Elementare Zahlentheorie

Filip Misev

Sommersemester 2020
Uni Regensburg

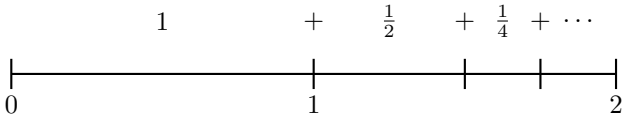
Erste Vorlesung – Eins, Zwei, Drei, ...

Eine unendliche Einleitung

Mit der Unendlichkeit verhält es sich zuweilen etwas anders, als man zunächst denken könnte. Es ist zum Beispiel möglich, unendlich viele Zahlen zusammenzuzählen und trotzdem ein sinnvolles (endliches) Resultat zu erhalten:

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{64} + \frac{1}{128} + \ldots = 2$$

(von einem Bruch zum nächsten teilen wir immer durch Zwei). Dass diese Rechnung stimmt, ist nicht einmal besonders schwer einzusehen, wenn man sich ein Bild davon macht:



Anders verhält es sich mit folgender Reihe:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \ldots$$

Wer lange genug rechnet, erhält als Zwischenergebnis schnell einen Wert größer als 2, mit einigen Summanden mehr[1] einen Wert größer als 10; mit sehr viel mehr Summanden wird das Zwischenergebnis größer als 10 000 000 000. Tatsächlich übertrifft diese Summe jede beliebige Grenze: Die Reihe *divergiert* gegen unendlich. Das ist nicht unmittelbar offensichtlich, aber man sieht es ein, sobald man die Rechnung in Pakete aufteilt:

$$1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \left(\frac{1}{9} + \frac{1}{10} + \ldots + \frac{1}{16}\right) + \ldots$$

Jedes Paket besteht aus doppelt sovielen Brüchen wie das vorherige – und jedes Paket für sich ist größer als $\frac{1}{2}$. Zum Beispiel: $(\frac{1}{3} + \frac{1}{4}) > (\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}$, genauso $(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}) > (\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}) = \frac{4}{8} = \frac{1}{2}$, und so weiter).

Die erste Reihe ist ein Beispiel für eine *geometrische Reihe*, die zweite Reihe ist bekannt under dem Namen *harmonische Reihe*.

[1] Genauer: mit 12 367 Summanden

Ein Satz Primzahlen und ein Primzahlsatz

Eine *Primzahl* ist eine natürliche Zahl, die genau zwei natürliche Zahlen als Teiler hat: 20 ist keine Primzahl, weil 20 durch 1, 2, 4, 5, 10 und 20 teilbar ist (also mehr als zwei Teiler hat). 17 ist nur durch 1 und durch 17 teilbar, ist also eine Primzahl. 1 ist keine Primzahl, weil 1 nur 1 als Teiler hat (also weniger als zwei Teiler).

Hier sind alle Primzahlen, die kleiner als 1000 sind:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89,
97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179,
181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271,
277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379,
383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479,
487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599,
601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701,
709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823,
827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941,
947, 953, 967, 971, 977, 983, 991, 997.

Frage. Wie häufig sind die Primzahlen unter den natürlichen Zahlen?

Direkt aus der Definition der Primzahlen ist nicht einmal unmittelbar klar, ob die Liste der Primzahlen irgendwo endet. Der folgende Satz zeigt nicht nur, dass es unendlich viele Primzahlen gibt, sondern auch, dass sie deutlich häufiger vorkommen als die Zweierpotenzen.

Satz 1 (Euler)**.** *Die Reihe*

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{23}+\dots,$$

deren Summanden von der Form $\frac{1}{p}$ *sind, wobei* p *alle Primzahlen durchläuft, divergiert gegen unendlich.*

Den ersten Beweis hat Leonhard Euler im Jahr 1737 gegeben. Der folgende Beweis stammt von Paul Erdős (1913–1996).

Beweis. Es sei $p_1, p_2, p_3, \dots$ die Folge der Primzahlen in aufsteigender Größe (zum Beispiel ist $p_7 = 17$). Die im Satz genannte Reihe schreibt sich also

folgendermaßen:

$$\sum_{i \geqslant 1} \frac{1}{p_i} \quad = \quad \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \frac{1}{p_4} + \frac{1}{p_5} + \dots$$

Nehmen wir an (im Gegensatz zur Aussage des Satzes), die Reihe konvergiert gegen einen endlichen Wert. Dann muss es eine Zahl k geben, so dass der hintere Teil der Reihe, ohne die ersten k Summanden, kleiner als $\frac{1}{2}$ ist:

$$\sum_{i \geqslant k+1} \frac{1}{p_i} \quad < \quad \frac{1}{2}$$

Wir unterscheiden nun zwischen den *kleinen* Primzahlen $p_1, p_2, \dots, p_k$ (das sind die ersten k Primzahlen) und den *grossen* Primzahlen $p_{k+1}, p_{k+2}, p_{k+3}, \dots$

Wir unterteilen die natürlichen Zahlen in zwei Sorten: $n \in \mathbb{N}$ gehört zur Sorte A, falls n durch mindestens eine große Primzahl teilbar ist. Andernfalls ist n nur durch kleine Primzahlen teilbar; dann gehört n zur Sorte B.

Für jede natürliche Zahl N betrachten wir jetzt die Zahlen von 1 bis N und zählen, wieviele davon zu welcher Sorte gehören: N_A ist die Anzahl der $n \leqslant N$, die zur Sorte A gehören und N_B ist die Anzahl der $n \leqslant N$, die zur Sorte B gehören. Wir werden jetzt zeigen, dass für ein geeignetes N gilt: $N_A + N_B < N$. Dies wird den gewünschten Widerspruch geben, denn natürlich ist $N_A + N_B = N$.

Zuerst betrachten wir N_A. Welche n haben p_i als Primteiler? Es sind alle Vielfachen von p_i, also $p_i, 2p_i, 3p_i, 4p_i, 5p_i, \dots$ Es gibt $\left\lfloor \frac{N}{p_i} \right\rfloor$ Vielfache von p_i, die zwischen 1 und N liegen (die Haken $\lfloor . \rfloor$ bedeuten: "abrunden"). Insgesamt erhalten wir die folgende Ungleichung[2]:

$$N_A \quad \leqslant \quad \sum_{i \geqslant k+1} \left\lfloor \frac{N}{p_i} \right\rfloor$$

Daraus folgt die Abschätzung:

$$N_A \quad \leqslant \quad \sum_{i \geqslant k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \quad \leqslant \quad \sum_{i \geqslant k+1} \frac{N}{p_i} \quad < \quad \frac{N}{2}$$

[2]Es ist keine Gleichung, weil eine Zahl gleichzeitig Vielfaches zweier verschiedener großer Primzahlen sein kann.

