ulm university universität **uulm**

Skript zur Vorlesung

Elementare Zahlentheorie

Sommersemester 2016

Prof. Dr. Helmut Maier
Dr. Hans- Peter Reck

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm

Inhaltsverzeichnis

Kapitel 0

Einführung

Der Gegenstand der elementaren Zahlentheorie sind die natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \ldots\}$ und deren Erweiterungen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (ganze Zahlen), sowie der Körper $\mathbb{Q}$ der rationalen Zahlen. Die algebraische Zahlentheorie, die in dieser Vorlesung nicht zur Sprache kommen wird, befasst sich mit algebraischen Erweiterungen von $\mathbb{Q}$, wie zum Beispiel dem Körper $\mathbb{Q}(\sqrt{2})$, dem kleinsten Körper, der außer $\mathbb{Q}$ noch die irrationale Zahl $\sqrt{2}$ enthält.
Die Analysis befasst sich schließlich mit der größeren Menge $\mathbb{R}$ der reellen Zahlen.

Obwohl der Gegenstand der Zahlentheorie damit elementarer ist als der der Analysis, sind Fragen der Zahlentheorie oft schwieriger zu behandeln. Der Grund hierfür ist, dass für die reellen Zahlen einfache Kriterien für die Lösbarkeit von Gleichungen zur Verfügung stehen. Zum Beispiel folgt aus dem Zwischenwertsatz, dass für Polynome von ungeradem Grad die Gleichung

$$P(x) = 0$$

stets lösbar ist.
Werden hingegen ganzzahlige Lösungen verlangt, so gibt es selbst im Falle linearer Polynome

$$P(x) = ax + b = 0 \quad \text{mit } a, b \in \mathbb{Z} \quad \text{und } a \neq 0 \tag{1}$$

keine einfachen Kriterien für die Lösbarkeit.
Hat die Gleichung (1) eine Lösung, so heißt b durch a teilbar.

Die Teilbarkeit wird das Thema des ersten Kapitels sein.

Kapitel 1

Elementare Zahlentheorie und algebraische Strukturen

1.1 Teilbarkeit ganzer Zahlen

Definition 1.1.1. Eine Zahl $b \in \mathbb{Z}$ heißt durch eine Zahl $a \in \mathbb{Z}\backslash\{0\}$ teilbar, falls es ein $x \in \mathbb{Z}$ gibt, so dass $b = ax$ ist, und wir schreiben $a|b$. Falls b nicht durch a teilbar ist, schreiben wir $a \nmid b$.

Satz 1.1.1. *i)* $a|b \Rightarrow a|bc$ *für alle* $c \in \mathbb{Z}$

ii) $a|b$ *und* $b|c \Rightarrow a|c$

iii) $a|b$ *und* $a|c \Rightarrow a|(bx + cy)$ *für alle* $x, y \in \mathbb{Z}$

iv) $a|b$ *und* $b|a \Rightarrow a = \pm b$

v) $a|b$ *und* $a, b > 0 \Rightarrow a \leq b$

vi) Ist $m \neq 0$*, dann gilt:* $a|b \Leftrightarrow ma|mb$.

Beweis. Die Beweise folgen unmittelbar aus Definition 1.1.1.
Als Beispiel führen wir den Beweis von (iii):

$$a|b \text{ und } a|c \underset{Def.1.1.1}{\Rightarrow} \exists u, v \in \mathbb{Z} \text{ mit } b = au \text{ und } c = av \Rightarrow bx + cy = a \cdot (ux + vy) \underset{Def.1.1.1}{\Rightarrow} a|(bx + cy).$$

□

Satz 1.1.2. *Jedes* $b \in \mathbb{Z}\backslash\{0\}$ *hat nur endlich viele Teiler.*

Beweis. Es sei $a|b$. Wegen Satz 1.1.1 (i) folgt $|a|\big|b$. Nach Satz 1.1.1 (v) ist $0 < |a| \leq b$, was nur für endlich viele Werte von $|a|$ gilt. Wegen $a = \pm|a|$ folgt die Behauptung. □

1.2 Größter Gemeinsamer Teiler, Euklidischer Algorithmus

Definition 1.2.1. Für $x \in \mathbb{R}$ sei $[x]$ die größte ganze Zahl kleiner oder gleich x.

Satz 1.2.1. *(Divisionsalgorithmus, Teilbarkeit mit Rest)*
Es seien $a, b \in \mathbb{Z}$ mit $a > 0$. Dann gibt es eindeutig bestimmte Zahlen q und r, so dass $b = q \cdot a + r$ mit $0 \leq r < a$ ist. Es ist $q = \left[\frac{b}{a}\right]$. Falls $a \nmid b$, so ist $0 < r < a$.

Beweis. i) Existenz: durch Nachrechnen

ii) Eindeutigkeit:
Es sei $b = q_1 a + r_1 = q_2 a + r_2$ mit $0 \leq r_1 < a$ und $0 \leq r_2 < a$. OBdA. sei $r_2 < r_1$.
Dann ist $0 < r_1 - r_2 < a$. Andererseits ist $0 = (q_1 - q_2)a + (r_1 - r_2)$, also $a|(r_1 - r_2)$.
Nach Satz 1.1.1 (v) folgt $a \leq r_1 - r_2$, ein Widerspruch.

□

Definition 1.2.2. Die ganze Zahl t heißt gemeinsamer Teiler von b und c, falls $t|b$ und $t|c$ gilt.

Satz 1.2.2. *Es seien $b, c \in \mathbb{Z}$ und nicht beide 0. Dann gibt es ein eindeutig bestimmtes $g \in \mathbb{N}$ mit $g|b$, $g|c$ und $g \geq t$ für jeden gemeinsamen Teiler t von b und c.*

Beweis. Da es nach Satz 1.1.2 nur endlich viele gemeinsame Teiler t gibt, gibt es einen größten. □

Definition 1.2.3. Es seien $b, c \in \mathbb{Z}$ und nicht beide 0. Die nach Satz 1.2.2 eindeutig bestimmte natürliche Zahl g heißt größter gemeinsamer Teiler von b und c (Schreibweise: $g = ggT(b, c)$).

Satz 1.2.3. *Es seien $b, c \in \mathbb{Z}$ und nicht beide 0. Weiter sei $g \in \mathbb{N}$. Folgende Aussagen sind äquivalent:*

i) $g = ggT(b, c)$

ii) Die Zahl g ist der kleinste positive Wert von $L(x, y) := bx + cy$, wenn x und y alle ganzen Zahlen durchläuft.

iii) Die Zahl g ist ein gemeinsamer Teiler von b und c, der durch jeden gemeinsamen Teiler von b und c teilbar ist.

Beweis. $(i) \Leftrightarrow (ii)$:
Wegen $L(-x, -y) = -L(x, y)$ und $L(1, 0) = b$ nimmt L positive Werte tatsächlich an.
Es seien x_0 und y_0 so gewählt, dass $l = bx_0 + cy_0$ der kleinste positive Wert von L ist.
Weiter sei $b = lq + r$ mit $0 \leq r < l$. Dann ist

$$r = b - lq = b \cdot (1 - qx_0) + c \cdot (-qy_0) = L(1 - qx_0, -qy_0).$$

Damit ist auch r ein Wert von L. Da aber l der kleinste positive Wert von L ist, muss $r = 0$ gelten. Also gilt $l|b$ und analog $l|c$.
Wegen $g = ggT(b, c)$ gibt es $B, C \in \mathbb{Z}$ mit $b = gB$, $c = gC$ und $l = bx_0 + cy_0 = g \cdot (Bx_0 + Cy_0)$. Damit gilt $g|l$ und nach Satz 1.1.1 (v) ist $g \leq l$. Da g der größte gemeinsame Teiler ist, ist $g < l$ aber unmöglich. Daher ist $g = l = bx_0 + cy_0$.

$(iii) \Rightarrow (i)$:
Es erfülle g die Aussage (iii).
Es sei t ein gemeinsamer Teiler von b und c. Also gilt $t|g$, woraus $t \leq g$ nach Satz 1.1.1 (v) folgt.
Somit ist $g = ggT(b, c)$.

$(i) \Rightarrow (iii)$:
Es sei $g = ggT(b, c)$ und t ein gemeinsamer Teiler von b und c.
Wegen (i) und (ii) gibt es $x_0, y_0 \in \mathbb{Z}$ mit $g = bx_0 + cy_0$, also gilt nach Satz 1.1.1 (iii) auch $t|g$. □

Satz 1.2.4. *Es seien $b, c \in \mathbb{Z}$ und nicht beide 0.*

i) Es sei $m \in \mathbb{N}$. Dann ist $ggT(mb, mc) = m \cdot ggT(b, c)$.

ii) Gilt $t|b$ und $t|c$ für $t \in \mathbb{N}$, so folgt

$$ggT\left(\frac{b}{t}, \frac{c}{t}\right) = \frac{1}{t} \cdot ggT(b, c).$$

Ist $ggT(b, c) = g$, so ist $ggT\left(\frac{b}{g}, \frac{c}{g}\right) = 1$.

Beweis. i) Nach Satz 1.2.3 ist $ggT(mb, mc)$, der kleinste positive Wert von $bx + cy$, gerade gleich dem m- fachen des kleinsten positiven Werts von $bx + cy$, also gleich $m \cdot ggT(b, c)$.

ii) Dies folgt aus (i).

□

Satz 1.2.5. *Es seien $b, c \in \mathbb{Z}$ und nicht beide 0. Ist $ggT(b, m) = ggT(c, m) = 1$, so ist $ggT(bc, m) = 1$.*

Beweis. Es gibt $x_0, y_0, x_1, y_1 \in \mathbb{Z}$, so dass $bx_0 + my_0 = cx_1 + my_1 = 1$ ist.
Damit folgt $bx_0cx_1 = 1 - my_2$ mit $y_2 = y_0 + y_1 - my_0y_1$. Also ist $bc(x_0x_1) + my_2 = 1$.
Jeder gemeinsame Teiler von bc und m teilt daher 1, also ist $ggT(bc, m) = 1$. □

Satz 1.2.6. *Es seien $b, c \in \mathbb{Z}$ und nicht beide 0. Für $x \in \mathbb{Z}$ gilt*

$$ggT(b, c) = ggT(c, b) = ggT(b, -c) = ggT(b, c + bx).$$

Beweis. Wir setzen $t = ggT(b, c)$ und $g = ggT(b, c + bx)$.
Offenbar gilt $t = ggT(b, c) = ggT(b, -c)$.
Nach Satz 1.2.3 gibt es $x_0, y_0 \in \mathbb{Z}$, so dass $t = bx_0 + cy_0$ gilt. Somit ist $t = b \cdot (x_0 - xy_0) + (c + bx) \cdot y_0$.
Es folgt $g|t$. Wegen $t|c + bx$ und $t|b$ folgt andererseits $t|g$.
Daraus und aus Satz 1.1.1 (iv) folgt $t = \pm g$. Wegen $t > 0$ und $g > 0$ ist $g = t$. □

Satz 1.2.7. *Es seien $b, c, t \in \mathbb{Z}$, $ggT(c, t) = 1$ und $t|bc$. Dann ist $t|b$.*

Beweis. Nach Satz 1.2.4 ist $ggT(bc, bt) = b \cdot ggT(c, t) = b$.
Aus $t|bc$ und $t|bt$ folgt mit Satz 1.2.3 dann auch $t|b$. □

Satz 1.2.8. *(Euklidischer Algorithmus)*
Es seien $b, c \in \mathbb{Z}$ und $c > 0$. Wir wenden den Divisionsalgorithmus wiederholt an und erhalten eine Reihe von Gleichungen:

$$\begin{array}{rcll} b & = & q_1 \cdot c + r_1, & 0 \le r_1 < c \\ c & = & q_2 \cdot r_1 + r_2, & 0 \le r_2 < r_1 \\ r_1 & = & q_3 \cdot r_2 + r_3, & 0 \le r_3 < r_2 \\ \vdots & & \vdots & \vdots \\ r_{j-2} & = & q_j \cdot r_{j-1} + r_j, & 0 \le r_j < r_{j-1} \\ r_{j-1} & = & q_{j+1} \cdot r_j. & \end{array}$$

Der größte gemeinsame Teiler von b und c, der $ggT(b, c)$, ist r_j, der letzte von 0 verschiedene Rest im Divisionsprozess. Die Werte von x_0 und y_0 in $ggT(b, c) = bx_0 + cy_0$ können durch rückwärtiges Einsetzen gewonnen werden. Die Linearkombination kann auch erhalten werden, indem man jedes r_j als eine Linearkombination von b und c schreibt, vgl. Tabellenschema (siehe Übungen).

Beweis. Es sei $g = ggT(b, c)$. Nach Satz 1.2.6 gilt

$$\begin{aligned} ggT(b,c) &= ggT(b - q_1 c, c) = ggT(r_1, c) = ggT(r_1, c - q_2 r_1) = ggT(r_1, r_2) \\ &= ggT(r_1 - q_3 r_2, r_2) = ggT(r_3, r_2). \end{aligned}$$

Durch vollständige Induktion folgt

$$ggT(b, c) = ggT(r_{j-1}, r_j) = r_j.$$

Jedes r_j ist eine Linearkombination von r_{j-1} und r_{j-2}. Durch vollständige Induktion können wir annehmen, dass r_{j-1} und r_{j-2} Linearkombinationen von b und c sind. Somit ist auch r_j eine Linearkombination von b und c. □

Beispiel 1.2.1. Bestimme den größten gemeinsamen Teiler von $a = 294$ und $b = 201$ und drücke ihn als ganzzahlige Linearkombination von a und b aus.

Lösung:
Der Euklidische Algorithmus ergibt:

$$\begin{aligned} 294 &= 201 + 93 \\ 201 &= 2 \cdot 93 + 15 \\ 93 &= 6 \cdot 15 + 3 \\ 15 &= 5 \cdot 3 \end{aligned}$$

Also ist $ggT(294, 201) = 3$.

Die Linearkombination wird durch sukzessive Auflösung der Gleichungskette erhalten:

1. Methode: Vorwärtiges Einsetzen:

$$\begin{aligned} 93 &= 294 - 201 \\ 15 &= 201 - 2 \cdot 93 = 201 - 2 \cdot (294 - 201) = -2 \cdot 294 + 3 \cdot 201 \\ 3 &= 93 - 6 \cdot 15 = 294 - 201 - 6 \cdot (-2 \cdot 294 + 3 \cdot 201) = 13 \cdot 294 - 19 \cdot 201 \end{aligned}$$

2. Methode: Rückwärtiges Einsetzen:

$$\begin{aligned} 3 &= 93 - 6 \cdot 15 = 93 - 6 \cdot (201 - 2 \cdot 93) \\ &= 13 \cdot 93 - 6 \cdot 201 = 13 \cdot (294 - 201) - 6 \cdot 201 \\ &= 13 \cdot 294 - 19 \cdot 201 \end{aligned}$$

Damit ist auch die lineare Diophantischen Gleichung $294x + 201y = 3$ gelöst worden. Sie hat die Lösung $x = 13$ und $y = -19$.

Allgemein lässt sich die Lösung der linearen Diophantischen Gleichung in zwei Variablen x und y stets mit dem Problem des größten gemeinsamen Teilers in Verbindung bringen.

Satz 1.2.9. *Die lineare Diophantische Gleichung $ax + by = c$ mit $a, b, c \in \mathbb{Z}$ hat genau dann ganzzahlige Lösungen x und y, wenn $t = ggT(a, b)|c$.*

Die Lösung kann erhalten werden, wenn zuerst t mittels des Euklidischen Algorithmus ermittelt wird, dann die Gleichung $ax_0 + by_0 = t$ gelöst wird und anschließend (x_0, y_0) mit einem passenden Faktor durchmultipliziert wird.

Beispiel 1.2.2. Finde eine Lösung der Diophantischen Gleichung $73685x + 25513y = 10$ oder zeige, dass sie unlösbar ist.

