2. Die Restklassenringe $\mathbb{Z}/n$.

Wir beschäftigen uns hier mit den Ringen $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}$, und zwar einerseits mit der additiven Gruppe $(\mathbb{Z}/n, +)$, andererseits mit der multiplikativen Halbgruppe $(\mathbb{Z}/n, \cdot)$. Ist $(H, *)$ eine Halbgruppe, so bezeichnen wir mit $U(H, *)$ die Menge ihrer invertierbaren Elemente (also der Elemente $h \in H$ für die es ein $h' \in H$ gibt mit $hh' = 1 = h'h$); diese Menge ist mit der gegebenen Multiplikation $*$ eine Gruppe, man nennt sie die *Einheitengruppe* von H. Wir interessieren uns also für die beiden Gruppen

$$(\mathbb{Z}/n, +), \quad U(\mathbb{Z}/n, *),$$

beides sind kommutative Gruppe endlicher Ordnung (die *Ordnung* einer Gruppe ist definiert als die Anzahl ihrer Elemente). Ist $n = p$ eine Primzahl, so ist $\mathbb{F}_p = \mathbb{Z}/p$ ein Körper, und man schreibt $\mathbb{T}_p^* = U(\mathbb{Z}/p, \cdot)$.

2.1. Der Satz von Lagrange.

2.1. (Satz von Lagrange). *Sei G eine endliche Gruppe, sei U eine Untergruppe. Dann ist $|U|$ ein Teiler von $|G|$.* Man nennt $|G|/|U|$ den *Index von U in G.*

Beweis: Ist $g \in G$, so nennt man $Ug = \{ug \mid u \in U\}$ die Rechtsnebenklasse von g in G. Da in einer Gruppe aus $u_1 g = u_2 g$ folgt, dass $u_1 = u_2$ gilt (= Kürzungsregel), haben alle Rechtsnebenklasse die gleiche Anzahl von Elementen. Wir zeigen, dass die Rechtsnebenklassen eine Partition von G bilden, dass also gilt: haben zwei Rechtsnebenklassen nicht-leeren Durchschnitt, so stimmen sie überein: Sei also $Ug_1 \cap Ug_2 \neq \emptyset$, also etwa $u_1 g_1 = u_2 g_2$ mit $u_1, u_2 \in U$, also $g_1 = u_1^{-1} u_2 g_2$. Sei $u \in U$. Es ist

$$ug_1 = uu_1^{-1} u_2 g_2 \in Ug_2,$$

also $Ug_1 \subseteq Ug_2$. Entsprechend sieht man $Ug_2 \subseteq Ug_1$. Ist demnach m die Anzahl der Rechtsnebenklassen von U in G, so gilt $m|U| = |G|$.

2.1.2. Folgerung und Definitionen. *Ist G eine endliche Gruppe der Ordnung n und $g \in G$, so gilt $g^n = 1$.* Die kleinste natürliche Zahl t mit $g^t = 1$ nennt man die *Ordnung* $\mathrm{ord}(g)$ von g. *Ist $ord(g) = t$, so sind die Elemente $1, g, g^2, \ldots, g^{t-1}$ paarweise verschieden und $\{1, g, g^2, \ldots, g^{t-1}\}$ ist eine Untergruppe von G.* Man schreibt $\langle g \rangle = \{1, g, g^2, \ldots, g^{t-1}\}$ und nennt dies die von g *erzeugte* Untergruppe.

Beweis: Sei G endliche Gruppe der Ordnung n und $g \in G$. Sei t die kleinste natürliche Zahl mit $g^t \in \{1, g, \ldots, g^{t-1}\}$ (so ein t existiert, denn G ist nach Voraussetzung endlich). Sei also $g^t = g^i$ mit $0 \leq i < t$. Multiplikation mit g^{-i} liefert $g^{t-i} = 1 \in \{1, g, \ldots, g^{t-1}\}$ und $1 \leq t - i \leq t$. Wegen der Minimalität von t ist $-i = t$, also $i = 0$, also $g^t = 1$. Wir sehen also: t ist die kleinste natürliche Zahl mit $g^t = 1$.

Es ist leicht zu sehen, dass $\{1, g, \ldots, g^{t-1}\}$ eine Untergruppe von G ist. Nach dem Satz von Lagrange ist demnach t ein Teiler von n. Ist also $n = tu$ mit $u \in \mathbb{N}$, so ist $g^n = g^{tu} = (g^t)^u = 1^u = 1$.

Ist $(G,+)$ eine additiv geschrieben Gruppe, so ist die Definition der Ordnung eines Elements folgendermaßen umzuformulieren: Die Ordnung von $g \in (G,+)$ ist die kleinste natürliche Zahl n mit $ng = 0$.

Im Abschnitt 2.3 werden wir die Euler'sche ϕ-Funktion einführen und zeigen, dass gilt:

$$|U(\mathbb{Z}/n,\cdot)| = \phi(n),$$

(man könnte dies natürlich auch als Definition von $\phi(n)$ nehmen).

Insbesondere gilt also: $\phi(p) = p-1$ für jede Primzahl p.

2.1.3. Satz von Euler. *Ist* $\overline{a} \in U(\mathbb{Z}/n,\cdot)$, *so ist* $a^{\phi(n)} \equiv 1 \mod n$.

Dies ist eine direkte Folge des Satzes von Lagrange: $\overline{a}$ ist ein Element der Gruppe $(\mathbb{Z}/n)^*$. Natürlich ist $|(\mathbb{Z}/n)^*| = \phi(n)$. Die Ordnung eines Elements ist **immer** ein Teiler der Gruppenordnung. Das wars.

2.1.4. Spezialfall: der kleine Fermat. *Sei p eine Primzahl. Für* $1 \le a \le p-1$ *gilt* $a^{p-1} \equiv 1 \mod p$.

Natürlich: $\phi(p) = p-1$.

2.1.5. Folgerung. *Sei p eine Primzahl. Für alle a gilt* $a^p \equiv a \mod p$.

Beweis: Ist a nicht durch p teilbar, so ist dies der "kleine Fermat". Ist a durch p teilbar, so ist auch a^p durch p teilbar, also $a^p \equiv 0 \equiv p \mod p$.

2.2. Zyklische Gruppen.

Eine Gruppe C heißt *zyklisch,* wenn es ein Element $g \in C$ gibt, sodass sich alle Elemente von C in der Form g^z mit $z \in \mathbb{Z}$ schreiben lassen; in diesem Fall nennt man g ein *erzeugendes Element* für C; man sagt auch: g erzeugt C und schreibt $G = \langle g \rangle$.

Sei nun $G = (G,\cdot)$ eine Gruppe. *Genau dann ist G zyklisch und von g erzeugt, wenn es keine echte Untergruppe U von G gibt mit $g \in U$.*

Ist $g \in G$. Wir bilden die Folge der Potenzen

$$1, g, g^2, g^3, \ldots$$

Fall 1: die Potenzen sind paarweise verschieden. Dann gilt: *die Zuordnung $(\mathbb{Z},+) \to G$, die durch $z \mapsto g^z$ definiert ist, liefert einen Gruppen-Isomorphismus $(\mathbb{Z},+) \to \langle g \rangle$.*

Fall 2: die Potenzen sind nicht paarweise verschieden (dies gilt insbesondere dann, wenn G eine endliche Gruppe ist). Sei n minimal mit $g^n \in \{1, g, \ldots, g^{n-1}\}$. Wie in 2.1.2 gezeigt, ist dann $g^n = 1$. *Die Zuordnung $(\mathbb{Z},+) \to G$, die durch $z \mapsto g^z$ definiert ist, liefert einen Gruppen-Isomorphismus $(\mathbb{Z}/n,+) \to \langle g \rangle$.*

Wir notieren hier einige ganz elementare Eigenschaften der Ordnung eines Gruppen-Elements (mit direkten Beweisen).

Lemma. (a) *Sei G eine Gruppe. Ist $g^d = 1$, mit $d \geq 1$, so ist die Ordnung von g ein Teiler von d.*

(b) *Das Element $g \in G$ habe die Ordnung n. Ist d ein Teiler von n, so hat g^d die Ordnung $\frac{n}{d}$. Sind die Zahlen t, n teilerfremd, so hat g^t die Ordnung n.*

(c) *Ist $\eta\colon G \to H$ ein Gruppen-Homomorphismus und hat $g \in G$ die Ordnung m, so ist die Ordnung von $\eta(g)$ ein Teiler von m.*

(d) *Sei G eine Gruppe, sei g ein Element von G der Ordnung d und h ein Element von G der Ordnung e. Sind die Zahlen d, e teilerfremd und gilt $gh = hg$, so ist gh ein Element der Ordnung de.*

Beweis: (a) Sei e die Ordnung von g. Sei d' der größte gemeinsame Teiler von d und e. Seien a, b ganze Zahlen mit $d' = ad + be$. Dann ist $g^{d'} = g^{ad+be} = (g^d)^a \cdot (g^e)^b = 1$. Wegen der Minimalität von e ist $e \leq d'$, also $e = d'$. Aber d' ist ein Teiler von d.