Schauen wir uns jetzt N_B an. Jede natürliche Zahl können wir in der Form vw^2 darstellen, wobei v ein Produkt *verschiedener* Primzahlen ist. Zum Beispiel: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = vw^2$ mit $v = 2 \cdot 5$ und $w = 2 \cdot 3$. Wenn $n = vw^2$ zur Sorte B gehört, sind v und w Produkte ausschließlich *kleiner* Primzahlen. Wieviele Möglichkeiten gibt es, eine solche Zahl n aus kleinen Primfaktoren zusammenzusetzen? Für v gibt es 2^k Möglichkeiten, da jede der k kleinen Primzahlen entweder als Teiler von v vorkommen kann, oder nicht. Da wir nur an den Zahlen $n \leqslant N$ interessiert sind, und $n = vw^2 \geqslant w^2$, kann w höchstens $\sqrt{N}$ verschiedene Werte annehmen. Insgesamt gibt es höchstens $2^k\sqrt{N}$ verschiedene n, die kleinergleich N sind und zur Sorte B gehören:

$$N_B \leqslant 2^k\sqrt{N}$$

Da diese Überlegung für *jede* natürliche Zahl N stimmt, stimmt sie auch für $N = 2^{2k+2}$. Damit erhalten wir:

$$N_B \leqslant 2^k 2^{k+1} \leqslant 2^{2k+1} = \frac{N}{2}$$

Kombinieren wir nun die Ungleichungen für N_A und N_B, ergibt sich

$$N_A + N_B < \frac{N}{2} + \frac{N}{2} = N,$$

der gewünschte Widerspruch. Also konnte die Annahme über die Konvergenz der Reihe nicht zutreffen, und der Satz ist bewiesen. □

In dieser Einleitung sind – teilweise versteckt – bereits einige Grundbegriffe der Elementaren Zahlentheorie aufgetreten: *natürliche Zahlen*, *ganze Zahlen*, *rationale Zahlen*, *(Zweier-)Potenzen*, *Vielfache*, *Teiler*, *Teilen mit Rest*, *Primzahlen*, *die Primfaktorzerlegung* und ihre Eindeutigkeit, *quadratfreie Zahlen*.

Beginnend mit der nächsten Vorlesung werden wir diese Begriffe schrittweise genauer definieren und studieren.

2/3. Vorlesung – Teilbarkeit

In der ersten Vorlesung haben wir unter Anderem gesehen, dass es unendlich viele Primzahlen gibt. Zum ersten Mal begegnet man der abstrakten Idee "unendlich" gewöhnlich als Kind, wenn man das Zählen lernt: 1, 2, 3, ... und begreift, dass dieses Zählen, zumindest in der Vorstellung, immer weitergehen kann, ohne Ende! Mit diesen sogenannten *natürlichen Zahlen* beginnt die Zahlentheorie. Die Menge aller natürlichen Zahlen wird mit dem Symbol $\mathbb{N}$ bezeichnet. Oft ist es zweckmäßig, die Zahl 0 zu den natürlichen Zahlen zu zählen:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots\}$$

Es gibt eine wichtige Eigenschaft, oder ein wichtiges Prinzip, welches die natürlichen Zahlen unterscheidet von anderen Zahlensystemen wie der Menge der *ganzen Zahlen* $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, der *rationalen Zahlen* $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}$ oder der *reellen Zahlen* $\mathbb{R}$, nämlich:

Jede nicht-leere Teilmenge von $\mathbb{N}$ *hat ein kleinstes Element.* $\qquad (\star)$

Unter einem *kleinsten Element* einer Teilmenge $A \subset \mathbb{N}$ (oder $A \subset \mathbb{Z}$ oder $A \subset \mathbb{Q}$ oder $A \subset \mathbb{R}$) verstehen wir ein Element $a \in A$, das kleiner ist als alle anderen Elemente von A, also $a \leqslant b$ für alle $b \in A$. Dieser Begriff bezieht sich auf eine zusätzliche Struktur, die auf den Mengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ festgelegt ist, nämlich auf die Relation "$\leqslant$". Falls A ein kleinstes Element hat, wird es auch als $\min A$ bezeichnet (für *Minimum*). Beispiel: $\min\{16, 5, 318\} = 5$.

Beispiele. Die folgenden Beispiele zeigen, dass sich das Prinzip $(\star)$ nicht auf Teilmengen von $\mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$ übertragen lässt.

- Die Menge $\{\frac{1}{n} \mid n \in \mathbb{N},\ n \geqslant 1\}$ ist eine Teilmenge von $\mathbb{Q}$. Sie ist von unten beschränkt (durch 0), hat aber kein kleinstes Element.
- $\mathbb{Z}$ ist eine Teilmenge von $\mathbb{Z}$ (und von $\mathbb{Q}$ und von $\mathbb{R}$), die kein kleinstes Element hat.

Beweis von $(\star)$. Nehmen wir an, $A \subset \mathbb{N}$ sei eine nicht-leere Teilmenge ohne kleinstes Element. Definiere die Menge $B := \{k \in \mathbb{N} \mid k \leqslant n \text{ für alle } n \in A\}$. Wir haben $0 \in B$. Falls $k \in B$, dann ist $k \notin A$ (sonst wäre k ein kleinstes Element von A), also $k < n$ für alle $n \in A$. Daraus folgt $k + 1 \leqslant n$ für alle $n \in A$, also $k + 1 \in B$. Wir haben gezeigt: $0 \in B$, und aus $k \in B$ folgt $k + 1 \in B$. Per Induktion folgt, dass *alle* natürlichen Zahlen in B enthalten sind: $B = \mathbb{N}$. Aber dann muss A leer sein; Widerspruch! $\square$

Satz 2 (Teilen mit Rest)**.** *Seien a und b zwei ganze Zahlen mit $b > 0$. Dann gibt es zwei eindeutig bestimmte ganze Zahlen q und r mit den folgenden Eigenschaften.*

$$a = qb + r \quad \textit{und} \quad 0 \leqslant r < b.$$

In der Situation des Satzes nennen wir q den *Quotient* und r den *Rest* der Division von a durch b. Dass q und r "eindeutig bestimmt sind", bedeutet, dass es zu gegebenen a, b nur *ein einziges* Zahlenpaar (q, r) mit den genannten Eigenschaften gibt.

Beispiele.

