Universität Stuttgart
PD. Dr. P. H. Lesky

Zahlentheorie und Verschlüsselung

Inhaltsverzeichnis

1 Lineare diophantische Gleichungen **2**

2 Kongruenz und Modulorechnung **3**

3 Rechnen mit Restklassen **4**

4 Der kleine Satz von Fermat **7**

5 Verschlüsselungsverfahren **8**

6 Der Chinesische Restsatz **10**

7 Die eulersche Phi-Funktion **11**

8 Dezimalbruchentwicklung **13**

9 Ergänzungen und Nachträge **18**

Hinweis:
Der Inhalt aller Kapitel ist ist nach geeigneter Aufbereitung für interessierte Schüler:innnen der Mittelstufe verständlich. Es gibt hierzu im *Schülerseminar* des *Schülerzirkels Mathematik* zwei Kurse, in denen diese Aufbereitung durchgeführt wurde. Die Kurse heißen *Zahlentheorie und Kryptographie* und *Primzahlen*. Alle Einheiten des Schülerseminars können (ohne Anmeldung) auf der Seite
`https://pnp.mathematik.uni-stuttgart.de/iadm/Zirkel/material-Schuelerseminar/`
angesehen werden.

1 Lineare diophantische Gleichungen

1.1 Definition: Seien $a \in \mathbb{Z}$, $k \in \mathbb{Z} \setminus \{0\}$. Dann heißt k **Teiler** von a, wenn

$$\exists l \in \mathbb{Z} : a = l \cdot k.$$

Schreibe $k \mid a$.

1.2 Bemerkungen: **1)** $k \mid a \;\Leftrightarrow\; (-k) \mid a$.

2) $a = 0 \;\Rightarrow$ alle $k \in \mathbb{Z} \setminus \{0\}$ sind Teiler von a.

1.3 Definition: **1)** Für $a, b \in \mathbb{Z}$, nicht beide 0, ist $\mathrm{ggT}(a,b) := \max\{k \in \mathbb{N} : k \mid a \;\wedge\; k \mid b\}$ der **größte gemeinsame Teiler**,

2) Für $a, b \in \mathbb{Z} \setminus \{0\}$ ist $\mathrm{kgV}(a,b) := \min\{k \in \mathbb{N} : a \mid k \;\wedge\; b \mid k\}$ das **kleinste gemeinsame Vielfache**.

Für $a, b \in \mathbb{Z} \setminus \{0\}$ gilt $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = |a \cdot b|$ (Beweis über Primfaktorzerlegung).

1.4 Definition: Gegeben seien $a, b, c \in \mathbb{Z}$. Gesucht sind Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung

$$ax + by \;=\; c. \qquad (*)$$

Dann heißt die Gleichung **lineare diophantische Gleichung**.

1.5 Satz: Seien $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. $(*)$ ist in $\mathbb{Z}^2$ genau dann lösbar, wenn $\mathrm{ggT}(a,b) \mid c$.

Beweis: $\Rightarrow$: Wenn $(*)$ eine Lösung $(x, y) \in \mathbb{Z}^2$ besitzt, dann ist $\mathrm{ggT}(a,b)$ Teiler von a und Teiler von b und auch von $ax + by = c$.

$\Leftarrow$: Nun sei $c = n \cdot \mathrm{ggT}(a,b)$ mit $n \in \mathbb{Z}$. Nach Satz 2.6 aus Teil I gibt es Zahlen $k, l \in \mathbb{Z}$, so dass

$$k|a| + l|b| \;=\; \mathrm{ggT}\big(|a|, |b|\big) \;=\; \mathrm{ggT}(a,b).$$

Dann folgt

$$\underbrace{n \cdot k \cdot \mathrm{sgn}(a)}_{=:x} \cdot a + \underbrace{n \cdot l \cdot \mathrm{sgn}(b)}_{=:y} \cdot b \;=\; n \cdot \mathrm{ggT}(a,b) \;=\; c.$$

□

1.6 Bemerkung: Dieser Beweis und Beispiel 2.5 aus Teil I zeigen, wie man eine ganzzahlige Lösung von $(*)$ mit Hilfe des euklidischen Algorithmus berechnen kann.

1.7 Satz: Seien $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. Ist $(x_0, y_0) \in \mathbb{Z}^2$ eine Lösung von $(*)$, dann sind alle Lösungen $(x, y) \in \mathbb{Z}^2$ gegeben durch

$$(x, y) \;=\; \Big(x_0 + k \cdot \frac{b}{\mathrm{ggT}(a,b)}, y_0 - k \cdot \frac{a}{\mathrm{ggT}(a,b)}\Big) \quad \text{mit } k \in \mathbb{Z}. \qquad (**)$$

Beweis: **1)** Durch Einsetzen: Alle Zahlenpaare aus $(**)$ sind Lösungen.

2) Sei nun $(x, y) \in \mathbb{Z}^2$ eine Lösung von $(*)$. Dann folgt

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0 \\ \Rightarrow\ y - y_0 &= -\frac{a}{b}(x - x_0) = -\frac{\frac{a}{\mathrm{ggT}(a,b)}}{\frac{b}{\mathrm{ggT}(a,b)}}(x - x_0). \end{aligned}$$

Die linke Seite $y - y_0$ ist ganzzahlig, der Bruch auf der rechten Seite ist gekürzt. Somit muss $x - x_0$ ganzzahliges Vielfaches vom Nenner sein.

$$\Rightarrow\ x - x_0 = k \cdot \frac{b}{\mathrm{ggT}(a,b)}, \quad y - y_0 = -\frac{\frac{a}{\mathrm{ggT}(a,b)}}{\frac{b}{\mathrm{ggT}(a,b)}} \cdot k \cdot \frac{b}{\mathrm{ggT}(a,b)} = -k \cdot \frac{a}{\mathrm{ggT}(a,b)}.$$

□

2 Kongruenz und Modulorechnung

2.1 Definition: Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Wir schreiben

$$a \equiv b \mod m \qquad (a \text{ ist } \textbf{kongruent} \text{ zu } b \textbf{ modulo } m),$$

falls $a - b$ durch den **Modul** m teilbar ist.

2.2 Satz (Kriterien für Kongruenz): Die folgenden Aussagen sind äquivalent.

(i) $a \equiv b \mod m$

(ii) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$

(iii) a und b lassen beim Teilen durch m den selben Rest.

Beweis: (i) $\Rightarrow$ (ii):

$$\begin{aligned} a \equiv b \mod m &\Leftrightarrow m \mid (a - b) \\ &\Rightarrow \text{Es gibt ein } k \in \mathbb{Z}, \text{ so dass } a - b = k \cdot m \\ &\Rightarrow a = b + km \end{aligned}$$

(ii) $\Rightarrow$ (iii): Sei r der Rest beim Teilen von b durch m, d.h. $b = lm + r$ mit $r, l \in \mathbb{Z}$, $0 \le r \le m - 1$.

$$\begin{aligned} \text{(ii)} \Rightarrow\ a &= b + km \\ &= lm + r + km \\ &= \underbrace{(l + k)}_{\in \mathbb{Z}} m + r \end{aligned}$$

$\Rightarrow$ a lässt beim Teilen durch m den selben Rest r wie b.