(b) Das Element $g \in G$ habe die Ordnung n. Sei d ein Teiler von n. Dann ist $(g^d)^{n/d} = g^n = 1$, also ist die Ordnung von g^d ein Teiler von $\frac{n}{d}$. Sei e die Ordnung von g^d. Dann ist $g^{de} = (g^d)^e = 1$, also ist $n \leq de$. Wegen $e|\frac{n}{d}$ ist aber auch $de \leq n$. Also $n = de$.

Für beliebiges $t \in \mathbb{Z}$ gilt $(g^t)^n = g^{tn} = (g^n)^t = 1$, Also ist die Ordnung e von g^t ein Teiler von n. Seien nun die Zahlen n, t teilerfremd. Wähle eine Bézout'sche Gleichung $1 = an + bt$ mit ganzen Zahlen a, b. Es ist $g^e = (g^{an+bt})^e = g^{ane} \cdot g^{bte} = 1$, also ist $n \leq e$ und demnach $n = e$.

(c) Aus $g^d = 1$ folgt $\eta(g)^d = 1$. Verwende nun (a).

(d) Aus $gh = hg$ folgt $(gh)^n = g^n h^n$ für jedes n. Insbesondere gilt $(gh)^{de} = g^{de}h^{de} = (g^d)^e \cdot (h^e)^d = 1$. Die Ordnung von gh ist also ein Teiler von de. Sei t die Ordnung von gh. Dann ist

$$1 = (gh)^t = (gh)^{te} = g^{te}h^{te} = g^{te}$$

(denn $h^{te} = 1$). Daraus folgt $d|te$, also $d|t$ (weil $(d, e) = 1$). Entsprechend sieht man: $e|t$, und demnach $de|t$, also $t = de$..

2.3. Die Euler'sche ϕ-Funktion.

Wir wollen für beliebige ganze Zahlen (nicht nur für natürliche Zahlen) den Begriff des **Teilers** verwenden: Wir schreiben $d|a$ falls $d \neq 0$ gilt und es $d' \in \mathbb{Z}$ gibt mit $dd' = a$ (wir erlauben also: $5|0$, aber nicht $0|0$).

Sind $a, b \in \mathbb{Z}$, nicht beide Null, so sei (a, b) der **größte gemeinsame Teiler:** also die größte ganze (und demnach natürliche) Zahl d mit $d|a, d|b$. Beispiel: $(10, 15) = 5$, $(10, -15) = 5$, $(-10, 0) = 10$, usw.

Erinnerung: Der Satz von Bézout. Sind $a, b \in \mathbb{Z}$, nicht beide Null, so gibt es $u, v \in \mathbb{Z}$ mit $ua + vb = (a, b)$. Beachte: u, v sind nicht eindeutig bestimmt.

Definition: Mit $\phi(n)$ für $n \in \mathbb{N}$ bezeichnen wir die Anzahl der Zahlen a mit $1 \leq a \leq n$ und $(a, n) = 1$, man nennt ϕ die Euler'sche ϕ-Funktion.

2.3.1. *Es gilt* $|U(\mathbb{Z}/n,\cdot)| = \phi(n)$.

Beweis: Ist $(a,n) = 1$, so gibt es nach Bezout $u, v \in \mathbb{Z}$ mit $ua + vn = 1$, also $\overline{ua} = \overline{1}$. Wir sehen also: $\overline{a}$ ist invertierbar.

Ist umgekehrt $\overline{ca} = \overline{1}$, so ist $1 - ca = tn$ für ein $t \in \mathbb{Z}$, also $1 = ca + tn$. Es ist dann aber (a,n) ein Teiler der rechten Seite, also ein Teiler von 1, also $(a,n) = 1$.

2.3.2. *Es ist* $\sum_{d|n} \phi(d) = n$.

Beweis. Betrachte die Zahlenfolge

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots \frac{n}{n}.$$

Kürze jeweils. Die Nenner, die dann auftreten, sind die Teiler $d|n$. Die Anzahl der Zahlen mit Nenner d ist gerade $\phi(d)$, nämlich die Anzahl der Zahlen b mit $(b,d) = 1$, und zwar wird

$$\frac{a}{n} = \frac{(a,n)b}{(a,n)d} = \frac{b}{d}$$

durch $\frac{b}{d}$ ersetzt mit $(b,d) = 1$.

2.4. Charakterisierung zyklischer Gruppen.

2.4.1. Satz *Sei G eine Gruppe der Ordnung n. Die folgenden Aussagen sind äquivalent:*

(1) *G ist zyklisch.*
(2) *Die Anzahl der Elemente g mit $g^d = 1$ ist d, für jeden Teiler d von n.*
(2′) *Die Anzahl der Elemente g mit $g^d = 1$ ist kleiner oder gleich d, für jeden Teiler d von n. Die Anzahl der Elemente der Ordnung d ist kleiner oder gleich $\phi(d)$, für jeden Teiler d von n.*
(3) *Die Anzahl der Elemente der Ordnung d ist $\phi(d)$, für jeden Teiler d von n.*
(3′) *Die Anzahl der Elemente der Ordnung d ist kleiner oder gleich $\phi(d)$, für jeden Teiler d von n.*

Beweis:

(1) impliziert (3): Wir betrachten hier eine **additive** Gruppe. Wir beginnen mit folgendem Lemma:

Lemma. Die kleinste natürliche Zahl t mit $n|ta$ ist $t = \frac{n}{(a,n)}$, also gilt: *die Ordnung von $\overline{a}$ in $(\mathbb{Z}/n,+)$ ist $\frac{n}{(a,n)}$.*

Beweis: Setze $n = d(a,n)$, und $a = b(a,n)$, mit $(d,b) = 1$. Es ist $n = d(a,n)|da$, also gilt $n|da$ (da $d = n/(a,n)$). Sei nun t gegeben mit $n|ta$. Also

$$d(a,n) = n|ta = tb(a,n),$$

kürzen liefert $d|tb$. Wegen $(d,b) = 1$ folgt $d|t$.

Sei d ein Teiler von n. Sei a eine natürliche Zahl mit $1 \leq a \leq n$ und $(a,n) = \frac{n}{d}$. Dann hat $\overline{a}$ in $(\mathbb{Z}/n, +)$ die Ordnung d. Sei $d' = \frac{n}{d}$ (also $n = dd'$). Jede natürliche Zahl a mit $1 \leq a \leq n$ und $(a,n) = \frac{n}{d} = d'$ ist durch d' teilbar, und das Teilen durch d' liefert eine Bijektion

$$\{a \mid 1 \leq a \leq n \text{ und } (a,n) = \tfrac{n}{d}\} \longrightarrow \{b \mid 1 \leq b \leq d \text{ und } (b,d) = 1\}$$

(beachte: $n/(d') = d$). Die Menge rechts hat nach Definition gerade die Kardinalität $\phi(d)$. Dies zeigt: *Es gibt genau $\phi(d)$ Elemente in $(\mathbb{Z}/n, +)$ der Ordnung d.*

(3) impliziert (1): Es ist $\phi(n) \geq 1$, also gibt es ein Element der Ordnung n.

(3′) impliziert (3): Für $d|n$ sei $M(d)$ die Menge der Elemente von G mit Ordnung d. Da G die disjunkte Vereinigung der Mengen $M(d)$ ist, ist $n = \sum_{d|n} |M(d)|$. Nun besagt (3′), dass jeweils $|M(d)| \leq \phi(d)$ gilt. Nach 2.3.2 ist aber $\sum_{d|n} \phi(d) = n$. Insgesamt sehen wir

$$n = \sum\nolimits_{d|n} |M(d)| \leq \sum\nolimits_{d|n} |\varphi(d)| = n,$$

Da alle auftretenden Zahlen nicht-negativ sind, muss $|M(d)| = \varphi(d)$ für alle $d|n$ gelten.

(3) impliziert (2): $\{g \mid g^d = 1\}$ ist die Menge der $g \in G$, deren Ordnung ein Teiler d' von d ist. Wegen (3) ist die Anzahl dieser Elemente $\phi(d')$ und es ist $d = \sum_{d'|d} \phi(d')$, also gilt:

$$|\{g \mid g^d = 1\}| = \sum_{d'|d} \phi(d') = d,$$

hier verwenden wir wieder 2.3.2.

(2) impliziert (2′) ist trivial.

