EDUARD-SPRANGER-BERUFSKOLLEG
Berufskolleg und Berufliches Gymnasium der Stadt Hamm
für Technik, Informatik und Gestaltung

Fachkonferenz Mathematik/Naturwissenschaften

Von der Teilbarkeit zum RSA-Verfahren

Grundlagen der Zahlentheorie

EDUARD-SPRANGER-BERUFSKOLLEG
Berufskolleg und Berufliches Gymnasium der Stadt Hamm
für Technik, Informatik und Gestaltung

Fachkonferenz Mathematik/Naturwissenschaften

Von der Teilbarkeit zum RSA-Verfahren

Grundlagen der Zahlentheorie

Dr. Frank Klinker [*,1], Dr. Lothar Mischke [1], Willy Pöttker [2]

[1] Eduard-Spranger-Berufskolleg, Hamm
[2] Freies Evangelisches Limbacher Schulzentrum, Limbach-Oberfrohna

[*] Korrespondenzautor

Version: April 2025

Inhaltsverzeichnis

1 Teilbarkeit, Teiler, Primzahlen und Teilen mit Rest

1.1 Teilbarkeit und Teiler

Sind a und b zwei positive natürliche Zahlen, dann gilt[1]

a **ist Teiler von** $b \iff$ Es gibt eine natürliche Zahl k, sodass $b = k \cdot a$

Statt a **ist Teiler von** b sagt man auch b **wird von** a **geteilt** oder a **teilt** b und schreibt $a|b$.

Beispiel 1.1. 3 teilt 102, denn $102 = 34 \cdot 3$. Deswegen teilt auch 34 die Zahl 102.

Fakt 1.2.

1. a und 1 sind immer Teiler von a. 1 ist die einzige Zahl mit nur einem Teiler.
2. Ist a ein Teiler von b und b ein Teiler von a, dann ist $a = b$.
3. Ist a ein Teiler von b und b ein Teiler von c, dann ist a ein Teiler von c.
4. Ist a ein Teiler von b, dann ist $a \leq b$.
5. Ist a ein Teiler von b, dann gibt es einen weiteren Teiler a' von b mit $a \cdot a' = b$, sodass Teiler immer in "Paaren" vorkommen.

   Ist keiner der beiden Teiler die Zahl 1, dann sind beide $\leq \frac{b}{2}$.

   Üblicherweise ist die Zahl der unterschiedlichen Teiler einer Zahl gerade. Lediglich in dem Fall $a \cdot a = b$ ist die Zahl der Teiler ungerade, also wenn $b \geq 4$ eine Quadratzahl ist.
6. Ist a ein Teiler von b und b ein Teiler von a, dann ist $a = b$.
7. Ist a ein Teiler von b und von c, dann ist a ein Teiler von $b \pm c$ und von $b \cdot c$.
8. Ist a ein Teiler von b oder von c, dann ist a ein Teiler von $b \cdot c$.
9. Die Umkehrung von 8. ist im Allgemeinen falsch, wie man an folgendem Beispiel sieht:

   12 teilt zwar $40 \cdot 30 = 1200$, aber 12 teilt weder 40 noch 30.

   Die Umkehrung von 4. kann aber richtig sein, wie das folgende Beispiel zeigt:

[1] In diesem Abschnitt sind alle Aussagen für positive natürliche Zahlen formuliert. Eine Erweiterung für negative Zahlen ist sinngemäß möglich.

12 teilt $24 \cdot 50 = 1200$, und 12 teilt den Faktor 24.

Ob die Umkehrung gilt, hängt also stark von der Zerlegung von 1200 in ein Produkt ab.

Später wird eine Situation besprochen, wo die Umkehrung unabhängig von der Zerlegung gilt (siehe Folgerung 2.3).

10. Ist a kein Teiler von $b \cdot c$, dann teilt a weder b noch c.

Fakt 1.3. Eine Zahl kann viele oder wenig Teiler haben:

- 60 hat viele Teiler: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 und 60
- 65 hat wenig Teiler: 1, 5, 13, 65
- 71 hat nur zwei Teiler: 1, 71

1.2 Primzahlen

Die Zahlen mit der minimalen Anzahl an Teilern werden eine wichtige Rolle spielen:

Definition 1.4. Eine Zahl p, die nur die zwei Teiler 1 und p hat, heißt **Primzahl**

Fakt 1.5.

- 1 ist keine Primzahl, da sie keine zwei Teiler hat.
- 2 ist die kleinste Primzahl.
- Außer 2 sind alle Primzahlen ungerade.
- Die Primzahlen zwischen 1 und 100 sind:

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
  43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

- Der **Sieb des Eratosthenes**[2] ist ein Verfahren, wie man die Primzahlen herausfiltern kann, die kleiner als eine vorgegebene Zahl sind: .

Man kann die Teiler einer Zahl a der Größe sortieren. Das gibt dann:

Fakt 1.6. Der kleinste Teiler $\neq 1$ einer Zahl ist eine Primzahl.

[2] Wikipedia: https://de.wikipedia.org/wiki/Sieb_des_Eratosthenes

Dass Fakt 1.6 wahr ist, sieht man wie folgt:

- Es wird vorausgesetzt, dass a der kleinste Teiler einer vorgegebenen Zahl b ist. Weiter wird angenommen, dass a keine Primzahl ist. Dann lässt a sich selbst in ein Produkt von zwei Zahlen zerlegen, die nicht 1 sind.
- Jeder dieser beiden Faktoren ist dann selbst ein Teiler von b. Beide sind außerdem kleiner als der Teiler a mit dem man gestartet ist.
- Da a aber selbst der kleinste Teiler von b gewesen ist, kann es diese Zerlegung von a nicht geben. Damit ist der kleinste Teiler a von b tatsächlich eine Primzahl.

1.3 Teilen mit Rest

Auch wenn eine Zahl kein Teiler einer anderen ist, dann gibt es eine sehr natürliche Zerlegung:

Fakt 1.7 (Teilbarkeit mit Rest). Ist $0 < a \leq b$, dann gibt es Zahlen k, r mit $k \geq 0$ und $0 \leq r < b - 1$, sodass

$$b = k \cdot a + r$$

Die Zahl r heißt **Rest von b beim Teilen durch a**. Der Rest r ist genau dann Null, wenn a ein Teiler von b ist.

Bemerkung 1.8.

- Praktisch erhält man den Rest r, indem man die Zahl a so lange von b abzieht, bis eine Zahl zwischen Null und b erreicht wird.
- Mit dem Taschenrechner berechnet man $b : a$ und nimmt vom Ergebnis nur den Teil vor dem Komma. Das ist dann k in der Zerlegung und r ist dann $b - k \cdot a$.

Folgerung 1.9. Es gibt unendlich viele Primzahlen.

1.4 Aufgaben zu Abschnitt 1

Aufgabe 1.10. Bestimmen Sie alle Teiler der folgenden Zahlen:

a)	36	b)	120	c)	98	d)	123
e)	99	f)	111	g)	1422	h)	299
i)	155	j)	657	k)	245	l)	63

Aufgabe 1.11. a) Markieren Sie in den Teilern von Aufgabe 1.10 a)-l) jeweils die Primzahlen.

b) Was lässt sich über die weiteren Teiler einer Zahl mit Blick auf die in der Teilermenge enthaltenen Primzahlen sagen?

Aufgabe 1.12. Führen Sie das Teilen mit Rest für die folgenden Zahlenpaare durch:

a) (120, 36) b) (450, 38)

c) (4350, 98) d) (1253, 123)

2 Der ggT und die Primfaktorzerlegung

2.1 Der größte gemeinsame Teiler zweier Zahlen

Man kann die Teiler zweier Zahlen a und b vergleichen und untersuchen, ob es gemeinsame Teiler gibt. Diese gemeinsamen Teiler kann man dann der Größe nach sortieren und bekommt so den größten gemeinsamen Teiler von a und b. Diesen bezeichnet man mit

$$\text{ggT}(a, b) = \textbf{größter gemeinsamer Teiler} \text{ von } a \text{ und } b$$

Zwei Zahlen a und b heißen **teilerfremd**, wenn sie nur 1 als gemeinsamen Teiler haben. Das ist dann auch gleichzeitig ihr größter gemeinsamer Teiler, also:

$$a \text{ und } b \text{ sind } \textbf{teilerfremd} \iff \text{ggT}(a, b) = 1$$

Fakt 2.1. 1. Ist p eine Primzahl, welche die Zahl b nicht teilt, dann gilt $\text{ggT}(p, b) = 1$.

2. Die Aussage in Punkt 1. ist so nicht unbedingt korrekt, wenn p keine Primzahl ist: 4 teilt zwar 10 nicht, aber $\text{ggT}(4, 10) = 2$ ist trotzdem nicht 1.
3. Ist $\text{ggT}(a, b) = g$, dann ist $\text{ggT}\left(\frac{a}{g}, \frac{b}{g}\right) = 1$
4. Ist $\text{ggT}(a, b) = g$, dann ist ebenfalls $\text{ggT}(a - b, b) = g$

2.2 Eigenschaften von Primzahlen und die Primfaktorzerlegung

Die folgenden Aussagen im Zusammenhang mit Primzahlen sind sehr natürlich aber auch sehr nützlich:

Fakt 2.2. Ist p eine Primzahl und a eine natürliche Zahl mit $\text{ggT}(a, p) = 1$, dann sind nur die Vielfachen

$$a \cdot p, \quad a \cdot 2 \cdot p, \quad a \cdot 3 \cdot p, \quad \ldots$$

durch p teilbar.

Diese Tatsache gibt uns die Möglichkeit, die Teilbarkeitseigenschaft von Produkten auch umzukehren:

Folgerung 2.3. Ist p eine Primzahl, dann gilt:

Ist p ein Teiler von $a \cdot b$, dann ist p Teiler von a oder Teiler von b

Die Primzahlen und ihre Eigenschaften ermöglichen uns nun, jede Zahl in ”minimale” Faktoren zu zerlegen

Fakt 2.4 (**Primfaktorzerlegung).** Ist a eine natürliche Zahl, dann gibt es eine Zerlegung

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

in ein Produkt von n Primzahlen $p_1, p_2, \ldots, p_n$.
Die Primzahlen $p_1, p_2, \ldots, p_n$ müssen nicht unterschiedlich sein aber die Zerlegung ist bis auf Reihenfolge eindeutig.

Beispiel 2.5.

$$\begin{aligned} 60 &= 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5\,, \\ 184 &= 2 \cdot 2 \cdot 2 \cdot 23 = 2^3 \cdot 23\,, \\ 1002 &= 2 \cdot 3 \cdot 167\,, \\ 32 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5\,. \end{aligned}$$

Folgerung 2.6. Ist die Primfaktorzerlegung einer Zahl bekannt, dann erhält man alle Teiler der Zahl, indem man die Primzahlen geeignet zu Produkten kombiniert.

2.3 Aufgaben zu Abschnitt 2

Aufgabe 2.7. a) Erläutern Sie mit Hilfe einer Liste der Primzahlen, wie man mit elementaren Rechnungen die Primfaktorzerlegung einer Zahl erhalten kann.

b) Berechnen Sie mit dem Ergebnis aus a) die Primfaktorzerlegung der folgenden Zahlen:

i)	36	ii)	120	iii)	111	iv)	580
v)	99	vi)	114	vii)	1420	viii)	180

Aufgabe 2.8. a) Erläutern Sie, wie man mit Hilfe der Primfaktorzerlegung einer Zahl ihre sämtlichen Teiler erhalten kann.

b) Berechnen Sie mit dem Ergebnis aus a) die Teiler der Zahlen aus Aufgabe 2.7 b).

3 Der euklidische Algorithmus

Den größten gemeinsamen Teiler zweier Zahlen zu bestimmen, indem zunächst für beide Zahlen alle Teiler bestimmt und dann den größten heraussucht, ist keine sonderlich effiziente Methode. Wünschenswert wäre eine Methode, mit der man den ggT berechnen kann.
Der **euklidische Algorithmus** ist ein Verfahren, welches das Gewünschte tut, denn mit ihm kann man

1. den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ zweier positiver, ganzen Zahlen a, b berechnen und
2. die Zahlen k und ℓ in der Zerlegung $\mathrm{ggT}(a, b) = k \cdot a + \ell \cdot b$ berechnen.

Im Punkt 2. spricht man auch vom erweiterten euklidischen Algorithmus.

3.1 Die Berechnung des größten gemeinsamen Teilers

Fakt 3.1. Mit dem euklidischen Algorithmus erhält man den $\mathrm{ggT}(a, b)$ zweier Zahlen a und b auf einem rechnerischem Weg ohne die Zerlegung der Zahlen in Primfaktoren zu verwenden.