(iii) $\Rightarrow$ (i): $a = km + r,\ b = lm + r$ mit $k, l \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow\ a - b &= km + r - (lm + r) \\ &= km + r - kl - r \\ &= \underbrace{(k - l)}_{\in \mathbb{Z}} m \end{aligned}$$

$$\begin{aligned} &\Rightarrow\ m \mid (a - b) \\ &\Leftrightarrow\ a \equiv b \mod m \end{aligned}$$

□

2.3 Satz (Rechenregeln für Kongruenzen): Seien $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$.

1) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann:

a) $a + c \equiv b + d \mod m$,

b) $a \cdot c \equiv b \cdot d \mod m$.

Insbesondere $-a \equiv -b \mod m$ und $a^2 \equiv b^2 \mod m$.

2) Die Relation $\mathcal{R} = \{(a, b) \in \mathbb{Z}^2 : a \equiv b \mod m\}$ ist eine Äquivalenzrelation auf $\mathbb{Z}$, d.h. es gelten

Reflexivität: $\forall a \in \mathbb{Z} : a \equiv a \mod m$ und

Symmetrie: $\forall a, b \in \mathbb{Z} : a \equiv b \mod m \Rightarrow b \equiv a \mod m$ und

Transitivität: $\forall a, b, c \in \mathbb{Z} : a \equiv b \mod m \wedge b \equiv c \mod m \Rightarrow a \equiv c \mod m$.

Beweis von 1b): Wir wissen $a = b + km$, $c = d + lm$ mit $k, l \in \mathbb{Z}$.
Wir suchen ein $j \in \mathbb{Z}$, so dass $ac = bd + jm$.

$$\begin{aligned} ac &= (b + km)(d + lm) \\ &= bd + blm + kmd + kmlm \\ &= bd + \underbrace{(bl + kd + klm)}_{=:j \in \mathbb{Z}} m \\ \Rightarrow \quad ac &= bd + jm \\ \Rightarrow \quad ac &\equiv bd \mod m \end{aligned}$$

□

3 Rechnen mit Restklassen

3.1 Definition: Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Die **Restklasse** $[a]$ von a modulo m ist definiert durch

$$[a] := \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

a heißt **Repräsentant** der Restklasse $[a]$.

3.2 Beispiele: modulo 5:

$$\begin{aligned} [0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} = [5] = [10] = \ldots \\ [1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} = [-4] = \ldots \end{aligned}$$

0, 5 und 10 sind verschiedene Repräsentanten von $[0]$.

3.3 Bemerkung: Die Restklassen sind die Äquivalenzklassen der Äquivalenzrelation $\mathcal{R}$. Im Fall $m = 1$ gilt $[0] = \mathbb{Z}$, es gibt nur eine Restklasse.

3.4 Satz: Ist $[a] = [a']$ und $[b] = [b']$, so gilt $[a \cdot b] = [a' \cdot b']$ und $[a + b] = [a' + b']$.

Beweis: Ist $[a] = [a']$ und $[b] = [b']$, so folgt:

$$\begin{array}{ll} & a \equiv a' \mod m \quad \text{und} \quad b \equiv b' \mod m \\ \overset{\text{Rechenregeln für Kongruenzen}}{\Rightarrow} & ab \equiv a'b' \mod m \quad \text{und} \quad a+b \equiv a'+b' \mod m \\ \Rightarrow & [ab] = [a'b'] \quad \text{und} \quad [a+b] = [a'+b'] \end{array}$$

□

3.5 Definition: Für $a, b \in \mathbb{Z}$ definiert man

$$\begin{aligned} [a] + [b] &:= [a+b] \\ [a] \cdot [b] &:= [ab] \end{aligned}$$

3.6 Bemerkungen: **1)** Nach Satz 3.4 sind die so definierte Summe bzw. Produkt unabhängig vom gewählten Repräsentanten.

2) Hier werden Addition und Multiplikation von Restklassen definiert. Da die Definitionen über die Addition und Multiplikation von ganzen Zahlen erfolgen, verwendet man die selben Symbole.

3.7 Satz und Definition: Die Menge aller Restklassen modulo m mit der oben definierten Addition und Multiplikation bildet einen kommutativen Ring mit Einselement und heißt **Restklassenring modulo** m, geschrieben $\mathbb{Z}/m\mathbb{Z}$.

Beispiel: $\mathbb{Z}/4\mathbb{Z} = \{[0],[1],[2],[3]\}$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Beweis: Einfaches Nachrechnen.
$(\mathbb{Z}/m\mathbb{Z}, +)$ ist kommutative Gruppe, die Multiplikation ist assoziativ und
es gelten die Distributivgesetze $a \cdot (b+c) = a \cdot b + a \cdot c$, $(a+b) \cdot c = a \cdot c + b \cdot c$
Daher ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein Ring.
Zusätzlich ist $[1]$ das Einselement: $[1] \cdot [a] = [1 \cdot a] = [a] = [a \cdot 1] = [a] \cdot [1]$,
und die Multiplikation ist kommutativ.

□

3.8 Satz: Für $[a] \in \mathbb{Z}/m\mathbb{Z}$ gilt $-[a] = [-a]$. Hieraus folgt

$$[a] - [b] := [a] + \big(-[b]\big) = [a-b] \quad \text{für } [a],[b] \in \mathbb{Z}/m\mathbb{Z}.$$

Beweis: $[a] + [-a] = [a-a] = [0] \Rightarrow -[a] = [-a]$.

□

3.9 Bemerkung: $(\mathbb{Z}/4\mathbb{Z} \setminus \{[0]\}, \cdot)$ ist keine Gruppe, denn $[2]$ besitzt kein inverses Element.

3.10 Satz vom Dividieren: Ist p eine Primzahl, und ist $[a] \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, so besitzt die Gleichung

$$[a] \cdot [x] \;=\; [1] \qquad \text{in } \mathbb{Z}/p\mathbb{Z}$$

genau eine Lösung $[x]$, d.h. $[a]$ besitzt ein inverses Element $[a]^{-1} = [x]$.

Beweis: $[1] \;=\; [a] \cdot [x] \;=\; [ax] \;\Leftrightarrow\; 1 \equiv ax \mod p$

$\Leftrightarrow\; 1 - ax \;=\; kp$ für ein $k \in \mathbb{Z}$

$\Leftrightarrow\; 1 \;=\; a\underbrace{x}_{\text{gesucht}} + m\underbrace{k}_{\text{unbekannt}}$

Dies ist eine lineare diophantische Gleichung für $(x, k) \in \mathbb{Z}^2$.

Da $\mathrm{ggT}(a, p) = 1$, ist die Gleichung lösbar, d.h. für jedes $a \in \mathbb{N}$ existiert eine Lösung (x_0, k_0). Alle Lösungen sind durch

$$(x, k) \;=\; (x_0 + lp, k - la) \text{ mit } l \in \mathbb{Z}$$

gegeben. Wir suchen nur $x = x_0 + lp$ und sehen $[x] \;=\; [x_0]$ in $\mathbb{Z}/p\mathbb{Z}$.
$\Rightarrow\; [x] \in \mathbb{Z}/p\mathbb{Z}$ eindeutig. □

3.11 Satz: Ist $m \in \mathbb{N}$, $m \geq 2$ keine Primzahl, dann gibt es mindestens ein Element $[b] \in \mathbb{Z}/m\mathbb{Z}$, so dass die Gleichung

$$[b] \cdot [x] \;=\; [1] \qquad \text{in } \mathbb{Z}/m\mathbb{Z}$$

keine Lösung besitzt.