Lösung:
Der Euklidische Algorithmus ergibt:

$$\begin{aligned} 73685 &= 2 \cdot 25513 + 22659 \\ 25513 &= 1 \cdot 22659 + 2854 \\ 22659 &= 7 \cdot 2854 + 2681 \\ 2854 &= 1 \cdot 2681 + 173 \\ 2681 &= 15 \cdot 173 + 86 \\ 173 &= 2 \cdot 86 + 1 \\ 86 &= 86 \cdot 1 \end{aligned}$$

Also ist $ggT(73685, 25513) = 1$.

Wir lösen nun zunächst die Gleichung $73685x' + 25513y' = 1$:

$$\begin{aligned} 1 &= 173 - 2 \cdot 86 = 173 - 2 \cdot (2681 - 15 \cdot 173) \\ &= 31 \cdot 173 - 2 \cdot 2681 = 31 \cdot (2854 - 2681) - 2 \cdot 2681 \\ &= -33 \cdot 2681 + 31 \cdot 2854 = 31 \cdot 2854 - 33 \cdot (22659 - 7 \cdot 2854) \\ &= 262 \cdot 2854 - 33 \cdot 22659 = 262 \cdot (25513 - 22659) - 33 \cdot 22659 \\ &= -295 \cdot 22659 + 262 \cdot 25513 = -295 \cdot (73685 - 2 \cdot 25513) + 262 \cdot 25513 \\ &= -295 \cdot 73685 + 852 \cdot 25513 \end{aligned}$$

Die Diophantische Gleichung $73685x' + 25513y' = 1$ hat also die Lösung $x' = -295$ und $y' = 852$.
Eine Lösung von $73685x + 25513y = 10$ ergibt sich daraus durch Multiplikation mit 10:

$$x = -2950 \quad \text{und} \quad y = 8520.$$

Definition 1.2.4. i) Es seien $b_1, \ldots, b_n \in \mathbb{Z}$. Es heißt $t \in \mathbb{Z}$ gemeinsamer Teiler von $b_1, \ldots, b_n$, falls $t | b_j$ für alle $1 \leq j \leq n$.

ii) Falls $b_1, \ldots, b_n$ nicht alle 0 sind, heißt g der größte gemeinsamer Teiler von $b_1, \ldots, b_n$, falls $g | b_j$ für alle $1 \leq j \leq n$ und falls $t \leq g$ für jeden gemeinsamen Teiler t von $b_1, \ldots, b_n$ gilt.
Schreibweise: $g = ggT(b_1, \ldots, b_n)$.

Wir geben ohne Beweis die Verallgemeinerungen der Sätze 1.2.2 und 1.2.3 an:

Satz 1.2.10. *Es seien $b_1, \ldots, b_n \in \mathbb{Z}$ und nicht alle 0. Dann existiert der $ggT(b_1, \ldots, b_n)$ und ist eindeutig bestimmt.*

Satz 1.2.11. *Es seien $b_1, \ldots, b_n \in \mathbb{Z}$ und nicht alle 0 und $g \in \mathbb{N}$. Folgende Aussagen sind äquivalent:*

i) $g = ggT(b_1, \ldots, b_n)$

ii) Die Zahl g ist der kleinste positive Wert von $L(x_1, \ldots, x_n) := b_1 x_1 + \ldots + b_n x_n$, wenn die x_j für $1 \leq j \leq n$ alle ganzen Zahlen durchlaufen.

iii) Die Zahl g ist ein gemeinsamer Teiler von $b_1, \ldots, b_n$, der durch jeden gemeinsamen Teiler von $b_1, \ldots, b_n$ teilbar ist.

Definition 1.2.5. Es seien $a_1, \ldots, a_n \in \mathbb{Z}$ nicht alle 0.
Dann heißt $b \in \mathbb{Z}$ ein gemeinsames Vielfaches von $a_1, \ldots, a_n$, falls $a_j | b$ für alle $1 \leq j \leq n$ gilt.
Weiter heißt $V \in \mathbb{N}$ kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$, falls $V \leq b$ für jedes positives Vielfache b von $a_1, \ldots, a_n$ ist. Schreibweise: $V = kgV(a_1, \ldots, a_n)$.

Satz 1.2.12. *Es seien $a_1, \ldots, a_n$ nicht alle 0.*

i) Falls b ein gemeinsames Vielfaches von $a_1, \ldots, a_n$ ist, so gilt $kgV(a_1, \ldots, a_n) | b$.

ii) Es seien $b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$. Dann ist $kgV(mb, mc) = m \cdot kgV(b, c)$.
Außerdem ist $kgV(b, c) \cdot ggT(b, c) = |bc|$.

Beweis. ohne Beweis. □

1.3 Primfaktorzerlegung

Definition 1.3.1. Eine natürliche Zahl $p > 1$ heißt Primzahl, falls sie keine positiven Teiler außer 1 und sich selbst besitzt. Eine natürliche Zahl $n > 1$, die keine Primzahl ist, heißt zusammengesetzt.

Satz 1.3.1. *Jede natürliche Zahl kann als Produkt von Primzahlen geschrieben werden. Dabei wird das leere Produkt als 1 gedeutet.*

Beweis. Wir führen den Beweis durch vollständige Induktion nach n:
$n = 1$:
Wir haben das leere Produkt.
$n \to n + 1$:
Die Behauptung sei für $m \leq n$ bereits bewiesen.
Ist $n + 1 = p$ eine Primzahl, so gilt die Behauptung auch für $n + 1$. Ist $n + 1$ zusammengesetzt, so gilt $n + 1 = m_1 \cdot m_2$ mit $1 < m_1, m_2 < n$. Nach Induktionsannahme sind m_1 und m_2 Produkte von Primzahlen. Es sei $m_1 = p_1 \cdots p_r$ und $m_2 = q_1 \cdots q_s$. Dann ist auch $n + 1 = p_1 \cdots p_r \cdot q_1 \cdots q_s$ ein Produkt von Primzahlen. □

Satz 1.3.2. *Es sei p eine Primzahl und $a, b \in \mathbb{Z}$. Aus $p | ab$ folgt $p | a$ oder $p | b$.*
Allgemeiner: Wenn $p | (a_1 \cdot a_2 \cdots a_n)$, dann teilt p mindestens einen Faktor a_i des Produkts.

Beweis. Aus $p \nmid a$ folgt $ggT(p, a) = 1$ und aus Satz 1.2.7 folgt $p | b$.
Der Beweis des allgemeinen Falles folgt durch vollständige Induktion. □

Satz 1.3.3. *(Fundamentalsatz der Arithmetik)*
Jede natürliche Zahl n kann bis auf die Anordnung der Faktoren eindeutig als Produkt von Primfaktoren geschrieben werden.

Beweis. Wir nehmen an, es gebe ein $n \in \mathbb{N}$ mit zwei verschiedenen Faktorisierungen. Wir kürzen alle Primzahlen, die in beiden Faktorisierungen auftreten, heraus und erhalten eine Gleichung der Form

$$p_1 \cdots p_r = q_1 \cdots q_s,$$

wobei die Mengen $\{p_1, \ldots, p_r\}$ und $\{q_1, \ldots, q_s\}$ disjunkt sind. Dies ist jedoch wegen $p_1 | q_1 \cdots q_s$ unmöglich. Nach Satz 1.3.2 muss daher p_1 mindestens ein q_j teilen, also $p_1 = q_j$ sein. □

Definition 1.3.2. Unter der kanonischen Primfaktorzerlegung einer natürlichen Zahl $n > 1$ versteht man eine Darstellung der Gestalt

$$n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$$

mit $p_1 < \ldots < p_r$ und $\gamma_j \in \mathbb{N}$ für $j = 1, \ldots, r$.

Um Faktorisierungen von verschiedenen Zahlen besser vergleichen zu können, macht man auch von unendlichen Produkten Gebrauch:

$$n = \prod_p p^{\gamma(p)}$$

mit $\gamma(p) \in \mathbb{N}_0$. Es ist dann $\gamma(p) = 0$ mit höchstens endlich vielen Ausnahmen.

Bei $\sum_p$ bzw. $\prod_p$ bedeutet der Index p unter dem Summen- bzw. dem Produktzeichen, dass die Summe bzw. das Produkt über alle Primzahlen erstreckt wird. Wie wir später sehen werden, gibt es unendlich viele Primzahlen. Es handelt sich also um unendliche Reihen bzw. unendliche Produkte.
Die Eigenschaft der Teilbarkeit, sowie der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache lassen sich nun mit den Exponenten $\gamma(p)$ beschreiben.

Satz 1.3.4. *Es seien $m = \prod_p p^{\gamma(p)}$ und $n = \prod_p p^{\delta(p)}$ mit $\gamma(p), \delta(p) \in \mathbb{N}_0$.*

i) Es gilt $m|n \Leftrightarrow \gamma(p) \leq \delta(p)$ für alle p.

ii) Es ist $ggT(m,n) = \prod_p p^{\min\{\gamma(p),\delta(p)\}}$.

iii) Es ist $kgV(m,n) = \prod_p p^{\max\{\gamma(p),\delta(p)\}}$.

Beweis. i) "$\Leftarrow$":
Es sei $\gamma(p) = \delta(p)$. Dann ist $n = m \cdot \prod_p p^{\delta(p)-\gamma(p)}$, also $m|n$ nach Definition 1.1.1.
"$\Rightarrow$":
Es gelte $m|n$. Annahme: Für die Primzahl p_0 gelte $\gamma(p_0) > \delta(p_0)$.
Dann ist

$$mp_0^{-\delta(p_0)} = \left(\prod_{p \neq p_0} p^{\gamma(p)} \right) \cdot p_0^{\gamma(p_0)-\delta(p_0)} \in \mathbb{Z} \quad \text{und} \quad np_0^{-\delta(p_0)} = \prod_{p \neq p_0} p^{\delta(p)} \in \mathbb{Z}.$$

Aus $m|n$ folgt mit Satz 1.1.1 (vi) dann $mp_0^{-\delta(p_0)} \big| np_0^{-\delta(p_0)}$. Also gilt $p_0 \big| mp_0^{-\delta(p_0)}$, aber $p_0 \nmid np_0^{-\delta(p_0)}$, ein Widerspruch.

ii) Nach (i) gilt für jeden gemeinsamen Teiler $t = \prod_p p^{\epsilon(p)}$ von m und n

$$\epsilon(p) \leq \min\{\gamma(p), \delta(p)\}.$$

Die Behauptung folgt nach Satz 1.2.3.

iii) Die Behauptung folgt analog mit Satz 1.2.12.

□

Beispiel 1.3.1. Es sei $m = 120$ und $n = 252$. Bestimme $ggT(m,n)$ und $kgV(m,n)$.

Lösung:
Es ist

$$\begin{array}{rcccc} m = & 2^3 & \cdot 3 & \cdot 5 & \\ n = & 2^2 & \cdot 3^2 & & \cdot 7 \end{array}$$

Also ist $ggT(m,n) = 2^2 \cdot 3 = 12$ und $kgV(m,n) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$.

Kapitel 2

Kongruenzen

2.1 Kongruenzen und Restklassen

Definition 2.1.1. Es sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$.
Wir sagen, a ist kongruent zu b modulo m, wenn $m|(b-a)$ gilt, und wir schreiben dann $a \equiv b \bmod m$ (bzw. $a \not\equiv b \bmod m$, falls $m \nmid (b-a)$ ist). Für die Menge aller Zahlen b mit $a \equiv b \bmod m$ schreiben wir $a \bmod m$. In diesem Zusammenhang nennt man m den Modul der Kongruenz $a \equiv b \bmod m$.

Satz 2.1.1. *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und die Divisionen*

$$\begin{aligned} a &= q_1 m + r_1 \text{ mit } 0 \le r_1 < m \\ b &= q_2 m + r_2 \text{ mit } 0 \le r_2 < m \end{aligned} \tag{2.1}$$

durch m mit Rest vorgelegt. Dann gilt genau dann $a \equiv b \bmod m$, wenn $r_1 = r_2$ ist.

Beweis. Einsetzen von (2.1) in $a \equiv b \bmod m$ ergibt mit Definition 2.1.1

$$a \equiv b \bmod m \Leftrightarrow m|((q_2 - q_1) \cdot m + r_2 - r_1) \Leftrightarrow m|(r_2 - r_1) \underset{|r_2 - r_1| < m}{\Leftrightarrow} r_1 = r_2.$$

□

Aus Satz 2.1.1 folgt sofort

Satz 2.1.2. *Es sei $m \in \mathbb{N}$. Dann gibt es genau m Kongruenzklassen modulo m.*
Jede ganze Zahl ist zu genau einer der Zahlen $0, 1, \ldots, m-1$ kongruent.

Bemerkung 2.1.1. Die Relation "$\equiv \bmod m$" ist also eine Äquivalenzrelation.

Beispiel 2.1.1. Die Kongruenzklassen modulo 2 sind

$$\begin{aligned} 0 \bmod 2 &= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \text{ (gerade Zahlen)} \\ 1 \bmod 2 &= \{\ldots, -3, -1, 1, 3, 5, \ldots\} \text{ (ungerade Zahlen).} \end{aligned}$$

Die Kongruenzklassen modulo 10 sind

$$\begin{aligned} 0 \bmod 10 &= \{\ldots, -20, -10, 0, 10, 20, \ldots\} \\ 1 \bmod 10 &= \{\ldots, -19, -9, 1, 11, 21, \ldots\} \\ &\vdots \quad\quad \vdots \\ 9 \bmod 10 &= \{\ldots, -11, -1, 9, 19, 29, \ldots\}. \end{aligned}$$

Allgemein sind Kongruenzklassen modulo m arithmetische Progressionen der Form

$$a \bmod m = \{\ldots, a - 3m, a - 2m, a - m, a, a + m, a + 2m, \ldots\}.$$

2.2 Rechnen mit Kongruenzen

Da die Kongruenzrelation eine Aussage über die Gleichheit von Restklassen macht, ist sie eine Verallgemeinerung der Gleichheitsrelation. Daher kann man mit Kongruenzen weitgehend wie mit Gleichungen rechnen, es gibt jedoch auch Unterschiede. Dies wollen wir im folgenden diskutieren.

Satz 2.2.1. *Es seien $a, b, c, d \in \mathbb{Z}$ und $m \in \mathbb{N}$ mit $a \equiv b \bmod m$ und $c \equiv d \bmod m$. Dann ist*

i) $a + c \equiv b + d \bmod m$

ii) $a - c \equiv b - d \bmod m$

iii) $a \cdot c \equiv b \cdot d \bmod m$

Beweis. Wir beweisen nur (iii). Aus Definition 2.1.1 ergeben sich (i) und (ii) genauso wie (iii), aber noch einfacher.
Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt nach Definition 2.1.1 die Existenz von $x, y \in \mathbb{Z}$ mit $b = a+mx$ und $d = c + my$. Dann ist $bd = ac + (ay + cx + mxy) \cdot m$, also $ac \equiv bd \bmod m$. □

Satz 2.2.2. *Es seien $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, $d = ggT(c, m)$ und $ac \equiv bc \bmod m$. Dann ist $a \equiv b \bmod m/d$.*

Spezialfall:
Ist $ac \equiv bc \bmod m$ und $ggT(c, m) = 1$, so ist $a \equiv b \bmod m$.

Beweis. Nach Satz 1.2.4 ist

$$ggT\left(\frac{m}{d}, \frac{c}{d}\right) = 1. \tag{2.2}$$

Weiter ist

$$ac \equiv bc \bmod m \underset{Def.2.1.1}{\Rightarrow} m|(bc - ac) \underset{Satz\ 1.1.1(vi)}{\Rightarrow} \frac{m}{d}\Big|\left((b-a)\cdot\frac{c}{d}\right) \underset{Satz\ 1.2.7}{\overset{(2.2),}{\Rightarrow}} \frac{m}{d}|(b-a)$$

$$\underset{Def.2.1.1}{\Rightarrow} a \equiv b \bmod \frac{m}{d}.$$

□

Aus Satz 2.2.1 ergibt sich durch vollständige Induktion:

Satz 2.2.3. *Es seien $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$.*
Aus $a \equiv b \bmod m$ folgt $a^k \equiv b^k \bmod m$ für $k \geq 1$.

