)

Seien $p \neq q \in \mathbb{P} \setminus \{2\}$ zwei ungerade Primzahlen. Dann gelten:

(a)

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

(b)

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

(c)

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

Beweis: Die Teile (b) und (c) sind Satz 8.8 bzw. Folgerung 8.12, daher bleibt nur (a) zu beweisen.

(a) **1. Schritt:** Ist $p \equiv q \pmod{4}$, dann existiert $a \in \mathbb{Z}$ mit $p - q = 4a$ und $\text{ggT}(a, pq) = 1$. Ist $p \not\equiv q \pmod{4}$, also $p \equiv -q \pmod{4}$, dann existiert $a \in \mathbb{Z}$ mit $p + q = 4a$ mit $\text{ggT}(a, pq) = 1$. Also gilt für obiges a immer $p \equiv \pm q \pmod{4a}$ und $\text{ggT}(a, pq) = 1$.

2. Schritt: Nach Lemma 8.10 ist $\left(\frac{a}{p}\right) = (-1)^\nu$, wobei ν die Anzahl der $1 \leq j \leq \frac{p-1}{2}$ mit

$$j \cdot a \in \left(\frac{p}{2}, 2\frac{p}{2}\right] \sqcup \left(3\frac{p}{2}, 4\frac{p}{2}\right] \sqcup \dots = \bigsqcup_{\substack{i=2 \\ \text{gerade}}}^a \left((i-1)\frac{p}{2}, i\frac{p}{2}\right]$$

bezeichnet. Aus Lemma 8.13 folgt nun

$$\nu = \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor i\frac{p}{2a} \right\rfloor - \left\lfloor (i-1)\frac{p}{2a} \right\rfloor \right).$$

Ebenso ist $\left(\frac{a}{q}\right) = (-1)^\mu$ mit

$$\mu = \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor i\frac{q}{2a} \right\rfloor - \left\lfloor (i-1)\frac{q}{2a} \right\rfloor \right).$$

Wegen $p = \pm q + 4a$ gilt

$$\begin{aligned} \nu &= \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor i\frac{\pm q + 4a}{2a} \right\rfloor - \left\lfloor (i-1)\frac{\pm q + 4a}{2a} \right\rfloor \right) \\ &= \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor \frac{\pm iq}{2a} + 2i \right\rfloor - \left\lfloor \frac{\pm(i-1)q}{2a} + 2(i-1) \right\rfloor \right) \\ &= \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor \frac{\pm iq}{2a} \right\rfloor - \left\lfloor \frac{\pm(i-1)q}{2a} \right\rfloor + \underbrace{2i - 2(i-1)}_{\text{gerade}} \right) \\ &\equiv \sum_{\substack{i=2 \\ \text{gerade}}}^a \left(\left\lfloor \frac{\pm iq}{2a} \right\rfloor - \left\lfloor \frac{\pm(i-1)q}{2a} \right\rfloor \right) \pmod{2}. \end{aligned}$$

Im Fall $p = q + 4a$ zeigt dies bereits $\nu \equiv \mu \pmod{2}$. Sei jetzt $p = -q + 4a$. Hier verwenden wir

$$\lfloor -x \rfloor = -\lceil x \rceil = -\lfloor x \rfloor - 1 \quad \text{für alle } x \in \mathbb{R} \setminus \mathbb{Z}.$$

Angenommen $\frac{iq}{2a}$ wäre ganz, also $\frac{iq}{2a} = s \in \mathbb{Z}$. Dann ist $s \leq \frac{q}{2}$ und $iq = 2as$, aber q teilt weder 2 noch a noch s , Widerspruch!

Also sind $\frac{iq}{2a}, \frac{(i-1)q}{2a}$ nie ganz und es gilt

$$\begin{aligned} \left\lfloor \frac{-iq}{2a} \right\rfloor - \left\lfloor \frac{-(i-1)q}{2a} \right\rfloor &= -\left\lfloor \frac{iq}{2a} \right\rfloor - 1 + \left\lfloor \frac{(i-1)q}{2a} \right\rfloor + 1 \\ &= -\left(\left\lfloor \frac{iq}{2a} \right\rfloor - \left\lfloor \frac{(i-1)q}{2a} \right\rfloor \right). \end{aligned}$$