Algorithmus 3.2 (Euklidischen Algorithmus).

$$
\begin{aligned}
&\text{Schritt } 1: && b = k_1 \cdot a + r_1 \\
&\text{Schritt } 2: && a = k_2 \cdot r_1 + r_2 \\
&\text{Schritt } 3: && r_1 = k_3 \cdot r_2 + r_3 \\
& && \vdots \\
&\text{Schritt } i: && r_{i-2} = k_i \cdot r_{i-1} + r_i \\
& && \vdots \\
&\text{Schritt } m-1: && r_{m-3} = k_{m-1} \cdot r_{m-2} + r_{m-1} \\
&\text{Schritt } m: && r_{m-2} = k_m \cdot r_{m-1} + \boxed{r_m} \\
&\text{Schritt } m+1: && r_{m-1} = k_{m+1} \cdot r_m
\end{aligned}
$$

- Schritt 1: Man stellt b als Vielfaches von a mit Rest dar: Rest ist r_1.
- Schritt 2: Man stellt a als Vielfaches von r_1 mit Rest dar: Rest ist r_2.
- Schritt 3: Man stellt r_1 als Vielfaches von r_2 mit Rest dar: Rest ist r_3.
- Man wiederholt dies so lange, bis es keinen Rest mehr gibt (das klappt, da der positive Rest in jedem Schritt kleiner wird).
- Im vorletzten m-ten Schritt hat man dann als Rest $r_m = \mathrm{ggT}(a, b)$ stehen.

3.2 Der erweiterte euklidische Algorithmus

Der euklidische Algorithmus liefert eine Darstellung von $\mathrm{ggT}(a, b)$ durch die Zahlen a und b:

Fakt 3.3. Sind a und b ganze Zahlen, dann gibt es ganze Zahlen k und ℓ, sodass

$$k \cdot a + \ell \cdot b = \mathrm{ggT}(a, b) \,.$$

Algorithmus 3.4 (Erweiterter euklidischer Algorithmus).
Um die Zerlegung $\mathrm{ggT}(a, b) = k \cdot a + \ell \cdot b$ zu erhalten, nimmt man die Rechnung des euklidischen Algorithmus her und geht wie folgt vor:

- Man löst Schritt 1 des Algorithmus nach dem Rest r_1 auf
- Man löst Schritt 2 nach r_2 auf und ersetzt dort r_1 durch das vorige Ergebnis.
- Man löst Schritt 3 nach r_3 auf und ersetzt dort r_1 und r_2 durch die zwei vorigen Ergebnisse.
- Man löst Schritt 4 nach r_4 auf und ersetzt dort r_2 und r_3 durch die zwei vorigen Ergebnisse.
- Diesen letzten Punkt wiederholt man nun für Schritt 5 bis Schritt m.

Beispiel 3.5. Durchführung des erweiterten euklidischen Algorithmus für die Zahlen $a = 158$ und $b = 288$.
Dabei finden man links die Berechnung von $\mathrm{ggT}(a, b)$ und rechts die Berechnung der Zerlegung $\mathrm{ggT}(a, b) = k \cdot a + \ell \cdot b$:

$$
\begin{array}{lll}
\underline{288} = 1 \cdot \underline{158} + \underline{130} & \rightarrow & \underline{130} = 1 \cdot \underline{288} - 1 \cdot \underline{158} \\
\underline{158} = 1 \cdot \underline{130} + \underline{28} & \rightarrow & \underline{28} = \underline{158} - 1 \cdot \underline{130} \\
 & & \quad = \underline{158} - 1 \cdot (1 \cdot \underline{288} - 1 \cdot \underline{158}) \\
 & & \quad = 2 \cdot \underline{158} - 1 \cdot \underline{288} \\
\underline{130} = 4 \cdot \underline{28} + \underline{18} & \rightarrow & \underline{18} = \underline{130} - 4 \cdot \underline{28} \\
 & & \quad = (1 \cdot \underline{288} - 1 \cdot \underline{158}) - 4 \cdot (2 \cdot \underline{158} - 1 \cdot \underline{288}) \\
 & & \quad = 5 \cdot \underline{288} - 9 \cdot \underline{158} \\
\underline{28} = 1 \cdot \underline{18} + \underline{10} & \rightarrow & \underline{10} = \underline{28} - 1 \cdot \underline{18} \\
 & & \quad = (2 \cdot \underline{158} - 1 \cdot \underline{288}) - 1 \cdot (5 \cdot \underline{288} - 9 \cdot \underline{158}) \\
 & & \quad = 11 \cdot \underline{158} - 6 \cdot \underline{288} \\
\underline{18} = 1 \cdot \underline{10} + \underline{8} & \rightarrow & \underline{8} = \underline{18} - 1 \cdot \underline{10} \\
 & & \quad = (5 \cdot \underline{288} - 9 \cdot \underline{158}) - 1 \cdot (11 \cdot \underline{158} - 6 \cdot \underline{288}) \\
 & & \quad = 11 \cdot \underline{288} - 20 \cdot \underline{158} \\
\underline{10} = 1 \cdot \underline{8} + \boxed{2} & \rightarrow & \boxed{2} = \underline{10} - 1 \cdot \underline{8} \\
 & & \quad = (11 \cdot \underline{158} - 6 \cdot \underline{288}) - 1 \cdot (11 \cdot \underline{288} - 20 \cdot \underline{158}) \\
 & & \quad = 31 \cdot \underline{158} - 17 \cdot \underline{288} \\
\underline{8} = 4 \cdot \underline{2} & &
\end{array}
$$

Damit hat man schließlich

$$\mathrm{ggT}(288, 158) = 2 \quad \text{und} \quad 2 = 31 \cdot 158 - 17 \cdot 288\,.$$

3.3 Aufgaben zu Abschnitt 3

Aufgabe 3.6. a) Erläutern Sie, wie man mit Hilfe der Primfaktorzerlegungen zweier Zahlen ihren größten gemeinsamen Teiler bestimmen kann.

b) Berechnen Sie mit dem Ergebnis aus a) die ggT aller Paare, die sich aus den folgenden Zahlen bilden lassen:

$$36,\ 12,\ 111,\ 580,\ 99,\ 114,\ 1420,\ 180\,.$$

Aufgabe 3.7. Berechnen Sie mit Hilfe des erweiterten euklidischen Algorithmus

1) den größten gemeinsamen Teiler der Zahlen a und b, sowie

2) die ganzen Zahlen k und ℓ der Zerlegung $\operatorname{ggT}(a,b) = k \cdot a + \ell \cdot b$

für die folgenden Zahlenpaare:

a) $a = 580,\ b = 38$ b) $a = 5040,\ b = 582$

c) $a = 28,\ b = 744$ d) $a = 215,\ b = 64$

e) $a = 225,\ b = 85$ f) $a = 1521,\ b = 99$

4 Algebraische Grundlagen

In diesem Abschnitt werden einige algebraische Strukturen beschrieben, die man beim Umgang mit Zahlen –genauer: beim Rechnen mit Zahlen– bereits kennengelernt hat.
Da diese Strukturen auch in allgemeineren Situationen auftreten können, werden sie hier etwas systematischer und genauer untersucht.
Es wird jeweils zunächst eine allgemeine Beschreibung angegeben und direkt im Anschluss die bekannten Beispiele dazu aufgeführt.

Bezeichnung 4.1. Eine **Verknüpfung auf einer Menge** ist eine Operation, die zwei Elementen aus der Menge ein neues Element der Menge zuordnet.

Beispiel 4.2.
1. Zum Beispiel sind Addition "+" und Multiplikation "$\cdot$" Verknüpfungen auf der Menge der natürlichen Zahlen $\mathbb{N}$.
2. Genauso sind "+" und "$\cdot$" auch Verknüpfungen auf den anderen bekannten Zahlenmengen: den ganzen Zahlen $\mathbb{Z}$, den rationalen Zahlen $\mathbb{Q}$ und den reellen Zahlen $\mathbb{R}$.
3. Das Teilen ":" ist eine Verknüpfung auf der Menge der rationalen Zahlen $\mathbb{Q}$ und auf der Menge reellen Zahlen $\mathbb{R}$.
4. Das Teilen ":" ist keine Verknüpfung auf $\mathbb{N}$ und $\mathbb{Z}$.

Da das Ergebnis einer Verknüpfung auf einer Menge immer in der Menge enthalten sein muss, spricht man auch davon, die Verknüpfung sei **abgeschlossen**.

4.1 Gruppen

Definition 4.3. Eine **Gruppe** $(G, \circ)$ ist eine Menge G mit einer Verknüpfung $\circ$ mit den folgenden Eigenschaften 1.-3.:

1.	$(a \circ b) \circ c = a \circ (b \circ c)$ für alle a, b, c in G	**Assoziativgesetz** oder **Verbindungsgesetz**
2.	Es gibt in G ein Element n, sodass $n \circ a = a \circ n = a$ für alle a in G	Existenz eines **neutralen Elements**
3.	Zu jedem Element a in G gibt es ein Element a' in G, sodass $a \circ a' = a' \circ a = n$	Existenz von **inversen Elementen**

Gilt zusätzlich noch die Eigenschaft 4., dann heißt $(G, \circ)$ eine **kommutative Gruppe**:

4. $a \circ b = b \circ a$ für alle a, b in G — **Kommutativgesetz** oder **Vertauschungsgesetz**

Beispiel 4.4.

1. Die ganzen Zahlen $\mathbb{Z}$ mit der Addition + bilden eine kommutative Gruppe. Das neutrale Element ist die Null und das Inverse Element zu einer Zahl a ist die Zahl $-a$.
2. Auf die gleiche Art bilden die rationalen Zahlen $\mathbb{Q}$ und die reellen Zahlen $\mathbb{R}$ jeweils mit der Addition + eine kommutative Gruppe.
3. Die rationalen Zahlen ohne Null $\mathbb{Q}\setminus\{0\}$ bilden mit der Multiplikation $\cdot$ eine kommutative Gruppe. Das neutrale Element ist die Eins und zur Zahl q ist die Zahl $\frac{1}{q}$ das inverse Element.
4. Auf die gleiche Art bilden die reellen Zahlen ohne Null $\mathbb{R}\setminus\{0\}$ mit der Multiplikation $\cdot$ eine kommutative Gruppe.
5. Die Menge aller Vektoren mit der Addition ist eine kommutative Gruppe. Das neutrale Element ist der Nullvektor und das inverse Element zu $\vec{v}$ ist $-\vec{v}$.
6. Alle Funktionen von $\mathbb{R}$ nach $\mathbb{R}$, die eine Umkehrfunktion besitzen, bilden mit der Hintereinanderausführung eine (nicht kommutative) Gruppe. Das neutrale Element ist die identische Abbildung, die jede Zahl auf sich selbst abbildet. Das inverse Element zu $f(x)$ ist ihre Umkehrabbildung $f^{-1}(x)$.
7. In der Ebene bilden die Drehungen um den Ursprung eine kommutative Gruppe. Die Verknüpfung ist dabei die Hintereinanderausführung zweier Drehungen, das neutrale Element ist die Drehung um den Winkel $0°$ und das Inverse einer Drehung ist die Drehung in umgekehrter Richtung mit gleichem Winkel.

Definition 4.5. Ein **Ring** $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfung $+$ und $\cdot$ mit den folgenden Eigenschaften 1.-3.:

1.	$(R, +)$ ist kommutative Gruppe	Das neutrale Element n bzgl. $+$ heißt **Nullelement**
2.	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle a, b, c in R	Assoziativgesetz für $\cdot$
3.	$a \cdot (b + c) = a \cdot b + a \cdot c$ $(b + c) \cdot a = b \cdot a + c \cdot a$ für alle a, b, c in R	**Distributivgesetz** oder **Verteilungsgesetz**

Gilt in einem Ring zusätzlich noch die Eigenschaft 4., dann heißt $(R, +, \cdot)$ ein **kommutativer Ring**:

4.	$a \cdot b = b \cdot a$ für alle a, b in R	Kommutativgesetz für $\cdot$

Gilt in einem Ring zusätzlich noch die Eigenschaft 5., dann heißt $(R, +, \cdot)$ ein **Ring mit Eins**:

5.	Es gibt in R ein Element e, sodass $e \cdot a = a \cdot e = a$ für alle a in R	Das neutrale Element e bzgl. $\cdot$ heißt **Einselement**

Gilt in einem Ring zusätzlich noch die Eigenschaft 6., dann heißt $(R, +, \cdot)$ ein **nullteilerfreier Ring**:

6. Sind a und b ungleich dem Nullelement, dann ist auch $a \cdot b$ nicht das Nullelement

Fakt 4.6. Für einen kommutativen Ring $(R, +, \cdot)$ besteht die Menge R^* aus allen Elementen, die bezüglich $\cdot$ invertierbar sind.
R^* ist zusammen mit $\cdot$ eine kommutative Gruppe.