Satz 2.2.3 erlaubt es, die Restklasse modulo m von a^k auch für große Werte von k zu bestimmen. Dazu wird k als Summe von Zweierpotenzen geschrieben. Die Restklassen von a^{2^δ} werden durch wiederholtes Quadrieren bestimmt.

Beispiel 2.2.1. Man bestimme $6^{55} \mod 41$.
Lösung:
Es ist $55 = 2^5 + 2^4 + 2^2 + 2 + 1$. Wiederholtes Quadrieren ausgehend von $6^1 \equiv 6 \equiv \text{mod}41$ ergibt:

$$\begin{aligned} 6^2 &\equiv 36 \equiv -5 \bmod 41 \\ 6^4 &\equiv 25 \equiv -16 \bmod 41 \\ 6^8 &\equiv (-16)^2 \equiv 10 \bmod 41 \\ 6^{16} &\equiv 10^2 \equiv 18 \bmod 41 \\ 6^{32} &\equiv 18^2 \equiv -4 \bmod 41, \end{aligned}$$

also $6^{55} \equiv 6^{32} \cdot 6^{16} \cdot 6^4 \cdot 6^2 \cdot 6 \equiv (-4) \cdot 18 \cdot (-16) \cdot (-5) \cdot 6 \equiv 3 \bmod 41$.

2.3 Rechnen mit Restklassen

Die Regeln von Satz 2.2.1 ermöglichen es, Addition und Multiplikation von Restklassen zu definieren.

Beispiel 2.3.1. Wie sollte das Produkt der Restklassen 3 mod 11 und 5 mod 11 definiert werden? Wir nehmen dazu aus jeder Restklasse einen Repräsentanten, so etwa $3 \in 3 \bmod 11$ und $5 \in 5 \bmod 11$. Ihr Produkt ist $3 \cdot 5 = 15 \in 4 \bmod 11$. Das Ergebnis ist unabhängig von der Wahl der Repräsentanten: für $14 \in 3 \bmod 11$ und $-6 \in 5 \bmod 11$ ergibt sich $14 \cdot (-6) = -84 \in 4 \bmod 11$.
Also sollte das Produkt folgendermaßen definiert werden:

$$(3 \bmod 11) \cdot (5 \bmod 11) = 4 \bmod 11.$$

Diese Unabhängigkeit von der Wahl der Repräsentanten- auch für Summe und Differenz- folgt allgemein aus Satz 2.2.1.

Definition 2.3.1. Es sei $m \in \mathbb{N}$ und $a, c \in \mathbb{Z}$. Dann definieren wir

$$\begin{aligned} a \bmod m + c \bmod m &= (b+d) \bmod m \\ a \bmod m - c \bmod m &= (b-d) \bmod m \\ (a \bmod m) \cdot (c \bmod m) &= (b \cdot d) \bmod m, \end{aligned}$$

wobei b bzw. d beliebige Repräsentanten der Restklassen $a \bmod m$ bzw. $c \bmod m$ sind.
Die Menge aller Restklassen mod m wird auch $\mathbb{Z}/m\mathbb{Z}$ bezeichnet.

Beispiel 2.3.2. Das Rechnen mit Uhrzeiten bedeutet Rechnen mit Restklassen modulo 24 oder bei der alten Weise, bei der die Stunden nur von 1 bis 12 numeriert werden, Rechnen mit Restklassen modulo 12.
Welche Uhrzeit haben wir sieben Stunden nach 9 Uhr? Die Antwort erhalten wir, wenn wir den Stundenzeiger von 9 Uhr um sieben Stunden im Uhrzeigersinn (der mathematisch gesehen negativen Richtung) bewegen: 4 Uhr. Mittels Addition von Restklasen ergibt sich das Resultat wie folgt:

$$9 \bmod 12 + 7 \bmod 12 = 4 \bmod 12.$$

Beispiel 2.3.3. Das Rechnen mit Wochentagen bedeutet Rechnung mit Restklassen modulo 7:
Der 3. Mai 2016 ist ein Dienstag. Auf welchen Wochentag fällt der 27. Mai 2016?
Lösung:
Ordnen wir die Sonntage der Restklasse 0 mod 7 zu, so gehört dann der 3. Mai zur Restklasse 2 mod 7. Die Aufgabe läuft also auf die Addition $2 \bmod 7 + 24 \bmod 7 = 2 \bmod 7 + 3 \bmod 7 = 5 \bmod 7$ hinaus. Der 27. Mai 2016 fällt demnach auf einen Freitag.

Bemerkung 2.3.1. Es ist möglich, Verknüpfungstafeln für die Addition und die Multiplikation von Restklassen zu erstellen. Für $m = 5$ haben wir etwa die folgenden Tafeln, wobei wir $\overline{a}$ statt $a \bmod 5$ schreiben:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

und

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Die Verknüpfungstafeln zeigen, dass $\mathbb{Z}/5\mathbb{Z}$ mit der Verknüpfung der Addition eine Gruppe bildet. Ebenso bildet $\mathbb{Z}/5\mathbb{Z}-\{0 \bmod 5\}$ eine Gruppe bzgl. der Multiplikation. Bezüglich beider Verknüpfungen haben wir einen Körper mit fünf Elementen.
Allgemein kann gezeigt werden: $\mathbb{Z}/m\mathbb{Z}$ bildet mit Addition und Multiplikation einen Ring. Dieser ist genau dann ein Körper, wenn m eine Primzahl ist.
Da wir in dieser Vorlesung keine Algebrakenntnisse voraussetzen, lassen wir es mit dieser Bemerkung bewenden.

2.4 Polynomkongruenzen

Definition 2.4.1. Unter einer Polynomkongruenz verstehen wir eine Kongruenz der Form

$$P(x) \equiv 0 \bmod m, \tag{$*$}$$

wobei P ein Polynom mit ganzzahligen Koeffizienten und m eine natürliche Zahl ist.

Beispiel 2.4.1. Die Kongruenz

$$21x^4 + 15x^3 + x + 1 \equiv 0 \bmod 7$$

ist zu

$$15x^3 + x + 1 \equiv 0 \bmod 7,$$

äquivalent, da wegen $7|21$ auch $21x^4 \equiv 0 \bmod 7$ gilt.
Das ursprünglich gegebene Polynom vierten Grades kann also durch ein Polynom dritten Grades ersetzt werden.

Diese Beobachtung motiviert folgende

Definition 2.4.2. Hat $P(x)$ in $(*)$ die Form

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

mit $n \in \mathbb{N}$ und $a_n \not\equiv 0 \bmod m$, so nennt man $(*)$ eine Polynomkongruenz vom Grad n.
Im Fall $n = 1$ spricht man von linearen Kongruenzen, im Fall $n = 2$ von quadratischen Kongruenzen.

Satz 2.4.1. *Es sei $m \in \mathbb{N}$ und*

$$P(x) \equiv 0 \bmod m$$

eine Polynomkongruenz. Dann wird $P(x)$ für sämtliche $x \in a \bmod m$ gelöst oder für kein $x \in a \bmod m$.

Beweis. Dies folgt aus den Sätzen 2.2.1 und 2.2.3. □

Dies macht folgende Definition sinnvoll:

Definition 2.4.3. Es sei $m \in \mathbb{N}$ und P ein ganzzahliges Polynom.
Unter der Anzahl der Lösungen modulo m der Kongruenz $P(x) \equiv 0 \bmod m$ versteht man die Anzahl der Restklassen modulo m, die diese Kongruenz lösen.

2.5 Lineare Kongruenzen, multiplikatives Inverses

Wir untersuchen nun die Lösbarkeit der linearen Kongruenz

$$ax \equiv b \bmod m.$$

Wir beginnen mit dem Fall $b = 1$:

Definition 2.5.1. (multiplikatives Inverses)
Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Es heißt $x \bmod m$ muliplikatives Inverses von $a \bmod m$, falls $ax \equiv 1 \bmod m$ ist. Wir schreiben dann auch $x \bmod m = a^{-1} \bmod m$.

Beispiel 2.5.1. Die Multiplikationstafel in Bemerkung 2.3.1 zeigt, dass das multiplikative Inverse von $2 \bmod 5$ gerade $3 \bmod 5$ ist. Also gilt $2^{-1} \bmod 5 = 3 \bmod 5$.

Satz 2.5.1. *Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das multiplikative Inverse $a^{-1} \bmod m$ existiert genau dann und ist modulo m eindeutig bestimmt, wenn $ggT(a, m) = 1$ ist.*

Beweis. Existenz:
Die Lösbarkeit von $ax \equiv 1 \bmod m$ ist zur Lösbarkeit der Diophantischen Gleichung $ax + my = 1$ äquivalent. Diese ist nach Satz 1.2.9 genau dann gegeben, wenn $ggT(a, m) = 1$ ist.

Eindeutigkeit:
Nach Satz 2.2.2 folgt aus $ax_1 \equiv ax_2 \bmod m$ bereits $x_1 \equiv x_2 \bmod m$. □

Satz 2.5.2. *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und $d = ggT(a, m)$. Dann ist die Kongruenz $ax \equiv b \bmod m$ genau dann lösbar, wenn $d|b$. Ist diese Bedingung erfüllt, so bilden die Lösungen eine arithmetische Progression mit Differenz m/d. Es gibt also d Lösungen modulo m.*

Beweis. Nach Satz 2.2.2 ist die Kongruenz $ax \equiv b \bmod m$ zu

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \bmod \frac{m}{d}$$

äquivalent.
Das multiplikative Inverse $\frac{a}{d} \bmod \frac{m}{d}$ ist dann nach Satz 2.5.1 eindeutig bestimmt, etwa $\left(\frac{a}{d}\right)^{-1} \bmod \frac{m}{d}$. Es folgt

$$x \equiv \left(\frac{a}{d}\right)^{-1} \left(\frac{b}{d}\right) \bmod \frac{m}{d}.$$

Daraus ergibt sich die Behauptung. □

2.6 Der Chinesische Restsatz

Wir behandeln das Problem der Lösung von Systemen von Kongruenzen.

Beispiel 2.6.1. Es sei $N = 35 = 5 \cdot 7$.
Erfüllt eine ganze Zahl m eine Kongruenz modulo 35, so erfüllt m auch ein Paar von Kongruenzen, eine Kongruenz modulo 5 und eine Kongruenz modulo 7. Ist z. B.

$$m \equiv 12 \bmod 35, \tag{1}$$

so folgt

$$\begin{cases} m \equiv 2 \bmod 5 \\ m \equiv 5 \bmod 7. \end{cases} \tag{2}$$

Die folgende Tabelle zeigt, dass auch (1) aus (2) folgt.
Schärfer gilt, dass jedem Paar von Restklassen ($a \bmod 5$, $b \bmod 7$) genau eine Restklasse $c \bmod 35$ entspricht.

mod 5 \ mod 7	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

Jede Restklasse modulo 35 hat somit zwei Komponenten, eine modulo 7- und eine modulo 5- Komponente. Eine ähnliche Situation besteht in der Vektorrechnung: jeder Punkt der Ebene kann mit einem Koordinatenpaar (x, y) oder auch dem Vektor $\vec{v} = (x, y)$ identifiziert werden. Mit Vektoren kann komponentenweise gerechnet werden: Für $\vec{v}_1 = (x_1, y_1)$ und $\vec{v}_2 = (x_2, y_2)$ ist $\vec{v}_1 + \vec{v}_2 = (x_1 + x_2, y_1 + y_2)$. Dieses "komponentenweise" Rechnen ist auch bei Kongruenzen möglich.

Beispiel 2.6.2. Man bestimme das Produkt

$$(13 \bmod 35) \cdot (29 \bmod 35).$$

Lösung:
Aus der Tabelle in Beispiel 2.6.1 erhalten wir die Entsprechungen

$$\begin{aligned} 13 \bmod 35 &\Leftrightarrow (6 \bmod 7,\ 3 \bmod 5) \\ 29 \bmod 35 &\Leftrightarrow (1 \bmod 7,\ 4 \bmod 5). \end{aligned}$$

Komponentenweises Rechnen ergibt

$$(6 \bmod 7,\ 3 \bmod 5) \cdot (1 \bmod 7,\ 4 \bmod 5) = (6 \bmod 7,\ 2 \bmod 5).$$

Mit der Entsprechung

$$27 \bmod 35 \Leftrightarrow (6 \bmod 7,\ 2 \bmod 5).$$

erhalten wir

$$(13 \bmod 35) \cdot (29 \bmod 35) = 27 \bmod 35.$$

Beispiel 2.6.3. Es sei

$$P(x) = x^4 + 4x^3 + 10x^2 + 12x + 8.$$

Man bestimme sämtliche Lösungen von $P(x) \equiv 0 \bmod 35$.

Lösung:
Durch Rechnung erhält man folgende Tabelle:

x	-3	-2	-1	0	1	2	3
$P(x)$	35	8	3	8	35	120	323

Daraus ersieht man: die Lösungen von $P(x) \equiv 0 \bmod 7$ sind $x \equiv 1 \bmod 7$ und $x \equiv 4 \bmod 7$ und die Lösungen von $P(x) \equiv 0 \bmod 5$ sind $x \equiv 1 \bmod 5$ und $x \equiv 2 \bmod 5$.

Diese Lösungen lassen sich auf vier verschiedene Weisen kombinieren. Aus der Tabelle in Beispiel 2.6.1 erhält man folgende Zuordnungen:

$$\begin{aligned} 1 \bmod 35 &\Leftrightarrow (1 \bmod 7,\ 1 \bmod 5) \\ 22 \bmod 35 &\Leftrightarrow (1 \bmod 7,\ 2 \bmod 5) \\ 11 \bmod 35 &\Leftrightarrow (4 \bmod 7,\ 1 \bmod 5) \\ 32 \bmod 35 &\Leftrightarrow (4 \bmod 7,\ 2 \bmod 5). \end{aligned}$$

Damit hat die Kongruenz $P(x) \equiv 0 \bmod 35$ folgende Lösungen modulo 35:

$$1 \bmod 35,\ 11 \bmod 35,\ 22 \bmod 35,\ 32 \bmod 35.$$

Wir formulieren nun den Chinesischen Restsatz allgemein und geben auch einen Algorithmus, der ein System von Kongruenzen zu einer einzelnen Kongruenz reduziert.

Satz 2.6.1. *(Chinesischer Restsatz)*
Es seien $m_1, m_2, \ldots, m_r$ natürliche Zahlen, die paarweise teilerfremd sind und $a_1, a_2, \ldots, a_r$ ganze Zahlen. Dann besitzen die r Kongruenzen

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \quad\quad \vdots \\ x &\equiv a_{r-1} \bmod m_{r-1} \\ x &\equiv a_r \bmod m_r \end{aligned}$$

eine gemeinsame Lösung.
Diese ist nach dem Modul

$$m = m_1 \cdot m_2 \cdots m_r$$

eindeutig bestimmt.
Eine Lösung kann in der Form

$$x_0 = \sum_{j=1}^{r} M_j M_j^{-1} a_j$$

erhalten werden, wobei

$$M_j := \frac{m}{m_j} \quad \textit{und} \quad M_j M_j^{-1} \equiv 1 \bmod m_j$$

ist.

Beweis. Existenz:
Für $j \neq i$ ist $M_j \equiv 0 \bmod m_i$.
Also ist für alle $i \in \{1, \ldots, r\}$

$$x_0 = \sum_{j=1}^{r} M_j M_j^{-1} a_j \equiv M_i M_i^{-1} a_i \equiv a_i \bmod m_i.$$

Damit ist x_0 eine Lösung des obigen Systems.