Beweis: Sei $m = a \cdot b$ mit $a, b \in \mathbb{N}$, $a, b \geq 2$. Wie oben gilt

$$[b] \cdot [x] \;=\; [1] \text{ in } \mathbb{Z}/m\mathbb{Z} \;\Leftrightarrow\; b \cdot x + m \cdot k = 1$$

Nun gilt $\mathrm{ggT}(b, m) = b > 1$, also ist $\mathrm{ggT}(b, m)$ kein Teiler von 1
$\overset{1.5}{\Rightarrow}$ es gibt keine Lösung $(x, k) \in \mathbb{Z}^2$ der diophantischen Gleichung. □

3.12 Folgerung: Sei $m \in \mathbb{N}$, $m \geq 2$. Genau dann, wenn m eine Primzahl ist, ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein Körper.

Beweis: Ist m eine Primzahl, dann besitzt jedes Element $[a] \in \mathbb{Z}/m\mathbb{Z}$ mit $[a] \neq [0]$ ein inverses Element bezüglich der Multiplikation in $\mathbb{Z}/m\mathbb{Z}$. Die weiteren Körpereigenschaften sind erfüllt, da $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Einselement ist.

Ist m keine Primzahl, dann besitzt nicht jedes von $[0]$ verschiedene Element ein inverses Element bezüglich der Multiplikation. Also ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ kein Körper. □

4 Der kleine Satz von Fermat

4.1 Kleiner Satz von Fermat: Sei p Primzahl, $a \in \mathbb{N}$ kein Vielfaches von p. Dann gilt

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}/p\mathbb{Z} \qquad \text{bzw.} \qquad a^{p-1} \equiv 1 \mod p.$$

Beweis: Wir untersuchen die Teilmenge
$A = \{[0a], [1a], [2a], \ldots, [(p-1)a]\}$
von $\mathbb{Z}/p\mathbb{Z} = \{[0], [1], \ldots, [p-1]\}$.

Schritt 1: Wir beweisen, dass alle p Restklassen $[0a]$, $[1a]$, $[2a]$, $\ldots$, $[(p-1)a]$ verschieden sind.

Annahme: $[ja] = [ka]$ für zwei Restklassen mit $0 \le j < k \le p-1$. Dann folgt

$[0] = [ka] - [ja] = [ka - ja] = \big[(k-j)a\big] = [k-j] \cdot [a]$ mit $[k-j] \neq [0]$
$\overset{\text{Satz vom Dividieren}}{\Rightarrow} [a] = [0] \Rightarrow$ a ist Vielfaches von p ↯

Also muss $[ja] \neq [ka]$ gelten.

Schritt 2: Die Menge A hat p verschiedene Elemente und ist Teilmenge der p-elementigen Menge $\mathbb{Z}/p\mathbb{Z}$. Also sind die Mengen gleich.

Schritt 3: Es ist klar, das $[0a] = [0]$ gilt. Wir entfernen nun dieses Element aus beiden Mengen. Das Produkt der restlichen Elemente muss gleich sein:

$$\begin{aligned} & [a] \cdot [2a] \cdot [3a] \cdots [(p-1)a] &&= [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \Leftrightarrow \quad & [1] \cdot [2] \cdot [3] \cdots [p-1] \cdot [a]^{p-1} &&= [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \overset{\text{Satz vom Dividieren}}{\Rightarrow} \quad & [a]^{p-1} = [1]. \end{aligned}$$

□

4.2 Beispiele: Modulo 19: $2^{40} = 2^{19-1} \cdot 2^{19-1} \cdot 2^4 \equiv 1 \cdot 1 \cdot 16 = 16 \mod 19$

In $\mathbb{Z}/7\mathbb{Z}$: $\dfrac{[2]}{[5]} = [2] \cdot \dfrac{[1]}{[5]} = [2] \cdot \dfrac{[5]^6}{[5]} = [2] \cdot [5]^5 = [2] \cdot [5] \cdot [25]^2 = [10] \cdot [4]^2 = [3] \cdot [2] = [6]$.

Brüche können also durch Potenzieren berechnet werden.

4.3 Definition: Ein Element $[g] \in \mathbb{Z}/m\mathbb{Z}$ heißt **Primitivwurzel**, falls durch $[g]^k$, $k = 1, \ldots, m-1$, alle Elemente von $\mathbb{Z}/m\mathbb{Z}$ außer $[0]$ dargestellt werden können.

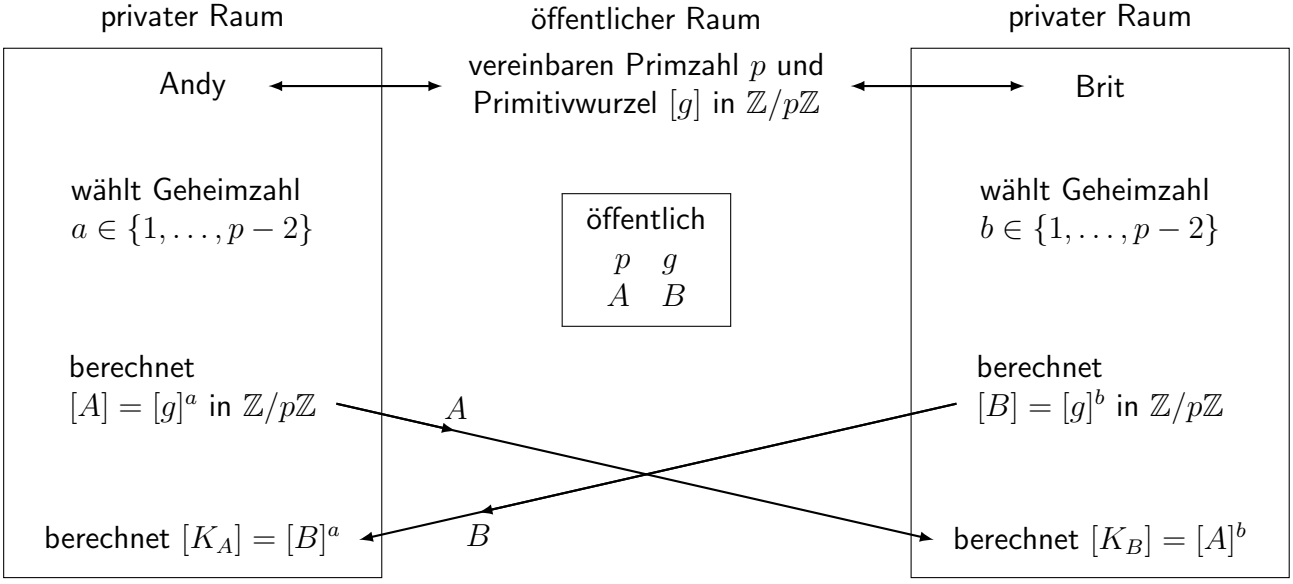
Beispiel: In $\mathbb{Z}/5\mathbb{Z}$:

$k =$	1	2	3	4
$[2]^k =$	[2]	[4]	[3]	[1]
$[4]^k =$	[4]	[1]		

$\Rightarrow$ [2] ist eine Primitivwurzel in $\mathbb{Z}/5\mathbb{Z}$,
aber [4] ist keine.