- Für $(a, b) = (34, 5)$ erhalten wir $34 = 6 \cdot 5 + 4$, und $0 \leqslant 4 < 5$.
- Für $(a, b) = (-86, 14)$ ist $-86 = (-7) \cdot 14 + 12$ und $0 \leqslant 12 < 14$.
- Für $(a, b) = (-3, 15)$ ist $-3 = (-1) \cdot 15 + 12$ und $0 \leqslant 12 < 15$.
- Für $(a, b) = (12, 4)$ ist $12 = 3 \cdot 4 + 0$, und $0 \leqslant 0 < 4$.

Bemerkung. Wenn wir beide Seiten der Gleichung $a = qb + r$ durch b dividieren, erhalten wir

$$\frac{a}{b} = q + \frac{r}{b} \quad \text{und} \quad 0 \leqslant \frac{r}{b} < 1.$$

Dies zeigt, dass man q durch Abrunden von $\frac{a}{b}$ zur nächsten ganzen Zahl erhält; in Symbolen: $q = \lfloor \frac{a}{b} \rfloor$. Das macht es leicht, q zu berechnen.

Beweis von Satz 2. Betrachten wir die Menge S aller Zahlen, die von a aus mit Schritten der Länge b erreichbar sind:

$$S := \{a - nb \mid n \in \mathbb{Z}\}$$

In S gibt es Elemente $\geqslant 0$ (setze zum Beispiel $n = -|a|$). Also ist $S \cap \mathbb{N}$ eine nicht-leere Teilmenge von $\mathbb{N}$. Wenden wir Prinzip $(\star)$ auf $A := S \cap \mathbb{N}$ an, folgt, dass $S \cap \mathbb{N}$ ein kleinstes Element hat, welches wir s nennen. Da s ein Element von S ist, ist es von der Form $s = a - nb$ für ein geeignetes $n \in \mathbb{Z}$. Diese Zahl s muss tatsächlich kleiner als b sein; andernfalls wäre nämlich $s - b \geqslant 0$ ein weiteres Element von $S \cap \mathbb{N}$, das aber kleiner als s ist – ein Widerspruch. Damit haben wir bereits Zahlen q und r mit den gewünschten Eigenschaften gefunden, nämlich $q := n$ und $r := s$.

Zur Eindeutigkeit: Angenommen, (q, r) und (q', r') seien zwei Zahlenpaare, die beide die gewünschten Eigenschaften hätten, also

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

Daraus folgt $|qb - q'b| = |r - r'| < b$, also $|q - q'| < 1$. Da $|q - q'|$ eine ganze Zahl ist, muss $q - q' = 0$ sein. Daraus folgt sofort $q = q'$, also auch $r = a - qb = a - q'b = r'$. Damit ist die Eindeutigkeit gezeigt. □

Definition 1 (Teiler)**.** Seien a, b zwei ganze Zahlen. Wir sagen, dass a ein *Teiler* von b ist, wenn eine ganze Zahl m existiert mit der Eigenschaft $b = a \cdot m$.

Synonyme Ausdrucksweisen sind: "*a teilt b*", "*b* ist durch *a teilbar*" und "*b* ist ein Vielfaches von *a*". Als Symbol verwendet man einen senkrechten Strich:

$$a|b \qquad\qquad \text{“}a \text{ teilt } b\text{”}$$

Beispiele.

$3|12$ (12 ist durch 3 teilbar, 3 ist ein Teiler von 12)

$7 \nmid 12$ (7 ist kein Teiler von 12)

$-3|12$ (denn $12 = (-3) \cdot (-4)$, und -4 ist eine ganze Zahl)

$3|0$ (denn $0 = 3 \cdot 0$, und 0 ist eine ganze Zahl)

Die Teiler von 12 sind -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6 und 12.

Lemma 1. *Falls $c|a$ und $c|b$, dann auch $c|(au + bv)$, für alle $u, v \in \mathbb{Z}$.*

Beweis. Falls $c|a$ und $c|b$, existieren $\alpha, \beta \in \mathbb{Z}$ so dass $a = c\alpha$ und $b = c\beta$. Daraus folgt $au + bv = c(\alpha u + \beta v)$. Da $\alpha u + \beta v$ eine ganze Zahl ist, folgt daraus, dass $c|(au + bv)$. □

Definition 2. Seien $a, b \in \mathbb{Z}$. Eine Zahl $c \in \mathbb{Z}$ mit den Eigenschaften $c|a$ und $c|b$ nennen wir einen *gemeinsamen Teiler* von a und b.

Definition 3 (größter gemeinsamer Teiler – ggT)**.** Seien a und b zwei ganze Zahlen, die nicht beide Null sind. Den *größten gemeinsamen Teiler* von a und b bezeichnen wir mit $\mathrm{ggT}(a, b)$.

Bemerkung. 0 ist durch jede ganze Zahl teilbar. Es gibt also keinen größten gemeinsamen Teiler von 0 und 0. Jede andere ganze Zahl hat endlich viele Teiler.

Beispiele.

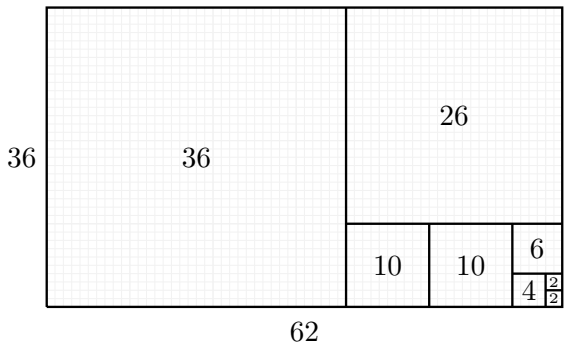
n	positive Teiler von n
60	1,2,3,4,5,6,10,12,15,20,30,60
34	1,2,17,34
32	1,2,4,8,16,32
17	1,17

$$\begin{aligned}
&\mathrm{ggT}(60,34) = 2\\
&\mathrm{ggT}(60,32) = 4\\
&\mathrm{ggT}(60,17) = 1\\
&\mathrm{ggT}(34,32) = 2\\
&\mathrm{ggT}(34,17) = 17\\
&\mathrm{ggT}(32,17) = 1
\end{aligned}$$

Lemma 2. *Wenn $a = qb + r$, dann ist $ggT(a, b) = ggT(b, r)$.*

Beweis. Nach Lemma 1 ist jeder gemeinsame Teiler von b und r auch ein Teiler von $qb + r = a$. Umgekehrt ist jeder gemeinsame Teiler von a und b auch ein Teiler von $a - qb = r$. Die beiden Zahlenpaare (a, b) und (b, r) haben also dieselben gemeinsamen Teiler, also auch denselben größten gemeinsamen Teiler. □