(2′) impliziert (3′). Es gelte (2′). Wir betrachten einen Teiler d von n. Wegen (2′) ist $|\{g \mid g^d = 1\}| \leq d$. Fall 1: es gibt in G kein g mit Ordnung d, dann gilt (3′) für dieses d. Gibt es aber ein $h \in G$ mit Ordnung d, so gibt es wegen (1) $\Longrightarrow$ (2) in $\langle h \rangle$ genau d Elemente g mit $g^d = d$; in G gibt es nach (2′) höchstens d solche Elemente, also gibt: Alle Elemente $g \in G$ mit $g^d = 1$ gehören zu $\langle h \rangle$. In $\langle h \rangle$ gibt es wegen (1) $\Longrightarrow$ (3) genau $\phi(d)$ Elemente der Ordnung d. Da alle Elemente von G der Ordnung d in $\langle h \rangle$ liegen, gibt es also in G genau $\phi(d)$ Elemente der Ordnung d.

2.4.2. Folgerung. *Ist G eine zyklische Gruppe der Ordnung n und ist d ein Teiler von n, so besitzt G genau eine Untergruppe der Ordnung d, und alle Untergruppen von G sind zyklisch.*

Genauer gilt: *Ist $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung n, und ist $n = de$ mit $d, e \in \mathbb{N}$, so ist $\langle g^e \rangle$ eine zyklische Untergruppe der Ordnung d und dies ist die einzige Untergruppe der Ordnung d.*

Beweis: Mit G besitzt auch jede Untergruppe von G die Eigenschaften (2′) und (3′) des Charakterisierungssatzes, also ist jede Untergruppe wieder zyklisch. Ist $n = de$, so wissen wir, dass die Ordnung von g^e gleich d ist, also ist $U = \langle g^e \rangle$ eine Untergruppe

der Ordnung d. Da U zyklisch der Ordnung d ist, gibt es in U genau $\phi(d)$ Elemente der Ordnung d. Die Anzahl der Elemente von G der Ordnung d ist ebenfalls $\phi(d)$; dies zeigt, dass jedes Element von G mit Ordnung d zu U gehört. Also ist U die einzige zyklische Untergruppe von G der Ordnung d. Da jede Untergruppe von G zyklisch ist, ist U die einzige Untergruppe der Ordnung d.

2.4.3. Folgerung. *Eine zyklische Gruppe G besitzt höchstens ein Element der Ordnung* 2 (und zwar existiert ein derartiges Element genau dann, wenn G endliche Gruppe mit gerader Ordnung ist).

Beweis: Ist G eine unendliche zyklische Gruppe, so hat nur das neutrale Element endliche Ordnung, nämlich Ordnung 1. Sei also G eine endliche zyklische Gruppe, mit Ordnung $|G| = n$. Ist n ungerade, so gibt es kein Element der Ordnung 2, denn die Ordnung eines jeden Elements ist ein Teiler der Gruppen-Ordnung. Ist n gerade, also 2 ein Teiler von $|G|$, so besagt die Aussage (3) des Charakterisierungssatzes: Es gibt genau $\phi(2)$ Elemente der Ordnung 2. Und $\phi(2) = 1$.

2.5. Endliche Untergruppen der multiplikativen Gruppe eines Körpers.

2.5.1. Satz. *Sei K ein Körper. Ist G eine endliche Untergruppe der multiplikativen Gruppe $K^* = (K \setminus \{0\}, \cdot)$ von K, so ist G zyklisch.*

Beweis: Sei $|G| = n$, sei d ein Teiler von n. Wir zeigen: Es gibt in G höchstens d Elemente g mit $g^d = 1$ und wenden den Charakterisierungssatz an (die Implikation $(2') \implies (1)$). Jedes derartige Element g ist Nullstelle des Polynoms $X^d - 1$. Dies ist ein Polynom vom Grad d mit Koeffizienten im Körper K. Ein Polynom vom Grad d mit Koeffizienten in einem Körper K hat in K höchstens d Nullstellen.

2.5.2. Folgerung. *Für jede Primzahl p gilt: Die Gruppe $(\mathbb{Z}/p)^*$ ist zyklisch.*

Beweis: $\mathbb{Z}/p$ ist ein Körper.

2.6. Primitivwurzeln modulo n.

Sei $n \in \mathbb{N}$. Gibt es eine ganze Zahl a, sodass $\overline{a} \in U(\mathbb{Z}/n, \cdot)$ ein erzeugendes Element ist, so nennt man a eine *Primitivwurzel modulo n*. Ist $n = p$ eine Primzahl, so haben wir im letzten Abschnitt gezeigt, dass es eine Primitivwurzel modulo p gibt. Aber es ist gar nicht einfach, zu einer Primzahl p eine Primitivwurzel modulo p zu finden — dafür gibt es Listen, ansonsten hilft nur Probieren.

Es gibt einen Satz von Gauß, der alle natürlichen Zahlen n beschreibt, für die die multiplikative Gruppe $U(\mathbb{Z}/n, \cdot)$ zyklisch ist, für die es also eine Primitivwurzel g modulo n gibt (siehe Ausblick 3).

Sei $U(\mathbb{Z}/n, \cdot)$ zyklisch, sei $U(\mathbb{Z}/n, \cdot) = \langle \overline{g} \rangle$, also g eine Primitivwurzeln modulo n. Die Abbildung

$$\psi \colon C_{\phi(n)} = (\mathbb{Z}/\phi(n), +) \longrightarrow U(\mathbb{Z}/n, \cdot) \qquad \text{mit} \qquad \psi(x) = g^x$$

ist ein Isomorphismus (dies bedeutet, dass man die Elemente von $U(\mathbb{Z}/n,\cdot)$ als Potenzen **eines** Elements g schreibt). Die Umkehrabbildung zu ψ wird mit ind_g bezeichnet, man nennt $\mathrm{ind}_g(y)$ den *Index* von y zur Basis g. Es gelten die folgenden Rechenregeln:

$$\begin{aligned}\mathrm{ind}_g(y_1y_2) &= \mathrm{ind}_g(y_1)+\mathrm{ind}_g(y_2)\\ \mathrm{ind}_g(y^{-1}) &= -\mathrm{ind}_g(y)\\ \mathrm{ind}_g(y^e) &= e\cdot\mathrm{ind}_g(y).\end{aligned}$$

Ist g' ebenfalls eine Primitivwurzel modulo n, so sind die beiden Funktionen ind_g und $\mathrm{ind}_{g'}$ zueinander proportial, es gilt:

$$\mathrm{ind}_g(y) = \mathrm{ind}_g(g')\cdot\mathrm{ind}_{g'}(y).$$

Bemerkung. Diese Regeln entsprechen den Regeln für das Rechnen mit Logarithmen - wir sind hier in einer ganz ähnlichen Situation. Sei $a\in\mathbb{R}_{>0}=\{r\in\mathbb{R}\mid r>0\}$ Die Exponentialabbildungen

$$\exp_a\colon(\mathbb{R},+)\longrightarrow(\mathbb{R}_{>0},\cdot)$$

ist ein Gruppen-Isomorphismus, die Umkehrabbildung wird mit $\log_a$ bezeichnet (also $\log_a(y)$ ist der Logarithmus von y zur Basis a, dies ist definiert für $y\in\mathbb{R}_{>0}$, es ist $\log_a(y)$ die eindeutig bestimmte reelle Zahl mit $a^{\log_a(y)}=y$.)

$$\begin{aligned}\log_a(y_1y_2) &= \log_a(y_1)+\log_a(y_2)\\ \log_a(y^{-1}) &= -\log_a(y)\\ \log_a(y^e) &= e\cdot\log_a(y).\\ \log_a(y) &= \log_a(a')\cdot\log_{a'}(y).\end{aligned}$$

Beispiel. Sei $p=11$. Es ist 2 eine Primitivwurzel modulo 11, und man berechnet leicht die folgende Index-Tabelle:

y	1	2	4	8	5	10	9	7	3	6
$\mathrm{ind}_2(y)$	0	1	2	3	4	5	6	7	8	9

Beispiel-Rechnung. Wir suchen eine Lösung der Gleichung $x^{18}\equiv 9 \mod 11$. Wegen

$$x^{10}\equiv 1 \mod 11$$

(kleiner Fermat) suchen wir also x mit $x^8\equiv 9 \mod 11$. Wir wenden ind_2 an und erhalten

$$8\cdot\mathrm{ind}_2(x)\equiv\mathrm{ind}_2(9) \mod 10.$$

die Tabelle zeigt: $\mathrm{ind}_2(9)=6$. Gesucht ist also $z(=\mathrm{ind}_2(x))$ mit $8\cdot z\equiv 6 \mod 10$, wir müssen uns demnach die Vielfachen von 8 modulo 10 ansehen. Man sieht sofort: $8\cdot 2=16\equiv 8 \mod 10$, also $z=2$. Demnach ist $x=2^2=4$. (Probe: Für $x=4$ ist $x^8=4^8\equiv 9 \mod 11$.)