Beispiel 4.7. 1. Die ganzen Zahlen $\mathbb{Z}$ mit der Addition $+$ und der Multiplikation $\cdot$ bilden einen kommutativen Ring mit Eins. Das Nullelement ist die Null und das Einselement ist die Eins.

$(\mathbb{Z}, +, \cdot)$ ist nullteilerfrei, denn in $a \cdot b = 0$ muss immer $a = 0$ oder $b = 0$

sein.

In $\mathbb{Z}$ sind nur die Zahlen ± 1 bezüglich der Multiplikation invertierbar. Damit besteht die Gruppe $(\mathbb{Z}^*, \cdot)$ nur aus diesen beiden Elementen.

2. Genauso sind auch $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ nullteilerfreie, kommutative Ringe mit Eins.

   In $\mathbb{R}$ und $\mathbb{Q}$ sind alle Zahlen außer der Null invertierbar bezüglich $\cdot$. Damit ist $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$ und $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$.

3. Die Menge aller geraden ganzen Zahlen mit Addition und Multiplikation bildet einen kommutativen Ring. Er ist nullteilerfrei, besitzt aber keine Eins.

4.3 Körper

Definition 4.8. Ein **Körper** $(K, +, \cdot)$ ist eine Menge K mit zwei Verknüpfung $+$ und $\cdot$ mit den folgenden Eigenschaften 1.-3.:

1. $(K, +)$ ist kommutative Gruppe mit Nullelement 0
2. $(K\setminus\{0\}, \cdot)$ ist kommutative Gruppe mit Einselement 1
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle a, b, c in K (Distributivgesetz)

Fakt 4.9.
- Jeder Körper ist ein kommutativer Ring mit Eins, in welchem jedes Element außer das Nullelement invertierbar ist.
- Jeder Körper ist nullteilerfrei.

Beispiel 4.10.
1. Die rationalen Zahlen $\mathbb{Q}$ mit Addition $+$ und Multiplikation $\cdot$ bilden einen Körper mit Nullelement 0 und Einselement 1.
2. Genauso bilden auch die reellen Zahlen $(\mathbb{R}, +, \cdot)$ einen Körper.
3. Die Menge der Paare (a, b) reeller Zahlen bezeichnet man mit $\mathbb{R}^2$. Auf dieser Menge werden zwei Verknüpfungen $\oplus$ und $\odot$ eingeführt:

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \odot (c, d) = (ac - bd, ad + bc).$$

   Dann ist $(\mathbb{R}^2, \oplus, \odot)$ ein Körper (die **komplexe Zahlen**):

- Das Nullelement ist $(0, 0)$.
- Das Einselement ist $(1, 0)$.
- Zu (a, b) ist $(-a, -b)$ das inverse Element bezüglich $\oplus$.
- Zu $(a, b) \neq (0, 0)$ ist $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ das inverse Element bezüglich $\odot$.

4.4 Aufgaben zu Abschnitt 4

Aufgabe 4.11. Führen Sie die Details zu den Beispielen in diesem Abschnitt durch.

Aufgabe 4.12. Überprüfen Sie, ob es sich bei den folgenden Operationen $\circ$ jeweils um Vernüpfungen auf den angegebenen Mengen handelt, d. h. ob sie abgeschlossen sind:

a) $a \circ b = a^2 - b$ auf $\mathbb{N}$

b) $a \circ b = a^2 - b$ auf $\mathbb{Z}$

c) $a \circ b = a^2 \cdot b^2$ auf $\mathbb{Q}$

d) $a \circ b = a \cdot b + a + b$ auf $\mathbb{N}$

e) $a \circ b = a^2 + b^2$ auf $\mathbb{N}$

f) $a \circ b = a^2 - b^2$ auf $\mathbb{R}$

Aufgabe 4.13. a) Untersuchen Sie die Verknüpfung aus Aufgabe 4.12 d) auf Kommutativität und Assoziativität.

b) Begründen Sie, warum 0 das neutrale Element der Verknüpfung aus Aufgabe 4.12 d) ist.

c) Begründen Sie, warum es bei der Verknüpfung aus Aufgabe 4.12 d) zu keinem Element außer 0 ein inverses Element gibt.

Aufgabe 4.14. a) Zeigen Sie durch eine allgemeine Rechnung, dass die Verknüpfung aus Aufgabe 4.12 f) die Eigenschaft $a \circ b = -b \circ a$ besitzt.

b) Untersuchen Sie mit Hilfe einer allgemeinen Rechnung, ob die Verknüpfung aus Aufgabe 4.12 f) assoziativ ist.

Aufgabe 4.15. a) Zeigen Sie durch allgemeine Rechnungen, dass die Verknüpfung aus Aufgabe 4.12 c) kommutativ und assoziativ ist.

b) Überprüfen Sie, ob es zur Verknüpfung aus Aufgabe 4.12 c) ein neutrales Element gibt.

5 Der Zahlenraum $\mathbb{Z}_N$

5.1 Die Restklassenmenge $\mathbb{Z}_N$

Teilt man eine ganze Zahl durch eine feste Zahl N, dann hat der Quotient einen Rest der zwischen 0 und $N-1$ liegt.
Ist z. B. $N = 7$, so hat jede Zahle beim Teilen durch 7 den Rest $0, 1, 2, 3, 4, 5$ oder 6.

Definition 5.1. Die Menge der Reste beim Teilen durch N nennt man die **Restklassenmenge** $\mathbb{Z}_N$. Man schreibt dafür

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\} .$$

Beispiel 5.2. Für $N = 7$ ist

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} .$$

5.2 Rechnen in $\mathbb{Z}_N$

Bemerkung 5.3. In der Menge $\mathbb{Z}_N$ kann man addieren, subtrahieren und multiplizieren wie mit ganzen Zahlen.
Man muss nach einer Rechnung das Ergebnis lediglich so "korrigieren", dass es tatsächlich in der Menge $\mathbb{Z}_N$ liegt. Das heißt, man berechnet den Rest beim Teilen durch N. Man spricht auch vom **modularen Rechnen**.
Die Schreibweise dafür ist

$$9 \equiv 2 \bmod 7 , \quad 123 \equiv 21 \bmod 51 , \quad 859 \equiv 3 \bmod 8 , \quad -18 \equiv 2 \bmod 5$$

Für die Zahlen $N = 7$ und $N = 10$ ist die Addition und Multiplikation hier beispielhaft durchgeführt:

Beispiel 5.4 (Addieren in $\mathbb{Z}_7$ und $\mathbb{Z}_{10}$)**.**

$$1 + 5 \equiv 6 \bmod 7 \qquad 6 + 8 \equiv 14 \equiv 4 \bmod 10$$

$$3 + 4 \equiv 7 \equiv 0 \bmod 7 \qquad 7 + 3 \equiv 10 \equiv 0 \bmod 10$$

Für $N = 7$ und $N = 10$ hat man die folgenden zwei **Additionstabellen**:

$\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\mathbb{Z}_{10}$

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Beispiel 5.5 (Multiplizieren in $\mathbb{Z}_7$ und $\mathbb{Z}_{10}$)**.**

$$1 \cdot 5 \equiv 5 \bmod 7 \qquad 6 \cdot 8 \equiv 48 \equiv 8 \bmod 10$$
$$3 \cdot 4 \equiv 12 \equiv 5 \bmod 7 \qquad 7 \cdot 3 \equiv 21 \equiv 1 \bmod 10$$

Das gibt für $N = 7$ und $N = 10$ die folgenden zwei **Multiplikationstabellen**:[3]

$\mathbb{Z}_7$

·	1	2	3	4	5	6
∗1	1	2	3	4	5	6
∗2	2	4	6	1	3	5
∗3	3	6	2	5	1	4
∗4	4	1	5	2	6	3
∗5	5	3	1	6	4	2
∗6	6	5	4	3	2	1

$\mathbb{Z}_{10}$

·	1	2	3	4	5	6	7	8	9
∗1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
∗3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
∗7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
∗9	9	8	7	6	5	4	3	2	1

Die Zeile und Spalte zu 0 wird in der Multiplikationstabelle weggelassen, weil die Ergebnisse immer 0 ergeben.

[3] Warum man in der Tabelle an manchen Stellen ein ∗ findet, wird ab Bemerkung 6.3 erklärt.

5.3 Aufgaben zu Abschnitt 5

Aufgabe 5.6. a) Berechnen Sie:

i) $3 \cdot 5 \bmod 12$ ii) $14 \cdot (-25) \bmod 4$

iii) $-7 + 19 \bmod 3$ iv) $(-4) + 18 \bmod 6$

v) $8 \cdot (114 + 300) \bmod 3$ vi) $(17 \cdot 9) \cdot 132 \bmod 12$

b) Überprüfen Sie die Rechnungen und korrigieren Sie gegebenenfalls:

i) $14 - 15 \equiv 3 \bmod 4$ ii) $157 \cdot 151 \equiv -5 \bmod 3$

iii) $583^3 \equiv 1 \bmod 4$ iv) $5^{121} \equiv 1 \bmod 6$

Aufgabe 5.7. Berechnen Sie möglichst geschickt unter Ausnutzung der gültigen Rechenregeln:

a) $12 \cdot 27 \bmod 13$ b) $112 \cdot 917856 \bmod 4$

c) $3100 + 201 \bmod 5$ d) $423 + 21 \cdot 313 \bmod 5$

e) $105 \cdot 82 + 213 \cdot 197 \bmod 9$ f) $5^{121} \equiv 5 \bmod 7$

Aufgabe 5.8. a) Stellen Sie die Additions- und die Multiplikationstabelle für das Rechnen modulo 11 auf.

b) Stellen Sie die Additions- und die Multiplikationstabelle für $\mathbb{Z}_8$ auf.

Aufgabe 5.9. a) Begründen Sie, warum eine Zahl genau dann durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist.

b) Begründen Sie, warum die "Quersummenregel" auch für den Teiler 9 gilt, aber für keinen anderen Teiler.

c) Formulieren Sie auf der Basis der bisherigen Überlegungen eine alternative Quersummenregel für den Teiler 11.

Aufgabe 5.10. Die 13-stellige Europäische Artikelnummer (EAN-13) besteht aus 12 Ziffern, die einen Artikel eindeutig identifizieren. Dazu kommt eine dreizehnte Prüfziffer, an der man erkennen kann, ob die vorigen Ziffern korrekt sind. Diese Nummer wird in der Regel durch einen Strichcode ergänzt.

Grafik: Wikipedia

Grafik: F.K.

Die Ziffern der EAN-13 werden von vorne nach hinten durchnummeriert, wobei P die Prüfziffer bezeichnet: $z_1\, z_2\, z_3\, z_4\, z_5\, z_6\, z_7\, z_8\, z_9\, z_{10}\, z_{11}\, z_{12}\, P$.
Die Prüfziffer ergibt sich aus den ersten zwölf Ziffern wie folgt:

$$(z_1 + z_3 + z_5 + z_7 + z_9 + z_{11}) + 3 \cdot (z_2 + z_4 + z_6 + z_8 + z_{10} + z_{12}) + P \equiv 0 \bmod 10$$

a) Überprüfen Sie durch Rechnung, ob die Prüfziffer in dem Beispiel aus der Wikipedia korrekt ist.

b) In der zweiten Grafik ist die Prüfziffer abhanden gekommen. Berechnen Sie diese.

Aufgabe 5.11 (Additive Verschlüsselung)**.** Eine einfache Art einen Text zu verschlüsseln ist die Caesar-Verschlüsselung. Bei ihr erhält man den verschlüsselten Buchstaben im Wesentlichen dadurch, dass man ihn durch einen im Alphabet verschobenen ersetzt. Beschreiben lässt sich das wie folgt:

- Man ersetzt jeden Buchstaben durch seine Stelle im Alphabet: $A = 1, B = 2, \ldots, Z = 26$
- Der Schlüssel s gibt die Anzahl der Stellen wieder, um die man verschiebt (dabei ist $s > 0$ oder $s < 0$ abhängig davon, ob man nach rechts oder nach links verschiebt).
- Entspricht x dem Buchstaben der Originalnachricht, dann entspricht $y \equiv x + s \bmod 26$ dem Buchstaben der verschlüsselten Nachricht.

a) Verschlüsseln Sie den Text *Das Kaninchen versteckt sich in seinem Bau* mit $s = 5$.

b) Erläutern Sie, warum die Gleichung $x \equiv y - s \bmod 26$ geeignet ist, um den verschlüsselten Text zu decodieren.

c) Entschlüsseln Sie den folgenden Text, der mit $s = 8$ verschlüsselt wurde: *lmz nckpa eizbmb dwz lmu jic*.

d) Erläutern Sie, warum die Verschlüsselungen mit den Schlüsseln s und $s' = -(26 - s) < 0$ das gleiche Resultat liefern.

e) Die spezielle Caesar-Verschlüsselung zum Schlüssel $s = 13$ nennt man **ROT13**. Erläutern Sie, was das Besondere an dieser Verschlüsselung ist.