5 Verschlüsselungsverfahren

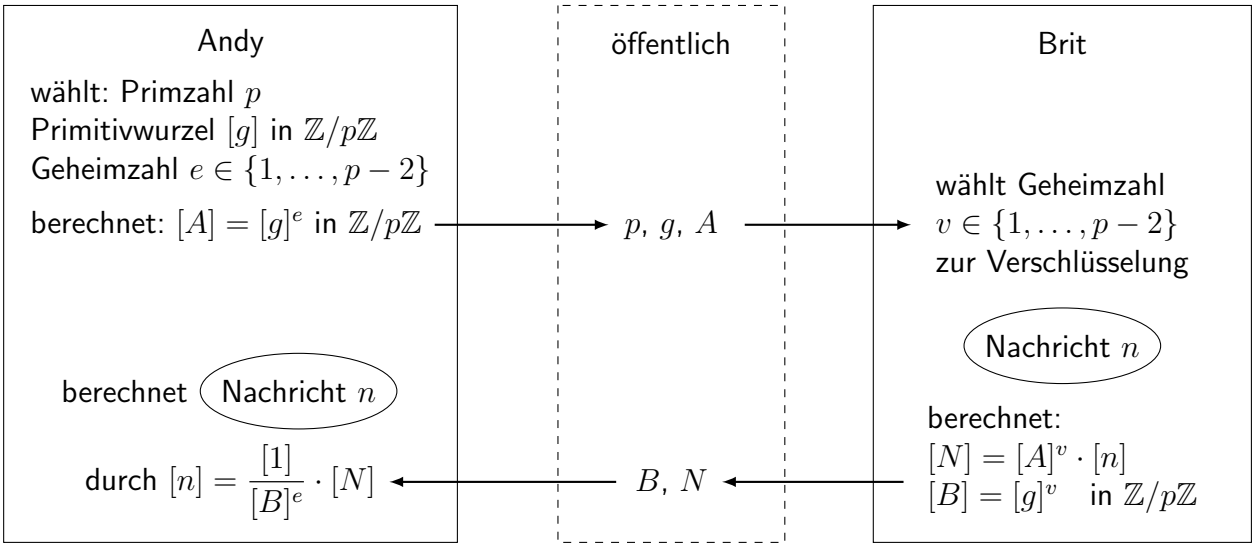
5.1 Diffie-Hellman-Merkle-Schlüsselaustausch:: Beim Schlüsseltausch vereinbaren zwei Personen eine geheime Zahl (Schlüssel), obwohl sie nur über öffentliche Kanäle kommunizieren können.



5.2 Satz: Es gilt $[K_A] = [K_B]$.

Beweis: $[K_A] = [B]^a = \left([g]^b\right)^a = [g]^{ab} = \left([g]^a\right)^b = [A]^b = [K_B]$. □

5.3 Elgamal-Verschlüsselung: Hier stellt Andy drei Zahlen öffentlich zur Verfügung. Mit Hilfe dieser Zahlen kann Brit eine Nachricht (die aus einer Zahl besteht) sicher verschlüsseln, so dass nur Andy die Nachricht entschlüsseln kann.



Begründung: $\frac{[1]}{[B]^e} \cdot [N] = \frac{[1]}{[B]^e} \cdot [A]^v \cdot [n] = \frac{[1]}{\left([g]^v\right)^e} \cdot \left([g]^e\right)^v \cdot [n] = [n]$ in $\mathbb{Z}/p\mathbb{Z}$.

Die Entschlüsselung funktioniert, weil $\left([g]^v\right)^e = \left([g]^e\right)^v$ ist.

5.4 RSA-Verschlüsselung:

Andy	wählt	zwei verschiedene Primzahlen p, q,
	berechnet	$m = pq$, $\widetilde{m} = (p-1)(q-1)$,
	wählt	Verschlüsselungsexponent v mit $1 < v < \widetilde{m}$ und ggT$(v, \widetilde{m}) = 1$,
	veröffentlicht	m und v auf seiner Homepage,
	berechnet	Entschlüsselungsexponent e mit $1 < e < \widetilde{m}$ und $ev \equiv 1 \mod \widetilde{m}$.

Brit kann nun ein Nachricht als Zahl n folgendermaßen übermitteln:

$$\text{Verschlüsselte Zahl } N \equiv n^v \mod m.$$

Frank bekommt die Zahl zurück durch

$$n \equiv N^e \mod m.$$

Hinweis: Die Zahlen n muss zwischen 1 und $m-1$ gewählt werden (denn $m \equiv 0 \mod m$).

5.5 Satz: Der RSA-Algorithmus ist korrekt.

Beweis: Seien $m = pq$, $\widetilde{m} = (p-1)(q-1)$, $ev \equiv 1 \mod \widetilde{m}$, $N \equiv n^v \mod m$.
Wir beweisen, dass $N^e \equiv n \mod m$ gilt.

Kleiner Fermat: Ist p Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p, so gilt $a^{p-1} \equiv 1 \mod p$.

Vorbemerkung 1: $\underbrace{a \equiv n \mod p}_{a-n \text{ durch } p \text{ teilbar}}$ und $\underbrace{a \equiv n \mod q}_{a-n \text{ durch } q \text{ teilbar}} \overset{p,q \text{ Primzahlen}}{\Leftrightarrow} a \equiv n \mod \underbrace{pq}_{=m}$.

Vorbemerkung 2: $e \cdot v \equiv 1 \mod \widetilde{m}$
$\Leftrightarrow\ e \cdot v = 1 + k\widetilde{m} = 1 + k(p-1)(q-1)$ mit einem $k \in \mathbb{Z}$.

Wir rechnen zunächst nur modulo p.
Vorbemerkung 1 $\Rightarrow\ N^e \equiv (n^v)^e = n^{e \cdot v} \mod p$

Fall $\mathrm{ggT}(n, p) = 1$:

$$n^{e \cdot v} \overset{\text{Vorbemerkung 2}}{=} n^{1+k(p-1)(q-1)} = n \cdot (n^{p-1})^{k(q-1)}$$
$$\overset{\substack{\text{kleiner} \\ \text{Fermat}}}{\equiv} n \cdot 1^{k(q-1)} = n \mod p$$

Fall $\mathrm{ggT}(n, p) = p$: Dann ist $n = l \cdot p$ und somit $n \equiv 0 \mod p$.
$\Rightarrow\ n^{e \cdot v} \equiv 0^{e \cdot v} = 0 \equiv n \mod p$.

In beiden Fällen (das sind alle möglichen Fälle) gilt also

$$N^e \equiv n^{e \cdot v} \equiv n \mod p. \tag{1}$$

Nun rechnen wir nur modulo q. Indem man p und q vertauscht, folgt genauso, dass

$$N^e \equiv n^{e \cdot v} \equiv n \mod q \tag{2}$$

gilt.

(1) und (2) $\overset{\substack{\text{Vorbemerkung 1} \\ pq=m}}{\Rightarrow} N^e \equiv n \mod m.$ □

5.6 Bemerkung: Mit dem Wissen aus den nächsten Kapiteln erkennt man, dass $\widetilde{m} = \varphi(m)$ (Eulersche Phi-Funktion), der Satz von Euler-Fermat ($a^{\varphi(m)} \equiv 1 \mod m$ falls a, m teilerfremd) und der chinesische Restsatz bei der Entwicklung des Algorithmus verwendet wurden.

6 Der Chinesische Restsatz

6.1 Chinesischer Restsatz: Seien $n \in \mathbb{N}$, $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremde Moduln und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann gelten

1) Die simultane Kongruenz

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_n \mod m_n \end{aligned}$$

besitzt mindestens eine Lösung $x \in \mathbb{Z}$.

2) Sei $M := m_1 \cdots m_n$. Ist $x_0 \in \mathbb{Z}$ eine Lösung der simultanen Kongruenz, dann sind alle Lösungen durch

$$x = x_0 + k \cdot M$$

mit $k \in \mathbb{Z}$ gegeben.