Damit ist auch in diesem Fall $\nu \equiv \mu \pmod{2}$, was bedeutet

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

3. Schritt: Nach Bemerkung 8.7(a),(b) und (c) gilt:

$$\left(\frac{p}{q}\right) = \left(\frac{\pm q + 4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{2^2}{q}\right) \left(\frac{a}{q}\right) = 1 \cdot \left(\frac{a}{q}\right)$$

Aber nach Schritt 2 ist

$$\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$$

un nun rechnen wir andersherum mit Bemerkung 8.7(a),(b) und (c):

$$\left(\frac{a}{p}\right) = \left(\frac{2^2}{p}\right) \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{-p + 4a}{p}\right) = \left(\frac{\mp q}{p}\right) = \left(\frac{\mp 1}{p}\right) \left(\frac{q}{p}\right)$$

und somit ist

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{-1}{p}\right) & p \equiv q \pmod{4} \\ 1 & p \not\equiv q \pmod{4} \end{cases} \stackrel{\text{Satz 8.8}}{=} \begin{cases} -1 & p \equiv 3 \equiv q \pmod{4} \\ 1 & p \equiv 1 \equiv q \pmod{4} \\ 1 & p \not\equiv q \pmod{4} \end{cases}$$

Anmerkung 8.15

Es folgt aus dem Beweis, dass Teil (a) auch so formuliert werden kann: Sind $p, q \in \mathbb{P} \setminus \{2\}$ ungerade Primzahlen, dann gilt

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

Damit erhalten wir eine sehr effiziente Methode zur Berechnung des Legendre-Symbols!!

Beispiel 8.16

(a) Ist 3 quadratischer Rest modulo 41?

$$\left(\frac{3}{41}\right) \stackrel{\text{Satz 8.14(a)}}{=} \left(\frac{41}{3}\right) \stackrel{\text{Bem. 8.7(a)}}{=} \left(\frac{2}{3}\right) \stackrel{\text{Satz 8.14(c)}}{=} -1$$

Also ist 3 kein quadratischer Rest modulo 41.

(b)

$$\begin{aligned} \left(\frac{503}{773}\right) &= \left(\frac{773}{503}\right) = \left(\frac{270}{503}\right) = \left(\frac{3^3 \cdot 2 \cdot 5}{503}\right) \\ &= \left(\frac{3^2}{503}\right) \left(\frac{3}{503}\right) \left(\frac{2}{503}\right) \left(\frac{5}{503}\right) \\ &= -\left(\frac{503}{3}\right) \cdot 1 \cdot \left(\frac{503}{5}\right) = -\left(\frac{2}{3}\right) \cdot \left(\frac{3}{5}\right) \\ &= -(-1) \cdot \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \end{aligned}$$

(c)

$$\begin{aligned}
 \left(\frac{501}{773}\right) &= \left(\frac{3 \cdot 167}{773}\right) = \left(\frac{773}{3}\right) \left(\frac{773}{167}\right) \\
 &= \left(\frac{2}{3}\right) \left(\frac{105}{167}\right) = -1 \cdot \left(\frac{3 \cdot 5 \cdot 7}{167}\right) = -\left(\frac{3}{167}\right) \left(\frac{5}{167}\right) \left(\frac{7}{167}\right) \\
 &= -\left(-\left(\frac{167}{3}\right)\right) \left(\frac{167}{5}\right) \left(-\left(\frac{167}{7}\right)\right) \\
 &= -\left(\frac{2}{3}\right) \left(\frac{2}{5}\right) \left(\frac{6}{7}\right) = 1
 \end{aligned}$$

Also hat die Kongruenzgleichung $X^2 \equiv 501 \pmod{773}$ eine Lösung.

25 Das Jacobi-Symbol

Das Jacobi-Symbol (benannt nach Carl Gustav Jacob Jacobi) ist eine Verallgemeinerung des Legendre-Symbols.

Definition 8.17 (Jacobi-Symbol)

Sei $a \in \mathbb{Z}$ und sei $b \in \mathbb{N}$ eine ungerade natürliche Zahl. Schreibe $b = p_1 \cdots p_m = \prod_{i=1}^m p_i$ ($m \in \mathbb{N}_0$) als Produkt von Primzahlen (nicht notwendig verschieden). Das **Jacobi-Symbol** ist

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_m}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right).$$

wobei für $i = 1, \dots, m$ das Symbol $\left(\frac{a}{p_i}\right)$ das Legendre-Symbol ist. Dabei werden $b = 1$ und somit auch $\left(\frac{a}{1}\right) = 1$ als leere Produkte verstanden (d.h. mit $m = 0$).