Aufgabe 5.12 (Multiplikative Verschlüsselung)**.** Das achtstellige Geburtsdatum $z_1\, z_2\, .\, z_3\, z_4\, .\, z_5\, z_6\, z_7\, z_8$ einer Person wird innerhalb einer Behörde

verschlüsselt weitergeleitet. Dazu wird jede Ziffer des Datums mit Hilfe der Formel

$$y_i \equiv 3 \cdot z_i \bmod 10$$

codiert .

a) Codieren Sie das Datum 17.03.1984.

b) Begründen Sie im Detail, warum $z_i \equiv 7 \cdot y_i \bmod 10$ die Formel zum Entschlüsseln der Daten ist.

c) Entschlüsseln Sie 32023714.

d) Begründen Sie, warum die Formel $y_i = 4 \cdot z_i \bmod 10$ nicht zum Verschlüsseln geeignet ist.

e) Erläutern Sie, welche Eigenschaft die Zahl a mindestens besitzen muss, damit $y_i = a \cdot z_i \bmod 10$ zum Verschlüsseln verwendet werden kann.

6 Teilerfremdheit und die Eulersche φ-Funktion

6.1 Teilerfremdheit und Ergänzungen zu den Restklassenmengen

Um die Multiplikationstabellen weiter untersuchen zu können, wiederholen wir:

Zwei Zahlen $a, b \in \mathbb{Z}$ mit $a, b \neq 0$ heißen **teilerfremd**, wenn sie als gemeinsamen Teiler lediglich die 1 haben. Dann ist die 1 auch der größte gemeinsame Teiler, also

$$\mathrm{ggT}(a, b) = 1 .$$

Beispiel 6.1.
- Die Zahlen 10 und 4 sind nicht teilerfremd, denn sie haben neben 1 noch den gemeinsamen Teiler 2, sodass $\mathrm{ggT}(4, 10) = 2$.
- Die Zahlen 10 und 9 sind teilerfremd, denn es ist $\mathrm{ggT}(9, 10) = 1$.
- Die Zahl 7 ist teilerfremd zu jeder Zahl außer zu ihren Vielfachen. Das gilt nicht nur für die 7, sondern für jede Primzahl p:

$$\mathrm{ggT}(p, a) = 1, \quad \text{für } a \neq kp, \ k \in \mathbb{Z}$$

Bemerkung 6.2. Addieren, Subtrahieren und Multiplizieren macht in der Restklassenmenge $\mathbb{Z}_N$ keine großen Probleme. Größere Probleme gibt es da beim Dividieren. Das ist allerdings zunächst nicht verwunderlich, denn die Division klappt ja schon in $\mathbb{Z}$ nicht uneingeschränkt.

Allerdings bemerkt man z. B. in $\mathbb{Z}_{10}$ das folgende Phänomen: Es gelten die Gleichungen

$$5 \cdot 3 \equiv 5 \cdot 17 \bmod 10 \qquad \text{und} \qquad 7 \cdot 3 = 7 \cdot 13 \bmod 10 .$$

Hier kann man in der rechten Gleichung die 7 kürzen, denn es ist $3 \equiv 13 \bmod 10$. Aber in der linken Gleichung darf man die 5 nicht kürzen, denn es ist $3 \not\equiv 17 \bmod 10$.

Der Unterschied besteht darin, dass $\mathrm{ggT}(7, 10) = 1$ (dann darf man kürzen), aber $\mathrm{ggT}(5, 10) \neq 1$ (dann darf man nicht kürzen).

Das kann man so zusammenfassen:

Ist $m \cdot a \equiv m \cdot b \bmod N$ und $\mathrm{ggT}(m, N) = 1$, dann ist $a \equiv b \bmod N$

Etwas allgemeiner gilt sogar:

Ist $m \cdot a \equiv m \cdot b \bmod N$ und $\mathrm{ggT}(m, N) = g$, dann ist $a \equiv b \bmod \frac{N}{g}$

Sieht man sich die zwei Multiplikationstabellen zu $N = 10$ und $N = 7$ genauer an, dann bemerkt man:

Bemerkung 6.3.

- In den Multiplikationstabellen ist auffällig, dass in einigen Zeilen und analogen Spalten jede mögliche Zahl $\neq 0$ auch als Ergebnis vorkommt (das sind die Zeilen mit $*$).
- In $\mathbb{Z}_7$ trifft dies für jede Zeile zu, in $\mathbb{Z}_{10}$ aber nur für die Zeilen zu 1,3,7 und 9.
- In den anderen Zeilen fehlen nicht nur Zahlen, sondern es tritt auch die Zahl 0 als Ergebnis einer Multiplikation auf.

  Das ist ein entscheidender Unterschied zur Multiplikation mit "gewöhnlichen Zahlen", wo das Produkt zweier Zahlen nie Null ist, wenn die beiden Faktoren nicht Null sind.

Fakt 6.4.

1. In der Multiplikationstabelle zu $\mathbb{Z}_N$ treten in der Zeile zur Zahl a alle Zahlen von 1 bis $N-1$ auf, wenn N und a teilerfremd sind, also wenn $\mathrm{ggT}(N, a) = 1$.
2. In der Multiplikationstabelle zu $\mathbb{Z}_N$ treten in den Zeilen zur Zahl a nicht alle Zahlen von 1 bis $N-1$ auf, wenn N und a nicht teilerfremd sind, also wenn $\mathrm{ggT}(N, a) = g > 1$.
   Genauer: Es treten als Reste nur die Vielfachen von g auf. Insbesondere tritt die 1 nicht auf, aber die 0 mindestens einmal.

Die Eigenschaften des modularen Rechnens in $\mathbb{Z}_N$ und Fakt 6.4 lassen sich so zusammenfassen:

Folgerung 6.5.

1. $\mathbb{Z}_N$ ist mit der modularen Addition eine kommutative Gruppe.
2. $\mathbb{Z}_N$ ist mit der modularen Addition und Multiplikation ein kommutativer Ring mit Eins.
3. $\mathbb{Z}_N^*$ enthält alle Elemente aus $\mathbb{Z}_N$, die teilerfremd zu N sind, siehe Fakt 4.6.

4. Sind $a \in \mathbb{Z}_N$ und N nicht teilerfremd, so gibt es eine Zahl $b \in \mathbb{Z}_N$, sodass $a \cdot b = 0 \bmod N$. Das heißt, $\mathbb{Z}_N$ ist nur nullteilerfrei, wenn N eine Primzahl ist.
5. $\mathbb{Z}_N$ ist genau dann ein Körper, wenn N eine Primzahl ist.
6. **Beispiele:**

   $\mathbb{Z}_{10}$ ist ein kommutativer Ring mit Eins, der nicht nullteilerfrei ist.

   $\mathbb{Z}_7$ ist ein Körper.

6.2 Die Eulersche φ-Funktion

Da zu einem vorgegebenen Modus N die hierzu teilerfremden Zahlen eine besondere Rolle spielen, ist es auch interessant, ihre Anzahl zu kennen:

Definition 6.6 (Die Eulersche φ-Funktion).
Für eine positive natürliche Zahl N bezeichnet

$$\varphi(N)$$

die Anzahl der zu N teilerfremden Zahlen in der Menge $\{1, 2, \ldots, N-1\}$. φ heißt die **Eulersche φ-Funktion**.

Beispiel 6.7.

1,2,3,4,5,6 sind teilerfremd zu 7,	$\varphi(7) = 6$
1,3,7,9 sind teilerfremd zu 10	$\varphi(10) = 4$
1,3,5,7 sind teilerfremd zu 8	$\varphi(8) = 4$
1,7,11,13,17,19,23,29 sind teilerfremd zu 30	$\varphi(30) = 8$
1,2,4,7,8,11,13,14 sind teilerfremd zu 15	$\varphi(15) = 8$
1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97, 101, 103, 107, 109, 113, 119 sind teilerfremd zu 120	$\varphi(120) = 32$

Fakt 6.8. Für eine Primzahl p ist die Berechnung von $\varphi(p)$ recht einfach. Da alle Zahlen $1, 2, \ldots, p-1$ teilerfremd zu p sind, gilt:

Ist p eine Primzahl, dann ist $\varphi(p) = p - 1$

Fakt 6.9 (Multiplikationsregel für die Eulersche φ-Funktion).

Lässt sich die Zahl N in das Produkt von zwei teilerfremden Zahlen N_1 und N_2 zerlegen, also $N = N_1 \cdot N_2$, dann gilt

$$\varphi(N) = \varphi(N_1) \cdot \varphi(N_2) .$$

Beispiel 6.10.
- Es ist $120 = 8 \cdot 15$ und $\mathrm{ggT}(8, 15) = 1$. Weiter ist $\varphi(8) = 4$ und $\varphi(15) = 8$. Damit ist $\varphi(8) \cdot \varphi(15) = 4 \cdot 8 = 32$ und das stimmt mit $\varphi(120) = 32$ überein.
- Anderseits ist aber auch $120 = 4 \cdot 30$ aber mit $\mathrm{ggT}(4, 30) = 2 > 1$. Es ist $\varphi(4) = 2$ und $\varphi(30) = 8$ und deshalb $\varphi(4) \cdot \varphi(30) = 2 \cdot 8 = 16$. Das stimmt nicht mit $\varphi(120) = 32$ überein.

Bemerkung 6.11.
- Die Multiplikationsregel ist leider nur bedingt nützlich, weil es ist in der Regel schwierig ist, eine Zahl in ein Produkt teilerfremder Zahlen zu zerlegen.
- Damit ist auch die Berechnung von $\varphi(N)$ in der Regel kompliziert, insbesondere für große N.

In speziellen Fällen lässt sich $\varphi(n)$ jedoch berechnen:

Bemerkung 6.12.
1. Die folgende Verallgemeinerung von Fakt 6.8 ist gültig:

   Ist p eine Primzahl, dann ist $\varphi(p^k) = p^{k-1} \cdot (p - 1)$

2. Hat N die Primkatorzerlegung $N = p_1^{k_1} \cdot_2^{k_2} \cdot \ldots p_r^{k_r}$, dann ist

$$\begin{aligned} \varphi(N) &= p_1^{k_1-1}(p_1 - 1) \cdot_2^{k_2-1} (p_2 - 1) \cdot \ldots p_r^{k_r-1}(p_r - 1) \\ &= N \cdot \left(1 - \tfrac{1}{p_1}\right) \cdot \left(1 - \tfrac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \tfrac{1}{p_r}\right) . \end{aligned}$$

   Insbesondere ist $\varphi(N)$ für alle Zahlen $N > 2$ stets gerade.

6.3 Aufgaben zu Abschnitt 6

Aufgabe 6.13. Bestimmen Sie $\varphi(N)$, indem Sie die Menge der zur Zahl N jeweils die teilerfremden Zahlen auflisten und diese abzählen:

a) $N = 18$ b) $N = 30$ c) $N = 74$ d) $N = 52$

Aufgabe 6.14. In den folgenden Aufgaben sind $p, p_1, p_2, \ldots, p_n$ unterschiedliche Primzahlen und $r, r_1, r_2, \ldots, r_n$ positive ganze Zahlen.
Begründen Sie folgende Aussagen:

a) Ist $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$, dann ist

$$\varphi(N) = (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_n - 1)\,.$$

c) Ist $N = p^r$, dann ist

$$\varphi(N) = p^{r-1}(p - 1) = N \cdot \left(1 - \tfrac{1}{p}\right).$$

e) Ist $N = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_n^{r_n}$, dann ist

$$\varphi(N) = N \cdot \left(1 - \tfrac{1}{p_1}\right) \cdot \left(1 - \tfrac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \tfrac{1}{p_n}\right).$$

Aufgabe 6.15. Mit Hilfe der Ergebnisse aus Aufgabe 6.14 berechnen Sie:

a) $\varphi(8)$ b) $\varphi(546)$

c) $\varphi(56)$ d) $\varphi(288)$

e) $\varphi(16200)$ f) $\varphi(391)$

7 Potenzieren in $\mathbb{Z}_N$ und der Satz von Euler

7.1 Potenzieren in $\mathbb{Z}_N$

Das Potenzieren mit natürlichen Zahlen in der Restklassenmenge $\mathbb{Z}_N$ ist eigentlich kein Problem, denn man muss ja "lediglich" Multiplikationen durchzuführen.
Dabei lohnt es sich Potenzgesetze zu verwenden und sich im Wesentlichen auf kleine Potenzen zurückzuziehen:

Beispiel 7.1.

$$\begin{aligned}
2^7 &\equiv 128 \equiv 9 \bmod 17\\
2^7 &\equiv 2^4 \cdot 2^3 \equiv 16 \cdot 8 \equiv (-1) \cdot 8 \equiv -8 \equiv 9 \bmod 17\\
2^{66} &\equiv (2^4)^{16} \cdot 2^2 \equiv (-1)^{16} \cdot 4 \equiv 4 \bmod 17\\
8^{10} &\equiv ((-3)^2)^5 \equiv (9)^5 \equiv (-2)^5 \equiv -32 \equiv 1 \bmod 11\\
8^{21} &\equiv 8 \cdot (((-3)^2)^2)^5 \equiv 8 \cdot ((-2)^2)^5 \equiv 8 \cdot (4)^5 \equiv 8 \cdot 4 \cdot (4^2)^2\\
&\equiv 8 \cdot 4 \cdot 5^2 \equiv 8 \cdot 4 \cdot 3 \equiv 8 \cdot 12 \equiv 8 \cdot 1 \equiv 8 \bmod 11
\end{aligned}$$

Fakt 7.2. Wenn man bereits weiß, dass es eine Potenz gibt, sodass $a^K \equiv 1 \bmod N$ gilt, dann kann man Rechnungen sehr vereinfachen: Man kann das nämlich nutzen, um einen beliebigen Exponenten zu verkleinern.
Im vorigen Beispiel kann man nutzen, dass $8^{10} \equiv 1 \bmod 11$ ist. Damit hat man

$$8^{21} = 8^{10\cdot 2+1} \equiv (8^{10})^2 \cdot 8 \equiv 1^2 \cdot 8 \equiv 8 \bmod 11\,.$$

Etwas formaler lautet das:

$$\boxed{\text{Gilt } a^K \equiv 1 \bmod N \text{ und } \ell \equiv m \bmod K, \text{ dann ist } a^\ell \equiv a^m \bmod N\,.}$$

Man braucht dann nur noch die Potenzen $a^1, a^2, \ldots, a^{K-1}$ zu berechnen und kennt danach bereits alle!