2.7. Produkte von Halbgruppen und Ringen.

Wir setzen voraus, dass bekannt ist, wie Halbgruppen, Gruppen, Ringe und Körper definiert sind. Ebenfalls wird vorausgesetzt, was man in der Algebra unter einem Homomorphismus versteht (z.B.: ein Ring-Homomorphismus $\eta\colon R \to R'$ ist eine Abbildung, die verträglich mit Addition und Multiplikation ist und für die $\eta(1_R) = 1'_R$ gilt, dabei bedeutet die Verträglichkeit mit der Addition, dass $\eta(r_1 + r_2) = \eta(r_1) + \eta(r_2)$ gilt, usw.) Um zu zeigen, dass ein Ring-Homomorphismus $\eta\colon R \to R'$ injektiv ist, braucht man nur zu verifizieren, dass $\eta(r) = 0$ nur für $r = 0$ gilt. (Denn ist $\eta(r_1) = \eta(r_2)$, so ist $\eta(r_1 - r_2) = 0$. Gilt nun $\eta(r) = 0$ nur für $r = 0$, so sieht man, dass $r_1 - r_2 = 0$ gilt und daher $r_1 = r_2$.)

Sind H, H' zwei Halbgruppen, so wird die Produktmenge $H \times H'$ mit komponentenweiser Verknüpfung eine Halbgruppe, das *Produkt* von H und H' (nach Definition ist also

$$(h_1, h'_1)(h_2, h'_2) = (h_1 h_2, h'_1 h'_2)$$

für $h_1, h_2 \in H$ und $h'_1, h'_2 \in H'$; das Einselement von $H \times H'$ ist $(1_H, 1_{H'})$. (Hier und im Folgenden ist einiges zu verifizieren — dies sollte aber keine Schwierigkeiten bereiten.) Sind H, H' Gruppen, so ist auch $H \times H'$ eine Gruppe; es ist dann $(h, h')^{-1} = (h^{-1}, (h')^{-1})$. Sind H, H' kommutativ, so ist auch $H \times H'$ kommutativ.

Sind R, R' Ringe, so ist wird die Produktmenge $R \times R'$ durch komponentenweise Addition und komponentenweise Multiplikation ein Ring, das *Produkt* von R, R'. Das Element $(1, 1) = (1_R, 1_{R'})$ ist das Einselement $1 = 1_{R\times R'}$ von $R \times R'$. Sind R, R' kommutative Ringe, so ist auch $R \times R'$ kommutativ. Beachte: die Elemente $e = (1, 0)$ und $e' = (0, 1)$ sind idempotent (ein Element e eines Rings heißt idempotent, wenn $e^2 = e$ gilt), es gilt $ee' = 0 = e'e$ und $e + e' = 1$.

Warnung. Sind K, K' Körper, so ist $K \times K'$ ein kommutativer Ring, aber kein Körper. Es gilt nämlich $(1, 0)(0, 1) = (0, 0)$, daher sind die Elemente $(1, 0)$ und $(0, 1)$ von Null verschiedene Nullteiler. In einem Körper ist nur das Nullelement ein Nullteiler!

Ist R ein Ring, so bezeichnen wir mit $U(R)$ die Menge der (bezüglichder Multiplikation) invertierbaren Elemente, dies ist eine Gruppe. Man nennt sie die *Einheitengruppe* des Rings R. Es gilt:

$$U(R \times R') = U(R) \times U(R')$$

(links und rechts stehen Teilmengen von $R \times R'$; behauptet wird also die Gleichheit dieser Teilmengen, zusätzlich aber auch, dass diese eine Gleichheit von Gruppen ist: dies gilt, weil sowohl im Produkt-Ring $R\times R'$ als auch in der Produkt-Gruppe $U(R)\times U(R')$ die Multiplikation komponentenweise definiert ist.

2.8. Der Chinesische Restsatz.

2.8.1. *Für beliebige natürliche Zahlen m, n gilt: Die kanonische Abbildung*

$$\eta\colon \mathbb{Z}/(mn) \to \mathbb{Z}/m \quad \textit{mit} \quad \eta(\overline{u}) = \overline{u}$$

ist ein surjektiver Ring-Homomorphismus. (Achtung: die Bezeichnung $\overline{u}$ steht hier für zwei ganz verschiedene Elemente, nämlich für Elemente, die man genauer mit $\overline{u}^{(nm)}, \overline{u}^{(n)}$ bezeichnen sollte...).

Beweis: Zu zeigen ist eigentlich gar nichts. Man muss sich nur überlegen, was zu zeigen ist, und dass all dies offensichtlich ist. Wichtig ist allerdings, dass man sich klar macht, dass die angegebene Abbildung "wohldefiniert" ist: sind $u_1, u_2 \in \mathbb{Z}$ mit $\overline{u_1}^{(nm)} = \overline{u_2}^{(nm)}$, so gilt auch $\overline{u_1}^{(m)} = \overline{u_2}^{(m)}$ (denn wenn nm ein Teiler von $u_1 - u_2$, so ist auch m ein Teiler von $u_1 - u_2$).

2.8.2. Satz. *Seien m, n teilerfremde natürliche Zahlen. Die kanonische Abbildung $\mathbb{Z}/(mn) \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ mit $\overline{u} \mapsto (\overline{u}, \overline{u})$ ist ein Isomorphismus von Ringen.* (Nochmals: die Bezeichnung $\overline{u}$ steht auch hier für drei verschiedene Elemente, nämlich für Elemente, die man genauer mit $\overline{u}^{(nm)}, \overline{u}^{(m)}, \overline{u}^{(n)}$ bezeichnen sollte...).

Beweis: Gar nicht offensichtlich ist, dass die Abbildung surjektiv ist. Sie ist aber offensichtlich injektiv: Denn sei $u \in \mathbb{Z}$ mit $(\overline{u}, \overline{u}) = 0 = (0, 0)$. Es gilt also $\overline{u} = 0$ in $\mathbb{Z}/m$ wie auch in $\mathbb{Z}/n$. Demnach ist u durch m teilbar und durch n teilbar. Da m, n teilerfremd sind, ist u auch durch mn teilbar, also gilt auch $\overline{u} = 0$ in $\mathbb{Z}/(mn)$. (Wir verwenden hier, dass man für die Injektivität eines Gruppen-Homomorphismus nur zeigen muss, dass der Kern einelementig ist; hier wird dies auf die additiven Gruppen angewandt.)

Nun ist aber $\mathbb{Z}/(mn)$ eine Menge der Kardinalität mn, und auch $(\mathbb{Z}/m)\times(\mathbb{Z}/n)$ hat die Kardinalität mn. Demnach ist eine injektive Abbildung $\mathbb{Z}/(mn) \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ auch surjektiv.

Zweiter Beweis der Surjektivität (**konstruktiv**, deshalb auf jeden Fall von Interesse): Wir konstruieren explizit Urbilder. Wir beginnen folgendermaßen: Da m, n teilerfremd sind, gibt es nach Bézout Zahlen a, b mit

$$an + bm = 1.$$

Sei nun $(\overline{u}, \overline{v})$ in $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ gegeben. Setze

$$x = anu + bmv.$$

Es gilt

$$\begin{aligned} x = anu + bmv \equiv anu \equiv anu + bmu = (an + bm)u = 1 \cdot u = u \mod m, \\ x = amu + bmv \equiv bmv \equiv anv + bmv = (an + bm)v = 1 \cdot v = v \mod n. \end{aligned}$$

also ist $(\overline{x}, \overline{x}) = (\overline{u}, \overline{v})$, die Zuordnung ist also surjektiv.

Zusatz: Die Linearkombination $an + bm = 1$ ist gerade so gewählt, dass die Restklasse von an modulo m das Einselement von $\mathbb{Z}/m$ liefert (und an ein Vielfaches von n also Null in $\mathbb{Z}/n$ ist), während die Restklasse von bm modulo n das Einselement von $\mathbb{Z}/n$ liefert (und bm ein Vielfaches von m, also Null in $\mathbb{Z}/m$ ist). Unter der kanonischen Abbildung $\mathbb{Z} \to (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ wird also an auf das Idempotent $(1, 0)$, und bm auf das Idempotent $(0, 1)$ abgebildet.

$$\begin{array}{ccc} \mathbb{Z}/mn & \longrightarrow & \mathbb{Z}/m \times \mathbb{Z}/n \\ an & \longmapsto & (1,0) \\ bm & \longmapsto & (0,1) \\ anu + bmv & \longmapsto & (\overline{u}, \overline{v}) \end{array}$$

2.8.3. Allgemeiner Fall. *Seien $n_1, \ldots, n_t$ natürliche Zahlen, die paarweise teilerfremd sind. Dann ist die kanonische Abbildung*

$$\mathbb{Z}/(n_1 \cdots n_t) \to (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_t)$$

ein Ring-Isomorphismus (insbesondere also bijektiv).