Es ist meist aufwändig, sämtliche Teiler einer ganzen Zahl zu bestimmen. Durch wiederholtes Anwenden von Satz 2 und Lemma 2 lässt sich der größte gemeinsame Teiler zweier ganzer Zahlen leichter berechnen. Die zugrundeliegende Idee ist in der Skizze am Beispiel $\mathrm{ggT}(62, 36)$ illustriert:



$$\begin{aligned}
62 &= 1 \cdot 36 + 26\\
36 &= 1 \cdot 26 + 10\\
26 &= 2 \cdot 10 + 6\\
10 &= 1 \cdot 6 + 4\\
6 &= 1 \cdot 4 + \boxed{2}\\
4 &= 2 \cdot 2 + 0
\end{aligned}$$

$$\mathrm{ggT}(62,36) = 2$$

Euklids Algorithmus. Seien $a, b \in \mathbb{Z}$, nicht beide Null. Falls $a = 0$, ist $\mathrm{ggT}(a, b) = |b|$, und wenn $b = 0$, dann ist $\mathrm{ggT}(a, b) = |a|$. Wir können uns also auf den Fall konzentrieren, wo weder a noch b Null ist. Ausserdem gilt

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

und falls $a = b$ ist $\mathrm{ggT}(a, b) = |a| = |b|$. Daher genügt es, den Fall $a > b > 0$ zu betrachten.
Wir verwenden jetzt Satz 2, um a mit Rest durch b zu teilen. Es gibt also $q_1, r_1 \in \mathbb{Z}$ mit

$$a = q_1 b + r_1 \quad \text{und} \quad 0 \leqslant r_1 < b.$$

Falls $r_1 = 0$, haben wir $b|a$, also $\mathrm{ggT}(a, b) = b$ und wir sind fertig.
Falls dagegen $r_1 \neq 0$, teilen wir b mit Rest durch r_1 (wieder mit Satz 2), also

$$b = q_2 r_1 + r_2 \quad \text{mit} \quad 0 \leqslant r_2 < r_1.$$

Dank Lemma 2 wissen wir nun, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_1)$. Falls $r_2 = 0$, folgt also $\mathrm{ggT}(a, b) = r_1$ und wir sind fertig. Andernfalls:

$$r_1 = q_3 r_2 + r_3 \quad \text{mit} \quad 0 \leqslant r_3 < r_2,$$

und so weiter. Weil $b > r_1 > r_2 > \ldots \geqslant 0$, erhalten wir zwangsläufig einmal $r_n = 0$ (nämlich nach höchstens b solcher Schritte), und wir haben

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_1) = \mathrm{ggT}(r_1, r_2) = \ldots = \mathrm{ggT}(r_{n-2}, r_{n-1}) = r_{n-1}.$$

Beispiel. Für die Berechnung von $\mathrm{ggT}(-492, 2020)$ liefert der Algorithmus von Euklid: $\mathrm{ggT}(-492, 2020) = \mathrm{ggT}(2020, 492)$ und

$$\begin{aligned} 2020 &= 4 \cdot 492 + 52 \\ 492 &= 9 \cdot 52 + 24 \\ 52 &= 2 \cdot 24 + \boxed{4} \\ 24 &= 6 \cdot 4 + 0, \end{aligned}$$

also $\mathrm{ggT}(-492, 2020) = 4$ (der letzte Rest, der nicht Null ist).

Satz 3 (Bézout, erster Teil)**.** *Seien $a, b \in \mathbb{Z}$, nicht beide Null. Dann existieren $u, v \in \mathbb{Z}$ mit der Eigenschaft*

$$ggT(a, b) = ua + vb.$$

Bemerkung. Zum Beispiel ist $1 = \mathrm{ggT}(3, 2) = 1 \cdot 3 + (-1) \cdot 2 = 3 \cdot 3 + (-4) \cdot 2$. Die Zahlen u, v mit der Eigenschaft $\mathrm{ggT}(a, b) = ua + vb$ sind also nicht eindeutig bestimmt.

Beweis von Satz 3. Wir wenden Euklids Algorithmus an, um $\mathrm{ggT}(a, b)$ zu berechnen als den zweitletzten Rest: $\mathrm{ggT}(a, b) = r_{n-1}$. Der zweitletzte Schritt des Algorithmus,

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1},$$

lässt sich umschreiben als

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}.$$

Wir haben also $\mathrm{ggT}(a, b) = r_{n-1}$ als ein Vielfaches von r_{n-3} plus ein Vielfaches von r_{n-2} ausgedrückt. Der Schritt davor,

$$r_{n-2} = r_{n-4} - q_{n-2} r_{n-3},$$

erlaubt es, darin r_{n-2} zu ersetzen und $\mathrm{ggT}(a, b)$ als Vielfaches von r_{n-4} plus ein Vielfaches von r_{n-3} darzustellen. So arbeiten wir uns rückwärts durch die Gleichungen des Algorithmus, bis wir schließlich $\mathrm{ggT}(a, b)$ als Vielfaches von a plus ein Vielfaches von b dargestellt haben. □

Beispiel. Im Beispiel von oben ($a = -492$ und $b = 2020$) haben wir

$$\begin{aligned}
\mathrm{ggT}(2020, 492) &= 4 \\
&= 52 - 2 \cdot 24 \\
&= 52 - 2 \cdot (492 - 9 \cdot 52) \\
&= -2 \cdot 492 + 19 \cdot 52 \\
&= -2 \cdot 492 + 19 \cdot (2020 - 4 \cdot 492) \\
&= 19 \cdot 2020 + (-78) \cdot 492
\end{aligned}$$

und $\mathrm{ggT}(-492, 2020) = 4 = 78 \cdot (-492) + 19 \cdot 2020$. Wir können also $u = 78$ und $v = 19$ nehmen.

Satz 4 (Bézout, zweiter Teil)**.** *Seien $a, b \in \mathbb{Z}$, nicht beide Null. Dann gilt*

$$ggT(a,b) = \min\{ua + vb \mid u, v \in \mathbb{Z},\ ua + vb \geqslant 1\}.$$

Beweis. Sei $C := \{ua + vb \mid u, v \in \mathbb{Z}\}$. Wir wollen zeigen, dass C gerade aus allen Vielfachen von $\mathrm{ggT}(a, b)$ besteht.

Ist nämlich $c \in C$ irgend ein Element, so ist $c = ua + vb$ für geeignete $u, v \in \mathbb{Z}$. Da $\mathrm{ggT}(a, b)$ sowohl a als auch b teilt, teilt $\mathrm{ggT}(a, b)$ auch c (dank Lemma 1), also ist c ein Vielfaches von $\mathrm{ggT}(a, b)$.