Eindeutigkeit:
Es seien x_1 und x_2 zwei Lösungen des obigen Systems. Dann folgt $m_i | (x_1 - x_2)$ für alle $i \in \{1, \ldots, r\}$.
Nach Satz 1.2.12 ist $x_2 \equiv x_1 \bmod m$. □

Beispiel 2.6.4. Gesucht ist die kleinste positive Lösung des Systems

$$\begin{aligned} x &\equiv 2 \bmod 5 \\ x &\equiv 4 \bmod 11 \\ x &\equiv 7 \bmod 17. \end{aligned}$$

Lösung:
Mit den Bezeichnungen von Satz 2.6.1 ist $m_1 = 5$, $m_2 = 11$, $m_3 = 17$, $m = 5 \cdot 11 \cdot 17 = 935$, $a_1 = 2$, $a_2 = 4$ und $a_3 = 7$.
Weiter ist

$$\begin{aligned} M_1 &:= \frac{m}{m_1} = 187 \\ M_2 &:= \frac{m}{m_2} = 85 \\ M_3 &:= \frac{m}{m_3} = 55. \end{aligned}$$

Mit dem Euklidischen Algorithmus finden wir

$$\begin{aligned} 187 \cdot M_1^{-1} \equiv 1 \bmod 5 &\Leftrightarrow 2 \cdot M_1^{-1} \equiv 1 \bmod 5, \text{ also } M_1^{-1} \equiv 3 \bmod 5 \\ 85 \cdot M_2^{-1} \equiv 1 \bmod 11 &\Leftrightarrow 8 \cdot M_2^{-1} \equiv 1 \bmod 11, \text{ also } M_2^{-1} \equiv 7 \bmod 11 \Rightarrow M_2^{-1} \equiv -4 \bmod 11 \\ 55 \cdot M_3^{-1} \equiv 1 \bmod 17 &\Leftrightarrow 4 \cdot M_3^{-1} \equiv 1 \bmod 17, \text{ also } M_3^{-1} \equiv 13 \bmod 17 \Rightarrow M_3^{-1} \equiv -4 \bmod 17. \end{aligned}$$

Wir erhalten die Lösung

$$x_0 = \sum_{j=1}^{3} M_j M_j^{-1} a_j = 187 \cdot 3 \cdot 2 + 85 \cdot (-4) \cdot 4 + 55 \cdot (-4) \cdot 7 = -1778.$$

Die allgemeine Lösung hat die Form

$$x = x_0 + k \cdot m = -1778 + 935k.$$

Die kleinste positive Lösung erhalten wir für $k = 2$, nämlich $x = 92$.

2.7 Restsysteme, Eulersche φ- Funktion

Definition 2.7.1. i) Ein vollständiges Restsystem modulo m ist eine Menge $\mathcal{R}$ ganzer Zahlen, so dass es zu jeder Restklasse $a \bmod m$ genau ein $r \in \mathcal{R}$ mit $r \in a \bmod m$ gibt.

ii) Ein reduziertes Restsystem modulo m ist eine Menge $\mathcal{R}'$ ganzer Zahlen, so dass es zu jeder Restklasse $a \bmod m$ mit $ggT(a, m) = 1$ genau ein $r \in \mathcal{R}'$ mit $r \in a \bmod m$ gibt.

Definition 2.7.2. i) Die Menge $\{0, 1, \ldots, m-1\}$ heißt die Menge der kleinsten nichtnegativen Reste modulo m.

ii) Ist m ungerade, so heißt

$$\left\{ -\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2} \right\}$$

die Menge der absolut kleinsten Reste modulo m.

Beispiel 2.7.1. Es sei $m = 15$. Die folgenden Mengen sind vollständige Restsysteme modulo 15.

i) Die Menge der kleinsten nichtnegativen Reste $\mathcal{R}_1 = \{0, 1, 2, \ldots, 14\}$.

ii) Die Menge der absolut kleinsten Reste $\mathcal{R}_2 = \{-7, -6, -5, \ldots, -1, 0, 1, \ldots, 6, 7\}$.

iii) Die Menge $\mathcal{R}_3 = \{90, 31, -13, 48, 4, -10, 6, 22, 98, -21, -50, 26, 57, -32, 74\}$.

Jedes vollständige Restsystem enthält ein reduziertes Restsystem.
Im Fall der Systeme $\mathcal{R}_j$ mit $j \in \{1, 2, 3\}$ sind das die Mengen

$$\begin{aligned} \mathcal{R}_1 &= \{1, 2, 4, 7, 8, 11, 13, 14\} \\ \mathcal{R}_2 &= \{-7, -4, -2, -1, 1, 2, 4, 7\} \\ \mathcal{R}_3 &= \{31, -13, 4, 22, 98, 26, -32, 74\}. \end{aligned}$$

Nach Satz 1.2.6 ist $ggT(a, m) = ggT(a + km, m)$ für alle $k \in \mathbb{Z}$. Also hängt der $ggT(a, m)$ nur von der Restklasse von a mod m ab. Daher ist folgende Definition sinnvoll:

Definition 2.7.3. Es sei $m \in \mathbb{N}$. Die Restklasse a mod m heißt teilerfremde Restklasse modulo m, wenn für ein (und damit für alle) $x \in a$ mod m die Bedingung $ggT(x, m) = 1$ gilt.

Satz 2.7.1. *Es sei $m \in \mathbb{N}$. Jedes reduzierte Restsystem modulo m besitzt dieselbe Anzahl an Elementen. Sie ist gleich der Anzahl an teilerfremden Restklassen modulo m.*

Definition 2.7.4. Für $m \in \mathbb{N}$ wird die Anzahl der teilerfremden Restklassen modulo m mit $\varphi(m)$ bezeichnet. Diese Funktion heißt die Eulersche φ- Funktion.

Eine grundlegende Eigenschaft der Eulerschen φ- Funktion ist ihre Multiplikativität.

Definition 2.7.5. i) Unter einer arithmetischen (oder zahlentheoretischen) Funktion versteht man eine Abbildung $f : \mathbb{N} \to \mathbb{C}$.

ii) Diese Funktion f heißt additiv, falls

$$f(m \cdot n) = f(m) + f(n) \tag{A}$$

für alle $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ gilt.

iii) Die Funktion f heißt multiplikativ, falls

$$f(m \cdot n) = f(m) \cdot f(n) \tag{M}$$

für alle $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ gilt.

iv) Gelten (A) bzw. (M) ohne die Einschränkung $ggT(m, n) = 1$, so heißt f vollständig additiv bzw. vollständig multiplikativ.

Beispiel 2.7.2. Es sei $\omega(n)$ die Anzahl der verschiedenen Primfaktoren von n. Dann ist ω additiv, aber nicht vollständig additiv.

Beweis. Es sei $ggT(m, n) = 1$. Weiter seien

$$m = p_1^{\mu_1} \cdots p_r^{\mu_r} \quad \text{und} \quad n = q_1^{\nu_1} \cdots q_s^{\nu_s}$$

die kanonischen Primfaktorzerlegungen von m und n. Dann sind die Mengen der p_i und der q_i disjunkt. Es ist $\omega(m) = r$ und $\omega(n) = s$, woraus $\omega(m \cdot n) = r + s$ folgt.
Allerdings ist ω nicht vollständig addditiv, denn es gilt etwa $\omega(6) = \omega(15) = 2$, aber es gilt auch $\omega(90) = 3 < \omega(6) + \omega(15)$. □

Additive und Multiplikative Funktionen sind bekannt, wenn ihre Werte für Primzahlpotenzen bekannt sind.

Satz 2.7.2. *Es sei $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die kanonische Primfaktorzerlegung von n.*

i) Ist f additiv, so ist $f(1) = 0$ und

$$f(n) = f(p_1^{\gamma_1}) + \ldots + f(p_r^{\gamma_r}) = \sum_{j=1}^{r} f(p_j^{\gamma_j}).$$

ii) Ist f multiplikativ, so ist $f(1) = 1$ und

$$f(n) = f\left(p_1^{\gamma_1}\right) \cdots f\left(p_r^{\gamma_r}\right) = \prod_{j=1}^{r} f(p_j^{\gamma_j}).$$

Beweis. Dies folgt mittels vollständiger Induktion aus den Gleichungen

$$f(m \cdot n) = f(m) + f(n) \quad \text{und} \quad f(m \cdot n) = f(m) \cdot f(n)$$

für $ggT(m, n) = 1$. □

Die Grundidee für den Beweis der Multiplikativität der Eulerschen φ- Funktion kann mit der Tabelle in Beispiel 2.6.1 illustriert werden:

mod 5 \	0	1	2	3	4	5	6	mod 7
0	0	15	30	10	25	5	20	
1	21	1	16	31	11	26	6	
2	7	22	2	17	32	12	27	
3	28	8	23	3	18	33	13	
4	14	29	9	24	4	19	34	

Die teilerfremden Restklassen modulo 5 sind in vier Zeilen dieser Matrix enthalten, und zwar in den Zeilen

$$1 \bmod 5,\ 2 \bmod 5,\ 3 \bmod 5,\ 4 \bmod 5. \tag{1}$$

Es ist $\varphi(5) = 4$.

Die teilerfremden Restklassen modulo 7 sind in sechs Spalten dieser Matrix enthalten, und zwar in den Spalten

$$1 \bmod 7, \ldots, 6 \bmod 7. \tag{2}$$

Es ist $\varphi(7) = 6$.

Satz 2.7.3. *Die Eulersche φ- Funktion ist multiplikativ.*

Beweis. Es seien $m, n \in \mathbb{N}$ und $ggT(m, n) = 1$. Nach dem Chinesischen Restsatz (Satz 2.6.1) gibt es eine Bijektion zwischen

$$(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \quad \text{und} \quad \mathbb{Z}/(mn)\mathbb{Z},$$

also zwischen der Menge der Paare von Restklassen $(x \bmod m, y \bmod m)$ und der Menge der Restklassen $z \bmod (mn)$. Es ist

$$ggT(z, mn) = 1 \Leftrightarrow ggT(x, m) = 1 \quad \text{und} \quad ggT(y, n) = 1.$$

Die Anzahl $\varphi(mn)$ der teilerfremden Restklassen modulo mn ist also gleich der Anzahl der Paare, bestehend aus einer teilerfremden Restklasse modulo m und einer teilerfremden Restklasse modulo n, also gerade $\varphi(m) \cdot \varphi(n)$. □

Satz 2.7.4. *Es sei $n = \prod_{j=1}^{r} p_j^{\gamma_j}$ die kanonische Primfaktorzerlegung von n. Dann ist*

$$\varphi(n) = \prod_{j=1}^{r} p_j^{\gamma_j - 1} \cdot (p_j - 1) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Beweis. Es sei $m = p^\alpha$, $\alpha \in \mathbb{N}$ und p eine Primzahl. Von dem vollständigen Restsystem modulo m, der Menge $\mathcal{R} = \{1, 2, \ldots, p^\alpha\}$ sind genau die Vielfachen von p, nämlich kp mit $1 \leq k \leq p^{\alpha-1}$ nicht zu m teilerfremd. Also gilt

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

Die Behauptung folgt nun aus Satz 2.7.2 und Satz 2.7.3. □

2.8 Die Sätze von Euler und Fermat, Primzahltests

Satz 2.8.1. *Es sei $m \in \mathbb{N}$ und $\mathcal{R} = \{x_1, \ldots, x_m\}$ ein vollständiges Restsystem modulo m sowie $\mathcal{R}' = \{y_1, \ldots, y_{\varphi(m)}\}$ ein reduziertes Restsystem modulo m.*
Ist $ggT(a, m) = 1$, so ist auch $a\mathcal{R} = \{ax_1, \ldots, ax_m\}$ ein vollständiges Restsystem modulo m und $a\mathcal{R}' = \{ay_1, \ldots, ay_{\varphi(m)}\}$ ein reduziertes Restsystem modulo m.

Beweis. Nach Satz 2.2.2 folgt

$$ax_j \equiv ax_k \bmod m \Leftrightarrow x_j \equiv x_k \bmod m \Leftrightarrow j = k$$

für alle $1 \leq j, k \leq m$ und

$$ay_j \equiv ay_k \bmod m \Leftrightarrow j = k$$

für alle $1 \leq j, k \leq \varphi(m)$.
Nach Satz 1.2.4 ist $ggT(ay_j, m) = 1$. In der Menge $a\mathcal{R}$ ist daher jede Restklasse modulo m genau einmal vertreten und in der Menge $a\mathcal{R}'$ jede reduzierte Restklasse. □

Bemerkung 2.8.1. Im allgemeinen werden die Restklassen in $a\mathcal{R}$ bzw. in $a\mathcal{R}'$ in anderer Reihenfolge als in $\mathcal{R}$ bzw. in $\mathcal{R}'$ durchlaufen.
Es sei z.B. $m = 10$ und $a = 3$. Es ist $\mathcal{R}' = \{1, 3, 7, 9\}$ ein reduziertes Restsystem modulo 10. Dann ist auch $3\mathcal{R}' = \{3, 9, 21, 27\}$ ein reduziertes Restsystem modulo 10. Es treten wieder die teilerfremden Restklassen 1 mod 10, 3 mod 10, 7 mod 10 und 9 mod 10 auf, aber in anderer Reihenfolge.

Satz 2.8.2. *(Satz von Euler)*
Es sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ und $ggT(a, m) = 1$. Dann ist

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

Beweis. Es sei $R_1 = \{r_1, \ldots, r_{\varphi(m)}\}$ ein reduziertes Restsystem modulo m. Damit ist nach Satz 2.8.1 aber auch $aR_1 = \{ar_1, \ldots, ar_{\varphi(m)}\}$ ein reduziertes Restsystem modulo m. Somit folgt

$$r_1 \cdots r_{\varphi(m)} \equiv (ar_1) \cdots (ar_{\varphi(m)}) \bmod m,$$

da links und rechts dieselben Restklassen (i.a. in unterschiedlicher Reihenfolge) auftreten. Also ist

$$r_1 \cdots r_{\varphi(m)} \equiv a^{\varphi(m)}(r_1 \cdots r_{\varphi(m)}) \bmod m.$$

Kürzen von $r_1 \cdots r_{\varphi(m)}$ ergibt die Behauptung. □

Schon etwa 100 Jahre vor dem Satz von Euler war der (kleine) Satz von Fermat (Pierre de Fermat, 1607- 1665) bekannt, der sich aus dem Satz von Euler durch die Spezialisierung $m = p$ mit einer Primzahl p ergibt.

Satz 2.8.3. *(kleiner Satz von Fermat)*
Es sei p eine Primzahl und $a \in \mathbb{Z}$ nicht durch p teilbar. Dann ist

$$a^{p-1} \equiv 1 \bmod p.$$

Satz 2.8.3 liefert einen einfachen (negativen) Primzahltest (Fermattest):
Aus $n|(a^{n-1} - 1)$ folgt

$$a^n \equiv a \bmod n. \qquad (*)$$

Ist n eine Primzahl, so ist $(*)$ nach Satz 2.8.3 erfüllt.
Ist $(*)$ nicht erfüllt, was für festes a (z. B. $a = 2$) für die meisten zusammengesetzten Zahlen der Fall ist, so kann man schließen, dass n keine Primzahl ist.

Der Fermattest und andere raffiniertere Tests sind für große Zahlen oft einfacher durchzuführen, als der Versuch, Faktoren zu finden.
So ist z. B. seit 1963 (Selfridge und Hurwitz) bekannt, dass die Fermatzahl $F_{14} = 2^{2^{14}} + 1$ mit 4933 Dezimalstellen zusammengesetzt ist. Jedoch konnte erst 2010 (Rajala und Woltman) ein Primfaktor (mit 53 Dezimalstellen) gefunden werden.

Primzahltests und Faktorisierungsmethoden sind auch seit 1978 in Anwendungen, wie etwa der Kryptographie, von Wichtigkeit.

2.9 Elementare Teilbarkeitsregeln

Die elementaren Teilbarkeitsregeln lassen sich durch Rechnen mit Kongruenzen leicht beweisen. Wir legen unseren Überlegungen die Darstellung natürlicher Zahlen im Dezimalsystem zugrunde.

Satz 2.9.1. *Jede natürliche Zahl $n \in \mathbb{N}$ kann eindeutig als*

$$n = \sum_{k=0}^{m} a_k \cdot 10^k$$

mit $a_k \in \{0, 1, \ldots, 9\}$ und $a_m \neq 0$ geschrieben werden. Die a_k heißen die Ziffern von n (im Dezimalsystem).