7.2 Der Satz von Euler

Das Problem in Bemerkung 7.2 besteht nun darin: Wie findet man zu vorgegebener Basis a einen solchen Exponenten K?
Da hilft der folgende Satz von Euler (daher hat die Funktion φ ihren Namen):

Satz 7.3 (Satz von Euler).

Ist N eine positive, natürliche Zahl und $a \in \mathbb{Z}$ teilerfremd zu N, d. h. $\mathrm{ggT}(a, N) = 1$, so gilt

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

Das kann man auch in der folgenden Form formulieren:

$$a^m \equiv a^r \bmod N \quad \text{für } r \equiv m \bmod \varphi(N)$$

Bemerkung 7.4.

1. Das Ergebnis des Satzes ist erstaunlich, denn es besagt, dass es einen Exponenten mit der in Bemerkung 7.2 gewünschten Eigenschaft gibt, der für alle (interessanten) Basen der gleiche ist!

2. Ist p eine Primzahl, dann ist $\varphi(p) = p - 1$. Damit gilt für alle Zahlen $a = 1, 2, \ldots, p-1$:
$$a^{p-1} = 1 \bmod p\,.$$
Schreibt man das etwas anders, so gibt das den Satz von Euler für Primzahlen:

> Für alle Primzahlen p und alle Zahlen a gilt
> $$a^p \equiv a \bmod p\,.$$

Eine Variante des Satzes von Euler kann man formulieren, auch wenn a und N nicht teilerfremd sind. In diesem Fall ist eine zusätzliche Eigenschaft und eine Einschränkung nötig:

Satz 7.5 (Variante des Satzes von Euler)**.**
Es sei N eine positive, natürliche Zahl, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = g \neq 1$ und $N = g \cdot N'$, $a = g \cdot a'$, also $\mathrm{ggT}(a', N') = 1$. Gilt nun zusätzlich $\mathrm{ggT}(a', g) = \mathrm{ggT}(N', g) = 1$, so gilt

$$a^m \equiv a^r \bmod N \quad \text{für } r \equiv m \bmod \varphi(N') \ \underline{\text{und}}\ m \not\equiv 0 \bmod \varphi(N')\,.$$

Hinweis: Die einfache Formulierung wie im klassischen Satz von Euler gilt in Satz 7.5 nicht, denn es ist $a^{\varphi(N')} \not\equiv 1 \bmod N$.

7.3 Aufgaben zu Abschnitt 7

Aufgabe 7.6. Berechnen Sie:

a) $9^{81} \bmod 11$ b) $14^{722} \bmod 5$ c) $(-9)^{182} \bmod 7$ d) $166^{138} \bmod 24$

Aufgabe 7.7. Zeigen Sie mit Hilfe der Eulerschen φ-Funktion, dass

a) $632^{107} \equiv 42 \bmod 53$ b) $1739^{1739} \equiv 11 \bmod 24$ c) $208^{325} \equiv 5 \bmod 7$

Aufgabe 7.8. a) Begründen Sie, warum es zum Bestimmen der letzten beiden Ziffern einer Zahl reicht, ihren Wert modulo 100 zu berechnen.

b) Bestimmen Sie die letzten beiden Stellen der Zahl 7^{1283}.

8 Das RSA-Verschlüsselungsverfahren

8.1 Die Grundidee der RSA-Verfahrens und eine Babyvariante

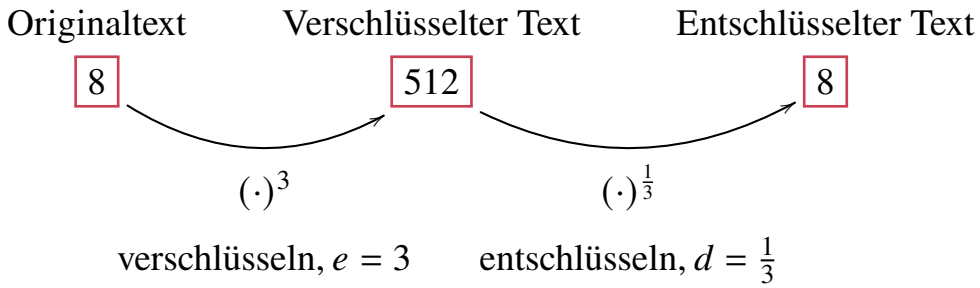
Die Idee des RSA-Verfahrens (RSA-Verschlüsselung) ist es, eine Nachricht durch Potenzieren zu verschlüsseln.
Dazu übersetzt man zunächst das zu codierende Alphabet in Zahlen, zum Beispiel A = 1, B = 2, . . . , Z = 26.
Als nächstes wählt man einen Schlüssel[4], zum Beispiel $e = 3$.
Unsere Nachricht lautet 'AHBZ=1,8,2,26'. Diese verschlüsseln wir:

$$\begin{aligned} \mathrm{A} = 1 &\mapsto 1^3 = 1 \\ \mathrm{H} = 8 &\mapsto 8^3 = 512 \\ \mathrm{B} = 2 &\mapsto 2^3 = 8 \\ \mathrm{Z} = 26 &\mapsto 26^3 = 17576 \end{aligned}$$

Damit lautet der verschlüsselte Text

$$\mathrm{AHBZ} = 1, 8, 2, 26 \mapsto 1, 512, 8, 17576$$

Wie entschlüsselt man nun den codierten Text?
Das ist hier recht einfach: man mmuss lediglich eine Wurzel ziehen, und zwar die dritte Wurzel. Das lässt sich auch mit Hilfe von Potenzieren formulieren: Das Entschlüsseln erfolgt über das Potenzieren mit dem Exponenten $d = \frac{1}{3}$.



[4] e: encrypt (verschlüsseln), d: decrypt (entschlüsseln)

Problem 8.1. • Kennt man e, so auch d. Dabei spielt es keine Rolle ob e ganzzahlig ist, denn man erhält d als Lösung der einfachen Gleichung

$$ex = 1 \tag{1}$$

- Man kann durch Raten und Probieren e herausfinden, wenn man etwa weiß, dass e und die Originalnachricht natürliche Zahlen sind und man den verschlüsselten Text kennt:

  Der verschlüsselte Text sei $512 = 2^9$. Dann sind die möglichen Schlüssel $e = 9$, $e = 3$ oder $e = 1$ mit den Originalnachrichten

e	9	3	1
Nachricht	2	8	512

  Hat man nun mehrere verschlüsselte Texte, so kann man durch einfache Ausschlussverfahren auf das korrekte e schließen.

Der Grund für das simple Dekodieren ist:

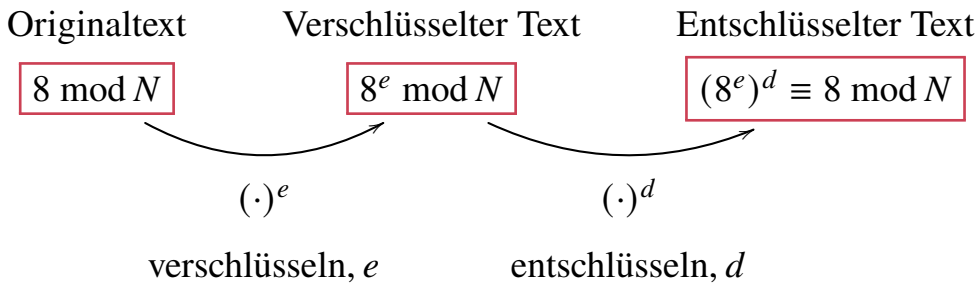
Rechnen über den reellen Zahlen $\mathbb{R}$ ist zu einfach

8.2 RSA-Verfahren über $\mathbb{Z}_N$

Statt über den reellen Zahlen zu rechnen, verwendet man als Zahlenmenge die Restklassenmenge $\mathbb{Z}_N$ der Reste beim Teilen durch die positive ganze Zahl N:

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$$

Die Idee ist wieder die gleiche wie im ersten Abschnitt:



- Man startet mit einem Schlüssel e, den man zum Potenzieren unserer Originalnachricht verwendet. Die Rechnung führt man in $\mathbb{Z}_N$ durch.
- Um eine Chance zum Entschlüsseln zu haben, auch wenn man den passenden Schlüssel d hat, ist der Modus N nötig.
- Dass heißt der Schlüssel zum Verschlüsseln ist $(e; N)$ und der zum Entschlüsseln ist $(d; N)$.

8.2.1 Erzeugen der Schlüssel $(e;N)$ und $(d;N)$

Das Problem der Schlüsselgenerierung ist im Prinzip das gleiche wie in der Babyvariante: Wenn ich den Schlüssel e kenne, dann muss ich, um den Schlüssel d herauszufinden bzw. zu bestimmen, 'nur' ein d finden mit

$$(a^e)^d \equiv a^{ed} \equiv a \bmod N$$

oder etwas umgeschrieben

$$a^{ed-1} \equiv 1 \bmod N\,.$$

Mit Hilfe des Satzes von Euler weiß man, dass $a^{ed-1} = 1$ immer dann gilt, wenn d so gewählt ist, dass $ed-1$ ein Vielfaches von $\varphi(N)$ ist. Also benötigt man ein d sodass $ed - 1 \equiv 0 \bmod \varphi(N)$.
Das heißt, zur Bestimmung von d löst man die Gleichung

$$ex \equiv 1 \bmod \varphi(N)\,, \tag{2}$$

siehe auch die analoge Gleichung (1) im Babybeispiel.

Bemerkung 8.2. Man kann nicht mit jedem Schlüssel e starten, denn man muss gewährleisten, dass die Gleichung (2) auch lösbar ist. Dazu müssen e und $\varphi(N)$ teilerfremd sein, also $\mathrm{ggT}(e, \varphi(N)) = 1$.

Bemerkung 8.3.

- Kenne man nun als Hersteller des Verschlüsselungsverfahrens N und $\varphi(N)$, so kann man den öffentlichen Schlüssel $(e;N)$ und den geheimen Schlüssel $(d;N)$ mit Hilfe von (2) erzeugen.
- Man weiß dass es in der Regel schwierig ist $\varphi(N)$ zu berechnen. Da man aber, nachdem man einmal d erzeugt hat, $\varphi(N)$ nicht mehr benötigt, kann man diese Information löschen. Damit ist ein wichtiger Teil nicht mehr verfügbar, den man zur Rekonstruktion des (geheimen) Schlüssels $(d;N)$ benötigt! Ein Angriff auf dieses Verfahren ist somit sehr schwierig.
- Aus dem gleichen Grund ist es auch nicht sinnvoll Primzahlen als Modus zu wählen, da dann $\varphi(N)$ leicht zu bestimmen ist.

Bemerkung 8.4. Man trifft folgende Wahlen zur Bestimmung von N:

- Man wählt zwei große Primzahlen p und q.
- Man wählt $N = p \cdot q$.

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

Diese Wahlen sind sinnvoll, da die Rekonstruktion von p und q aus der Kenntnis von N und damit die Bestimmung von $\varphi(N)$ ein sehr schwieriges Problem ist.
Damit ist ein Angriff auf das Verfahren, d. h. die Bestimmung von $(d; N)$ aus $(e; N)$, ebenfalls sehr schwierig.