2.8.4. Umformulierung der Bijektivität. *Seien $n_1, \ldots, n_t$ natürliche Zahlen, die paarweise teilerfremd sind. Seien $u_1, \ldots, u_t \in \mathbb{Z}$. Dann gibt es eine Zahl $x \in \mathbb{Z}$ mit*

$$x \equiv u_i \mod n_i \qquad \textit{für} \qquad 1 \leq i \leq t,$$

und die Menge der Zahlen x mit dieser Eigenschaft bildet eine Restklasse modulo $n_1 \cdots n_t$.

Beweis mit Induktion. Oder auch explizit: Setze $m_i = n/n_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_t$. Dann gilt $(m_i, n_i) = 1$. Nach Bézout finden wir $a_i, b_i \in \mathbb{Z}$ mit

$$a_i m_i + b_i n_i = 1.$$

Eine gesuchte Lösung x ist

$$\boxed{x = \sum\nolimits_i a_i m_i u_i}$$

Unter der kanonischen Abbildung $\mathbb{Z} \to (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_t)$ wird $a_i m_i$ auf das Element $(0, \ldots, 0, 1, 0, \ldots, 0)$ mit der Eins an der i-ten Stelle abgebildet (denn $a_i m_i$ ist ein Vielfaches von n_j für $j \neq i$, andererseits ist $a_i m_i = 1 - b_i n_i \equiv 1 \mod n_i$).

$$\begin{array}{ccc} \mathbb{Z}/n_1 \cdots n_i & \longrightarrow & \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t \\ am_i & \longmapsto & (0, \ldots, 0, 1, 0, \ldots, 0) \\ \sum a_i m_i u_i & \longmapsto & (\overline{u}_1, \ldots, \overline{u}_t) \end{array}$$

Beispiel. Betrachte das Gleichungssystem

$$x \equiv 2 \mod 9, \quad x \equiv 1 \mod 5, \quad x \equiv 3 \mod 7.$$

Hier ist also

$$n_1 = 9 \qquad n_2 = 5 \qquad n_3 = 7$$

$$m_1 = 5 \cdot 7 = 35 \qquad m_2 = 9 \cdot 7 = 63 \qquad m_3 = 9 \cdot 5 = 45.$$

Als erstes suchen wir also Lösungen der drei Bézout'schen Gleichungen

$$35a_1 + 9b_1 = 1, \quad 63a_2 + 5b_2 = 1, \quad 45a_3 + 7b_3 = 1.$$

Zum Beispiel können wir nehmen:

$$\begin{aligned} a_1 &= -1 & b_1 &= 4 \\ a_2 &= 2 & b_2 &= -25 \\ a_3 &= -2 & b_3 &= 13 \end{aligned}$$

und demnach

$$a_1 m_1 = -1 \cdot 35 = -35, \quad a_2 m_2 = 2 \cdot 63 = 126, \quad a_3 m_3 = -2 \cdot 45 = -90.$$

Dies sind also die benötigten Zahlen, mit denen wir **jedes** Gleichungssystem der Form

$$x \equiv u_1 \mod 9, \quad x \equiv u_2 \mod 5, \quad x \equiv u_3 \mod 7.$$

lösen können.

In unserem Beispiel ist $u_1 = 2,\ u_2 = 1,\ u_3 = 3$. Also erhalten wir als Lösung

$$x = \sum\nolimits_i a_i m_i u_i = (-35) \cdot 2 + 126 \cdot 1 + (-90) \cdot 3 = -214.$$

Statt -214 nehmen wir lieber die positive Zahl $-214 + 315 = 101$. Offensichtlich ist $x = 101$ wirklich eine Lösung unseres Gleichungssystems.

Zusammenfassung. Der Chinesische Restsatz besagt, dass für jede natürliche Zahl n mit Primfaktorzerlegung $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$ die kanonische Abbildung $\eta(\overline{a}) = (\overline{a}, \ldots, \overline{a})$ ein Ring-Isomorphismus ist:

$$\eta\colon \mathbb{Z}/n \longrightarrow (\mathbb{Z}/p_1^{e_1}) \times \cdots \times (\mathbb{Z}/p_t^{e_t}).$$

Dies besagt, dass man sich beim Rechnen mit Kongruenzen modulo n immer auf den Fall zurückziehen kann, wo n eine Primzahlpotenz ist. Insbesondere liefert η einen Isomorphismus der Einheitengruppen:

$$U(\mathbb{Z}/n) \longrightarrow U(\mathbb{Z}/p_1^{e_1}) \times \cdots \times U(\mathbb{Z}/p_t^{e_t}).$$

2.9. Die Multiplikativität der Euler'schen ϕ-Funktion.

2.9.1. Satz. *Sind m, n teilerfremde natürliche Zahlen, so ist $\phi(mn) = \phi(m)\phi(n)$.*

Beweis: Nach dem chinesischen Restsatz ist $\mathbb{Z}/mn$ zu $\mathbb{Z}/m \times \mathbb{Z}/n$ isomorph, also ust $U(\mathbb{Z}/mn)$ zu $U(\mathbb{Z}/m) \times U(\mathbb{Z}/n)$ isomorph. Es ist $\phi(mn) = |U(\mathbb{Z}/mn)|, \phi(m) = |U(\mathbb{Z}/m)|, \phi(n) = |U(\mathbb{Z}/n)|$, also

$$\phi(mn) = |U(\mathbb{Z}/mn)| = |U(\mathbb{Z}/m) \times U(\mathbb{Z}/n)| = |U(\mathbb{Z}/m)| \cdot |U(\mathbb{Z}/n)| = \phi(m)\phi(n).$$

2.9.2. *Ist p eine Primzahl und $e \in \mathbb{N}$, so gilt*

$$\boxed{\phi(p^e) = p^{e-1}(p-1) = p^e(1 - \tfrac{1}{p})}$$

Beweis: Die Anzahl der durch p teilbaren Zahlen kleiner oder gleich p^e ist p^{e-1}, also ist die Anzahl der a mit $1 \leq a \leq p^e$ mit $(a, p^e) = 1$ gleich $p^e - p^{e-1} = p^{e-1}(p-1)$.

2.9.3. Folgerung. *Ist $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ mit Primzahlen $p_1 < p_2 < \cdots < p_t$ und $e_1, \ldots, e_t \in \mathbb{N}$, so ist*

$$\boxed{\phi(n) = \prod_i \phi(p_i^{e_i}) = \prod_i p_i^{e_i - 1}(p_i - 1) = n \prod_{p|n} (1 - \tfrac{1}{p}).}$$

Im Teil 3 werden wir ganz allgemein Funtkionen $f\colon \mathbb{N} \to \mathbb{R}$ (oder sogar $f\colon \mathbb{N} \to \mathbb{C}$) betrachten, man nennt derartige Funktionen *zahelntheoretische Funktionen.* In der Zahlentheorie nennt man eine zahlentheoretische Funktion f *multiplikativ*, falls f nicht die Nullfunktion ist und falls gilt: Sind n, n' teilerfremd, so ist $f(nn') = f(n)f(n')$. (Insbesondere gilt dann $f(1) = 1$; denn wäre $f(1) = 0$, so wäre f wegen $f(1 \cdot n) = f(1)f(n)$ die Nullfunktion, dies ist ausgeschlossen; aus $f(1) = f(1 \cdot 1) = f(1)f(1)$ und $f(1) \neq 0$ folgt aber $f(1) = 1$.) Der Satz 2.9.1 besagt also gerade: *die Eulersche ϕ-Funktion ist multiplikativ.*

Warnung: In der Algebra würde man eine Funktion nur dann "multiplikativ" nennen, wenn die Regel $f(nn') = f(n)f(n')$ für **alle** n, n' gilt, nicht nur für teilerfremde Paare. In der Zahlentheorie heißt eine zahlentheoretische Funktion *stark multiplikativ* oder "vollständig multiplikativ", wenn $f(nn') = f(n)f(n')$ für alle $n, n' \in \mathbb{N}$ gilt. Beachte: *Die Euler'sche ϕ-Funktion ist nicht stark multiplikativ,* denn es gilt zum Beispiel $\phi(4) = 2$, aber $\phi(2) = 1$; ganz allgemein gilt $\phi(p^2) = (p-1)p$, und $\phi(p) = p - 1$.