Umgekehrt lässt sich $\mathrm{ggT}(a, b)$ in der Form $\mathrm{ggT}(a, b) = ua + vb$ darstellen, für geeignete $u, v \in \mathbb{Z}$ (nach Satz 3). Also ist auch jedes Vielfache von $\mathrm{ggT}(a, b)$ ein Element von C, nämlich $n \cdot \mathrm{ggT}(a, b) = (nu)a + (nv)b$.

Die Zahl $\min\{ua + vb \mid u, v \in \mathbb{Z},\ ua + vb \geqslant 1\} = \min(C \cap \mathbb{N}_{\geqslant 1})$ ist also das kleinste positive Vielfache von $\mathrm{ggT}(a, b)$, was zu beweisen war. □

$7-3$. Vorlesung – Primzahlen

Definition 4 (Primzahl)**.** Eine *Primzahl* ist eine natürliche Zahl, die genau zwei natürliche Zahlen als Teiler hat (nämlich 1 und die Zahl selbst). Eine natürliche Zahl ist *zusammengesetzt*, falls sie mehr als zwei natürliche Zahlen als Teiler hat.

Lemma 3. *Seien a, b zwei ganze Zahlen und p eine Primzahl mit $p|ab$. Dann gilt $p|a$ oder $p|b$.*

Beweis. Falls $p|a$, sind wir fertig. Andernfalls ist $\mathrm{ggT}(a,p) = 1$. Nach Satz 3 (Bézout) gibt es $u, v \in \mathbb{Z}$ mit $1 = ua + vp$. Daraus folgt: $b = uab + vpb$. Da $p|ab$, folgt mit Lemma 1, dass $p|(uab + vpb)$, also $p|b$. □

Beispiel. Für $a = 2$, $b = 9$ und $n = 6$ gilt: $n|ab$, aber $n \nmid a$ und $n \nmid b$. Dies widerspricht Lemma 3 nicht, da 6 keine Primzahl ist.

Definition 5. Sei $a \in \mathbb{Z}$. Ein *Primteiler* (oder ein *Primfaktor*) von a ist eine Primzahl, die a teilt.

Satz 5 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $n \geqslant 2$ hat eine eindeutige Primfaktorzerlegung der Form*

$$n = p_1 p_2 \cdots p_k$$

wobei $k \geqslant 1$ eine natürliche Zahl und $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k$ Primzahlen sind.

Beispiel. $n = 600$ hat die Primfaktorzerlegung $600 = 2{\cdot}2{\cdot}2{\cdot}3{\cdot}5{\cdot}5 = 2^3{\cdot}3{\cdot}5^2$. Hier sind $k = 6$, $p_1 = p_2 = p_3 = 2$, $p_4 = 3$ und $p_5 = p_6 = 5$.

Bemerkung. Die Bedingung, dass die Primfaktoren $p_1, p_2, \ldots, p_k$ der Größe nach geordnet sind, stellt die Eindeutigkeit sicher. Sonst wäre zum Beispiel $2 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 5$ eine andere Primfaktorzerlegung derselben Zahl 600, nämlich mit $p_1 = 2$, $p_2 = 5$, $p_3 = p_4 = 2$, $p_5 = 3$ und $p_6 = 5$.

Die Primzahlen sind also die "multiplikativen atomaren Bausteine", aus denen die natürlichen Zahlen zusammengesetzt sind. Im Gegensatz dazu genügt bezüglich der *additiven* Struktur von $\mathbb{N}$ ein einziger additiver Baustein, um alle natürlichen Zahlen zu bilden: die Zahl 1. Darauf beruht das Prinzip der Induktion.

Beweis von Satz 5. Zuerst zeigen wir die Existenz der Primfaktorzerlegung und verwenden dazu das Prinzip der Induktion.
Da $n \geqslant 2$, beginnt die Induktion mit dem Fall $n = 2$. Da 2 eine Primzahl ist, haben wir die Primfaktorzerlegung bereits gefunden: $k = 1$ und $p_1 = 2$.
Jetzt nehmen wir an, die natürlichen Zahlen $2, 3, \ldots, n$ hätten alle eine Primfaktorzerlegung und wollen zeigen, dass dann auch die Zahl $n+1$ eine Primfaktorzerlegung hat (dann folgt per Induktion, dass *alle* natürlichen Zahlen $n \geqslant 2$ eine Primfaktorzerlegung haben). Falls $n+1$ eine Primzahl ist, sind wir fertig. Andernfalls hat $n+1$ einen Teiler $a \in \mathbb{N}$, der von 1 und von $n+1$ verschieden ist: $n + 1 = ab$ für geeignete $a, b \in \mathbb{N}$ mit $2 \leqslant a, b \leqslant n$. Nach Induktionsannahme haben a, b beide eine Primfaktorzerlegung, also auch ab.
Zur Eindeutigkeit: Angenommen, n hätte zwei Primfaktorzerlegungen

$$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_\ell$$

mit den im Satz genannten Eigenschaften. Die erste Gleichung zeigt, dass $p_1 | n$. Aus Lemma 3 folgt, dass $p_1 | q_i$ für ein $i \in \{1, \ldots, \ell\}$. Da q_i eine Primzahl ist, also nur 1 und q_i als Teiler hat, muss $p_1 = q_i$ sein. Wir können die Gleichung also auf beiden Seiten um einen Primfaktor kürzen und erhalten

$$p_2 \cdots p_k = q_1 \cdots q_{i-1} q_{i+1} \cdots q_\ell$$

Nun wiederholen wir diese Überlegung mit p_2, dann mit p_3, etc. und können so nach und nach auf beiden Seiten gleichviele Primfaktoren wegkürzen, bis auf einer Seite der Gleichung keine Primfaktoren mehr übrig sind. In dem Moment steht auf dieser Seite der Gleichung die Zahl 1, während auf der anderen Seite entweder ebenfalls 1, oder ein Produkt von Primzahlen steht. Letzteres ist jedoch unmöglich, da Primzahlen größer als 1 sind. Also standen von Beginn an auf beiden Seiten gleichviele Primfaktoren: $k = \ell$, und jeder Primfaktor kommt auf beiden Seiten gleich oft vor. Da sowohl die p_i als auch die q_j der Größe nach geordnet sind, folgt $p_1 = q_1,\ p_2 = q_2,\ \ldots\ , p_k = q_k$. □

Dass jede natürliche Zahl eine Primfaktorzerlegung hat, haben wir bereits in der ersten Vorlesung im Beweis von Eulers Satz verwendet. Eine unmittelbare Folgerung daraus ist folgender Satz:

Satz 6. *Es gibt unendlich viele Primzahlen.*

Wir wollen jetzt einen weiteren, klassischen Beweis vorstellen (einen unter sehr vielen weiteren Beweisen), der bereits dem altgriechischen Mathematiker Euklid bekannt war.