Man spricht dies auch „ a über b “ aus.

Anmerkung 8.18


- (1) Ist b eine ungerade Primzahl, so ist das Jacobi-Symbol gleich dem Legendre-Symbol.
- (2) Es folgt aus der Definition, dass $\left(\frac{a}{b}\right) \in \{-1, 0, 1\}$, weil dies schon für das Legendre-Symbol gilt. Außerdem gilt:

$$\left(\frac{a}{b}\right) = 0 \Leftrightarrow \text{ggT}(a, b) \neq 1.$$

- (3) Ist a ein quadratischer Rest modulo b , so gilt $\left(\frac{a}{b}\right) = 1$.

Beweis:

$$\begin{aligned}
 a \text{ QR mod } b &\implies \exists x \in \mathbb{Z} \text{ mit } a - x^2 = c \cdot b = c \cdot p_1 \cdots p_m \implies a \text{ ist QR mod } p_i \forall 1 \leq i \leq m \\
 &\implies \left(\frac{a}{p_i}\right) = 1 \forall 1 \leq i \leq m \implies \left(\frac{a}{b}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right) = \prod_{i=1}^m 1 = 1.
 \end{aligned}$$

- (4)  Die Umkehrung gilt nicht: i.A. $\left(\frac{a}{b}\right) = 1 \not\Rightarrow a$ ist quadratischer Rest modulo b .

Gegenbeispiel: Nehme $b = 3^2$ und $a = 2$. Es gilt $\left(\frac{a}{b}\right) = \left(\frac{2}{3^2}\right) = \left(\frac{2}{3}\right)^2 = 1$ aber 2 ist kein quadratischer Rest modulo 9, weil die Quadrate modulo 9 kongruent zu 0,1,4 oder 7 sind.

(5) Sind $a, a' \in \mathbb{Z}$ mit $a \equiv a' \pmod{b}$, so gilt $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$.

Beweis:

$a \equiv a' \pmod{b} \implies \exists c \in \mathbb{Z}$ mit $a - a' = c \cdot b = c \cdot p_1 \cdots p_m \implies a \equiv a' \pmod{p_i}$
 $\forall 1 \leq i \leq m \implies \left(\frac{a}{p_i}\right) = \left(\frac{a'}{p_i}\right) \forall 1 \leq i \leq m$ nach Bemerkung 8.7(a) und somit gilt

$$\left(\frac{a}{b}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right) = \prod_{i=1}^m \left(\frac{a'}{p_i}\right) = \left(\frac{a'}{b}\right).$$

(6) Mit ähnlichen Argumenten zeigt man, dass das Jacobi-Symbol multiplikativ im Zähler und im Nenner ist, d.h.

$$\left(\frac{a_1 \cdot a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right) \quad \text{für alle } a_1, a_2 \in \mathbb{Z}$$

und

$$\left(\frac{a}{b_1 \cdot b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right) \quad \text{für alle } b_1, b_2 \in \mathbb{Z} \text{ ungerade.}$$

Zur expliziten Berechnung des Jacobi-Symbols benutzen wir die folgende Verallgemeinerung des quadratischen Reziprozitätsgesetzes:

Satz 8.19

Seien $a, b \in \mathbb{N}$ zwei ungerade natürliche Zahlen. Dann gelten:

(a)

$$\left(\frac{a}{b}\right) = (-1)^{\frac{b-1}{2} \frac{a-1}{2}} \left(\frac{b}{a}\right) = \begin{cases} (-1) \cdot \left(\frac{b}{a}\right) & \text{falls } a \equiv b \equiv 3 \pmod{4}, \\ \left(\frac{b}{a}\right) & \text{sonst;} \end{cases}$$

(b)

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} 1 & \text{wenn } b \equiv 1 \pmod{4}, \\ -1 & \text{wenn } b \equiv -1 \pmod{4}; \end{cases}$$

(c)

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

Beweis: Beobachtung 1. Für $r_1, \dots, r_m \in \mathbb{Z}$ ungerade ganze Zahlen gilt

$$\frac{r_1 \cdots r_m - 1}{2} \equiv \sum_{i=1}^m \frac{r_i - 1}{2} \pmod{2}.$$

Beobachtung 2. Für $r_1, \dots, r_m \in \mathbb{Z}$ ungerade ganze Zahlen gilt

$$\frac{r_1^2 \cdots r_m^2 - 1}{8} \equiv \sum_{i=1}^m \frac{r_i^2 - 1}{8} \pmod{2}.$$

Beobachtung 3. Bei allen 3 Aussagen reicht es die erste Gleichheit zu beweisen. Die zweite Gleichheit ist klar (Begründungen dafür haben wir schon beim Legendre-Symbol gegeben).