Beispiel 2.9.1.

$$n = 283967 = 2 \cdot 10^5 + 8 \cdot 10^4 + 3 \cdot 10^3 + 9 \cdot 10^2 + 6 \cdot 10 + 7.$$

Definition 2.9.1. Unter der Quersumme einer Zahl $n = \sum_{k=0}^{m} a_k \cdot 10^k$ mit Ziffern a_k versteht man

$$Q(n) = \sum_{k=0}^{m} a_k.$$

Unter der alternierenden Quersumme versteht man

$$AQ(n) = \sum_{k=0}^{m} (-1)^k \cdot a_k.$$

Satz 2.9.2. *i) Eine natürliche Zahl ist genau dann durch 2 teilbar (gerade), wenn die letzte Ziffer durch 2 teilbar (gerade) ist.*

ii) Eine Zahl ist genau dann durch 5 teilbar, wenn die letzte Ziffer 0 oder 5 ist.

iii) Eine Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

iv) Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

v) Eine Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

Beweis. Wir nehmen $n = \sum_{k=0}^{m} a_k 10^k$, $a_k \in \{0, 1, \ldots, 9\}$ und $a_m \neq 0$ an.

i) Wegen $10^k \equiv \begin{cases} 0 \mod 2, & \text{für} \quad k \geq 1 \\ 1 \mod 2, & \text{für} \quad k = 0 \end{cases}$ folgt $n \equiv a_0 \mod 2$.

ii) Wegen $10^k \equiv \begin{cases} 0 \mod 5, & \text{für} \quad k \geq 1 \\ 1 \mod 5, & \text{für} \quad k = 0 \end{cases}$ folgt $n \equiv a_0 \mod 5$.

iii) Es ist $10 \equiv 1 \mod 3$. Nach Satz 2.2.3 folgt $10^k \equiv 1 \mod 3$. Damit ist nach Satz 2.2.1

$$n = \sum_{k=0}^{m} a_k 10^k = \sum_{k=0}^{m} a_k \mod 3.$$

iv) Es ist $10 \equiv 1 \mod 9$. Die Behauptung folgt wie in iii), wenn Kongruenzen modulo 3 durch Kongruenzen modulo 9 ersetzt werden.

v) Es ist $10 \equiv -1 \mod 11$. Nach Satz 2.2.3 folgt $10^k \equiv (-1)^k \mod 11$. Damit ist

$$n = \sum_{k=0}^{m} a_k 10^k = \sum_{k=0}^{m} (-1)^k a_k \mod 11.$$

□

Kapitel 3

Elementare Sätze zur Primzahlverteilung

3.1 Einleitung

Die einfachste Aussage über die Verteilung der Primzahlen ist, dass es unendlich viele gibt. Hierfür hatte schon Euklid (ca. 300 v. Chr.) einen Beweis gegeben.
Feinere Aussagen verwenden die Primzahlzählfunktion $\pi(x)$.

Definition 3.1.1. Es sei $x \geq 1$. Dann bedeutet $\pi(x)$ die Anzahl der Primzahlen kleiner gleich x.

Beispiel 3.1.1. Die Primzahlen kleiner gleich 10 sind gerade 2,3,5,7. Damit ist $\pi(10) = 4$.

Gauß vermutete um 1792 die Gültigkeit des Primzahlsatzes

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1. \tag{1}$$

3.2 Euklids Beweis für die Unendlichkeit der Primzahlen

Euklids Beweis, der ca. 2500 Jahre alt ist, ist so etwas wie ein Musterbeispiel für einen mathematischen Beweis.
Er besticht durch seine Einfachheit und Eleganz.

Satz 3.2.1. *(Euklid)*
Es gibt unendlich viele Primzahlen.

Beweis. Beweis durch Widerspruch: wir nehmen, es gebe nur endlich viele Primzahlen, welche wir mit $\{p_1, p_2, p_3, \cdots p_n\}$ bezeichnen wollen. Wir bilden die Zahl $N = p_1 \cdot p_2 \cdots p_n + 1$, welche durch keine der Zahlen $p_1, p_2, \ldots, p_n$ teilbar ist. Damit ist N entweder eine neue Primzahl oder durch eine andere, in der oberen Liste nicht auftretende Primzahl teilbar. Also kann man jeder endlichen Liste von Primzahlen weitere hinzufügen. □

3.3 Der Satz von Tschebyschew

Die Ergebnisse von Tschebyschew beruhen auf der Analyse der Primfaktoren der Binomialkoeffizienten.

Lemma 3.3.1. *Es sei $n \in \mathbb{N}$.*

i) Es gilt

$$\frac{1}{2n+1} \cdot 4^n \leq \binom{2n}{n} \leq 4^n.$$

ii) Für Primzahlen p mit $\frac{2}{3}n < p \leq n$ gilt $p \nmid \binom{2n}{n}$.

iii) Für Primzahlen p mit $n < p \leq 2n$ gilt $p | \binom{2n}{n}$ und $p^2 \nmid \binom{2n}{n}$.

Beweis. i) Nach dem Binomischen Lehrsatz ist

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}. \qquad (*)$$

Daraus folgt sofort $\binom{2n}{n} \leq 4^n$.
Wegen

$$\frac{\binom{2n}{k+1}}{\binom{2n}{k}} = \frac{k! \cdot (2n-k)!}{(k+1)! \cdot (2n-k-1)!} = \frac{2n-k}{k+1}$$

nimmt die Folge $\binom{2n}{k}$ für $k = n$ ihr Maximum an. Da die Summe in $(*)$ genau $2n+1$ Summanden besitzt, folgt

$$\binom{2n}{n} \geq \frac{1}{2n+1} \cdot 4^n.$$

ii) Es sei $\frac{2}{3}n < p \leq n$.
In dem Produkt $(2n)! = 1 \cdot 2 \cdots 2n$ sind genau die Faktoren p und $2p$ durch p teilbar. Damit sind in

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

Zähler und Nenner genau durch p^2 teilbar. Damit ist $\binom{2n}{n}$ nicht durch p teilbar.

iii) Es sei $n < p \leq 2n$.
Dann gilt $p \nmid n!$ Von den Faktoren in $(2n)! = 1 \cdot 2 \cdots 2n$ ist genau p durch p teilbar. Also gilt

$$p | \binom{2n}{n} = \frac{(2n)!}{(n!)^2},$$

also $p^2 \nmid n$.

□

Lemma 3.3.2. *Für $n \in \mathbb{N}$ haben wir*

$$\pi(2n) - \pi(n) \leq 2 \log 2 \cdot \frac{n}{\log n}.$$

Beweis. Nach Lemma 3.3.1 ist

$$\prod_{n<p\leq 2n} p \leq 4^n,$$

also $n^{\pi(2n)-\pi(n)} \leq 4^n$. Logarithmieren liefert

$$\pi(2n) - \pi(n) \leq 2\log 2 \cdot \frac{n}{\log n}.$$

□

Satz 3.3.1. *Es sei $\epsilon > 0$. Dann gibt es ein $x_0 = x_0(\epsilon)$, so dass für alle $x \geq x_0$ gilt:*

$$\pi(x) \leq (2\log 2 + \epsilon) \cdot \frac{x}{\log x}.$$

Beweis. Wir wählen $\delta > 0$ beliebig klein. Es sei $l_0 \in \mathbb{N}$ so gewählt, dass

$$\frac{x}{2^{l_0+1}} < x^{1-\delta} \leq \frac{x}{2^{l_0}}$$

gilt. Dann ist

$$\pi(x) \leq \left(\pi(x) - \pi\left(\frac{x}{2}\right)\right) + \ldots + \left(\pi\left(\frac{x}{2^l}\right) - \pi\left(\frac{x}{2^{l+1}}\right)\right) + \ldots + \left(\pi\left(\frac{x}{2^{l_0-1}}\right) - \pi\left(\frac{x}{2^{l_0}}\right)\right) + 2x^{1-\delta} \quad (1)$$

Für jedes l mit $0 \leq l \leq l_0 - 1$ gibt es ein n_l, so dass

$$2(n_l - 1) < \frac{x}{2^l} \leq 2n_l. \quad (2)$$

Dann folgt

$$n_l - 1 < \frac{x}{2^{l+1}} \leq n_l. \quad (3)$$

Aus (2) und (3) folgt

$$\pi\left(\frac{x}{2^l}\right) - \pi\left(\frac{x}{2^{l+1}}\right) \leq \pi(2n_l) - \pi(n_l) + 2. \quad (4)$$

Aus Lemma 3.3.2 folgt

$$\pi(2n_l) - \pi(n_l) \leq 2\log 2 \cdot \frac{n_l}{\log n_l}.$$

Wegen $n_l \geq x^{1-\delta}$ folgt $\log n_l \geq (1-\delta) \cdot \log x$, also

$$\pi(2n_l) - \pi(n_l) \leq 2\log 2 \cdot \frac{n_l}{\log x}(1-\delta)^{-1} \leq \frac{x}{2^l \log x} \log 2 \cdot (1-\delta)^{-1} + 2. \quad (5)$$

Aus (1), (4) und (5) erhalten wir

$$\pi(x) \leq \frac{x}{\log x} \cdot \left(1 + \frac{1}{2} + \ldots\right)(1-\delta)^{-1} + 2l_0.$$

Es ist $l_0 \leq \frac{\log x}{\log 2}$. Daher folgt die Behauptung, falls δ klein genug und $x_0 = x_0(\epsilon)$ groß genug gewählt wird. □

Definition 3.3.1. Es sei $n \in \mathbb{N}$ und p eine Primzahl. Der Exponent $\eta(n,p)$ ist durch

$$\binom{2n}{n} = p^{\eta(n,p)} \cdot q(n)$$

mit $p \nmid q(n)$ definiert.

Lemma 3.3.3. *Es sei $n \in \mathbb{N}$.*

i) Für Primzahlen p mit $\sqrt{2n} < p \leq \frac{2}{3}n$ gilt $\eta(n,p) \in \{0,1\}$.

ii) Für Primzahlen p mit $p \leq \sqrt{2n}$ gilt $\eta(n,p) \leq 2\log(2n)$.

Beweis. i) Für alle $d \in \mathbb{N}$ ist

$$\frac{n}{d} = \left[\frac{n}{d}\right] + \vartheta$$

mit $0 \leq \vartheta < 1$, also

$$\frac{2n}{d} = 2\left[\frac{n}{d}\right] + 2\vartheta$$

und somit

$$0 \leq \left[\frac{2n}{d}\right] - 2\left[\frac{n}{d}\right] < 2,$$

also

$$\left[\frac{2n}{d}\right] - 2\left[\frac{n}{d}\right] \in \{0,1\}. \tag{1}$$

Von den Faktoren in $(2n)! = 1 \cdot 2 \cdots 2n$ sind die Vielfachen von p durch p, aber nicht durch p^2 teilbar. Damit ist

$$(2n)! = p^{\gamma(n,p)} \cdot r(n,p)$$

mit $ggT(r(n,p),(2n)!) = 1$ und $\gamma(n,p) = \left[\frac{2n}{p}\right]$.
Dieselbe Überlegung für $n!$ ergibt

$$n! = p^{\delta(n,p)} \cdot s(n,p)$$

mit $ggT(s(n,p),n!) = 1$ und $\delta(n,p) = \left[\frac{n}{p}\right]$. Damit ist nach (1)

$$\eta(n,p) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \in \{0,1\}.$$

ii) Für $m \in \mathbb{N}$, $r \in \mathbb{N}_0$ und einer Primzahl p setzen wir

$$\chi(m,p,r) = \begin{cases} 1, & \text{falls} \quad p^r | m \\ 0, & \text{sonst.} \end{cases}$$

Ist $m = p^{\beta(m,p)} \cdot l$ mit $p \nmid m$ und $l \geq \beta(m,p)$, so ist

$$\beta(m,p) = \sum_{r=1}^{l} \chi(m,p,r).$$

Damit ist für $l \geq 2\log(2n)$

$$\begin{aligned}(2n)! &= \prod_{p<2n} p^{\beta(2n,p)} = \exp\left(\sum_{p<2n} \log p \cdot \beta(2n,p)\right) = \exp\left(\sum_{p<2n} \log p \cdot \sum_{m\leq 2n} \beta(m,p)\right) \\ &= \exp\left(\sum_{p<2n} \log p \cdot \sum_{r=1}^{l} \cdot \sum_{m\leq 2n} \chi(m,p,r)\right) = \prod_{p<2n} \exp\left(\sum_{r=1}^{l} \log p \cdot \left[\frac{2n}{p^r}\right]\right) \\ &= \prod_{p<2n} p^{\left(\sum_{r=1}^{l}\left[\frac{2n}{p^r}\right]\right)}.\end{aligned}$$

Also ist $\beta(2n,p) = \sum_{r=1}^{l} \left[\frac{2n}{p^r}\right]$.

Genauso zeigt man

$$\beta(n,p) = \sum_{r=1}^{l} \left[\frac{n}{p^r}\right].$$

Damit ist

$$\eta(n,p) = \sum_{r \le 2\log(2n)} \left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] \right).$$

Die Behauptung folgt aus (1).

□

Lemma 3.3.4. *Es sei $\epsilon > 0$. Dann gibt es ein $n_0 = n_0(\epsilon) \in \mathbb{N}$, so dass für alle natürlichen Zahlen $n \ge n_0$ gilt:*

$$\pi(2n) - \pi(n) \ge \left(\frac{2}{3}\log 2 - \epsilon\right) \cdot \frac{n}{\log n}.$$

Beweis. Wir wählen eine natürliche Zahl n so, dass $2n \le x < 2n+2$ gilt. Nach Definition 3.3.1 ist

$$\binom{2n}{n} = \prod_{p<2n} p^{\eta(n,p)}. \tag{1}$$

Da nach Lemma 3.3.1 für $n < p \le 2n$ wir $\eta(n,p) = 1$ und für $\frac{2}{3}n < p \le n$ dann $\eta(n,p) = 0$ haben, folgt

$$\binom{2n}{n} = \prod\nolimits_1 \cdot \prod\nolimits_2 \cdot \prod\nolimits_3$$

mit

$$\prod\nolimits_1 = \prod_{p \le \sqrt{2n}} p^{\eta(n,p)}, \quad \prod\nolimits_2 = \prod_{\sqrt{2n} < p \le \frac{2}{3}n} p^{\eta(n,p)} \quad \text{und} \quad \prod\nolimits_3 = \prod_{n < p \le 2n} p. \tag{2}$$

Nach Lemma 3.3.3 ist $\eta(n,p) \le 2\log(2n)$ für $p \le \sqrt{2n}$ und daher

$$\prod\nolimits_1 \le \prod_{m \le \sqrt{2n}} m^{2\log(2n)} \le \sqrt{2n}^{2\sqrt{2n}\log(2n)} \le \exp\left(2\sqrt{2n}(\log(2n))^2\right) \ll \exp(\epsilon n), \tag{3}$$

falls n genügend groß ist.