Beweis: **1)** Für $j = 1, \ldots, n$ gilt $\mathrm{ggT}\left(m_j, \frac{M}{m_j}\right) = 1$. Daher besitzt jede der linearen diophantischen Gleichungen

$$x_j m_j + y_j \frac{M}{m_j} = 1$$

eine Lösung (x_j, y_j) (sogar unendlich viele). Setze $e_j := y_j \frac{M}{m_j}$. Dann folgt $e_j \in \mathbb{Z}$ und

$$\begin{aligned} e_j &\equiv 1 \mod m_j \\ e_j &\equiv 0 \mod m_k \qquad \text{für } k \neq j, \text{ da } \frac{M}{m_j} \text{ durch } m_k \text{ teilbar ist.} \end{aligned}$$

$\Rightarrow\ x := \sum_{j=1}^{n} a_j e_j$ löst die simultane Kongruenz.

2) Offensichtlich lösen alle Zahlen $x = x_0 + kM$ die simultane Kongruenz, denn $kM \equiv 0 \mod m_j$ für $j = 1, \ldots, n$.

Sei nun x eine Lösung der simultanen Kongruenz. Dann folgt

$$x - x_0 \equiv 0 \mod m_j \text{ für } j = 1, \ldots, n.$$

D.h. $x - x_0$ ist durch jede der Zahlen m_j teilbar.
$m_1, \ldots, m_n$ paarweise teilerfremd $\Rightarrow$ $M = m_1 \cdots m_n$ ist Teiler von $x - x_0$. □

7 Die eulersche Phi-Funktion

7.1 Definition: Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ mit

$$\varphi(n) \ := \ \text{Anzahl der Zahlen } 1 \leq k \leq n, \text{ die teilerfemd zu } n \text{ sind einschießlich } k = 1$$

heißt **Eulersche Phi-Funktion**.

7.2 Beispiele: **1)**

n	Menge der zu n teilerfremden Zahlen	$\varphi(n)$
2	$\{1\}$	1
3	$\{1,2\}$	2
4	$\{1,3\}$	2
5	$\{1,2,3,4\}$	4
6	$\{1,5\}$	2
7	$\{1,2,3,4,5,6\}$	6
8	$\{1,3,5,7\}$	4
9	$\{1,2,4,5,7,8\}$	6

2) $p \in \mathbb{N}$ Primzahl: $\varphi(p) = p - 1$,
denn die Menge der teilerfremden Zahlen ist $\mathrm{TF}(p) = \{1, 2, \ldots, p-1\}$.

3) Ist $p \in \mathbb{N}$ Primzahl und Fermatzahl, dann gilt $\varphi(p) = p - 1 = 2^{2^n}$ für ein $n \in \mathbb{N}$.

4) Ist $p \in \mathbb{N}$ Primzahl und $k \in \mathbb{N}$, dann gilt $\varphi(p^k) = p^k - p^{k-1}$:
Aus der Menge $\{1, 2, \ldots, p^k\}$ müssen alle Vielfachen von p entfernt werden, dies sind

$$1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p,$$

also p^{k-1} Zahlen.

Z.B. $\varphi(121) = 121 - 11 = 110$.

7.3 Satz: Sind $m, n \in \mathbb{N}$ teilerfremd, dann gilt $\varphi(m \cdot n) = \varphi(n) \cdot \varphi(m)$.

Beweis: Setze $\mathrm{TF}(j) := \big\{k \in \{1, \ldots, j\} : \mathrm{ggT}(k, j) = 1\big\}$ für $j \in \mathbb{N}$. Dann $\varphi(j) = \big|\mathrm{TF}(j)\big|$.

Definiere

$$H : \mathrm{TF}(m \cdot n) \to \mathrm{TF}(m) \times \mathrm{TF}(n)$$

durch

$$H(k) \ := \ (k_m, k_n) \quad \text{mit } k_m \equiv k \mod m, \quad k_n \equiv k \mod n.$$

Behauptung: H ist bijektiv. Dann folgt

$$\varphi(m \cdot n) \ = \ \big|\mathrm{TF}(m \cdot n)\big| \ = \ \big|\mathrm{TF}(m) \times \mathrm{TF}(n)\big| \ = \ \big|\mathrm{TF}(m)\big| \cdot \big|\mathrm{TF}(n)\big| \ = \ \varphi(m) \cdot \varphi(n).$$

H ist injektiv, denn die simultane Kongruenz

$$x \equiv k_n \mod m, \quad x \equiv k_m \mod m$$

besitzt die Lösungen $x = k + jmn$ (chinesischer Restsatz), also nur eine Lösung $x \in \{1, \ldots, mn\}$.

H ist surjektiv, denn sei $(k_m, k_n) \in \mathrm{TF}(m) \times \mathrm{TF}(n)$. Sei weiter x die Lösung von

$$x \equiv k_m \mod m, \quad x \equiv k_n \mod n \quad \text{mit } x \in \{1, \dots, mn\}.$$

$x \equiv k_m \mod m \Leftrightarrow x = k_m + jm$

$$\Rightarrow \mathrm{ggT}(x, m) \mid k_m \Rightarrow \mathrm{ggT}(x, m) \mid \mathrm{ggT}(k_m, m) = 1 \Rightarrow \mathrm{ggT}(x, m) = 1$$

Genauso: $\mathrm{ggT}(x, n) = 1$

m, n teilerfremd $\Rightarrow \mathrm{ggT}(x, m \cdot n) = 1$
Also gilt $x \in \mathrm{TF}(m \cdot n)$ und $H(x) = (k_m, k_n)$. □

7.4 Folgerung: Ist $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{j=1}^{k} p_j^{l_j}$, wobei $p_1, \dots, p_k$ paarweise verschiedene Primzahlen sind, so gilt

$$\varphi(n) = \prod_{j=1}^{k} \varphi(p_j^{l_j}) = \prod_{j=1}^{k} \left(p_j^{l_j} - p_j^{l_j - 1}\right) = \prod_{j=1}^{k} p_j^{l_j - 1}(p_j - 1).$$

7.5 Satz: Ein regelmäßiges n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n) = 2^k$ für ein $k \in \mathbb{N}$ ist.

Beweis: Folgt aus der letzten Formel und aus den Sätzen 5.13 und 5.16 im Teil III (Konstruierbarkeit). □

7.6 Satz: Sei $(G, \circ)$ eine endliche abelsche Gruppe. Für jedes $g \in G$ gilt

$$g^{|G|} = e,$$

wobei $|G|$ die Anzahl der Elemente von G und e das neutrale Element von G bezeichnet.

Beweis: Sei $G = \{g_1, \dots, g_n\}$. Betrachte die Menge

$$M := \{g \circ g_1, g \circ g_2, \dots, g \circ g_n\} \subseteq G.$$

Es gilt $g \circ g_j \neq g \circ g_k$ für $j \neq k$ (denn $g \circ g_j = g \circ g_k \overset{g^{-1}\circ}{\Rightarrow} g_j = g_k \Rightarrow j = k$).
Die Mengen M und G haben also die selbe Anzahl von Elementen und sind folglich gleich.
Multiplikation aller Elementen von M bzw. von G ergibt

$$\begin{aligned} & g \circ g_1 \circ g \circ g_2 \cdots \circ g \circ g_n = g_1 \circ g_2 \cdots \circ g_n \\ \overset{\text{Kommutativität}}{\Rightarrow} \quad & g^n \circ g_1 \circ g_2 \cdots \circ g_n = g_1 \circ g_2 \cdots \circ g_n \\ \Rightarrow \quad & g^n = e. \end{aligned}$$

□

7.7 Satz (Fermat-Euler): Sind $a, n \in \mathbb{N}$ teilerfremd, so gilt $a^{\varphi(n)} \equiv 1 \mod n$.

Beweis: Sei $G := \left\{[b] \in \mathbb{Z}/n\mathbb{Z} : \mathrm{ggT}(b, n) = 1\right\}$. Dann ist $(G, \cdot)$ eine abelsche Gruppe, denn zu jeder Restklasse $[b] \in G$ gibt es ein inverses Element (vgl. Beweis zu 3.11). Die restlichen Gruppeneigenschaften sind klar. Und G besitzt $\varphi(n)$ Elemente.