Offensichtlich gilt für f multiplikativ: Kennt man die Werte $f(p^e)$, für alle Primzahlen p und alle natürlichen Zahlen e, so kennt man f, denn für $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$ gilt

$$f(p_1^{e_1} \cdots p_t^{e_t}) = f(p_1^{e_1}) \cdots f(p_t^{e_t}).$$

Umgekehrt kann man eine multiplikative Funktion g dadurch definieren, dass man beliebige Werte $g(p^e)$ (für p Primzahl, $e \in \mathbb{N}$) wählt, und diese Abbildung "multiplikativ fortsetzt":

$$g(p_1^{e_1} \cdots p_t^{e_t}) = g(p_1^{e_1}) \cdots g(p_t^{e_t})$$

(für paarweise verschiedene Primzahlen $p_1, \ldots, p_t$ und alle $e_i \in \mathbb{N}$).

2.10. RSA

Hier ist nun auf eine Anwendung hinzuweisen, die im täglichen Leben heute eine wichtige Rolle spielt: Das RSA-Verfahren zur Verschlüsselung von Nachrichten. Dabei sei an den Zahlentheoretiker Hardy erinnert, der noch 1941 formulierte, dass die Ergebnisse der Zahlentheorie zwar ihren ästhetischen Reiz haben, aber kein derartiges Ergebnis *has made, or is likely to make, for good or ill, the least difference to the amenity of the world* (amenity = Annehmlichkeit).

Beim Verschlüsseln von Nachrichten handelt es sich darum, eine Nachricht von A (Alice) nach B (Bob) zu schicken, die von niemandem sonst entziffert werden kann. sie wird von A verschlüsselt, von B entschlüsselt, die verschlüsselte Nachricht kann von allen eingesehen werden, nur Bob ist allerdings in der Lage, die Nachricht zu entschlüsseln. Auch der Schlüssel zum Verschlüsseln ist öffentlich zugänglich (*public key*), der Schlüssel zum Entschlüsseln (*private key*) natürlich nicht - ihn kennt nur Bob. Das RSA-Verfahren wurde von **Rivest, Shamir und Adleman** 1978 vorgestellt und wird gegenwärtig in vielen Situationen eingesetzt. Der mathematische Kern ist folgende Variante des Satzes von Euler-Fermat:

2.10.1. Satz. *Sei m eine quadratfreie natürliche Zahl. Sei f eine natürliche Zahl mit $f \equiv 1 \mod \phi(m)$. Dann ist $a^f \equiv a \mod m$ für alle ganzen Zahlen a.*

Beweis: Sei p ein Primteiler von m. Wir zeigen: es ist $a^f \equiv a \mod p$ für alle ganzen Zahlen a. Ist p ein Teiler von a ist, so ist p auch ein Teiler von a^f, also $a^f \equiv 0 \equiv a \mod p$. Ist p kein Teiler von a, so sind die Zahlen a, p teilerfremd, nach dem kleinen Fermat gilt also $a^{p-1} \equiv 1 \mod p$. Da p ein Teiler von m ist, ist $p-1$ ein Teiler von $\phi(m)$, also auch von $t\phi(m)$, etwa $t\phi(m) = (p-1)x$. Wegen $f \equiv 1 \mod \phi(m)$ gibt es y mit $f = 1 + \phi(m)y = 1 + (p-1)xy$. Also $a^f = a^{1+(p-1)xy} = a \cdot (a^{(p-1)})^{xy} \equiv a \cdot 1^{xy} = a \mod p$.

Nun ist m das Produkt seiner Primteiler ist, und diese sind paarweise verschieden, etwa $m = p_1 \cdots p_t$ mit paarweise verschiedenen Primzahlen p_i. Wie wir gesehen haben, gilt $a^f \equiv a \mod p_i$ für jedes i, es ist also jedes p_i ein Teiler von $a^f - a$. Da die p_i paarweise teilerfremd sind, folgt, dass m ein Teiler von $a^f - a$ ist.

2.10.2. Folgerung. *Sei m eine quadratfreie natürliche Zahl. Seien e, d natürliche Zahlen mit $de \equiv 1 \mod \phi(m)$, so liefert die Zuordnung $a \mapsto a^e$ eine bijektive Abbildung $\mathbb{Z}/m \longrightarrow \mathbb{Z}/m$, mit inverser Zuordnung $a \mapsto a^d$.*

Beweis: Wegen $(\overline{a}^e)^d = \overline{a}$ sehen wir, dass die Zuordnung $a \mapsto a^e$ injektiv ist. Als injektive Abbildung einer m-elementigen Menge in sich ist diese Zuordnung bijektiv. Und natürlich folgt aus $(\overline{a}^e)^d = \overline{a}$, dass $a \mapsto a^d$ die inverse Zuordnung ist.

Beachte: Der Satz ist im Fall dass $m = p$ eine Primzahl ist, gerade die übliche zweite Formulierung des kleinen Fermat: $a^p \equiv a \mod p$ für alle ganzen Zahlen a, denn $\phi(p) = p - 1$, also ist $p = 1 + (p - 1) \equiv 1 \mod \phi(p)$.

Hier die Beschreibung des RSA-Verfahrens. Bob wählt paarweise verschiedene Primzahlen $p_1, \ldots, p_t$ (üblicherweise große Primzahlen, und $t = 2$) und setzt $m = p_1 \cdots p_t$. Dann ist $\phi(m) = (p_1 - 1) \cdots (p_t - 1)$. Weiter wählt er eine zu $\phi(m)$ teilerfremde Zahl e (meist eine Zahl der Form $2^r + 1$, damit das e-fache Potenzieren so einfach wie möglich ist) und berechnet eine Bézout-Gleichung $de + t\phi(m) = 1$ mit $d \in \mathbb{N}$. Der öffentliche Schlüssel ist das Zahlenpaar $[m, e]$, sein privater Schlüssel ist das Zahlenpaar $[m, d]$. Verschlüsselt wird so: man ersetzt $0 \leq a < m$ durch $0 \leq b < m$ mit $b \equiv a^e \mod m$, entschlüsselt wird entsprechend durch d-faches Potenzieren.

Beispiel (wegen der kleinen Zahlen natürlich unrealististisch): Wir nehmen die Primzahlen $p = 11, q = 13$, also $m = 143$ und $\phi(m) = (p - 1)(q - 1) = 120$. Sei $e = 2^4 + 1 = 17$. Eine Bézout'sche Gleichung lautet $1 = 1 \cdot 120 - 7 \cdot 17$, wir wollen aber $d > 0$, also

$$1 = (1 - 17) \cdot 120 + (-7 + 120) \cdot 17 = -16 \cdot 120 + 113 \cdot 17 (= -1920 + 1921).$$

der öffentliche Schlüssel ist also das Paar $[143, 17]$, Bob's privater Schlüssel ist $[143, 113]$. Will Alice die Nachricht $a = 7$ übermitteln, so verschlüsselt sie sie: sie bildet $a^{17} \equiv 50 \mod 143$, also sendet sie $b = 50$. Bob entschlüsselt die Nachricht: $b^{113} \equiv 7 \mod 143$.

Statt $e = 17$ hätte man bei Vorgabe von $m = 143$ jede Zahl $1 \leq e \leq 120$ nehmen können, die nicht durch 2, 3 oder 5 teilbar ist, also $e = 7, 11, 13, 17, 19, \ldots$. Es ist also $[143, 11]$ ein möglicher öffentlicher Schlüssel; wegen $11 \cdot 11 = 121 = 1 + 120$ ist der zugehörige private Schlüssel ebenfalls $[143, 11]$.

2.11. Kongruenzen modulo einer Primzahl p.

Der Satz 2.5.2 besagt, dass die multiplikative Gruppe $\mathbb{F}_p^*$ des Körpers $\mathbb{F}_p = \mathbb{Z}/p$ zyklisch ist, dass es also eine Primitivwurzel modulo p gibt. Nach 2.4.3 folgt daraus, dass es es für $p \geq 3$ in $\mathbb{F}_p^*$ genau ein Element der Ordnung 2 gibt, dass es also genau eine Restklasse g mit $g^2 = g \neq 1$ gibt. Es ist $(-1)^2 = 1$ und für $p \geq 3$ ist $-1 \not\equiv 1 \mod p$, also gilt:

2.11.1. *Für $p \geq 3$ ist die Restklasse von -1 das einzige Element in $\mathbb{F}_p^*$ mit Ordnung 2.*

2.11.2. Satz von Wilson. *Ist p eine Primzahl, so ist $(p-1)! \equiv -1 \mod p$.*

Beweis: Für $p = 2$ ist $(p-1)! = 1! = 1$ und es ist $1 \equiv -1 \mod 2$. Sei nun p eine ungerade Primzahl. Die Gruppe $G = (\mathbb{Z}/p)^*$ ist zyklisch und hat gerade Ordnung, die linke Seite der behaupteten Kongruenz ist gerade das Produkt über alle Element von G. In einer zyklischen Gruppe gerader Ordnung gibt es genau ein Element der Ordnung 2. Sei also $g_0 \in G$ das Element der Ordnung 2 (es ist dies die Restklasse $\overline{-1}$). Wir nennen g, h in G äquivalent, falls $g = h$ oder $g = h^{-1}$. Es gibt zwei Äquivalenzklassen, die jeweils nur aus einem Element bestehen, nämlich die Äquivalenzklassen zu 1 und zu g_0. Alle anderen Äquivalenzklassen bestehen aus genau 2 Elementen: einem Element g und seinem Inversen g^{-1}. Bilden wir das Produkt über alle Elemente von G, und zwar, indem wir jeweils diese Äquivalenzklassen betrachten, so ist das Produkt für jede zweielementige Äquivalenzklasse gleich 1. Die beiden einelementigen Äquivalenzklassen liefern zusätzlich einen Faktor 1 und einen Faktor g_0. Insgesamt ist das Produkt also gleich g_0.