8.2.2 Zur Lösung der Gleichung $e \cdot x \equiv 1 \bmod \varphi(N)$

Die Bestimmung der Lösung von (2), also von

$$e \cdot x \equiv 1 \bmod \varphi(N)\,,$$

geschieht mit Hilfe des erweiterten euklidischen Algorithmus:

> Sind a und b ganze Zahlen, dann gibt es ganze Zahlen k und ℓ, sodass
>
> $$k \cdot a + \ell \cdot b = \mathrm{ggT}(a, b)\,.$$

e muss so gewählt werden muss, dass $\mathrm{ggT}(e, \varphi(N)) = 1$. Damit gibt es ganze Zahlen k und ℓ, sodass

$$k \cdot e + \ell \cdot \varphi(N) = 1\,. \tag{3}$$

Damit ist dann

$$k \cdot e + \ell \cdot \varphi(N) \equiv e \cdot k \equiv 1 \bmod \varphi(N)$$

und $d = k$ ist eine Wahl für den Schlüssel zum Entschlüsseln.[5]

[5] Liefert der euklidische Algorithmus für k keinen Wert zwischen 1 und $\varphi(N) - 1$, so kann man ein beliebiges Vielfaches von $\varphi(N)$ zu k addieren oder subtrahieren, und d als diesen Wert wählen. Das ändert nichts an der Eigenschaft $e \cdot d \equiv 1 \bmod \varphi(N)$.

8.3 Ein Fahrplan für das RSA-Verfahren

Die Zusammenfassung des vorigen Abschnitt in Form eines Fahrplans lautet:

Schritt 1. Man wählt zwei Primzahlen p und q und berechnet damit $N = p \cdot q$.

Schritt 2. Man berechnet $\varphi(N) = (p-1) \cdot (q-1)$ und bestimmt eine Zahl e mit $\text{ggT}\left(e, \varphi(N)\right) = 1$.
Das gibt den öffentlichen Schlüssel $(e; N)$.

Schritt 3. Man berechnet d aus dem Faktor vor e im erweiterten euklidischen Algorithmus für e und $\varphi(N)$: $k \cdot e + \ell \cdot \varphi(N) = 1$.
Ist $0 < k < \varphi(N)$, dann wählt man $d = k$, andernfalls addiert/subtrahiert man $\varphi(N)$ so oft zu/von k, bis der Wert die gewünschte Eigenschaft hat: das ist dann d.
Das gibt den geheimen Schlüssel $(d; N)$.

Schritt 4. Man verschlüsselt eine Originalnachricht A zur codierten Nachricht B, indem man $A^e \equiv B \bmod N$ berechnet.

Schritt 5. Man entschlüsselt eine codierte Nachricht B zur Originalnachricht A, indem man $B^d \equiv A \bmod N$ berechnet.

8.4 Beispiel: Das RSA-Verfahren in $\mathbb{Z}_{221}$

Als Beispiel dient zur Verschlüsselung und Entschlüsselung wieder die Nachricht 'AHBZ' aus dem Babybeispiel, jetzt nach dem obigen Fahrplan:

Schritt 1. Man wählt $p = 13$ und $q = 17$ und somit $N = 13 \cdot 17 = 221$.

Schritt 2. Damit ist $\varphi(N) = 12 \cdot 16 = 192$ und man kann $e = 23$ wählen, sodass $(23; 221)$ der öffentliche Schlüssel ist.

Das klappt, denn e und $\varphi(N)$ sind teilerfremd: Es ist $\varphi(N) = 192 = 2^6 \cdot 3$ und $e = 23$ ist eine Primzahl.

Schritt 3. Zur Bestimmung von d sucht man zunächst Zahlen k und ℓ, sodass

$$k \cdot 23 + \ell \cdot 192 = 1\,.$$

Das macht man mit dem erweiterten euklidischen Algorithmus:

$$
\begin{array}{lcl}
\underline{192} = 8 \cdot \underline{23} + \underline{8} & \longrightarrow & \underline{8} = \underline{192} - 8 \cdot \underline{23} \\
\underline{23} = 2 \cdot \underline{8} + \underline{7} & \longrightarrow & \underline{7} = \underline{23} - 2 \cdot \underline{8} \\
 & & \quad = \underline{23} - 2 \cdot (\underline{192} - 8 \cdot \underline{23}) \\
 & & \quad = 17 \cdot \underline{23} - 2 \cdot \underline{192} \\
\underline{8} = 1 \cdot \underline{7} + \boxed{1} & \longrightarrow & \boxed{1} = \underline{8} - \underline{7} \\
 & & \quad = (\underline{192} - 8 \cdot \underline{23}) - (17 \cdot \underline{23} - 2 \cdot \underline{192}) \\
 & & \quad = 3 \cdot \underline{192} - 25 \cdot \underline{23} \\
\underline{7} = 7 \cdot \underline{1} & &
\end{array}
$$

Das gibt $k = -25$ und $\ell = 3$. Weil $k < 0$ ist, setzt man

$$d = -25 + 192 = 167$$

Die Probe liefert

$$e \cdot d \equiv 23 \cdot 167 \equiv 3841 \equiv 20 \cdot 192 + 1 \equiv 1 \bmod 192\,.$$

Der private Schlüssel zum Decodieren ist $(167; 221)$.

Schritt 4. Verschlüsseln der Nachricht 'AHBZ':

$$
\begin{aligned}
\mathrm{A} = 1 \longmapsto 1^{23} &\equiv 1 \bmod 221 \\
\mathrm{B} = 2 \longmapsto 2^{23} &\equiv 8 \cdot (2^{10})^2 \equiv 8 \cdot 140^2 \\
&\equiv 8 \cdot 4 \cdot 70^2 \equiv 8 \cdot 4 \cdot 38 \equiv 111 \bmod 221 \\
\mathrm{H} = 8 \longmapsto 8^{23} &\equiv (2^{23})^3 \equiv 111^3 \equiv 111 \cdot 111^2 \equiv 111 \cdot 166 \\
&\equiv 83 \bmod 221 \\
\mathrm{Z} = 26 \longmapsto 26^{23} &\equiv 2^{23} \cdot 13^{23} \\
&\equiv 111 \cdot 13^2 \cdot (13^3)^7 \equiv 111 \cdot 13^2 \cdot (-13)^7 \\
&\equiv -111 \cdot (13^3)^3 \equiv -111 \cdot (-13)^3 \\
&\equiv -111 \cdot 13 \equiv 104 \bmod 221
\end{aligned}
$$

Damit ist der verschlüsselte Text:

$$\mathrm{AHBZ} = 1, 8, 2, 26 \longmapsto 1, 83, 111, 104$$

Schritt 5. Zum Decodieren muss man nun Folgendes berechnen:[6]

$$\begin{aligned}
1^{167} &\equiv 1 \bmod 221\\
83^{167} &\equiv (83^8)^{20} \cdot (83^2)^3 \cdot 83 \equiv 38^3 \cdot 83 \equiv 64 \cdot 83\\
&\equiv 8 \bmod 221\\
111^{167} &\equiv 111^2 \cdot (111^3)^{55} \equiv 111^2 \cdot (83)^{55}\\
&\equiv 111^2 \cdot 83 \cdot (83^{16} \cdot 83^2)^3 \equiv 111^2 \cdot 83 \cdot 38^3\\
&\equiv 111^2 \cdot 83 \cdot 64 \equiv 111^2 \cdot 8 \equiv 166 \cdot 8\\
&\equiv 2 \bmod 221\\
104^{167} &\equiv (8 \cdot 13)^{167} \equiv (2^{24})^{20} \cdot 2^{20} \cdot 2 \cdot (13^{23})^7 \cdot (13^3)^2\\
&\equiv 152 \cdot 2 \cdot (-13)^7 \cdot (-13)^2 \equiv -83 \cdot (13^3)^3\\
&\equiv 83 \cdot 13^3 \equiv -83 \cdot 13\\
&\equiv 26 \bmod 221
\end{aligned}$$

Der decodierte Text ist damit

$$1, 8, 2, 26 = \text{AHBZ}\,.$$

8.5 Aufgaben zu Abschnitt 8

Aufgabe 8.5. $p = 17$ und $q = 11$ sind zwei Primzahlen mit denen das RSA-Verfahren durchgeführt wird.

a) Begründen Sie, warum $(7; 187)$ ein möglicher öffentlicher Schlüssel ist. Überprüfen Sie, ob es sich auch um den kleinstmöglichen handelt.

b) Verschlüsseln Sie die Information 65 mit Hilfe des öffentlichen Schlüssels $(7; 187)$.

c) Berechnen Sie den zu $(7; 187)$ gehörigen privaten Schlüssel $(d; 187)$.

Aufgabe 8.6. Das RSA-Verfahren nutzt die Primzahlen $p = 31$ und $q = 37$.

a) Bestimmen Sie einen öffentlichen Schlüssel $(e; N)$ so, dass e so klein wie möglich ist.

b) Berechnen Sie den zu $(e; N)$ aus a) gehörigen privaten Schlüssel $(d; N)$.

c) Als öffentlicher Schlüssel wird nun verwendet $(11; 1147)$.
Begründen Sie mit Hilfe geeigneter Rechnungen, dass dann 174 die Verschlüsselung von 10 ist.

[6] Es ist nicht sinnvoll hier den Satz von Euler zu verwenden, da man $\varphi(221)$ "nicht kennt". Man kann allerdings die vorigen Rechnungen und z. B. $2^{24} \equiv 2^{23} \cdot 2 \equiv 111 \cdot 2 \equiv 222 \equiv 1 \bmod 221$, $38^4 \equiv 38^2 \cdot 38^2 \equiv 118^2 \equiv 1 \bmod 221$ oder $83^2 \equiv 38 \bmod 221$ nutzen.

9 Potenzieren mit Hilfe der Dualdarstellung

Der Satz von Euler kann sehr hilfreich sein, wenn man Potenzen $\bmod N$ mit großen Exponenten berechnen will. Allerdings benötigt man dazu den Wert $\varphi(N)$, welcher in der Regel schwierig zu bestimmen ist. Insbesondere ist genau diese Schwierigkeit die Grundlage der Sicherheit der RSA-Verschlüsselung.

Ein effizientes Verfahren zur Berechnung von Potenzen mit großen Exponenten basiert auf den **Dualzahlen** (auch **binäre Zahlen**) und führt in der Praxis dazu, dass man statt einer hohen Potenz im Wesentlichen nur nacheinander eine Reihe von Quadraten berechnet. Das im Zusammenhang mit der Möglichkeit Zwischenresultate mit Hilfe der modularen Rechnung zu verkleinern liefert ein sehr effizientes Potenzierungsverfahren.

9.1 Das Dualsystem und Umrechnung dezimal ↔ dual

Eine Zahl $z \in \mathbb{N}$ stellt man im Dezimalsystem mit Hilfe ihrer Ziffern dar: $z = \ldots z_3\, z_2\, z_1\, z_0$ wobei $z_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Kennt man die (endlich vielen) Ziffern $z_0, z_1, z_2, z_3, \ldots$, dann erhält man z zurück, indem man diese Zahl ausrechnet: $z = z_0 \cdot 10^0 + z_1 \cdot 10^1 + z_2 \cdot 10^2 + z_3 \cdot 10^3 + \ldots$

Beispiel 9.1. Die natürliche Zahl $z = 3098$ besitzt die Ziffern $z_0 = 8, z_1 = 9, z_2 = 0$ und $z_3 = 3$.

Statt der Basis 10, kann man prinzipiell jede andere Basis verwenden, um eine Zahl darzustellen. Im Folgenden ist die Basis 2 interessant.

Definition 9.2. Eine Zahl $z \in \mathbb{N}$ stellt man im **Dualsystem** mit Hilfe ihrer Dualziffern dar:[7] $z_{(2)} = \ldots d_3\, d_2\, d_1\, d_0$ wobei $d_i \in \{0, 1\}$. Kennt man die (endlich vielen) Ziffern $d_0, d_1, d_2, d_3, \ldots$, dann erhält man z zurück, indem man diese Zahl ausrechnet: $z = d_0 \cdot 2^0 + d_1 \cdot 2^1 + d_2 \cdot 2^2 + d_3 \cdot 2^3 + \ldots$

Beispiel 9.3. $z = 3098$ hat die Dualdarstellung $3098_{(2)} = 110000011010$, also die Ziffern $d_0 = 0, d_1 = 1, d_2 = 0, d_3 = 1, d_4 = 1, d_5 = d_6 = d_7 = d_8 = d_9 = 0, d_{10} = 1$ und $d_{11} = 1$. Es ist

$$3098 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + 0 \cdot 2^7 + 0 \cdot 2^8 + 0 \cdot 2^9 + 1 \cdot 2^{10} + 1 \cdot 2^{11}$$

Die Umrechnung einer positiven ganzen Zahl in eine Dualzahl kann mit einem einfachen Algorithmus geschehen, der lediglich die Halbierung von Zahlen benötigt:

[7] Der Index $_{(2)}$ soll lediglich die Verwendung des Dualsystems betonen.