Aus dem letzten Satz folgt dann $[b]^{\varphi(n)} = [1]$ für jedes Element $[b]$ von G. Da $\mathrm{ggT}(a, n) = 1$, gibt es eine Restklasse $[b] \in G$ mit $[a] = [b]$, also $a \equiv b \mod n$.

Es folgt $a^{\varphi(n)} \equiv b^{\varphi(n)} \equiv 1 \mod n$. □

8 Dezimalbruchentwicklung

8.1 Satz und Definition: **1)** Jede reelle Zahl $a \in]0,1[$ besitzt eine **Dezimalbruchentwicklung** oder kurz **Dezimaldarstellung**

$$a \;=\; \sum_{k=1}^{\infty} \frac{a_k}{10^k}$$

mit $a_k \in \{0,1,\ldots,9\}$ für $k \in \mathbb{N}$. Schließt man den Fall $\exists k_0 \in \mathbb{N}\ \forall k \geq k_0 : a_k = 9$ aus (Neunerperiode), dann ist die Dezimaldarstellung eindeutig. Man schreibt

$$a \;=\; 0{,}a_1a_2a_3\ldots\ .$$

2) Im Fall $\exists k_0 \in \mathbb{N}\ \forall k \geq k_0 : a_k = 0$ heißt die Dezimaldarstellung **abbrechend**.

3) Eine nicht abbrechende Dezimaldarstellung heißt **periodisch**, falls

$$\exists k_0, l \in \mathbb{N}\ \forall k \geq k_0 : a_{k+l} = a_k.$$

das kleinstmögliche l heißt **Periodenlänge**. Ist $k_0 = 1$ wählbar, dann ist die Dezimaldarstellung **reinperiodisch**. Man kennzeichnet die Periode durch Überstreichen, z.B. bei einer reinperiodischen Zahl mit Periodenlänge l

$$a \;=\; 0{,}\overline{a_1a_2\ldots a_l}.$$

8.2 Bemerkung: Für die Zahl $a = 0{,}4727272\ldots$ schreibt man $a = 0{,}4\overline{72}$. Man schreibt nicht $a = 0{,}47\overline{27}$ und auch nicht $a = 0{,}4\overline{7272}$.

8.3 Satz: Seien $m, n \in \mathbb{N}$ teilerfremd, $m < n$. Genau dann, wenn die Primfaktorzerlegung von n nur die Primzahlen 2 oder 5 (oder beide) enthält, ist die Dezimaldarstellung von $\frac{m}{n}$ abbrechend, d.h. es gilt

$$\frac{m}{n} \;=\; 0{,}a_1a_2\ldots a_k.$$

Beweis: Rückrichtung:

$$\begin{aligned} \frac{m}{n} \;&=\; 0{,}a_1a_2\ldots a_k \;=\; \frac{a_1a_2\ldots a_k}{10^k} \\ \Rightarrow\ \underbrace{n}_{\in\mathbb{N}} \;&=\; \frac{10^k \cdot m}{a_1a_2\ldots a_k} \;=\; \frac{2^k \cdot 5^k \cdot m}{a_1a_2\ldots a_k} \end{aligned}$$

Da der letzte Bruch eine natürliche Zahl darstellt, kann man den Nenner wegkürzen. Da m, n teilerfremd sind, muss

$$a_1a_2\ldots a_k \;=\; m \cdot 2^j \cdot 5^l$$

mit passendem $j, l \in \mathbb{N}_0$, $j, l \leq k$ gelten. Es folgt

$$n \;=\; 2^{k-j} \cdot 5^{k-l},$$

wobei wegen $n > 1$ eine der beiden Potenzen größer Null sein muss.

Hinrichtung: Sei $n = 2^j \cdot 5^l$ mit $j, l \in \mathbb{N}_0$

$$\Rightarrow\ \frac{m}{n} \;=\; \frac{m}{2^j \cdot 5^l} \cdot \frac{2^l \cdot 5^j}{2^l \cdot 5^j} \;=\; \frac{m \cdot 2^l \cdot 5^j}{10^{l+j}}.$$

Dies ergibt offensichtlich eine abbrechende Dezimaldarstellung. □

8.4 Satz: Seien $m, n \in \mathbb{N}$ teilerfremd, $m < n$. Enthält die Primfaktorzerlegung von n mindestens eine Primzahl $p \in \mathbb{N} \setminus \{2, 5\}$, dann ist die Dezimaldarstellung von $\frac{m}{n}$ periodisch. Die Periodenlänge ist höchstens $n - 1$.

Beweis: **1)** Aus dem letzten Satz folgt, dass $\frac{m}{n}$ keine abbrechende Dezimaldarstellung besitzt.

2) Schriftliches Dividieren:

$$
\begin{array}{rl}
m : n &= 0{,}a_1a_2\ldots a_j\ldots a_{k-1}\ldots \\
\underline{-n\cdot 0} & \\
r_1\cdot 10 & (r_1 = m) \\
\underline{-n\cdot a_1} & \\
r_2\cdot 10 & \\
\underline{-\ n\cdot a_2} & \\
r_3\cdot 10 & \\
\ddots & \\
r_j\cdot 10 & \\
\underline{-\ n\cdot a_j} & \\
r_{j+1}\cdot 10 & \\
\ddots & \\
r_{k-1}\cdot 10 & \\
\underline{-\quad n\cdot a_{k-1}} & \\
r_k\cdot 10 & \\
\ddots &
\end{array}
$$

Der Rest $r_j = 0$ kann nie auftreten, sonst wäre die Dezimaldarstellung abbrechend.
Also sind alle Reste $r_j \in \{1, \ldots, n-1\}$.
$\Rightarrow$ spätestens bei $k = n$ muss $r_k = r_j$ für ein $j < k$ gelten.
Ab hier wiederholt sich die Rechnung, es folgt $r_{k+l} = r_{j+l}$ für $l \in \mathbb{N}_0$
$\Rightarrow$ die Periodenlänge ist $k - j$, wenn r_k der erste doppelt auftretende Rest ist.
$\Rightarrow$ $\frac{m}{n} = 0{,}a_1a_2\ldots\overline{a_j\ldots a_{k-1}}$ mit Periodenlänge $k - j \leq n - 1$. □

8.5 Folgerung: Im letzten Beweis gilt

$$r_k = r_j \;\Leftrightarrow\; 10^{k-j} \equiv 1 \mod n.$$

Beweis:

$$
\begin{array}{rcll}
r_k &=& 10\cdot r_{k-1} - n\cdot a_{k-1} &\equiv 10\cdot r_{k-1} \mod n \\
&=& 10(10\cdot r_{k-2} - n\cdot a_{k-2}) &\equiv 10^2\cdot r_{k-2} \mod n \\
&\ldots& &\equiv 10^{k-j}\cdot r_j \mod n.
\end{array}
$$

D.h. es gilt $r_k \equiv 10^{k-j} r_j \mod n$. □

8.6 Beispiele:

n	11	13	14	17	21	37	41	109
Periodenlänge von $\frac{1}{n}$	2	6	6	16	6	3	5	108
$\varphi(n)$	10	12	6	16	12	36	40	108

8.7 Definition: Seien $a, n \in \mathbb{N}$ teilerfremd. Dann heißt

$$\mathrm{ord}_n(a) \;:=\; \min \underbrace{\left\{k \in \mathbb{N} : a^k \equiv 1 \mod n\right\}}_{\text{enthält } \varphi(n) \text{ (Fermat-Euler)}} \;\leq\; \varphi(n)$$

die **Ordnung** von a bezüglich n.