> Zur Illustration des Beweises lohnt es sich, ein Beispiel zu betrachten, etwa $p = 11$. Die Äquivalenzklassen sind $\{\overline{1}\}, \{\overline{2}, \overline{6}\}, \{\overline{3}, \overline{4}\}, \{\overline{5}, \overline{9}\}, \{\overline{7}, \overline{8}\}, \{\overline{10}\}$, denn $2 \cdot 6 = 12 \equiv 1 \mod 11$, usw. Also
>
> $$\begin{aligned}(p-1)! = 10! &= 1 \cdot 2 \cdot \cdots \cdot 10 \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) = -1 \mod 11.\end{aligned}$$

Umformulierung: Satz von Leibniz. *Ist p Primzahl, so ist $(p-2)! \equiv 1 \mod p$.*

Beweis: Die beiden Aussagen Wilson - Leibniz sind offensichtlich äquivalent! Im Fall $p = 2$ sollte man sich daran erinnern, dass nach Definition $0! = 1$ gilt.

2.11.3. Satz. *Sei $p \geq 3$ Primzahl. Dann gilt*

$$\left(\tfrac{p-1}{2}!\right)^2 \equiv \begin{cases} -1 \mod p & \textit{falls} \quad p \equiv 1 \mod 4, \\ 1 \mod p & \textit{falls} \quad p \equiv 3 \mod 4 \end{cases}$$

Beweis: Da p ungerade ist, ist $p-1$ gerade, also können wir $s = \frac{p-1}{2}!$ betrachten. Es ist

$$p - \frac{p-1}{2} = \frac{2p-p+1}{2} = \frac{p+1}{2} = \frac{p-1}{2} + 1.$$

Ist $p \equiv 1 \mod p$, so ist $\frac{p-1}{2}$ gerade, also ist auch

$$\begin{aligned} s = 1 \cdot 2 \cdot \cdots \cdot \tfrac{p-1}{2} &= (-1) \cdot (-2) \cdot \cdots \cdot (-\tfrac{p-1}{2}) \\ &\equiv (p-1)(p-2) \cdots (p - \tfrac{p-1}{2}) \mod p, \end{aligned}$$

und demnach $s^2 \equiv (p-1)! \equiv -1 \mod p$ nach dem Satz von Wilson.

Ist dagegen $p \equiv 3 \mod p$, so ist $\frac{p-1}{2}$ ungerade, also

$$s = -(-1) \cdot (-2) \cdot \cdots \cdot (-\tfrac{p-1}{2}) \equiv -(p-1)(p-2) \cdots (p - \tfrac{p-1}{2}) \mod p,$$

so ist $s(-s) \equiv (p-1)! \equiv -1 \mod p$ nach dem Satz von Wilson, also $s^2 \equiv 1 \mod p$.

2.11.4. Quadratische Reste und Nichtreste modulo p.

Sei p eine Primzahl, sei $a \in \mathbb{Z}$ nicht durch p teilbar. Man nennt a einen *quadratischen Rest modulo* p, falls es $b \in \mathbb{Z}$ gibt mit $b^2 \equiv a \mod p$ (natürlich ist dann auch b nicht durch p teilbar), falls also die Restklasse $\overline{a}$ in $\mathbb{F}_p^* = (\mathbb{Z}/p)^*$ ein Quadrat ist. Gibt es kein derartiges b, so nennt man a *quadratischen Nichtrest*.

Die Gruppe $\mathbb{F}_2^*$ besteht aus einem einzigen Element, es ist also jede ungerade Zahl ein quadratischer Rest modulo 2, das ist uninteressant. Wir betrachten daher nur die Primzahlen $p \geq 3$. Für $p \geq 3$ ist $p-1$ gerade, also $\frac{p-1}{2}$ eine natürliche Zahl. Sei $a \in \mathbb{Z}$ nicht durch p teilbar. Bilden wir $a^{\frac{p-1}{2}}$ so liefert der kleine Fermat:

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

also ist $a^{\frac{p-1}{2}}$ entweder zu 1 oder zu -1 kongruent (modulo p). Es gilt nun:

Satz (Euler-Kriterium). *Sei $p \geq 3$ Primzahl, sei $1 \leq a < p$. Es ist*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \mod p & \text{falls } a \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1 \mod p & \text{falls } a \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Also: *Genau dann ist a ein Quadrat in $(\mathbb{Z}/p)^*$, wenn $a^{(p-1)/2} \equiv 1 \mod p$ gilt.*

Bemerkung. Das hier notierte Ergebnis sollte jeden überraschen! Es besagt: Um festzustellen, dass a ein quadratischer Rest ist, also sich als Potenz $a \equiv b^p \mod p$ schreiben lässt, muss man eine Potenz von a anschauen...

Beweis: Ist $a \equiv b^2 \mod p$, so ist $a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \mod p$ (kleiner Fermat).

Umgekehrt setzen wir nun voraus: $a^{(p-1)/2} \equiv 1 \mod p$. Wir brauchen die Existenz einer Primitivwurzel g modulo p. Da g Primitivwurzel modulo p ist und p kein Teiler von a ist, gibt es ein $j \in \mathbb{N}$ mit $g^j \equiv a \mod p$. Es ist $(g^j)^{(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \mod p$, also ist $p-1$ ein Teiler von $j \cdot \frac{p-1}{2}$ (da g Primitivwurzel modulo p ist, hat g in $\mathbb{F}_p^*$ die Ordnung $p-1$; aus $g^m \equiv 1 \mod p$ folgt demnach, dass $p-1$ ein Teiler von m ist). Dies besagt aber, dass $\frac{j}{2}$ ganzzahlig ist. Setzen wir $b = g^{j/2}$, so sehen wir: $b^2 = (g^{j/2})^2 = g^j \equiv a \mod p$, also ist a ein Quadrat modulo p.

Legendre hat die folgende Notation eingeführt (das sogenannte *Legendre-Symbol*): Sei p eine Primzahl und $a \in \mathbb{N}$.

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

Natürlich gilt: Ist $a \equiv a' \mod p$, so ist $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.

Im Laufe der Vorlesung werden wir uns mehrfach damit beschäftigen, wie man $\left(\frac{a}{p}\right)$ berechnet und welche Bedeutung das Legendre-Symbol hat!

Umformulierung des Euler-Kriteriums. *Sei p eine Primzahl und $(a,p) = 1$. Dann ist*

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

Beweis: Für $p = 2$ ist nichts zu zeigen. Sei also $p \geq 3$. Ist a quadratischer Rest modulo p, so ist $a^{(p-1)/2} \equiv 1 \mod p$, nach 2.11.4. Nach Definition ist $\left(\frac{a}{p}\right) = 1$. Ist a quadratischer Nichtrest, so ist $a^{(p-1)/2} \equiv -1 \mod p$, nach 2.11.4. Nach Definition ist $\left(\frac{a}{p}\right) = -1$.

Beispiel: $a = -1$**.** *Ist $p \equiv 1 \mod 4$, so ist -1 quadratischer Rest modulo p, ist dagegen $p \equiv 3 \mod 4$, so ist -1 kein quadratischer Rest modulo p.*

Beweis: Ist $p \equiv 1 \mod 4$, so besagt 2.11.3, dass -1 das Quadrat von $\frac{p-1}{2}$ ist. Sei nun $p \equiv 3 \mod 4$. Angenommen, -1 ist quadratischer Rest modulo p. Nach 2.11.4 gilt $(-1)^{\frac{p-1}{2}} \equiv 1 \mod p$. Wegen $p \equiv 3 \mod 4$ ist $\frac{p-1}{2}$ ungerade, und demnach $(-1)^{\frac{p-1}{2}} = -1$. Aber $-1 \equiv 1 \mod p$ ist unmöglich (für $p \geq 3$). Dieser Widerspruch zeigt, dass -1 quadratischer Nichtrest modulo p ist.