Beweis. Sei $\{p_1, \ldots, p_k\}$ eine beliebige endliche Menge von Primzahlen. Betrachten wir nun die natürliche Zahl $n := 1 + p_1 p_2 \cdots p_k$. Sei p ein Primteiler von n. Falls $p = p_i$ für ein $i \in \{1, \ldots, k\}$, so teilt p sowohl n als auch $p_1 p_2 \cdots p_k$. Mit Lemma 1 folgt daraus $p|1$, was unmöglich ist. Eine endliche Menge $\{p_1, \ldots, p_k\}$ kann also nie alle Primzahlen enthalten. □

Das folgende Beispiel zeigt, dass wir in diesem Beweis nicht einfach $p = n$ wählen können, sondern wirklich einen *Primteiler* von n betrachten sollten.

Beispiel. $1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30\,031 = 59 \cdot 509$.

Satz 7. *Es gibt unendlich viele Primzahlen der Form* $4m + 3$*,* $m \in \mathbb{Z}$*.*

Beweis. Sei $\{p_1, \ldots, p_k\}$ eine beliebige endliche Menge von Primzahlen dieser Form. Sei $n := 4p_1 \cdots p_k - 1$ und sei p ein Primteiler von n. Da n ungerade ist, muss auch p ungerade sein, also ist entweder $p = 4\ell + 1$ oder $p = 4\ell + 3$ für ein geeignetes $\ell \in \mathbb{N}$. Falls *jeder* Primteiler von n von der Form $4\ell + 1$ wäre, dann wäre n ein Produkt solcher Zahlen und müsste ebenfalls von dieser Form sein[3]. Dies ist unmöglich, weil n bei Division durch 4 den Rest 3 hat (denn $n = 4q + 3$ mit $q = p_1 \cdots p_k - 1$). Also hat n mindestens einen Primteiler der Form $p = 4\ell + 3$. Falls $p = p_i$ für ein $i \in \{p_1, \ldots, p_k\}$, dann teilt p sowohl n als auch $4p_1 \cdots p_k$, also $p|1$, was unmöglich ist. Also kann $\{p_1, \ldots, p_k\}$ niemals die Menge *aller* Primzahlen der Form $4n + 3$ sein. □

Satz 7 ist ein Spezialfall des folgenden Satzes von Dirichlet, der auf das Jahr 1837 zurückgeht.

Satz (Dirichlet)**.** *Seien* a, b *zwei teilerfremde ganze Zahlen. Dann gibt es unendlich viele Primzahlen der Form* $am + b$*,* $m \in \mathbb{Z}$*.*

Den Beweis geben wir hier nicht wieder; allerdings gibt die zugrundeliegende Idee selbst einen sehr interessanten Hinweis auf die Verteilung der Primzahlen: Dirichlet betrachtet für eine gegebene Zahl a die möglichen Reste, die bei Division einer Primzahl durch a entstehen können (das sind alle b mit der Eigenschaft, dass a, b teilerfremd sind), und zeigt, dass alle diese möglichen Reste gleich häufig auftreten. Da es unendlich viele Primzahlen gibt, folgt daraus, dass es auch unendlich viele Primzahlen mit gegebenem Rest b geben muss. Dirichlets Satz sagt jedoch nicht, dass die Zahlen der

[3]Falls $a = 4u + 1$ und $b = 4v + 1$, dann ist nämlich $ab = 4w + 1$, mit $w = 4uv + u + v$.

Form $am + b$, $m \in \mathbb{Z}$, lückenlos alle prim sind (sondern "nur", dass unendlich viele darunter prim sind).

Den folgenden berühmten Satz haben Ben Green und Terence Tao im Jahr 2004 gegeben – mehr als 150 Jahre später.

Satz (Green-Tao)**.** *Sei $n \in \mathbb{N}$. Dann existieren $a, b \in \mathbb{N}$, $a, b \geqslant 1$, so dass die Zahlen $am + b$ alle prim sind, für $0 \leqslant m \leqslant n$.*

Der Satz von Green und Tao sagt, dass es tatsächlich beliebig lange arithmetische Folgen von Primzahlen gibt. Es ist nicht leicht, solche arithmetischen Folgen explizit zu finden. Das folgende Beispiel war bis vor wenigen Monaten[4] die längste bekannte arithmetische Folge von Primzahlen.

Beispiel (Entdeckt von Benoãt Perichon im Jahr 2010, mit Software von Wróblewski und Geoff Reynolds im PrimeGrid-Projekt)**.**

$$23\,681\,770 \cdot 223\,092\,870 \cdot m + 43\,142\,746\,595\,714\,191, \text{ für } 0 \leqslant m \leqslant 25.$$

Als Anwendung der Primfaktorzerlegung wollen wir jetzt eine praktische Methode zur Berechnung von ggT und kgV angeben. Zur Erinnerung:

Definition 6. Das *kleinste gemeinsame Vielfache* zweier natürlicher Zahlen a, b ist die kleinste natürliche Zahl $c \geqslant 1$ mit der Eigenschaft $a|c$ und $b|c$. Es wird mit $\mathrm{kgV}(a, b)$ bezeichnet.

Satz 8. *Seien a, b zwei natürliche Zahlen, dargestellt als*

$$a = p_1^{r_1} p_2^{r_2} \cdots p_d^{r_d} \quad \textit{und} \quad b = p_1^{s_1} p_2^{s_2} \cdots p_d^{s_d},$$

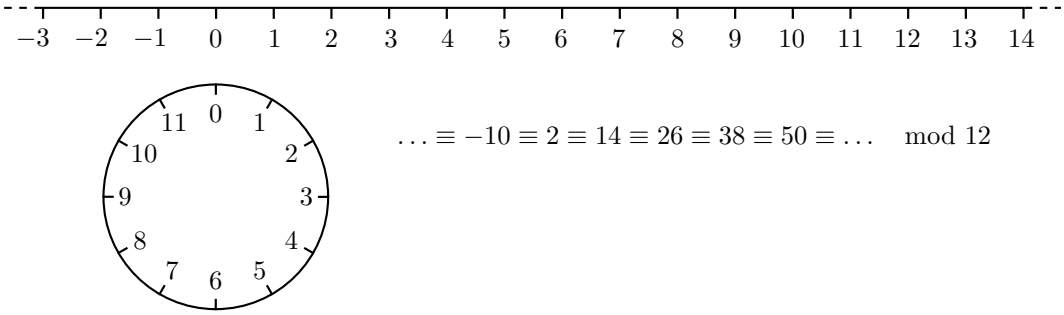
wobei $d \in \mathbb{N}$, $r_1, \ldots, r_d$, $s_1, \ldots, s_d \in \mathbb{N}$ und $p_1 < \ldots < p_d$ Primzahlen sind. Dann gilt:

$$ggT(a, b) = \prod_{i=1}^{d} p_i^{\min\{r_i, s_i\}} \quad \textit{und} \quad kgV(a, b) = \prod_{i=1}^{d} p_i^{\max\{r_i, s_i\}}.$$

Beispiel. $a = 56$ und $b = 588$ können wir darstellen als $a = 2^3 \cdot 3^0 \cdot 7^1$ und $b = 2^2 \cdot 3^1 \cdot 7^2$. Mit Satz 8 folgt: $\mathrm{ggT}(56, 588) = 2^2 \cdot 3^0 \cdot 7^1 = 28$ und $\mathrm{kgV}(56, 588) = 2^3 \cdot 3^1 \cdot 7^2 = 1176$.