8.8 Beispiel: $\mathrm{ord}_{37}(10) = 3$:

$$\begin{aligned} 10^1 &= 10 \\ 10^2 &= 100 \equiv 100 - 2 \cdot 37 = 26 \mod 37 \\ 10^3 &\equiv 260 \equiv 260 - 7 \cdot 37 = 1 \mod 37 \end{aligned}$$

Zum Vergleich: $\varphi(37) = 36$

8.9 Satz: Seien $m, n \in \mathbb{N}$ teilerfremd, $m < n$ und $n, 10$ teilerfremd. Dann ist die Dezimaldarstellung von $\frac{m}{n}$ periodisch mit Periodenlänge $\mathrm{ord}_n(10)$. Insbesondere hängt die Periodenlänge nicht vom Zähler m ab, wenn der Bruch $\frac{m}{n}$ gekürzt ist.

Beweis: Nach Satz 8.4 ist die Dezimaldarstellung von $\frac{m}{n}$ periodisch.

Die Aussage über die Periodenlänge folgt direkt aus Folgerung 8.5 und daraus, dass die Periodenlänge die kleinste Differenz $|k - j|$ ist, für die $r_k = r_j$ gilt. □

8.10 Satz: Seien $a, n \in \mathbb{N}$ teilerfremd. Dann ist $\mathrm{ord}_n(a)$ ein Teiler von $\varphi(n)$.

Beweis: Teile $\varphi(n)$ durch $\mathrm{ord}_n(a)$ mit Rest:

$$\varphi(n) \;=\; l \cdot \mathrm{ord}(a) + r \text{ mit } 0 \leq r \leq \mathrm{ord}_n(a) - 1.$$

Dann folgt

$$1 \;\equiv\; a^{\varphi(n)} \;=\; a^{l \cdot \mathrm{ord}_n(a) + r} \;=\; (a^{\mathrm{ord}(a)})^l \cdot a^r \;\equiv\; a^r \mod n,$$

also

$$a^r \equiv 1 \mod n \quad \text{und} \quad 0 \leq r \leq \mathrm{ord}_n(a) - 1.$$

$\Rightarrow\; r = 0$, also $\varphi(n) = l \cdot \mathrm{ord}_n(a)$. □

8.11 Beispiel: $p = 109$: $\varphi(p) = p-1 = 108 = 2^2 \cdot 3^3$ hat die Teiler $2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108$.

$$\begin{array}{rcl} 10^2 &=& 100 \\ 10^3 &=& 1000 \equiv 1000 - 981 = 19 \\ 10^6 &\equiv& 19^2 \equiv 361 - 327 = 34 \\ 10^{12} &\equiv& 34^2 \equiv 1156 - 1090 = 66 \end{array} \qquad \begin{array}{rcl} 10^{18} &\equiv& 34 \cdot 66 \equiv 2244 - 2180 = 64 \\ 10^{36} &\equiv& 64^2 \equiv 4096 - 4033 = 63 \\ 10^{54} &\equiv& 64 \cdot 63 \equiv 4032 - 4033 = -1 \\ \Rightarrow & \multicolumn{2}{l}{\text{für alle Teiler } k \text{ von } 54 \text{ gilt } 10^k \not\equiv 1 \mod 109} \\ & \multicolumn{2}{l}{(\text{sonst müsste } 10^{54} \equiv +1 \mod 109 \text{ gelten})} \end{array}$$

Die Teiler $k = 12$ und $k = 36$ von 108 sind bereits kontrolliert.
Es fehlt noch $k = 4$: $10^4 \equiv 190 \equiv 190 - 109 = 81$

$\Rightarrow$ für alle Teiler $k < 108$ von 108 gilt $10^k \not\equiv 1 \mod 109$

$\Rightarrow$ $\mathrm{ord}_{109}(10) = 108$, also hat $\frac{1}{109}$ maximal mögliche Periodenlänge 108.

8.12 Satz: Mit $k \in \mathbb{N}$ gilt

$$0{,}\overline{a_1 a_2 \ldots a_k} = \frac{a_1 a_2 \ldots a_k}{99 \ldots 9},$$

wobei im Nenner der rechten Seite die natürliche Zahl steht, die aus k Neunen gebildet wird.

Beweis:

$$\begin{array}{rcl} 0{,}\overline{a_1 a_2 \ldots a_k} &=& a_1 a_2 \ldots a_k \cdot \sum_{j=1}^{\infty} 10^{-jk} \\ &=& \frac{a_1 a_2 \ldots a_k}{10^k} \cdot \sum_{j=0}^{\infty} (10^{-k})^j \\ &\underset{\text{Reihe}}{\overset{\text{geometrische}}{=}}& \frac{a_1 a_2 \ldots a_k}{10^k} \cdot \frac{1}{1 - 10^{-k}} \\ &=& \frac{a_1 a_2 \ldots a_k}{10^k - 1} \end{array}$$

□

8.13 Spezialfall: $0{,}\overline{9} = \frac{9}{10-1} = 1$. D.h. $0{,}\overline{9}$ ist nur eine andere Darstellung der Zahl 1.

8.14 Satz: Sei p Primzahl, $p \neq 2$, $p \neq 5$ und

$$N = \underbrace{99 \ldots 9}_{\mathrm{ord}_p(10) \text{ Neunen}} .$$

Dann ist N durch p teilbar, und N ist die kleinste aus Neunen gebildete natürliche Zahl, die durch p teilbar ist.

Beweis: $N = \underbrace{99 \ldots 9}_{k \text{ Neunen}} = 10^k - 1$ ist genau dann durch p teilbar, wenn $10^k \equiv 1 \mod p$ gilt. Und $k = \mathrm{ord}_p(10)$ ist die kleinste natürliche Zahl k, für die das gilt.

□

8.15 Satz: Ist p prim, $p \neq 2$, $p \neq 5$ und $k = \mathrm{ord}_p(10)$ durch 2 teilbar, so ist $10^{k/2} + 1$ durch p teilbar.

Beweis: Mit 3. binomische Formel gilt

$$(10^{k/2}+1)(\underbrace{10^{k/2}-1}_{\text{nicht durch } p \text{ teilbar}}) = \underbrace{10^k-1}_{\text{durch } p \text{ teilbar}}.$$

□

8.16 Satz: Ist p prim, $p \neq 2$, $p \neq 5$ und $k = \mathrm{ord}_p(10)$ durch 2 teilbar, so ergänzen sich die j-te Periodenziffer von $\frac{1}{p}$ und die $\frac{k}{2}+j$-te Periodenziffer zu 9.