Nun, schreibe $b = \prod_{i=1}^m p_i$ ($m \in \mathbb{N}_0$) und $a = \prod_{j=1}^\ell q_j$ ($\ell \in \mathbb{N}_0$) als Produkte von Primzahlen.

- (a) Falls $\text{ggT}(a, b) \neq 1$, so existieren $i \in \{1, \dots, m\}$ und $j \in \{1, \dots, \ell\}$ mit $\text{ggT}(a, p_i) \neq 1 \neq \text{ggT}(b, q_j)$.
Somit gelten $\left(\frac{a}{p_i}\right) = 0 = \left(\frac{b}{q_j}\right)$ und daher gilt

$$\left(\frac{a}{b}\right) = 0 = \left(\frac{b}{a}\right),$$

so dass die erste Gleichheit in diesem Fall erfüllt ist.

Wir können also annehmen, dass $\text{ggT}(a, b) = 1$. Somit gilt $p_i \neq q_j$ für alle $i \in \{1, \dots, m\}$ und für alle $j \in \{1, \dots, \ell\}$. Die Definition, Satz 8.14(a) und die Beobachtung liefern

$$\begin{aligned} \left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) &= \prod_{i=1}^m \prod_{j=1}^\ell \left(\frac{q_j}{p_i}\right) \cdot \left(\frac{p_i}{q_j}\right) \\ &= \prod_{i=1}^m \prod_{j=1}^\ell (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} \\ &= (-1)^{\sum_{i=1}^m \sum_{j=1}^\ell \frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} \\ &= (-1)^{(\sum_{i=1}^m \frac{p_i-1}{2}) \cdot (\sum_{j=1}^\ell \frac{q_j-1}{2})} \\ &= (-1)^{\frac{\prod_{i=1}^m p_i - 1}{2} \cdot \frac{\prod_{j=1}^\ell q_j - 1}{2}} \\ &= (-1)^{\frac{b-1}{2} \cdot \frac{a-1}{2}}. \end{aligned}$$

Nun ist $\left(\frac{b}{a}\right)^{-1} = \left(\frac{b}{a}\right)$, da $\left(\frac{b}{a}\right)^{-1} \in \{\pm 1\}$. Somit liefert die Multiplikation mit $\left(\frac{b}{a}\right)$ die gewünschte Formel:

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

- (b) Nach Definition, Satz 8.14(b) und Beobachtung 1 gelten

$$\left(\frac{-1}{b}\right) = \prod_{i=1}^m \left(\frac{-1}{p_i}\right) = \prod_{i=1}^m (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^m \frac{p_i-1}{2}} = (-1)^{\frac{\prod_{i=1}^m p_i - 1}{2}} = (-1)^{\frac{b-1}{2}}.$$

- (c) Nach Definition, Satz 8.14(c) und Beobachtung 2 gelten

$$\left(\frac{2}{b}\right) = \prod_{i=1}^m \left(\frac{2}{p_i}\right) = \prod_{i=1}^m (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^m \frac{p_i^2-1}{8}} = (-1)^{\frac{\prod_{i=1}^m p_i^2 - 1}{8}} = (-1)^{\frac{b^2-1}{8}}.$$

■

Mit diesen Rechenregeln können wir nun das Jacobi-Symbol sehr effizient berechnen, wie das folgende Beispiel zeigt:

Beispiel 8.20

Wir betrachten das Jacobi-Symbol $\left(\frac{131311}{151515}\right)$. Wir beobachten, dass $131311 \equiv 151515 \equiv 3 \pmod{4}$.