Weiter ist nach Lemma 3.3.3 dann $\eta(n,p) \in \{0,1\}$, falls $\sqrt{2n} < p \le \frac{2}{3}n$, und daher

$$\prod\nolimits_2 \le \prod_{p \le \frac{2}{3}n} p \le \left(\frac{2}{3}n\right)^{\pi\left(\frac{2}{3}n\right)}. \tag{4}$$

Nach Satz 3.3.1 ist

$$\pi\left(\frac{2}{3}n\right) \le (2\log 2 + \epsilon) \cdot \frac{2n}{3\log\left(\frac{2}{3}n\right)},$$

falls n hinreichend groß ist. Wegen

$$\frac{1}{\log\left(\frac{2}{3}n\right)} \le (1+\epsilon) \cdot \frac{1}{\log n}$$

folgt für hinreichend große n

$$\pi\left(\frac{2}{3}n\right) \le \left(\frac{4}{3}\log 2 + 3\epsilon\right) \cdot \frac{n}{\log n},$$

und damit nach (4)

$$\prod_2 \leq \exp\left(\left(\frac{4}{3}\log 2 + 3\epsilon\right) \cdot \frac{n}{\log n} \cdot \log\left(\frac{2}{3}n\right)\right)$$

für hinreichend große n, bzw.

$$\prod_2 \leq \exp\left(\left(\frac{4}{3}\log 2 + 3\epsilon\right) \cdot n\right) \tag{5}$$

für hinreichend große n. Nach Lemma 3.3.1 ist

$$\binom{2n}{n} \geq \frac{1}{2n+1} \cdot 4^n$$

und damit nach (1)

$$\prod_1 \cdot \prod_2 \cdot \prod_3 \geq \frac{1}{2n+1} \cdot 4^n = \frac{1}{2n+1} \cdot \exp(2n \log 2) \geq \exp((2\log 2 - \epsilon) \cdot n) \tag{6}$$

für hinreichend große n. Aus (3), (5) und (6) folgt nun

$$\prod_3 = \prod_{n<p\leq 2n} p \geq \exp\left(\left(\frac{2}{3}\log 2 - 5\epsilon\right) \cdot n\right)$$

für hinreichend große n. Es ist

$$(2n)^{\pi(2n)-\pi(n)} \geq \prod_{n<p\leq 2n} p \geq \exp\left(\left(\frac{2}{3}\log 2 - 5\epsilon\right) \cdot n\right),$$

also

$$\pi(2n) - \pi(n) \geq \left(\frac{2}{3}\log 2 - 5\epsilon\right) \cdot \frac{n}{\log n + \log 2}.$$

Da $\epsilon > 0$ beliebig gewählt werden kann, folgt die Behauptung. □

Satz 3.3.2. *Es sei $\epsilon > 0$. Dann gibt es ein $x_1 = x_1(\epsilon) \in \mathbb{N}$, so dass für alle $x \geq x_1$ gilt:*

$$\pi(x) \geq \left(\frac{2}{3}\log 2 + \epsilon\right) \cdot \frac{x}{\log x}.$$

Beweis. Es sei $\delta > 0$ beliebig und $l_1 \in \mathbb{N}$ so gewählt, dass

$$\frac{x}{2^{l_1+1}} < x^{1-\delta} \leq \frac{x}{2^{l_1}}.$$

Dann ist

$$\pi(x) \geq \left(\pi(x) - \pi\left(\frac{x}{2}\right)\right) + \ldots + \left(\pi\left(\frac{x}{2^l}\right) - \pi\left(\frac{x}{2^{l+1}}\right)\right) + \ldots + \left(\pi\left(\frac{x}{2^{l_1-1}}\right) - \pi\left(\frac{x}{2^{l_1}}\right)\right). \tag{1}$$

Für jedes l mit $0 \leq l \leq l_1 - 1$ gibt es ein n_l, so dass

$$2(n_l - 1) < \frac{x}{2^l} \leq 2n_l.$$

Dann ist

$$\pi\left(\frac{x}{2^l}\right) - \pi\left(\frac{x}{2^{l+1}}\right) \geq \pi(2n_l) - \pi(n_l) - 1,$$

also nach Lemma 3.3.4

$$\begin{aligned}\pi\left(\frac{x}{2^l}\right) - \pi\left(\frac{x}{2^{l+1}}\right) &\geq \left(\frac{2}{3}\log 2 - \epsilon\right) \cdot \frac{n_l}{\log n_l} - 1 \\ &\geq \left(\frac{1}{3}\log 2 - 2\epsilon\right) \cdot \frac{x}{2^l} \cdot \left(\log \frac{x}{2^l}\right)^{-1} \geq \left(\frac{1}{3}\log 2 - 2\epsilon\right) \cdot \frac{x}{2^l \log x}\end{aligned}$$

für hinreichend große x.
Die Behauptung folgt, wenn wir (1) über alle l mit $1 \leq l \leq l_1$ summieren. □

Kapitel 4

Faktorisierungverfahren, Pollardsches Rho- Verfahren

4.1 Einleitung

Seit langem waren Mathematiker an der Frage interessiert, wie man Primfaktoren von zusammengesetzten Zahlen finden kann.
Der einfachste Algorithmus ist die Probedivision.
Sie beruht auf folgendem

Satz 4.1.1. *Es sei $N \in \mathbb{N}$ zusammengesetzt. Dann gibt es einen Primfaktor $p_1|N$ mit $p_1 \leq \sqrt{N}$.*

Beweis. Da N zusammengesetzt ist, gibt es Primzahlen $p_1 < p_2$ mit $p_1|N$ und $p_2|N$ oder eine Primzahl $p_1|N$ mit wenigstens $p_1^2|N$. In beiden Fällen folgt $N \geq p_1^2$, also $p_1 \leq \sqrt{N}$. □

Das Faktorisierungsverfahren verläuft also wie folgt:
Es sei $2 = p_1 < p_2 < \ldots$ die Folge der Primzahlen. Prüfe der Reihe nach, ob $p_i|N$ gilt. Sobald ein p_i mit $p_i|N$ gefunden ist, ist der Algorithmus beendet. Dann hat N den Faktor p_i.
Ist $p_i \nmid N$ für alle $p_i \leq \sqrt{N}$, so ist N eine Primzahl.

Beispiel 4.1.1. Ist 3107 zusammengesetzt? Wie lautet in diesem Fall der kleinste Primfaktor?

Wir überprüfen also die Reihe der Primzahlen nacheinander bis maximal $[\sqrt{3107}] = 55$.
Wegen $3107 \equiv 1 \bmod 2$ gilt $2 \nmid 3107$, wegen $Q(3107) = 11 \not\equiv 0 \bmod 3$ gilt $3 \nmid 3107$ und aufgrund von $3107 \not\equiv 0 \bmod 5$ gilt auch $5 \nmid 3107$.
Beim nächsten Primfaktor 7 wenden wir die Probedivision an und erhalten ebenfalls $7 \nmid 3107$, analoges folgt für $11 \nmid 3107$. Bei Division durch 13 sehen wir schließlich, dass diese Primzahl die Zahl 3107 teilt. Also ist 3107 zusammengesetzt und der kleinste Primfaktor ist 13 (der andere ist 239).

In neuerer Zeit sind Faktorisierungsalgorithmen entwickelt worden, die wesentlich schneller sind.
Das schnellste heute bekannte Faktorisierungsverfahren, das Zahlkörpersieb, benötigt zur Faktorisierung einer hinreichend großen Zahl N höchstens $\exp(C \cdot (\log N)^{1/3} (\log \log N)^{2/3})$ Rechenschritte, wobei die Konstante C der Ungleichung $C > \left(\frac{64}{9}\right)^{1/3}$ zu genügen hat.
Dieser Algorithmus basiert auf fortgeschrittenen theoretischen Grundlagen. Wir werden einen etwas älteren Faktorisierungsalgorithmus, das Pollardsche Rho- Verfahren besprechen. Es ist nicht ganz so schnell wie das Zahlkörpersieb, jedoch wesentlich schneller als die Probedivision und benötigt meistens nicht mehr als $C \cdot N^{1/4}$ Rechenschritte.

4.2 Das Pollardsche Rho- Verfahren

Es sei $N \in \mathbb{N}$ eine zusammengesetzte Zahl mit einem (zunächste unbekanntem) Primteiler p, und es sei $F\colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ eine beliebige Funktion.
Wir betrachten die rekursiv definierte Folge von Elementen $a_n \in \mathbb{Z}/N\mathbb{Z}$ mit $a_0 \in \mathbb{Z}/N\mathbb{Z}$ (Anfangswert) und $a_{j+1} = F(a_j)$ (Rekursion). Da die Folge nur endlich viele Werte annehmen kann, müssen sich die Werte ab einem bestimmten Punkt wiederholen, d.h. es gibt m und $l = m + k$ mit $a_m = a_l$. Wegen der Rekursion gilt dann $a_n = a_{n+k}$ für alle $n \geq m$, d.h. die Folge hat die Periode k.

Zu der bekannten Folge (a_n) auf $\mathbb{Z}/N\mathbb{Z}$ gehört eine "verborgene" Folge (b_n) mit $b_n \in \mathbb{Z}/p\mathbb{Z}$, die mittels des "verborgenen" Primfaktors p von N aus (a_n) konstruiert wird.
Sie ist durch $a_n \mod N \subset b_n \mod p$ definiert.

Beispiel 4.2.1. Es sei $N = 35 = 5 \cdot 7$ und $p = 5$. Weiter betrachten wir $F\colon x \to x^2 + 1$ und $a_0 = 2$. Dann ist

n	a_n	b_n
0	2 mod 35	2 mod 5
1	5 mod 35	0 mod 5
2	26 mod 35	1 mod 5
3	12 mod 35	2 mod 5
4	5 mod 35	0 mod 5

Die Folge (b_n) hat die Periode 3, d.h. es gilt $b_{n+3} = b_n$. Daraus folgt, dass $a_{n+3} - a_n$ den Faktor 5 enthält.
Dieser (im allgemeinen unbekannte) Primfaktor 5 kann nun z. B. dadurch entdeckt werden, indem man $ggT(a_{n+3} - a_n, N)$ bestimmt. Es ergibt sich etwa $ggT(a_3 - a_0, 35) = ggT(12 - 2, 35) = 5$.

Das ursprüngliche Pollardsche Rho- Verfahren bestand darin, für sämtliche Paare (i, j) die Zahl $ggT(a_i - a_j, N)$ zu berechnen.

Wir beschreiben nun das verfeinerte Pollardsche Rho- Verfahren:

Es sei $N \in \mathbb{N}$ und $F\colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ eine beliebige Funktion. (Anmerkung: In der Praxis wird meist $F(x \mod N) = (x^2 + c) \mod N$ genommen.) Es sei $x_0 \in \mathbb{Z}/N\mathbb{Z}$ beliebig. Bestimme die beiden Folgen (x_i), (y_i) durch $y_0 = x_0$ und $x_{i+1} = F(x_i)$ sowie $y_{i+1} = F(F(y_i))$ und daraus dann $d_i = ggT(y_i - x_i, N)$. Fahre solange damit fort, bis ein i mit $d_i \neq 1$ gefunden worden ist.
Ist $d_i = N$, so ist der Versuch gescheitert. Wiederhole ihn dann mit einem neuen Anfangswert x_0.
Ist $1 < d_i < N$, so ist der nichttriviale Faktor d_i gefunden.

Beispiel 4.2.2. Es sei $N = 41 \cdot 53 = 2173$ und $F(x \mod N) = (x^2 + 1) \mod N$ sowie $x_0 = 0$. Wir erhalten

i	x_i	y_i	$y_i - x_i$	$d_i = ggT(y_i - x_i, N)$
0	0	0	0	2173
1	1	2	1	1
2	2	26	24	1
3	5	2000	1995	1
4	26	862	836	1
5	677	1604	927	1
6	2000	226	399	1
7	1681	1763	82	41.

Kapitel 5

Potenzreste, Quadratisches Reziprozitätsgesetz

5.1 Ordnung, Primitivwurzel, Potenzreste

Definition 5.1.1. Es sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ und $ggT(a,m) = 1$. Unter der Ordnung von $a \bmod m$ (Schreibweise: $\operatorname{ord}_m a$) versteht man

$$\operatorname{ord}_m a := \min\{k \in \mathbb{N} \colon a^k \equiv 1 \bmod m\}.$$

Beispiel 5.1.1. Aus der Tafel

k	1	2	3
$2^k \bmod 7$	2	4	1

ergibt sich $\operatorname{ord}_7 2 = 3$.

Satz 5.1.1. *Es gilt*

i) $a^k \equiv 1 \bmod m \Leftrightarrow (\operatorname{ord}_m a) | k$

ii) $a^k \equiv a^l \bmod m \Leftrightarrow k \equiv l \bmod \operatorname{ord}_m a$

iii) $(\operatorname{ord}_m a) | \varphi(m)$.

Beispiel 5.1.2. Wir wollen $\operatorname{ord}_{89} 2$ bestimmen. Mittels der Gleichung $2^{11} = 23 \cdot 89 + 1$ gilt dann $2^{11} \equiv 1 \bmod 89$. Also ist die Ordnung von 2 modulo 89 kleiner gleich 11. Da sie ebenfalls ein Teiler von $\varphi(89) = 88$ sein muss, kommen als kleinere Ordnungen nur 2,4 oder 8 in Frage. Es gilt aber $2^2 = 4 \not\equiv 1 \bmod 89$, $2^4 = 16 \not\equiv 1 \bmod 89$ und $2^8 = 256 \equiv -11 \not\equiv 1 \bmod 89$. Daher gilt $\operatorname{ord}_{89} 2 = 11$.

Definition 5.1.2. Es sei $m \in \mathbb{N}$.
Eine ganze Zahl r heißt Primitivwurzel modulo m, wenn $\operatorname{ord}_m r = \varphi(m)$ ist.

Satz 5.1.2. *Eine Primitivwurzel* $r \bmod m$ *existiert genau dann, wenn* $m = 1, 2, 4$ *oder wenn* $m = p^\gamma$ *oder* $m = 2p^\gamma$ *für eine Primzahl* $p > 2$ *und* $\gamma \in \mathbb{N}$ *gilt.*

Beweis. ohne Beweis. □

Satz 5.1.3. *Ist* r *eine Primitivwurzel modulo* m*, so bilden die Potenzen* $\{r, \ldots, r^{\varphi(m)}\}$ *ein reduziertes Restsystem modulo* m*.*

Beweis. ohne Beweis. □

Definition 5.1.3. Es sei $k, m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $ggT(a, m) = 1$. Die Zahl a heißt dann k- ter Potenzrest modulo m, falls die Kongruenz

$$x^k \equiv a \bmod m$$

lösbar ist, andernfalls ein k- ter Potenznichtrest.
Im Fall $k = 2$ spricht man von quadratischen Resten bzw. Nichtresten.

Satz 5.1.4. *Der Modul $m \in \mathbb{N}$ besitze eine Primitivwurzel. Weiter sei $k \in \mathbb{N}$ und $d = ggT(k, \varphi(m))$. Die Anzahl der k- ten Potenzreste modulo m beträgt $\frac{\varphi(m)}{d}$. Ist $a \in \mathbb{Z}$ ein k- ter Potenzrest modulo m, d.h. gilt $ggT(a, m) = 1$ und*

$$x^k \equiv a \bmod m \qquad (*)$$

lösbar, so hat $(*)$ genau d Lösungen in $x \bmod m$.
Zudem ist $a \in \mathbb{Z}$ genau dann ein k- ter Potenzrest modulo m, wenn

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \bmod m$$

ist.

Beweis. Es sei r eine Primitivwurzel modulo m.
Für jedes Paar (x, a) von ganzen Zahlen mit $ggT(x, m) = ggT(a, m) = 1$ gibt es nach Satz 5.1.1 modulo $\varphi(m)$ eindeutig bestimmte Zahlen y, j mit

$$x \equiv r^y \bmod m \quad \text{und} \quad a \equiv r^j \bmod m.$$

Die Lösungen $x \bmod m$ entsprechen umkehrbar eindeutig den Lösungen $y \bmod \varphi(m)$ der linearen Kongruenz

$$ky \equiv j \bmod \varphi(m). \qquad (**)$$

Weiter ist $(**)$ genau dann lösbar, wenn $d|j$ gilt. Es gibt dann d Lösungen modulo $\varphi(m)$:

$$d|j \Leftrightarrow \varphi(m) \Big| \left(j \cdot \frac{\varphi(m)}{d} \right) \Leftrightarrow (r^j)^{\varphi(m)/d} \equiv 1 \bmod m.$$

Die Lösbarkeit von $(*)$ ist also äquivalent zu $a^{\varphi(m)/d} \equiv 1 \bmod m$.
Es gibt $\frac{\varphi(m)}{d}$ Werte von j, welche die Bedingungen $d|j$ erfüllen. □

Wir formulieren den Spezialfall für $k = 2$, d.h. quadratische Reste, und $m = p > 2$ sei eine ungerade Primzahl:

Korollar 5.1.1. *In diesem Fall gibt es genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste. Es gilt das Eulersche Kriterium:*
Die ganze Zahl a ist genau dann quadratischer Rest modulo p, wenn $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ ist.
Die ganze Zahl a ist genau dann quadratischer Nichtrest modulo p, wenn $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ ist.

Beispiel 5.1.3. Es sei $p = 11$. Bestimme die quadratischen Reste und Nichtreste modulo p.
Lösung:
Wegen $x^2 \equiv (-x)^2 \bmod p$ genügt es, die Quadrate modulo 11 der Zahlen x mit $1 \leq x \leq \frac{11-1}{2} = 5$ zu berechnen. Man erhält

x	1	2	3	4	5
$x^2 \bmod 11$	1	4	9	5	3

Die quadratischen Reste sind also 1,3,4,5,9 modulo 11 und die Nichtreste 2,6,7,8,10 modulo 11.