Gruppentheoretische Umformulierung. Ist $p \geq 3$ eine Primzahl, so ist p ungerade, also $p-1$ gerade, also $p-1 \equiv 1 \mod 4$ or $p-1 \equiv 3 \mod 4$. Faktorisieren wir $p-1 = 2^t m$ mit m ungerade, so ist im ersten Fall $t \geq 2$, im zweiten Fall $t = 1$. Dies ist ein wesentlicher Unterschied!

Betrachten wir die zyklische Gruppe $\mathbb{F}_p^*$. Sie ist von der Form $C_{2^t} \times C_m$, dabei entspricht die Restklasse $\overline{-1} \in \mathbb{F}_p^*$ dem Element der Form $(g,1)$, wobei g das einzige

Element in C_{2^t} mit Ordnung 2 ist. Ist $t \geq 2$, so gibt es $h \in C_{2^t}$ mit $h^2 = g$ (das heißt: -1 ist ein quadratischer Rest modulo p). Ist $t = 1$, so gibt es kein derartiges Element, also ist -1 quadratischer Nichtrest modulo p.

2.11.5. Starke Multiplikativität von $\left(\frac{-}{p}\right)$: *Es ist* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Beweis: Ist a oder b durch p teilbar, so ist auch ab durch p teilbar, also ist $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 0 = \left(\frac{ab}{p}\right)$. Seien also a, b beide zu p teilerfremd. Es ist

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

Aus $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \mod p$ folgt aber $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$, denn p ist ungerade.

2.11.6. Primzahl-Tests. Wir haben gesehen: Ist p eine Primzahl, so gilt
(a) $(p-1)! \equiv -1 \mod p$. (Satz von Wilson)
(b) $a^p \equiv a \mod p$ für jedes a. (Kleiner Fermat)
(c) $2^p \equiv 2 \mod p$ (Spezialfall des kleinen Fermat)
(d) $a^p \equiv a \mod p$ für jedes a mit $(a, n) = 1$. (Euler)

Es gilt die Umkehrung für den Satz von Wilson (a):

Lemma. *Ist $n > 1$ und $(n-1)! \equiv -1 \mod n$, so ist n eine Primzahl.*

Beweis: Sei also $n > 1$ und $(n-1)! \equiv -1 \mod n$, also n ein Teiler von $(n-1)!+1$. Ist $1 \leq d < n$, so ist d Teiler von $(n-1)!$. Ist d auch ein Teiler von n, so auch von $(n-1)!+1$, also von 1, und demnach $d = 1$.

Die Aussage (b) (und erst recht nicht die schwächeren Aussagen (b) und (c)) implizieren dagegen nicht, dass p eine Primzahl ist! Aber man kann sie natürlich dazu verwenden, um zu zeigen, dass eine gegebene Zahl **keine** Primzahl ist.

Beispiel. Die (Fermat-)Zahl $m = F_6 = 2^{64} + 1$ ist keine Primzahl, denn man kann zeigen: $3^{m-1} \neq 1 \mod m$. Beachte, dass man auf diese Weise zeigt, dass m echte Primteiler besitzt, ohne dass man ohne weiteres einen solchen angeben kann.

2.11.7. Pseudo-Primzahlen, Carmichael-Zahlen. Man nennt eine Zahl n eine *Pseudo-Primzahl* zur Basis a, falls die folgenden Bedingungen erfüllt sind: Es ist $n > 1$, zweitens $(a, n) = 1$, und drittens $a^n \equiv a \mod n$, aber n ist keine Primzahl. Pseudo-Primzahlen zur Basis 2 heißen auch *Poulet-Zahlen* (für eine solche Zahl n gilt also $2^{n-1} \equiv 1 \mod n$).

Beispiel: $n = 341 = 11 \cdot 31$ ist eine Pseudo-Primzahl zur Basis 2 (und zwar die kleinste). Beweis: Es ist

$$2^{10} = 1024 = 3 \cdot 11 \cdot 31 + 1, \qquad \text{also} \qquad 2^{10} \equiv 1 \mod 341$$

und daher

$$2^{341} = 2 \cdot 2^{340} = 2 \cdot (2^{10})^{34} \equiv 2 \mod 341.$$

Lemma. *Ist n eine Pseudo-Primzahl zur Basis 2, so ist auch $2^n - 1$ eine Pseudo-Primzahl zu dieser Basis.*

(Da wir mindestens eine Pseudo-Primzahl zur Basis 2 kennen, nämlich 341, gibt es also unendlich viele Pseudo-Primzahlen.)

Beweis. Sei n Pseudo-Primzahl zur Basis 2, also ist $2^n \equiv 2 \mod n$. Demnach gibt es t mit $tn = 2^n - 2$. Also $2^{tn} = 2^{2^n-2}$, und daher

$$(2^n)^t - 1 = 2^{tn} - 1 = 2^{2^n-2} - 1$$

Die linke Seite wird von $2^n - 1$ geteilt (im Polynomring $\mathbb{Z}[X]$ gilt: $X - 1$ teilt $X^t - 1$, hier setzen wir 2^n für X ein), also ist

$$(2^n - 1) \mid (2^{2^n-2} - 1) \mid 2^{2^n-1} - 2.$$

Natürlich ist $(2, 2^n - 1) = 1$. Es bleibt noch zu zeigen, dass $2^n - 1$ keine Primzahl ist: Ist $d|n$ mit $1 < d < n$, so ist $2^d - 1$ ein Teiler von $2^n - 1$ (wieder verwenden wir, dass $X - 1$ ein Teiler von $X^m - 1$ ist, für jedes $m \in \mathbb{N}$).

Ist n eine Pseudo-Primzahl für alle Basen a mit $(a, n) = 1$, so nennt man n eine *Carmichael-Zahl*. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Es gilt (ohne Beweis): Eine Carmichael-Zahl n ist ungerade, quadratfrei und hat mindestens drei Primfaktoren. Es gibt unendlich viele Carmichael-Zahlen.

Bemerkung. Wenn man wissen möchte, ob eine Zahl eine Primzahl ist, verwendet man einen Primzahltest. Das bekannteste und älteste Verfahren ist das Sieb des Eratosthenes. In der Praxis wird am häufigsten der **Miller-Rabin-Test** verwendet, der eine extrem schnelle Laufzeit hat, allerdings mit kleiner Wahrscheinlichkeit daneben liegen kann. Für Aufsehen hat in den letzten Jahren der **AKS-Primzahltest** (Agrawal-Kayal-Saxena, 2002) gesorgt: er erlaubt es, Zahlen in polynomialer Laufzeit zu testen *(Primes is in P)*, allerdings ist dieses Verfahren in der Praxis deutlich langsamer als der Miller-Rabin-Test ("polynomiale Laufzeit" bedeutet, dass es ein Polynom gibt $f(n)$ gibt, sodass die Anzahl der Rechenoperationen, die zum Test einer n-stelligen Zahl durchzuführen sind, durch $f(n)$ nach oben beschränkt ist).

2.11.8. Mersenne'sche und Fermat'sche Primzahlen. Primzahlen der Form $2^t - 1$ heißen *Mersenne'sche Primzahlen*; solche der Form $2^t + 1$ heißen *Fermat'sche Primzahlen.*

Lemma. *Ist $2^t - 1$ eine Primzahl, so ist t eine Primzahl. Ist $2^t + 1$ eine Primzahl, so ist t eine Zweierpotenz.*

Beweis: Ist $1 < d < t$ ein Teiler von t, so ist $2^d - 1$ ein echter, von 1 verschiedener Teiler von $2^t - 1$ (wieder verwendet man, dass $X - 1$ ein Teiler von $X^m - 1$ ist).

Ist $1 < d < t$ ein ungerader Teiler von t, etwa $de = t$, so ist $2^e + 1$ ein Teiler von $2^t + 1$ (denn $X + 1$ ist ein Teiler von $X^d + 1$; hier verwenden wir, dass für d ungerade $(X + 1)(X^{d-1} - X^{d-2} + - \cdots - X + 1) = X^d + 1$ gilt; man setzt in diese Formel für X die Zahl 2^e ein).

Es wird vermutet, dass es unendlich viele Mersenne'sche Primzahlen gibt, und man kennt sehr viele (aber nicht für jede Primzahl p ist $2^p - 1$ wieder eine Primzahl — Beispiel: $2^{11} - 1 = 2047 = 23 \cdot 89$.) Man kennt nur 5 Fermat'sche Primzahlen, nämlich $F_n = 2^{2^n} + 1$ mit $n = 0, 1, 2, 3, 4$, also

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537,$$

und man vermutet, dass dies die einzigen sind. (Die Fermat'schen Primzahlen spielen eine Rolle bei der Frage, welche regelmäßigen n-Ecken mit Zirkel und Lineal konstruiert werden können ...).