Mit den Rechenregeln aus Anmerkung 8.18 und Satz 8.19 erhalten wir

$$\begin{aligned}
 \left(\frac{131311}{151515}\right) &= \left(\frac{131311 - 151515}{151515}\right) = \left(\frac{(-1) \cdot (151515 - 131311)}{151515}\right) \\
 &= \left(\frac{(-1)}{151515}\right) \cdot \left(\frac{151515 - 131311}{151515}\right) = (-1) \cdot \left(\frac{20204}{151515}\right) \\
 &= (-1) \cdot \left(\frac{2^2 \cdot 5051}{151515}\right) = (-1) \cdot \left(\frac{2^2}{151515}\right) \cdot \left(\frac{5051}{151515}\right) \\
 &= (-1) \cdot (-1) \cdot \left(\frac{151515}{5051}\right) = 1 \cdot \left(\frac{30 \cdot 5051 - 15}{5051}\right) \\
 &= \left(\frac{-15}{5051}\right) = \left(\frac{-1}{5051}\right) \cdot \left(\frac{15}{5051}\right) = (-1) \cdot (-1) \cdot \left(\frac{5051}{15}\right) \\
 &= \left(\frac{337 \cdot 15 - 4}{15}\right) = \left(\frac{-1}{15}\right) \cdot \left(\frac{2^2}{15}\right) = (-1) \cdot 1 = -1
 \end{aligned}$$

Nach Anmerkung 8.18(3) kann also 131311 kein quadratischer Rest modulo 151515 sein. Daher muss 131311 quadratischer Nichtrest modulo 151515 sein.

26 Aufgaben zu Kapitel 8

Aufgabe 31

(a) Berechnen Sie

$$\left(\frac{241}{5}\right), \left(\frac{242}{5}\right), \left(\frac{243}{5}\right), \left(\frac{244}{5}\right), \text{ und } \left(\frac{81}{97}\right).$$

(b) Sei nun $p \in \mathbb{P} \setminus \{2\}$ eine ungerade Primzahl. Zeigen Sie, dass

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

Aufgabe 32

(a) Berechnen Sie $\left(\frac{503}{773}\right)$ mithilfe des quadratischen Reziprozitätsgesetz.

(b) Sei p eine ungerade Primzahl und sei $a \in \mathbb{Z}$ mit $\text{ggT}(a, p) = 1$. Zeigen Sie: a ist genau dann quadratischer Rest modulo p , wenn a quadratischer Rest modulo p^2 ist.

Aufgabe 33

(a) Sei $p \in \mathbb{P}$ eine Primzahl mit $p \equiv 3 \pmod{4}$ und a ein Quadrat modulo p . Zeigen Sie, dass $a^{(p+1)/4}$ eine Lösung von $x^2 \equiv a \pmod{p}$ ist.

(b) Beweisen Sie, dass $a = 83$ ein quadratischer Rest modulo $n = 361$ ist und finden Sie eine Lösung der Gleichung $x^2 \equiv a \pmod{361}$.

[Hinweise: $361 = 19^2$ und 2 ist Primitivwurzel modulo 361.]

Aufgabe 34

Verwenden Sie das Lemma von Gauß (Lemma 8.10 im Skript) zu zeigen, dass

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

Aufgabe 35

- (a) Berechnen Sie $\left(\frac{501}{773}\right)$ mithilfe des quadratischen Reziprozitätsgesetz.
- (b) Zeigen Sie, dass es unendlich viele Primzahlen $p \in \mathbb{P}$ existieren, so dass $p \equiv \pm 1 \pmod{8}$ gilt.

[Hinweise:

(1) Verwenden Sie das folgende Ergebnis aus der Algebra I: Es existieren unendlich viele Primzahlen $p \in \mathbb{P}$, so dass das Polynom $X^2 - [2]_p \in \mathbb{Z}/p\mathbb{Z}[X]$ eine Nullstelle in $\mathbb{Z}/p\mathbb{Z}$ besitzt.

(2) Verwenden Sie Aufgabe 2.]

Aufgabe 36

Für welche ungeraden natürlichen Zahlen n gilt für das Jacobi-Symbol $\left(\frac{15}{n}\right) = 1$? Geben Sie dabei Ihre Antwort modulo 60 an.

- (1) Geben Sie eine Bedingung auf $\text{ggT}(15, n)$ an.
- (2) Unterscheiden Sie weiter zwei Fälle:
- (i) $n \equiv 1 \pmod{4}$; und
 - (ii) $n \equiv 3 \pmod{4}$.

[Hinweise: Verwenden Sie die Multiplikativität des Jacobi-Symbols und das quadratische Reziprozitätsgesetz. Betrachten Sie auch n modulo 3 und modulo 5, und wenden Sie den Chinesischen Restsatz an.]

Aufgabe 37

- (a) Ist 1001 ein quadratischer Rest modulo 2433?
- (b) Berechnen Sie $\left(\frac{52344}{5001}\right)$ mithilfe des quadratischen Reziprozitätsgesetz für das Jacobi-Symbol.