Algorithmus 9.4. Die Ziffern $d_0, d_1, d_2, \ldots$ der Dualdarstellung einer Zahl $z > 0$ erhält man wie folgt:

Beginn: $a_0 = z$

Schritt: $\begin{cases} \text{Falls } a_i \text{ gerade, setzt man } a_{i+1} = a_i/2 \text{ und } d_i = 0 \\ \text{Falls } a_i \text{ ungerade, setzt man } a_{i+1} = (a_i - 1)/2 \text{ und } d_i = 1 \end{cases}$

Ende: $a_i = 1$

Beispiel 9.5. $z = 3098$ ist dual 110000011010, denn:

i	0	1	2	3	4	5	6	7	8	9	10	11
a_i	3098	1549	774	387	193	96	48	24	12	6	3	1
d_i	0	1	0	1	1	0	0	0	0	0	1	1

Zur Berechnung der Dezimaldarstellung einer Dualzahl kann man die Summe aus Beispiel 9.3 berechnen.

Stattdessen kann man auch den Algorithmus 9.4 umkehren: Man berechnet $z = a_0$ indem man nach und nach a_i durch a_{i+1} ersetzt. Dadurch muss man im Wesentlichen lediglich Verdoppelungen durchführen.

Am Beispiel 9.5 kann man die Idee gut nachvollziehen:

$$
\begin{aligned}
3098 &= a_1 \cdot 2 && d_0 = 0 \\
&= (a_2 \cdot 2 + 1) \cdot 2 && d_1 = 1 \\
&= ((a_3 \cdot 2) \cdot 2 + 1) \cdot 2 && d_2 = 0 \\
&= (((a_4 \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_3 = 1 \\
&= ((((a_5 \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_4 = 1 \\
&= (((((a_6 \cdot 2) \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_5 = 0 \\
&= ((((((a_7 \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_6 = 0 \\
&= (((((((a_8 \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_7 = 0 \\
&= ((((((((a_9 \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_8 = 0 \\
&= (((((((((a_{10} \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_9 = 0 \\
&= ((((((((((a_{11} \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2 + 1) \cdot 2) \cdot 2 + 1) \cdot 2 && d_{10} = 1
\end{aligned}
$$

Insbesondere ist $a_{11} = 1$, sodass man 3098 hier nur mit Verdoppelungen und der Addition von Einsen berechnet – je nachdem, ob an der jeweiligen Stelle in der Dualdarstellung eine 0 oder eine 1 stand: bei 0 nur verdoppeln, bei 1 verdoppeln und plus 1.

Auch wenn diese Darstellung im Gegensatz zur Berechnung aus Beispiel 9.3 zunächst kompliziert erscheinen mag, ist sie ein sinnvolles Werkzeug, um zu Potenzieren.

9.2 Das schnelle duale Potenzieren

Das **schnelle duale Potenzieren** basiert auf der – zunächst komplizierten Art – eine Dualzahl in eine Dezimalzahl umzurechnen.

Man sieht das gut an dem bereits vorbereiteten Beispiel:

$$
\begin{aligned}
x^{3098} &= x^{((((((((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2+1)\cdot 2+1)\cdot 2)\cdot 2+1)\cdot 2} \\
&= \left(x^{((((((((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2+1)\cdot 2+1)\cdot 2)\cdot 2+1}\right)^2 \\
&= \left(\left(x^{(((((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2+1)\cdot 2+1)\cdot 2}\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(x^{(((((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2+1)\cdot 2+1}\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(x^{((((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2+1}\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(x^{(((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2)\cdot 2}\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(\left(x^{((((2+1)\cdot 2)\cdot 2)\cdot 2)\cdot 2}\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(\left(x^{(((2+1)\cdot 2)\cdot 2)\cdot 2)2}\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(\left(\left(x^{((2+1)\cdot 2)\cdot 2}\right)^2\right)^2\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(\left(\left(\left(x^{(2+1)\cdot 2}\right)^2\right)^2\right)^2\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(\left(\left(\left(\left(x^{2+1}\right)^2\right)^2\right)^2\right)^2\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2 \\
&= \left(\left(\left(\left(\left(\left(\left(\left(\left(\left(x^2 \cdot x\right)^2\right)^2\right)^2\right)^2\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2\right)^2 \cdot x\right)^2
\end{aligned}
$$

Die Beziehung zur Dualzahl erkennt man, indem man sich diese Formel von ”innen nach außen” ansieht:

- Man streicht die höchste Dualziffer (hier d_{11})
- Ausgehend von der zweithöchsten Dualziffer (hier d_{10}) geht man die Ziffern bis zur letzten durch (hier von d_{10} bis d_0): in jedem Schritt quadriert man das vorige Ergebnis, wenn die jeweilige Ziffer 0 ist, oder man quadriert das vorige Ergebnis und multipliziert mit x, wenn die Ziffer 1 ist.
- Am Schluss erhält man die gewünschte Potenz.

Zusammenfassen kann man das genauer im folgenden Algorithmus.

Algorithmus 9.6 (Berechnung von $x^m \bmod N$)**.**
Man bestimmt zunächst die Dualdarstellung $m_{(2)} = d_k d_{k-1} \ldots d_2 d_1 d_0$. Dann streicht man $d_k = 1$ und geht die verbleibenden Ziffern von d_{k-1} bis d_0 durch:

Beginn: $z_0 = x$

Schritt:
$$\begin{cases} \text{Falls } d_{k-i} = 0, \text{ dann setzt man } z_i = z_{i-1}^2 \bmod N \\ \text{Falls } d_{k-i} = 1, \text{ dann setzt man } z_i = z_{i-1}^2 \cdot x \bmod N \end{cases}$$

Ende: $z_k = x^m \bmod N$

Wichtig: Nach jedem Rechenschritt sollte man die Zahl mit Hilfe der modularen Rechnung verkleinern!

Beispiel 9.7. 1. Zur Berechnung von $17^{3098} \bmod 21$ muss man wegen $3098_{(2)} = 110000011010$ wie folgt vorgehen (man streicht die führende Ziffer $d_{11} = 1$ und es bleiben 10000011010):

	$z_0 = x$	$z_0 = 17 \bmod 21$
$d_{10} = 1 \rightarrow$	$z_1 = x^2 \cdot x$	$z_1 = 17^2 \cdot 17 \equiv 16 \cdot 17 \equiv -1 \bmod 21$
$d_9 = 0 \rightarrow$	$z_2 = z_1^2$	$z_2 = (-1)^2 \equiv 1 \bmod 21$
$d_8 = 0 \rightarrow$	$z_3 = z_2^2$	$z_3 = 1^2 \equiv 1 \bmod 21$
$d_7 = 0 \rightarrow$	$z_4 = z_3^2$	$z_4 = 1^2 \equiv 1 \bmod 21$
$d_6 = 0 \rightarrow$	$z_5 = z_4^2$	$z_5 = 1^2 \equiv 1 \bmod 21$
$d_5 = 0 \rightarrow$	$z_6 = z_5^2$	$z_6 = 1^2 \equiv 1 \bmod 21$
$d_4 = 1 \rightarrow$	$z_7 = z_6^2 \cdot x$	$z_7 = 1^2 \cdot 17 \equiv 17 \bmod 21$
$d_3 = 1 \rightarrow$	$z_8 = z_7^2 \cdot x$	$z_8 = 17^2 \cdot 17 \equiv -1 \bmod 21$
$d_2 = 0 \rightarrow$	$z_9 = z_8^2$	$z_9 = 1^2 \equiv 1 \bmod 21$
$d_1 = 1 \rightarrow$	$z_{10} = z_9^2 \cdot x$	$z_{10} = 1^2 \cdot 17 \equiv 17 \bmod 21$
$d_0 = 0 \rightarrow$	$z_{11} = z_{10}^2$	$z_{11} = 17^2 \equiv 289 \equiv 16 \equiv 17^{3098} \bmod 21$

2. Als weiteres Beispiel ist $17^{482} \bmod 33$ gesucht. Wegen $482_{(2)} = 111100010$ geht man wie folgt vor (man streicht die führende Ziffer $d_8 = 1$ und es

bleiben 11100010):

$z_0 = x$	$z_0 = 17 \bmod 33$
$d_7 = 1 \rightarrow z_1 = z_0^2 \cdot x$	$z_1 = 17^2 \cdot 17 \equiv 25 \cdot 17 \equiv -4 \bmod 33$
$d_6 = 1 \rightarrow z_2 = z_1^2 \cdot x$	$z_2 = (-4)^2 \cdot 17 \equiv 16 \cdot 17 \equiv 8 \bmod 33$
$d_5 = 1 \rightarrow z_3 = z_2^2 \cdot x$	$z_3 = 8^2 \cdot 17 \equiv -2 \cdot 17 \equiv -1 \bmod 33$
$d_4 = 0 \rightarrow z_4 = z_3^2$	$z_4 = (-1)^2 \equiv 1 \bmod 33$
$d_3 = 0 \rightarrow z_5 = z_4^2$	$z_5 = 1^2 \equiv 1 \bmod 33$
$d_2 = 0 \rightarrow z_6 = z_5^2$	$z_6 = 1^2 \equiv 1 \bmod 33$
$d_1 = 1 \rightarrow z_7 = z_6^2 \cdot x$	$z_7 = 1^2 \cdot 17 \equiv 17 \bmod 33$
$d_0 = 0 \rightarrow z_8 = z_7^2$	$z_8 = 17^2 \equiv 289 \equiv 25 \equiv 17^{482} \bmod 33$

3. Als letztes Beispiel betrachte man $111^{167} \bmod 221$ aus Entschlüsselung im RSA-Beispiel in Abschnitt 8.4. Es ist $167_{(2)} = 10100111$ (man streicht die führende Ziffer $d_7 = 1$ und es bleiben 0100111) und man erhält:

$z_0 = x$	$z_0 = 111 \bmod 221$
$d_6 = 0 \rightarrow z_1 = z_0^2$	$z_1 = 111^2 \equiv 166 \equiv -55 \bmod 221$
$d_5 = 1 \rightarrow z_2 = z_1^2 \cdot x$	$z_2 = (-55)^2 \cdot 111 \equiv -69 \cdot 111 \equiv 76 \bmod 221$
$d_4 = 0 \rightarrow z_3 = z_2^2$	$z_3 = 76^2 \equiv 30 \bmod 221$
$d_3 = 0 \rightarrow z_4 = z_3^2$	$z_4 = 30^2 \equiv 16 \bmod 221$
$d_2 = 1 \rightarrow z_5 = z_4^2 \cdot x$	$z_5 = 16^2 \cdot 111 \equiv 35 \cdot 111 \equiv -93 \bmod 221$
$d_1 = 1 \rightarrow z_6 = z_5^2 \cdot x$	$z_6 = (-93)^2 \cdot 111 \equiv 30 \cdot 111 \equiv 15 \bmod 221$
$d_0 = 1 \rightarrow z_7 = z_6^2 \cdot x$	$z_7 = 15^2 \cdot 111 \equiv 4 \cdot 111 \equiv 2 \equiv 111^{167} \bmod 221$

10 Die Begründungen für einige der Aussagen

10.1 Die Begründung für Folgerung 1.9

Es gibt unendlich viele Primzahlen

Man zeigt, dass es zu einer endlichen, lückenlos aufsteigenden Menge an Primzahlen immer eine weitere Primzahl geben muss, die dann größer ist als alle bisherigen.
Man nimmt also die ersten n Primzahlen her: $p_1 < p_2 < \ldots < p_n$. Die neue Zahl, die man berechnet ist

$$q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \,.$$

Diese Zahl ist durch keine der vorigen n vielen Primzahlen teilbar, da sie beim Teilen jeweils den Rest 1 hat, siehe Fakt 1.7.
Wegen Fakt 1.6 ist der kleinste Teiler von q, der ungleich 1 ist, eine Primzahl. Dies ist entweder q selbst oder eine neue Primzahl. In beiden Fällen muss dieser Primzahlteiler aber größer als p_n sein, da es bei $p_1, \ldots, p_n$ keine Lücke gab.

10.2 Die Begründung für Fakt 2.2

Ist p eine Primzahl und a eine natürliche Zahl mit $\mathrm{ggT}(a, p) = 1$, dann sind nur die Vielfachen

$$a \cdot p, \quad a \cdot 2 \cdot p, \quad a \cdot 3 \cdot p, \quad \ldots$$

durch p teilbar.