Beweis: Am Beispiel $p = 13$ mit Periodenlänge $k = \mathrm{ord}_{13}(10) = 6$.

$$\begin{aligned} \frac{1}{p} &= 0{,}076923076923\ldots \\ 10^3 \cdot \frac{1}{p} &= 76{,}923076923076\ldots \\ \underbrace{(10^3+1)\cdot\frac{1}{p}}_{\text{letzter Satz: ganze Zahl}} &= 76{,}9999999999999\ldots = 77 \end{aligned}$$

Da auf der linken Seite eine ganze Zahl steht, muss auf der rechten Seite eine Neunerperiode stehen.
□

8.17 Beispiel: $p = 23$: Es gilt $\mathrm{ord}_{23}(10) = 22$. Ein Taschenrechner zeigt

$$\frac{1}{23} = 0,\underbrace{04347826086}_{11\text{Stellen}}96$$

Wir sehen, dass 9 die Ergänzung zur 0 ist, und dass die letzte Stelle 6 gerundet ist, denn hier muss 5 stehen. Wir können nun auf die volle Periode ergänzen und erhalten

$$\frac{1}{23} = 0,\overline{04347826086\,95652173913}.$$

8.18 Bemerkung: Seien $n, k \in \mathbb{N}$, $n \geq 3$. Hat $\frac{1}{n}$ eine reinperiodische Dezimaldarstellung mit Periodenlänge k, so folgt

$$\frac{1}{n} = 0,\overline{a_1 \ldots a_k} = \frac{a_1 \ldots a_k}{10^k - 1}$$

bzw.

$$n = \frac{10^k - 1}{a_1 \ldots a_k}.$$

Also muss n ein Teiler von $10^k - 1 = 99\ldots9$ sein.

Fall $k = 1$: $9 = 3 \cdot 3 \Rightarrow$ Periodenlänge 1 nur bei $\frac{1}{3}$, $\frac{1}{9}$.

Fall $k = 2$: $99 = 3 \cdot 3 \cdot 11 \Rightarrow$ Periodenlänge 2 nur bei $\frac{1}{11}$, $\frac{1}{33}$, $\frac{1}{99}$.

Fall $k = 3$: $999 = 3 \cdot 3 \cdot 3 \cdot 37 \Rightarrow$ Periodenlänge 3 nur bei $\frac{1}{27}$, $\frac{1}{37}$, $\frac{1}{3\cdot37} = \frac{1}{111}$, $\frac{1}{9\cdot37} = \frac{1}{333}$, $\frac{1}{999}$.

Multipliziert den Nenner n mit Faktoren $2^j \cdot 5^l$, so ändert sich die Periodenlänge nicht. Z.B.

$$\begin{aligned} \frac{1}{5\cdot11} &= \frac{2}{10}\cdot\frac{1}{11} = \frac{2}{10}\cdot\frac{9}{99} = \frac{1}{10}\cdot\frac{18}{99} = 0,0\overline{18} \\ \frac{1}{4\cdot11} &= \frac{25}{100}\cdot\frac{1}{11} = \frac{25}{100}\cdot\frac{9}{99} = \frac{1}{100}\cdot\frac{225}{99} = 0,02\overline{27} \end{aligned}$$

9 Ergänzungen und Nachträge

9.1 Definition: **1)** Sei $n \in \mathbb{N}$. Gibt es $k, l \in \mathbb{N}$, $k, l \neq 1$, so dass

$$n = k \cdot l,$$

so heißt n **zusammengesetzte Zahl**.

2) Eine Zahl $n \in \mathbb{N}$ heißt **Primzahl**, falls $n \neq 1$ und n nur die Teiler 1 und n besitzt. Man sagt: n **ist prim**.

9.2 Folgerung: Für jedes $n \in \mathbb{N}$ gilt genau eine der drei Aussagen
$n = 1$,
n ist zusammengesetzt,
n ist prim.

9.3 Satz: Jede natürliche Zahl $n \geq 2$ kann als Produkt von Primzahlen dargestellt werden. Dieses Produkt wird **Primfaktorzerlegung** genannt. (Ist n prim, dann besteht das „Produkt“ nur aus einem Faktor.)

Beweis: Beweis mit vollständiger Induktion.

Induktionsanfang $n = 2$: Für $n = 2$ stimmt die Behauptung, da 2 eine Primzahl ist.

Induktionsschritt: Es sei bereits bewiesen, dass die Behauptung für $n = 2, 3, \ldots, m$ gilt.

Wir beweisen, dass die Behauptung dann auch für $n = m + 1$ gilt.

Fall 1: $m + 1$ ist prim.
$\Rightarrow$ $n = m + 1$ ist die Primfaktorzerlegung

Fall 2: $m + 1$ ist zusammengesetzt: $m + 1 = k \cdot l$, wobei $k, l \leq m$ (da $k, l \neq 1$).
Für k, l ist die Behauptung bereits bewiesen, d.h.

$$k = p_1 \cdot p_2 \cdots p_j, \quad l = q_1 \cdot q_2 \cdots q_i,$$

wobei $= p_1, p_2, \ldots, p_j, q_1, q_2, \ldots, q_i$ Primzahlen sind.

$\Rightarrow$ $n = m + 1 = p_1 \cdot p_2 \cdots p_j \cdot q_1 \cdot q_2 \cdots q_i =$ Produkt von Primzahlen

Damit ist bewiesen, dass die Behauptung auch für $n = m + 1$ wahr ist.

Induktionsschluss: Die Behauptung ist für alle $n \geq 2$ bewiesen.

□

9.4 Satz: Es gibt unendlich viele Primzahlen.

Beweis: Annahme: Es gibt nur endlich viele Primzahlen. Seien diese $p_1, p_2, \ldots, p_n$.

Betrachte $m = p_1 \cdot p_2 \cdots p_n + 1$.
Dann kann m keine Primzahl sein, denn m ist größer als alle Primzahlen $p_1, p_2, \ldots, p_n$.

Nach dem letzten Satz kann m als Produkt von Primzahlen dargestellt werden:

$$m \;=\; p_1^{l_1} \cdot p_2^{l_2} \cdots p_n^{l_n},$$

wobei für mindestens eine der Zahlen $l_1, \ldots, l_n \geq 1$ gelten muss. Sei z.B. $l_1 \geq 1$.

$$\begin{aligned}
\Rightarrow \quad & m \;=\; p_1 \cdot \underbrace{p_1^{l_1-1} \cdots p_n^{l_n}}_{=k} \\
\Rightarrow \quad & p_1 \cdot k \;=\; p_1 \cdot p_2 \cdots p_n + 1 \quad \Big| - p_1 \cdot p_2 \cdots p_n \\
\Leftrightarrow \quad & p_1 \cdot k - p_1 \cdot p_2 \cdots p_n \;=\; 1 \quad \Big| p_1 \text{ Ausklammern} \\
\Leftrightarrow \quad & p_1 \cdot (k - p_2 \cdots p_n) \;=\; 1
\end{aligned}$$

$\Rightarrow$ p_1 ist Teiler von 1. Widerspruch!

p_1 kann nicht Teiler von 1 sein, also muss unsere Annahme falsch gewesen sein. Es gibt also unendlich viele Primzahlen. □

9.5 Definition:

Sind p und $p+2$ Primzahlen, so heißt das Paar $(p, p+2)$ **Primzahlzwilling**.

9.6 Beispiel: $(3,5)$, $(11,13)$, $(41,43)$ sind Primzahlzwillinge.

9.7 Bemerkungen: **1)** Es ist nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt.

2) In Wikipedia gibt es einen Artikel über eine illegale Primzahl.