[4]Im September 2019 hat Rob Gahan mit dem PrimeGrid-Projekt die erste arithmetische Primzahlfolge der Länge 27 entdeckt. http://primerecords.dk/aprecords.htm

Fünfte und sechste Vorlesung ≡ Kongruenzen



Definition 7. Sei $n \in \mathbb{Z}$. Zwei ganze Zahlen a, b sind *kongruent modulo* n, falls $n|(a-b)$. Notation: $a \equiv b \mod n$.

Beispiele.

$27 \equiv -21 \mod 24$ (denn $27-(-21)$ ist durch 24 teilbar)

$3 \equiv 27 \mod 24$ (3 und 27 sind ebenfalls kongruent modulo 24)

$6 \not\equiv 3 \mod 4$ (6 und 3 sind nicht kongruent modulo 4)

$n^2 \equiv n \mod 2$, für alle $n \in \mathbb{Z}$ (denn $n^2 - n = n(n-1)$ ist gerade)

Lemma 4. *a und b sind genau dann kongruent modulo n, wenn a und b bei Division durch n denselben Rest haben.*

Beweis. Seien $a = gn + r$ und $b = hn + s$ mit $0 \leqslant r, s < n$ die Divisionen mit Rest. Aus $a \equiv b \mod n$ folgt $n|(g-h)n + (r-s)$, also $n|(r-s)$. Da $0 \leqslant r, s < n$, folgt daraus $r - s = 0$, also $r = s$. Umgekehrt, falls $r = s$, ist $a - b = (g-h)n$, also $n|(a-b)$. □

Kongruenzen kommen im Alltag vor: Die Uhr zeigt nicht die Zahl der Stunden, die seit Beginn der Zeitrechnung vergangen sind, sondern nur die Reste bei Division durch 12 (oder 24 – je nach Uhr). Um den Wochentag in 52 Tagen zu kennen, braucht man nicht 52 Tage im Kalender abzuzählen. Es genügt festzustellen, dass 52 bei Division durch 7 den Rest 3 hat und bloß 3 Tage im Kalender abzuzählen. Betätigt man einen Lichtschalter n Mal, entscheidet der Rest von n bei Division durch 2 darüber, ob das Licht angeht oder nicht. Wir werden sehen, dass sich auch einige zahlentheoretische Probleme durch Kongruenzen vereinfachen.

Beispiel. Ist 71 544 308 das Quadrat einer natürlichen Zahl? Man könnte selbstverständlich $\sqrt{71\,544\,308}$ berechnen und entscheiden, ob es sich um eine natürliche Zahl handelt, oder verschiedene Zahlen quadrieren, um zu sehen, ob man 71 544 308 erhält. Leichter ist es jedoch, den Rest bei Division durch 5 zu betrachten (dieser ist offensichtlich 3) und sich an Aufgabe 3 vom 3. Übungsblatt zu erinnern: Das Quadrat einer natürlichen Zahl kann bei Division durch 5 niemals den Rest 3 haben.

Bemerkung. Aus Lemma 4 folgen direkt die Eigenschaften, die Kongruenz modulo n zu einer *Äquivalenzrelation* auf $\mathbb{Z}$ machen.

- $a \equiv a \mod n$ für alle $a \in \mathbb{Z}$
- Falls $a \equiv b \mod n$, dann $b \equiv a \mod n$
- Falls $a \equiv b$ und $b \equiv c \mod n$, dann $a \equiv c \mod n$

Als Nächstes wollen wir zeigen, dass sich mit Resten modulo n (beinahe) genauso rechnen lässt wie mit ganzen Zahlen. Dazu werden alle Zahlen mit demselben Rest zu einer *Restklasse* zusammengefasst:

Definition 8. Seien $a, n \in \mathbb{Z}$. Die *Restklasse* von a modulo n wird mit $\overline{a}$ bezeichnet und ist definiert als die folgende Teilmenge von $\mathbb{Z}$.

$$\overline{a} := \{k \in \mathbb{Z} \mid k \equiv a \mod n\}$$

Die Menge aller Restklassen modulo n wird mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.

Vorsicht! Wie die Restklasse $\overline{a}$ definiert ist, hängt von n ab. Wenn wir $\overline{a}$ schreiben, setzen wir also voraus, dass im Kontext klar ist, auf welche Zahl n wir uns geeinigt haben.

Beispiele.

- Die Restklasse von 3 modulo 7 ist

$$\overline{3} = \{\ldots, -18, -11, -4, 3, 10, 17, 24, 31, 38, \ldots\}$$

- Die Restklasse von 17 modulo 7 ist dieselbe Menge:

$$\overline{17} = \{\ldots, -18, -11, -4, 3, 10, 17, 24, 31, 38, \ldots\}$$

- Die Restklasse von 3 modulo 2 ist

$$\overline{3} = \{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11, 13, \ldots\}$$

- Als wir in der zweiten Vorlesung die Division mit Rest einer ganzen Zahl a durch eine positive ganze Zahl b diskutiert haben, haben wir bereits Restklassen betrachtet: Die Menge S im Beweis von Satz 2 ist genau die Restklasse $\overline{a}$ modulo b.