Zunächst sieht man direkt, dass alle Zahlen in der Liste durch p teilbar sind.
Man muss also noch begründen, dass es keine weiteren Zahlen gibt, die zwar durch p teilbar sind aber nicht von der speziellen Form.
Die Begründung erfolgt in mehreren Schritten:

1. Man sucht das kleinste Vielfache von a heraus, dass durch p teilbar ist.

   Diese Zahl ist dann von der Form $a \cdot m$. Dabei muss $1 < m \leq p$ gelten, denn 1 ist ausgeschlossen, da a nicht durch p teilbar sein soll, und $m > p$ ist ausgeschlossen, da dann $a \cdot p$ kleiner als $a \cdot m$ wäre.

2. Man nimmt jetzt ein weiteres Vielfaches von a her, dass ebenfalls durch p teilbar ist. Das kann man als $a \cdot h$ schreiben. Es muss $h \geq m$ gelten, da $a \cdot m$ das kleinste durch p teilbare Vielfache war.
3. Für die beiden Vielfachen aus 1. und 2. gibt es (wegen $h \geq m$) zwei Zahlen k und r mit $h = k \cdot m + r$ und $0 \leq r < m$, siehe Fakt 1.7.
4. Damit ist $a \cdot r = a \cdot h - a \cdot k \cdot m$ ebenfalls durch p teilbar, weil $a \cdot h$ und $a \cdot k \cdot m$ durch p teilbar sind.

   Weil aber $a \cdot r < a \cdot m$ ist und $a \cdot m$ das kleinste Vielfache war, dass durch p teilbar war, muss $r = 0$ sein.
5. Wegen 4. ist $h = k \cdot m$ und das beliebige(!) Vielfache $a \cdot h$, das durch p teilbar ist, ist von der Form $a \cdot k \cdot m$.

Bis jetzt hat man: Alle Vielfachen von a, die von p geteilt werden, sind von der Form $a \cdot k \cdot m$. Dabei ist $a \cdot m$ das kleinste aller Vielfachen ist, die durch p teilbar sind.
Jetzt bleibt nur noch zu begründen, warum m selber p ist:

6. Auf alle Fälle wird $a \cdot p$ von p geteilt. Daher muss $a \cdot p$ auch von der Form $a \cdot p = a \cdot k \cdot m$ sein und damit $p = k \cdot m$. Das heißt, m ist ein Teiler von p, also $m = 1$ oder $m = p$, weil p eine Primzahl ist. Wegen $m > 1$ aus Punkt 1. ist damit $m = p$.

10.3 Die Begründung für Fakt 2.4

Ist a eine natürliche Zahl, dann gibt es eine eindeutige Zerlegung

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

in ein Produkt von n Primzahlen $p_1, p_2, \ldots, p_n$. Diese müssen nicht unterschiedlich sein.

Der Zusatz, dass die Primzahlen nicht unterschiedlich sein müssen, hat man bereits in den Beispielen gesehen.
Dass es so eine Zerlegung immer gibt, sieht man, indem man beschreibt, wie man sie erhält. Dazu wendet man den folgenden Algorithmus an:

i. Ist a eine Primzahl, dann ist man fertig.
ii. Ist a keine Primzahl, dann gibt es Zahlen b und c, die nicht 1 sind und die a zerlegen: $a = b \cdot c$.

iii. Mit b und c startet man nun neu mit Schritt i. und ii.

iv. Das Verfahren endet, wenn man in Schritt iii. nur noch Primzahlen hat.

Man muss jetzt noch begründen, warum es keine zwei unterschiedlichen Zerlegungen geben kann. Das geschieht in mehreren Schritten:

1. Man nimmt an, es gäbe zwei Zerlegungen für a, nämlich

$$p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_m \,.$$

   Darin sollen die Primzahlen der Größe nach sortiert sein und es soll $n \leq m$ sein.

2. Da p_1 die Zahl $q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_m$ teilt, muss diese von der Form $p_1 \cdot k$ sein.
   Das heißt, p_1 muss unter den Primzahlen $q_1, \ldots, q_m$ vorkommen, etwa $p_1 = q_1$. Man kann diese Primzahl jetzt auf beiden Seiten dividieren und behalten

$$p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_2 \cdot q_3 \cdot \ldots \cdot q_m \,.$$

3. Den Schritt aus 2. wiederholt man jetzt n mal und erhält $p_1 = q_1, p_2 = q_2, \ldots, p_n = q_n$. Die Gleichung, die nach Division übrig bleibt, ist

$$1 = q_{n+1} \cdot \ldots \cdot \ldots \cdot q_m \,.$$

   Diese Gleichung darf auf der rechten Seite aber keine weiteren Faktoren haben. Das geht jedoch nur, wenn $n = m$ ist und damit beide Zerlegung von vornherein gleich sind.

10.4 Die Begründung für Fakt 6.4

1. Man befindet sich in $\mathbb{Z}_N$ und sieht sich dort die Zahl a an. Es gilt

   Ist $\mathrm{ggT}(a, N) = 1$, dann haben die Werte $k \cdot a$ mit $k = 0, 1, \ldots, (N-1)$ alle verschiedene Rest modulo N. D. h. durchlaufen alle Reste $0, 1, \ldots, N-1$ und decken ganz $\mathbb{Z}_N$ ab.

   Denn ist $k \cdot a \equiv \ell \cdot a \bmod N$, also $(k - \ell) \cdot a \equiv 0 \bmod N$, dann wäre wegen Bemerkung 6.2.2 auch $k - \ell \equiv 0 \bmod N$, also $k = \ell \bmod N$. Das passiert aber in der aufgeführten Menge nicht.

2. Ist aber $\text{ggT}(a, N) = g > 1$, dann ist wegen Fakt 2.1.3 $\text{ggT}(\frac{a}{g}, \frac{N}{g}) = 1$.

   Damit durchlaufen die Zahlen $k \cdot \frac{a}{g}$ mit $k = 0, \ldots m-1$ alle Reste $0, 1, \ldots, m-1$ modulo $\frac{N}{g}$, wobei $m = \frac{N}{g}$ ist.

   Multipliziert man das mit g, dann sieht man, dass $k \cdot a = k \cdot \frac{a}{g} \cdot g$ die Reste $0, g, 2 \cdot g, \ldots (m-1)g$ modulo N durchlaufen.

   Ist nun $\ell \geq m$, dann gibt es ein $0 \leq r < m$ und eine Zahl j, sodass $\ell = j \cdot m + r$. Dann ist $\ell \cdot a = (j \cdot m + r) \cdot a = j \cdot m \cdot a + r \cdot a = j \cdot \frac{N}{g} \cdot a + r \cdot a = r \cdot a + j \cdot \frac{a}{g} \cdot N$, also $\ell \cdot a \equiv r \cdot a \bmod N$ und man erhält einen Rest, der bereits vorhanden war.

   Zusammengefasst heißt das:

   > Ist $\text{ggT}(a, N) = g$, dann nehmen die Werte $k \cdot a$ mit $k = 0, 1, \ldots, N-1$ nur die Reste $0, g, 2 \cdot g, \ldots N - g$ modulo N an.
   >
   > Insbesondere ist 1 nicht darunter und alle Werte wiederholen sich genau g mal.

10.5 Die Begründung für Fakt 6.9

Für die Begründung von Fakt 6.9 wird die folgenden natürlichen Eigenschaften ganzer Zahlen benötigt:

- Ist $a \equiv b \bmod N$ und teilt q die Zahl N, dann gilt auch $a \equiv b \bmod q$.
- Ist $\text{ggT}(a, m) = g$, dann ist auch $\text{ggT}(a + k \cdot m, m) = g$.
- Ist $\text{ggT}(a, m) = 1$ und $\text{ggT}(a, n) = 1$, dann ist auch $\text{ggT}(a, m \cdot n) = 1$.

Man geht in drei Schritten vor, um Fakt 6.9 zu begründen. Dabei gilt immer die Voraussetzung, dass N_1 und N_2 teilerfremd sind, also $\text{ggT}(N_1, N_2) = 1$.

1. > Durchläuft k alle Reste modulo N_2 und ℓ alle Reste modulo N_1, dann durchläuft $k \cdot N_1 + \ell \cdot N_2$ alle Reste modulo $N_1 \cdot N_2$.

   Da die Anzahl der berechneten Werte mit der Anzahl aller möglichen Reste übereinstimmt, muss man lediglich zeigen, dass ihre Reste unterschiedlich sind.

   Ist aber $k \cdot N_1 + \ell \cdot N_2 \equiv k' \cdot N_2 + \ell' \cdot N_2 \bmod N_1 \cdot N_2$, dann ist auch $k \cdot N_1 \equiv k' \cdot N_1 \bmod N_2$ und $\ell \cdot N_2 \equiv \ell' \cdot N_2 \bmod N_1$. Wegen $\text{ggT}(N_1, N_2) = 1$ ist dann aber auch $k \equiv k' \bmod N_2$ und $\ell \equiv \ell' \bmod N_1$.

   Damit sind alle oben beschriebenen Reste modulo $N_1 \cdot N_2$ tatsächlich verschieden und geben somit alle möglichen Reste.

2. Durchläuft k alle teilerfremden Reste modulo N_2 und ℓ alle teilerfremden Reste modulo N_1, dann durchläuft $k \cdot N_1 + \ell \cdot N_2$ nur teilerfremde Reste modulo $N_1 \cdot N_2$.

   Mit $\text{ggT}(N_1, N_2) = 1$, $\text{ggT}(k, N_2) = 1$ und $\text{ggT}(\ell, N_1) = 1$ gilt auch $\text{ggT}(k \cdot N_1 + \ell \cdot N_2, N_1) = 1$ und $\text{ggT}(k \cdot N_1 + \ell \cdot N_2, N_2) = 1$. Die beiden letzten zusammen geben dann $\text{ggT}(k \cdot N_1 + \ell \cdot N_2, N_1 \cdot N_2) = 1$.

3. Ist k nicht teilerfremd zu N_2 oder ℓ nicht teilerfremd zu N_1, dann ist auch $k \cdot N_1 + \ell \cdot N_2$ nicht teilerfremd zu $N_1 \cdot N_2$.

   Hat z. B. der Rest k einen gemeinsamen Teiler d mit N_2, also $k = d \cdot k'$, $N_2 = d \cdot n$, dann hat auch $k \cdot N_1 + \ell \cdot N_2 = d \cdot k' \cdot N_1 + d \cdot \ell \cdot n$ einen gemeinsamen Teiler mit $N_1 \cdot N_2 = d \cdot N_1 \cdot n$.

1.-3. geben uns nun, dass in Punkt 2. alle teilerfremden Reste modulo $N_1 \cdot N_2$ durchlaufen werden. Da es genau $\varphi(N_1)$ viele teilerfremde Reste von N_1 gibt und $\varphi(N_2)$ viele teilerfremde Reste von N_2, hat man nun gezeigt, dass es im Fall $\text{ggT}(N_1, N_2) = 1$ genau $\varphi(N_1) \cdot \varphi(N_2)$ viele teilerfremde Reste von $N_1 \cdot N_2$ gibt, also:

$$\varphi(N_1 \cdot N_2) = \varphi(N_1) \cdot \varphi(N_2) \quad \text{falls } \text{ggT}(N_1, N_2) = 1$$

10.6 Die Begründung für den Satz von Euler (Satz 7.3)

Ist N eine positive, natürliche Zahl mit $\text{ggT}(a, N) = 1$ so gilt

$$a^{\varphi(N)} = 1 \bmod N\,.$$

Man nimmt zur Begründung der Aussage alle Zahlen zwischen 0 und N her, die teilerfremd zu N sind. Davon gibt es $\varphi(N)$ Stück, etwa $r_1 < r_2 < \ldots < r_{\varphi(N)}$.

- Man multipliziert jetzt diese Zahlen mit a, also $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(N)}$.

  Dann sind die Ergebnisse weiterhin teilerfremd zu N.

- Keine zwei dieser neuen Zahlen haben den gleichen Rest modulo N.

  Das liegt daran, dass aus $a \cdot r_i \equiv a \cdot r_j \bmod N$ die Gleichung $r_i \equiv r_j \bmod N$ folgt (wegen $\text{ggT}(a, N) = 1$ darf man durch a teilen). Weil aber $0 < r_i, r_j < N$ ist, folgt schließlich $r_i = r_j$.

  Die Reste der Zahlen $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(N)}$ modulo N sind also die gleichen wie die Zahlen $r_1, r_2, \ldots, r_{\varphi(N)}$.

- Deshalb ist

$$
\begin{aligned}
& (a \cdot r_1) \cdot (a \cdot r_2) \cdot \ldots \cdot (a \cdot r_{\varphi(N)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)} \bmod N \\
\Longleftrightarrow\ & a^{\varphi(N)} \cdot (r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)} \bmod N \\
\Longleftrightarrow\ & a^{\varphi(N)} \equiv 1 \bmod N
\end{aligned}
$$

  Den letzte Schritt darf man wieder machen, weil $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)}$, wie jeder der Faktoren, teilerfremd zu N ist.

11 Stichwortverzeichnis