5.2 Das quadratische Reziprozitätsgesetz

Wir wollen nun quadratische Reste nach Primzahlmoduln genauer untersuchen. Insbesondere werden wir einen schnellen Algorithmus vorstellen, der es erlaubt zu entscheiden, ob eine gegebene Zahl $a \in \mathbb{Z}$ ein quadratischer Rest modulo einer gegebenen Primzahl p ist oder nicht.

Definition 5.2.1. (Legendre- Symbol)
Es sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann setzen wir

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

Dabei heißt $\left(\frac{a}{p}\right)$ das Legendre- Symbol.

Beispiel 5.2.1. Beispiel 5.1.3 ergibt

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

und

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Satz 5.2.1. *Es sei p eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Dann gilt*

i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

ii) $\left(\frac{a^2}{p}\right) = 1$

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

iv) $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Beweis. Teil (iii) folgt nach dem Eulerschen Kriterium in Korollar 5.1.1. Aus (iii) folgen unmittelbar auch die Teile (i) und (ii). □

Satz 5.2.2. *(quadratisches Reziprozitätsgesetz)*
Es seien p und q ungerade Primzahlen. Dann gilt

i) $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Ergänzungssätze:

ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Beweis. ohne Beweis. □

Man rechnet leicht nach, dass aus Satz 5.2.2 folgendes Korollar folgt:

Korollar 5.2.1. *Es seien p und q ungerade Primzahlen.*

i) Ist $p \equiv 1 \bmod 4$ oder $q \equiv 1 \bmod 4$, so ist $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, d.h. p ist genau dann ein quadratischer Rest modulo q, wenn q ein quadratischer Rest modulo p ist.
Sind $p \equiv 3 \bmod 4$ und $q \equiv 3 \bmod 4$, so ist p genau dann ein quadratischer Rest modulo q, wenn q ein quadratischer Nichtrest modulo p ist.

ii) Es ist 2 genau dann ein quadratischer Rest modulo p, wenn $p \equiv \pm 1 \bmod 8$ gilt, bzw. genau dann ein quadratischer Nichtrest modulo p, wenn $p \equiv \pm 3 \bmod 8$ ist.

iii) Weiter ist -1 genau dann ein quadratischer Rest modulo p, wenn $p \equiv 1 \bmod 4$ ist und genau dann ein quadratischer Nichtrest modulo p, wenn $p \equiv 3 \bmod 4$ ist.

Das quadratische Reziprozitätsgesetz erlaubt es nun, schnell zu entscheiden, ob eine gegebene Kongruenz $x^2 \equiv a \bmod p$ mit einer Primzahl p lösbar ist. Es ist jedoch kein Mittel, diese Lösung zu finden.

Beispiel 5.2.2. Entscheide, ob die Kongruenz $x^2 \equiv 641 \bmod 2011$ lösbar ist.

Lösung:
Es gilt

$$\begin{aligned}\left(\frac{641}{2011}\right) &\underset{641\equiv 1 \bmod 4}{=} \left(\frac{2011}{641}\right) \underset{2011=3\cdot 641+88}{=} \left(\frac{88}{641}\right) \underset{88=2^3\cdot 11}{=} \left(\frac{2}{641}\right)^3 \cdot \left(\frac{11}{641}\right) \\ &\underset{641\equiv 1 \bmod 8}{=} \left(\frac{11}{641}\right) \underset{641\equiv 1 \bmod 4}{=} \left(\frac{641}{11}\right) \underset{641=58\cdot 11+3}{=} \left(\frac{3}{11}\right) \underset{\substack{11\equiv 3 \bmod 4\\ 3\equiv 3 \bmod 4}}{=} -\left(\frac{11}{3}\right) \\ &\underset{11=3^2+2}{=} -\left(\frac{2}{3}\right) \underset{3\equiv 3 \bmod 8}{=} -(-1) = 1.\end{aligned}$$

Also gilt $\left(\frac{641}{2011}\right) = 1$. Die Kongruenz $x^2 \equiv 641 \bmod 2011$ ist damit lösbar.
Nach dem Eulerschen Kriterium gilt damit $641^{\frac{2011-1}{2}} \equiv 641^{1005} \equiv 1 \bmod 2011$.

Auch die Lösbarkeit nach zusammengesetzten Moduln kann mit dem quadratischen Reziprozitätsgesetz entschieden werden. Die Kongruenz $x^2 \equiv a \bmod pq$ ist nach dem Chinesischen Restsatz genau dann lösbar, wenn jede der beiden Kongruenzen $x^2 \equiv a \bmod p$ und $x^2 \equiv a \bmod q$ lösbar ist.

Beispiel 5.2.3. Es ist $851 = 23 \cdot 37$. Entscheide, ob die Kongruenz $x^2 \equiv 41 \bmod 851$ lösbar ist.

Lösung:
Es ist

$$\left(\frac{41}{23}\right) = \left(\frac{18}{23}\right) = \left(\frac{2}{23}\right) \cdot \left(\frac{3}{23}\right)^2 \underset{23\equiv -1 \bmod 8}{=} 1$$

und

$$\left(\frac{41}{37}\right) = \left(\frac{4}{37}\right) = \left(\frac{2}{37}\right)^2 = 1.$$

Die Kongruenzen $x^2 \equiv 41 \bmod 23$ und $x^2 \equiv 41 \bmod 37$ sind also beide lösbar. Nach dem Chinesischen Restsatz lässt sich auch eine Lösung modulo 851 gewinnen.

Beispiel 5.2.4. Es ist $341 = 11 \cdot 31$. Entscheide, ob die Kongruenz $x^2 \equiv -28 \bmod 341$ lösbar ist.

Lösung:
Die Kongruenz $x^2 \equiv -28 \bmod 341$ ist äquivalent zum System

$$\begin{cases} x^2 \equiv 5 \bmod 11 \\ x^2 \equiv 3 \bmod 31 \end{cases}$$

Es ist

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$$

und

$$\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Die erste Kongruenz ist also lösbar, die zweite nicht. Damit ist $x^2 \equiv -28 \bmod 341$ unlösbar.

Kapitel 6

Anwendungen in der Kryptologie, Primzahltests

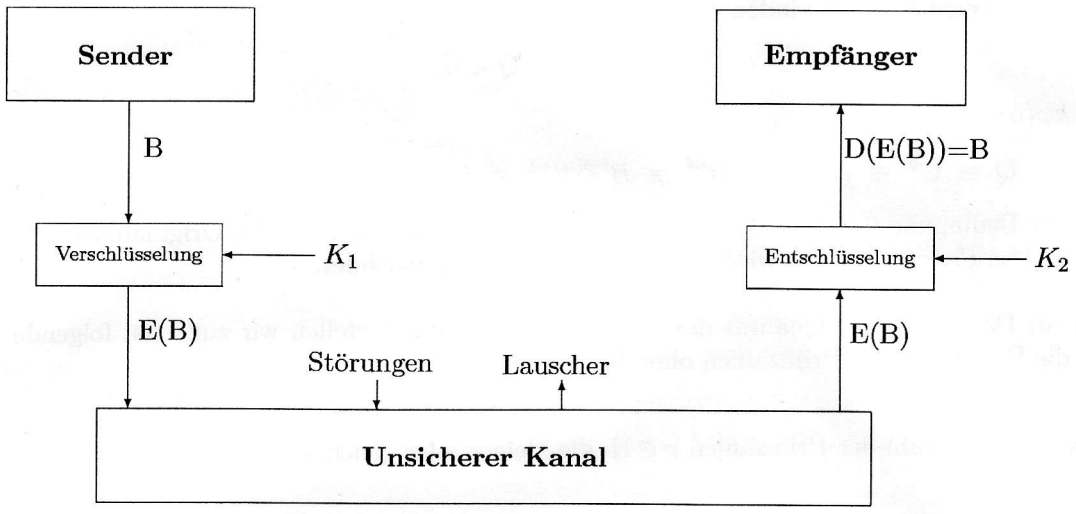
6.1 Public- Key- Codes, RSA- Verfahren

Der Gegenstand der Kryptologie ist die Übermittlung geheimer Botschaften unter Verwendung von Codes. Die Kryptologie besteht aus zwei Teilgebieten:

i) In der Kryptographie wird der Entwurf von Geheimcodes untersucht.

ii) In der Kryptoanalyse wird nach Methoden gesucht, diese zu knacken.

Bei der Übermittlung einer geheimen Nachricht wird zunächst eine vorliegende Botschaft B in einen Geheimtext $E(B)$ umgeändert. Dieses Verfahren für eine solche Umänderung bezeichnet man als Verschlüsselung E (von eng. "encryption"). Die verschlüsselte Botschaft wird dann an den Empfänger gesandt. Dieser benutzt ein Entschlüsselungsverfahren D (von engl. "decryption"), um dann die ursprüngliche Botschaft zurück zu gewinnen.
Diese sogenannten Chiffrierverfahren sind öffentlich bekannt. Das Verschlüsselungsverfahren wird dabei meist durch einen Schlüssel K_1 gesteuert, die Entschlüsselung durch einen Schlüssel K_2.
Die Übermittlung erfolgt also nach folgendem Schema:



Ziel der Chiffrierverfahren ist es, die Nachricht B vor dritten Personen geheimzuhalten und gegen Veränderungen bei der Übertragung zu schützen. Dazu ist es erforderlich, den Schlüssel K_2 vor eventuellen Lauschern geheimzuhalten. Bei den konventionellen Verfahren (den symmetrischen Chiffrierverfahren) ist es möglich, das Entschlüsselungsverfahren aus dem Verschlüsselungsverfahren zu gewinnen (meist sind diese sogar identisch, und es gilt: $K_1 = K_2$). Also war auch K_1 geheimzuhalten.
In gewissen Umständen ist es jedoch wünschenswert, auf die Geheimhaltung von K_1 zu verzichten. Haben wir zum Beispiel ein Netzwerk von sehr vielen Teilnehmern, so ist es wünschenswert, dass jeder Teilnehmer T_i an jeden anderen Teilnehmer T_j eine Botschaft schicken kann, ohne sich zunächst direkt bei T_j nach dem Schlüssel zu erkundigen. Dazu veröffentlicht jeder Teilnehmer T_j seinen Schlüssel S_j für die Verschlüsselung in einer Art Telefonbuch. Will ein anderer Teilnehmer T_i eine Botschaft an T_j senden, so benutzt er dazu den Schlüssel S_j. Es muss also ein System gefunden werden, bei dem es unmöglich ist, den Schlüssel für die Entschlüsselung aus S_j zu berechnen.
Einen solchen Code nennt man Public- Key- Code oder auch asymmetrisches Chiffrierverfahren.
Wir werden das RSA- System (benannt nach Rivest, Shamir und Adleman, die es 1978 vorgeschlagen haben) betrachten.

Der öffentliche Schlüssel $S = (e, n)$ ist ein Zahlenpaar bestehend aus dem Exponenten $e \in \mathbb{N}$ und dem Modul n, so dass $n = p \cdot q$ das Produkt zweier verschiedener Primzahlen ist und außerdem auch $ggT(e, \varphi(n)) = 1$ gilt. Während e und n allgemein zugänglich sind, ist die Faktorisierung $n = p \cdot q$ und auch $\varphi(n)$ nur dem Empfänger bekannt, dem der öffentliche Schlüssel gehört.
Das Verfahren gilt als sicher, wenn p und q groß genug gewählt sind. Aktuelle Schlüssel (Stand: 2005) sind von der Größenordnung 2^{1024}.

Wir beschreiben nun das Verschlüsselungsverfahren:
Jeder Buchstabe der Nachricht wird nach einem Standardverfahren in eine Ziffernfolge umgewandelt. Eine feste Anzahl dieser Ziffernfolgen werden aneinander gehängt, so dass sie eine Zahl $B < n$ bilden. Dabei soll B jedoch von derselben Größenordnung wie n sein, d.h. in etwa die gleiche Anzahl an Stellen besitzen. Ist die Botschaft länger, kann sie in einzelne Blöcke unterteilt werden. Der Absender berechnet dann die eindeutig bestimmte Zahl C mit $C \equiv B^e \bmod n$ mit $0 < C < n$. Die Zahl C ist der Geheimtext, der an den Empfänger gesendet wird.

Wir kommen zur Beschreibung des nur dem Empfänger bekannten Entschlüsselungsverfahrens:
Da der Empfänger die Faktorisierung $n = p \cdot q$ kennt, kann er auch $\varphi(n) = (p-1) \cdot (q-1)$ ausrechnen. Wegen $ggT(e, \varphi(n)) = 1$ kann der Empfänger ein $d > 0$ berechnen, so dass $ed \equiv 1 \bmod \varphi(n)$ ist. Erhält er den Geheimtext $C \equiv B^e \bmod n$, so berechnet er die eindeutig bestimmte Zahl Q mit $Q \equiv C^d \bmod n$ mit $0 < Q < n$.
Dann ist $ed = k\varphi(n) + 1$ für ein $k \in \mathbb{N}_0$, also gilt

$$Q \equiv C^d \equiv (B^e)^d \equiv B^{ed} \equiv B^{k\varphi(n)+1} \equiv \left(B^{\varphi(n)}\right)^k \cdot B \equiv B \bmod n.$$

Also ist wegen der Bedingung $0 < Q < n$ dann $Q = B$, d.h. der Empfänger hat die Originalnachricht zurückgewonnen. Das Paar $T = (d, n)$ wird als privater Schlüssel bezeichnet.

Wir kommen nun zur Diskussion der Qualität des RSA- Systems:

i) Ein öffentlicher Schlüssel (e, n) ist leicht zu konstruieren. Dazu wählt man irgendeine Zahl p der Größenordnung $\sim 2^k$ nach dem Zufallsprinzip. Die Wahrscheinlichkeit, dass p eine Primzahl ist, beträgt nach dem Primzahlsatz

$$\frac{\pi(2^k)}{2^k} \sim \frac{1}{\log(2^k)} \sim \frac{1}{k}.$$

Ein Rechner benötigt daher im Durchschnitt k Versuche, um eine Primzahl p der gewünschten Größenordnung zu finden. Der Teilnehmer T berechnet zwei verschiedene Primzahlen p und q auf diese Weise und veröffentlicht den Schlüssel (e, n) mit $n = p \cdot q$.

ii) Verschlüsselung und Entschlüsselung können leicht mit Computern durchgeführt werden, es wird nur die Potenzierung mit einer natürlichen Zahl benötigt, die modulo n effiizient durch wiederholtes Quadrieren durchgeführt werden kann. Das Inverse d zu e kann mit dem Euklidischen Algorithmus berechnet werden, wenn p und q bekannt sind.

iii) Es gibt zur Zeit kein Verfahren, das die Originalnachricht B aus $C \equiv B^e \bmod n$ ohne Kenntnis von $\varphi(n)$ oder der Faktorisierung $n = p \cdot q$, welche die Kenntnis von $\varphi(n) = (p-1) \cdot (q-1)$ impliziert, mit akzeptablem Aufwand ausrechnen kann.

6.2 Primzahltests

Aus dem kleinen Satz von Fermat (Satz 2.8.3) wissen wir bereits, dass für eine Primzahl n und ein beliebiges $a \in \mathbb{Z}$, das nicht durch n teilbar ist, die Kongruenz

$$a^{n-1} \equiv 1 \bmod n$$

gilt.
Wenn wir umgekehrt eine Zahl a finden können, so dass $a^{n-1} \not\equiv 1 \bmod n$ ist, so wissen wir bereits, dass n zusammengesetzt ist.

Beispiel 6.2.1. Es sei $n = 63$ und $a = 2$. Es ist $2^6 = 64 \equiv 1 \bmod n$. Es ist $1 < 2^l < 63$ für $1 \leq l \leq 5$, weswegen $\operatorname{ord}_{63} 2 = 6$ ist. Also gilt nach Satz 5.1.1

$$2^{62} \equiv 2^2 \equiv 4 \bmod 63.$$

Insbesondere ist $a^{n-1} \not\equiv 1 \bmod n$ für $a = 2$, weshalb 63 zusammengesetzt ist.

Dies ist natürlich nicht der einfachste Weg, um zu zeigen, dass $n = 63$ zusammengesetzt ist, da die Faktoren 3 und 7 sehr schnell gefunden werden können. Doch ist die Methode für größere Werte von n die erfolgreichste. Es wäre wünschenswert, wenn durch Überprüfen der Kongruenz auch gezeigt werden könnte, dass eine Zahl n auch ein Primzahl ist. Dies ist leider nicht möglich, da die Umkehrung des kleinen Satzes von Fermat falsch ist.

Beispiel 6.2.2. Es sei $n = 341 = 11 \cdot 31$.
Nach den kleinen Satz von Fermat ist $2^{10} \equiv 1 \bmod 11$, also $2^{340} \equiv 1 \bmod 11$.
Außerdem ist $2^{340} = \left(2^5\right)^{68} \equiv 1 \bmod 31$, also folgt $2^{340} \equiv 1 \bmod 341$, obwohl 341 keine Primzahl ist.

Definition 6.2.1. Es sei $a \in \mathbb{N}$.
Ist n zusammengesetzt und gilt $a^{n-1} \equiv 1 \bmod n$, so heißt n eine Pseudoprimzahl zur Basis a.

Pseudoprimzahlen bzgl. einer Basis a sind viel seltener als Primzahlen.
Insbesondere gibt es 455 025 512 Primzahlen kleiner gleich 10^{10}, aber nur 14884 Pseudoprimzahlen kleiner gleich 10^{10} zur Basis 2. Dennoch gibt es zu jeder Basis unendlich viele Pseudoprimzahlen.

Satz 6.2.1. *Es gibt unendlich viele Pseudoprimzahlen zur Basis 2.*

Beweis. Übungen. □

Folglich ist es nicht immer möglich, durch Überprüfen einer einzelnen Kongruenz $a^{n-1} \equiv 1 \bmod n$ zu zeigen, dass n zusammengesetzt ist. Eine weitergehende Idee besteht darin, die Kongruenz für verschiedene Basen a zu testen. So ist $n = 341$ beispielsweise eine Pseudoprimzahl zur Basis 2, jedoch keine Pseudoprimzahl zur Basis 3, da $3^{340} \equiv 56 \not\equiv 1 \bmod 341$ ist. Der Test mit der Basis $a = 3$ zeigt also, dass 341 zusammengesetzt ist. Es gibt jedoch auch Zahlen, die Pseudoprimzahlen bzgl. jeder Basis sind.

Definition 6.2.2. Eine zusammengesetzte Zahl $n \in \mathbb{N}$, für die $a^{n-1} \equiv 1 \bmod n$ für alle natürlichen Zahlen a mit $ggT(a,n) = 1$ gilt, heißt Carmichael- Zahl.

Es wurde 1992 von Alford, Granville und Pomerance gezeigt, dass es unendlich viele Carmichael-Zahlen gibt.

Satz 6.2.2. *Eine Zahl $n \in \mathbb{N}$ ist genau dann eine eine Carmichael- Zahl, wenn $n = p_1 \cdot p_2 \cdots p_r$ mit $r \geq 3$ und paarweise verschiedenen ungeraden Primzahlen p_i ist, für die $(p_i - 1)|(n-1)$ für $i = 1, \ldots, r$ gilt.*

Beweis. Übungen. □

Wir kommen nun zur Beschreibung von Primzahltests:
Ist n eine Primzahl, so folgt aus der Kongruenz $a^{n-1} \equiv 1 \bmod n$ die Aussage $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$.
Man kann also versuchen zu zeigen, dass n zusammengesetzt ist, indem man diese Kongruenz überprüft.

Beispiel 6.2.3. Es sei $n = 561 = 3 \cdot 11 \cdot 17$.
Nach Satz 6.2.2 ist n wegen $2|560$, $10|560$ und $16|560$ eine Carmichael- Zahl.
Also ist insbesondere $5^n \equiv 5 \bmod n$. Es ist jedoch

$$5^{\frac{561-1}{2}} = 5^{280} \equiv 67 \bmod 561.$$

Dies zeigt, dass $n = 561$ zusammengesetzt ist.

Definition 6.2.3. Es sei n eine natürliche Zahl mit $n - 1 = 2^s \cdot t$ mit $s \in \mathbb{N}_0$ und t eine ungerade natürliche Zahl. Wir sagen, n besteht den Test von Miller für die Basis a, wenn entweder $a^t \equiv 1 \bmod n$ oder $a^{2^j t} \equiv -1 \bmod n$ für ein j mit $0 \leq j \leq s - 1$ gilt.

Satz 6.2.3. *Ist n prim und a eine natürliche Zahl mit $n \nmid a$, dann besteht n den Test von Miller für die Basis a.*

Beweis. Es sei $n - 1 = 2^s \cdot t$ mit $s \in \mathbb{N}_0$ und t eine ungerade natürliche Zahl. Wir setzen

$$x_k = a^{\frac{n-1}{2^k}} = a^{2^{s-k}t}$$

für $k = 0, 1, 2, \ldots, s$.
Da n eine Primzahl ist, gilt nach dem kleinen Fermat $x_0 = a^{n-1} \equiv 1 \bmod n$.
Aus $x_1^2 = a^{n-1} \equiv 1 \bmod n$ folgt $n|(x_1^2 - 1) = (x_1 + 1) \cdot (x_1 - 1)$ also $x_1 \equiv -1 \bmod n$ oder $x_1 \equiv 1 \bmod n$.
Ist $x_1 \equiv 1 \bmod n$, so gilt wegen $x_2^2 \equiv x_1 \equiv 1 \bmod n$ nun $x_2 \equiv -1 \bmod n$ oder $x_2 \equiv 1 \bmod n$.
Induktiv folgt aus $x_0 \equiv x_1 \equiv \ldots \equiv 1 \bmod n$ dann $x_{k+1} \equiv -1 \bmod n$ oder $x_{k+1} \equiv 1 \bmod n$.
Es gilt also entweder $x_k \equiv 1 \bmod n$ für alle $k = 0, \ldots, s$ oder $x_k \equiv -1 \bmod n$ für ein k.
Damit besteht n den Test von Miller zur Basis a. □

Dies führt zu folgender Definition:

Definition 6.2.4. Ist n zusammengesetzt und besteht dennoch den Test von Miller für eine Basis a, so heißt n eine starke Pseudoprimzahl zur Basis a.

Obwohl starke Pseudoprimzahlen sehr selten sind, gibt es dennoch wiederum unendlich viele zu jeder Basis a.
Es gibt jedoch kein Analogon der Carmichael- Zahlen zu starken Pseudoprimzahlen: ist n zusammengesetzt, so kann man immer eine Basis a finden, für die n den Test von Miller nicht besteht, für die also n keine starke Pseudoprimzahl ist.

Satz 6.2.4. *Es sei n eine ungerade zusammengesetzte Zahl.*
Dann besteht n den Test von Miller für höchstens $\frac{n-1}{4}$ Basen a mit $1 \leq a \leq n-1$.

Beweis. Wir setzen $n-1 = 2^s \cdot t$ mit $s \in \mathbb{N}_0$ und $t \in \mathbb{N}$ ungerade.
Falls n eine starke Pseudoprimzahl zur Basis a ist, gilt $a^{n-1} \equiv 1 \bmod n$. Es sei

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \tag{1}$$

die Primfaktorzerlegung von n. Nach den Sätzen 5.1.2 und 5.1.4 hat die Kongruenz

$$x^{n-1} \equiv 1 \bmod p_j^{e_j}$$

genau $N_j = ggT(n-1, p_j^{e_j-1}(p_j-1)) = ggT(n-1, p_j-1)$ Lösungen modulo $p_j^{e_j}$.
Nach dem Chinesischen Restsatz gibt es daher genau

$$N = \prod_{j=1}^{r} ggT(n-1, p_j-1) = \prod_{j=1}^{r} N_j$$

inkongruente Lösungen von $x^{n-1} \equiv 1 \bmod n$.

Fall 1:
In (1) sei $\alpha_k \geq 2$ für mindestens ein k. Es ist

$$\frac{p_k-1}{p_k^{\alpha_k}} = \frac{1}{p_k^{\alpha_k-1}} - \frac{1}{p_k^{\alpha_k}} \leq \frac{1}{3} - \frac{1}{3^2} = \frac{2}{9}.$$

Daher ist

$$N = \prod_{j=1}^{r} ggT(n-1, p_j-1) \leq \frac{2}{9} \cdot p_k^{e_k} \prod_{\substack{j=1 \\ j \neq k}}^{r} p_j \leq \frac{2}{9} \cdot n.$$

Da $\frac{2}{9}n \leq \frac{1}{4}(n-1)$ für $n \geq 9$ ist, folgt $N \leq \frac{n-1}{4}$.
Es gibt also höchstens $\frac{n-1}{4}$ Zahlen a mit $1 \leq a \leq n$, für die n eine starke Pseudoprimzahl zur Basis a ist.

Fall 2:
Es sei $n = p_1 \cdots p_r$ mit ungeraden und paarweise verschiedenen p_i. Es sei $p_i - 1 = 2^{s_i} t_i$ für $i = 1, 2, \ldots, r$.
Wir numerieren die p_i so, dass $s_1 \leq s_2 \leq \ldots \leq s_r$ gilt und betrachten die Kongruenz

$$x^{2^j t} \equiv -1 \bmod p_i. \tag{2}$$

Es sei $d_i = ggT(2^j t, p_i - 1) = ggT(2^j, 2^{s_i}) \cdot ggT(t, t_i)$. Nach Satz 5.1.4 ist -1 genau dann ein $(2^j t)$- ter Potenzrest modulo p_i, wenn

$$(-1)^{\frac{p_i-1}{d_i}} \equiv 1 \bmod p_i$$

ist, also wenn $0 \leq j \leq s_i - 1$ ist. Die Kongruenz (2) hat dann $d_i = 2^j T_i$ Lösungen modulo p_i mit $T_i = ggT(t, t_i)$. Nach dem Chinesischen Restsatz gibt es $T_1 \cdot T_2 \cdots T_r$ inkongruente Lösungen von $x^t \equiv 1 \bmod n$ und $2^{jr} T_1 \cdots T_r$ inkongruente Lösungen von $x^{2^j t} \equiv -1 \bmod n$, wenn $0 \leq j \leq s_1 - 1$ ist.
Es gibt daher insgesamt höchstens

$$T_1 \cdot T_2 \cdots T_r \cdot \left(1 + \sum_{j=1}^{s_1-1} 2^{jr}\right) = T_1 \cdot T_2 \cdots T_r \cdot \left(1 + \frac{2^{rs_1}-1}{2^r-1}\right) \tag{3}$$

Zahlen a mit $1 \leq a \leq n-1$, für die n eine starke Pseudoprimzahl ist.

Wir zeigen im folgenden, dass der Ausdruck (3) nicht größer als $\frac{\varphi(n)}{4} \leq \frac{n-1}{4}$ ist.
Wegen $T_1 \cdot T_2 \cdots T_r \leq t_1 \cdot t_2 \cdots t_r$ genügt es,

$$\frac{1 + \frac{2^{rs_1}-1}{2^r-1}}{2^{s_1+s_2+\ldots+s_r}} \leq \frac{1}{4} \tag{4}$$

zu zeigen.
Aus $s_1 \leq s_2 \leq \ldots \leq s_r$ folgt

$$\begin{aligned} \frac{1 + \frac{2^{rs_1}-1}{2^r-1}}{2^{s_1+s_2+\ldots+s_r}} &\leq \left(1 + \frac{2^{rs_1}-1}{2^r-1}\right) \cdot 2^{-rs_1} = \frac{1}{2^{rs_1}} + \frac{2^{rs_1}-1}{2^{rs_1} \cdot (2^r-1)} \\ &= \frac{1}{2^{rs_1}} + \frac{1}{2^r-1} - \frac{1}{2^{rs_1} \cdot (2^r-1)} = \frac{1}{2^r-1} + \frac{2^r-2}{2^{rs_1} \cdot (2^r-1)} \leq \frac{1}{2^r-1}. \end{aligned}$$

Die Ungleichung (4) ist also erfüllt, wenn $r \geq 3$ ist.
Der verbleibende Fall ist $r = 2$, also $n = p_1 \cdot p_2$ mit $p_1 - 1 = 2^{s_1}t_1$ und $p_2 - 1 = 2^{s_2}t_2$ (ohne die Einschränkung $s_1 \leq s_2$).
Falls $s_1 < s_2$ ist, folgt (4): es gilt $s_1 \geq 1$ und $s_2 \geq 2$, denn $p_j - 1$ ist gerade, und damit

$$\begin{aligned} \frac{1 + \frac{2^{2s_1}-1}{3}}{2^{s_1+s_2}} &= 2^{-s_1-s_2} + \frac{1}{3} \cdot \left(2^{s_1-s_2} - 2^{-s_1-s_2}\right) = \frac{2}{3} \cdot 2^{-s_1-s_2} + \frac{1}{3} \cdot 2^{s_1-s_2} \\ &\leq \frac{2}{3} \cdot 2^{-3} + \frac{1}{3} \cdot 2^{-1} = \frac{1}{12} + \frac{1}{6} = \frac{1}{4}. \end{aligned}$$

Falls $s_1 = s_2 = s$ ist, so gilt $ggT(n-1, p_1-1) = 2^sT_1$ und $ggT(n-1, p_2-1) = 2^sT_2$. Es sei $p_1 > p_2$, dann ist $T_1 \neq t_1$. Wäre $T_1 = t_1$, also $(p_1-1)|(n-1)$, so wäre $n = p_1 \cdot p_2 \equiv p_2 \equiv 1 \bmod (p_1-1)$, ein Widerspruch zu $p_1 > p_2$. Wegen $T_1 \neq t_1$ ist $T_1 \leq \frac{1}{3}t_1$. Analog folgt auch $T_2 \leq \frac{1}{3}t_2$, falls $p_1 < p_2$ ist.
In beiden Fällen ist also $T_1 \cdot T_2 \leq \frac{1}{3}t_1 \cdot t_2$ mit

$$\left(1 + \frac{2^{2s_1}-1}{3}\right) \cdot 2^{-s_1} \leq \frac{1}{2},$$

also

$$T_1 \cdot T_2 \cdot \left(1 + \frac{2^{2s_1}-1}{3}\right) \leq t_1 \cdot t_2 \cdot \frac{1}{6} \cdot 2^{s_1} = \frac{\varphi(n)}{6}.$$

Damit ist (4) auch in diesem Fall bewiesen. □

Satz 6.2.4 liefert die Grundlage für den probabilistischen Primzahltest von Rabin.
Dieser Test liefert keine vollständige Gewissheit, dass eine Zahl eine Primzahl ist, jedoch ist er für praktische Zwecke ausreichend. Seine Formulierung verwendet das Konzept der Wahrscheinlichkeiten.

Satz 6.2.5. *(Probabilistischer Primzahltest von Rabin)*
Es sei n eine natürliche Zahl. Man wähle nach dem Zufallsprinzip k natürliche Zahlen kleiner n und führe den Test von Miller mit n für jede dieser Basen durch.
Wenn n zusammengesetzt ist, ist die Wahrscheinlichkeit, dass n alle k Tests besteht, kleiner als $\left(\frac{1}{4}\right)^k$.

Falls eine der berühmtesten Vermutungen aus der Zahlentheorie, die sogenannte verallgemeinerte Riemannsche Vermutung, richtig ist, gilt sogar, dass zu jeder zusammengesetzten Zahl n eine Basis a mit $a < 70\left(\frac{\log n}{\log 2}\right)^2$ existiert, so dass n den Test von Miller für die Basis a nicht besteht.
Eine Konsequenz dieser Vermutung ist also die Gültigkeit des folgenden Primzahltests:
Es sei n eine ungerade natürliche Zahl. Besteht n den Test von Miller für alle Basen $a < 70\left(\frac{\log n}{\log 2}\right)^2$, so ist n eine Primzahl.