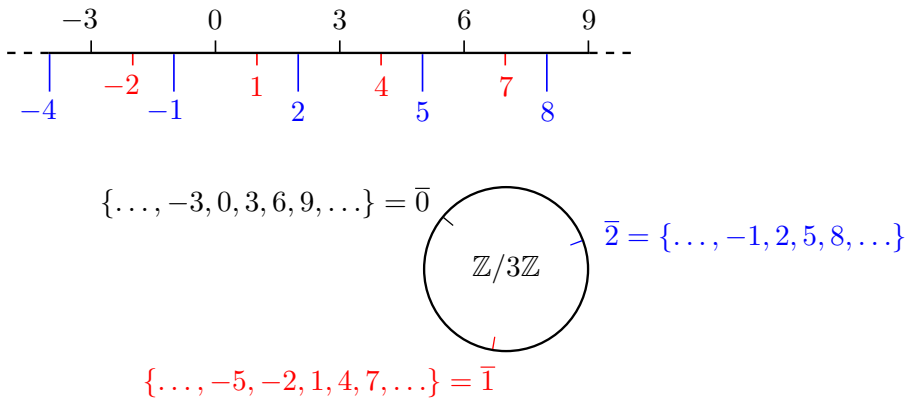
Lemma 5. *Seien $\overline{a}$ und $\overline{b}$ zwei Restklassen modulo n. Dann gilt:*

$$a \equiv b \mod n \quad \Leftrightarrow \quad \overline{a} = \overline{b} \quad \Leftrightarrow \quad a \in \overline{b} \quad \Leftrightarrow \quad b \in \overline{a}$$

Beweis. $b \in \overline{a}$ bedeutet per Definition von $\overline{a}$ genau, dass $a \equiv b \mod n$. Außerdem sind $a \equiv b$ und $b \equiv a$ äquivalent. Dies zeigt die Äquivalenzen $b \in \overline{a} \Leftrightarrow a \equiv b \Leftrightarrow b \equiv a \Leftrightarrow a \in \overline{b}$ (alles modulo n). Da $a \equiv a$, folgt aus $\overline{a} = \overline{b}$ sofort $a \in \overline{b}$. Um den Beweiskreis zu schließen, genügt es also zu zeigen, dass aus $a \equiv b \mod n$ folgt: $\overline{a} = \overline{b}$. Wir nehmen also an, $a \equiv b$. Falls $c \in \overline{a}$, ist $a \equiv c$, also $b \equiv c$ und daher $c \in \overline{b}$. Genauso folgt aus $c \in \overline{b}$, dass $c \in \overline{a}$. □

Lemma 6. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ *ist die Menge der Restklassen* mod n.

Beweis. Zu zeigen ist, dass jede Restklasse $\overline{a}$ modulo n (wobei a eine beliebige ganze Zahl ist) bereits in der Liste $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ vorkommt. Sei also $a \in \mathbb{Z}$. Teilen wir a mit Rest durch n, erhalten wir $a = qn + r$ für $q, r \in \mathbb{Z}$ mit $0 \leqslant r < n$. Daraus folgt: $a - r = qn$ ist durch n teilbar, also $\overline{a} = \overline{r}$. □



Bemerkung. Natürlich können wir in Lemma 6 statt $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ genau so gut $\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n}$ nehmen (denn $\overline{n} = \overline{0}$), oder auch $\overline{15}, \overline{16}, \ldots, \overline{14+n}$, oder die Restklassen von beliebigen n aufeinanderfolgenden ganzen Zahlen.

Lemma 7. *Falls $a \equiv a'$ und $b \equiv b' \mod n$, dann folgt*

$$a + b \equiv a' + b' \qquad \textit{und} \qquad ab \equiv a'b' \mod n$$

Beweis. Falls $a \equiv a' \mod n$, gibt es eine ganze Zahl k, so dass $a = a' + kn$. Genauso gibt es $\ell \in \mathbb{Z}$ mit $b = b' + \ell n$, falls $b \equiv b' \mod n$. Daraus folgt $a + b = a' + b' + (k + \ell)n$, also $a + b \equiv a' + b' \mod n$. Die zweite behauptete Kongruenz folgt aus $ab = (a' + kn)(b' + \ell n) = a'b' + (kb' + \ell a' + k\ell n)n$. □

Dank Lemma 7 können wir Restklassen genau wie ganze Zahlen addieren und multiplizieren und stoßen dabei nicht auf Widersprüche.

Definition 9 (Summe und Produkt von Restklassen modulo n)**.**

$$\overline{a} + \overline{b} := \overline{a + b} \qquad \text{und} \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}.$$

Die Menge $\mathbb{Z}/n\mathbb{Z}$ erhält dadurch eine ähnliche Struktur wie die Menge der ganzen Zahlen $\mathbb{Z}$ (in der Algebra sagt man, $\mathbb{Z}/n\mathbb{Z}$ sei ein *kommutativer Ring*) – mit dem wichtigen Unterschied, dass $\mathbb{Z}/n\mathbb{Z}$ nur n Elemente hat, statt wie $\mathbb{Z}$ unendlich viele.

Bemerkung. Man könnte versucht sein, genauso auch Potenzen von Restklassen zu definieren: $\overline{a}^{\overline{k}} := \overline{a^k}$. Allerdings folgt aus $a \equiv b$ und $k \equiv \ell$ nicht unbedingt, dass $a^k \equiv b^\ell$, wie das folgende Beispiel (modulo 3) zeigt: $1 \equiv 4$, aber $2^1 \not\equiv 2^4 \mod 3$. Dies ist ein Problem, da man schnell auf Widersprüche stößt: $\overline{2^1} =: \overline{2}^{\overline{1}} = \overline{2}^{\overline{4}} := \overline{2^4}$, aber $\overline{2^1} \neq \overline{2^4}$. Lemma 7 ist also essenziell, um die Summe und das Produkt von Restklassen sinnvoll zu definieren. Natürlich gilt aber $\overline{a^k} = \overline{a \cdot \ldots \cdot a} = \overline{a} \cdot \ldots \cdot \overline{a}$ (mit k Faktoren; dazu wenden wir den zweiten Teil der Definition 9 wiederholt an, beziehungsweise die zweite Aussage in Lemma 7). Also $\overline{a^k} = \overline{a}^k$. Dies werden wir später bei den Beispielen immer wieder verwenden.

Bemerkung. Vorsicht! Das Kürzen von Restklassen in einer Gleichung ist nicht immer möglich, wie das folgende Beispiel zeigt:

$$\overline{8} \cdot \overline{2} = \overline{5} \cdot \overline{2} \mod 6, \quad \text{aber} \quad \overline{8} \neq \overline{5} \mod 6$$

Die Restklasse $\overline{2}$ lässt sich also nicht kürzen, obwohl $\overline{2} \neq \overline{0} \mod 6$. Wie wir später sehen werden, liegt das daran, dass 2 und 6 einen gemeinsamen Teiler haben.

Wir wollen jetzt an einigen Beispielen illustrieren, wie der Übergang zu Restklassen das Rechnen mit ganzen Zahlen vereinfachen kann.

Beispiele.

- Welchen Rest hat die Zahl $35 \cdot 40 \cdot 374$ bei Division durch 37? Natürlich kann man die Zahlen multiplizieren und mit Rest durch 37 teilen. Aber es geht einfacher, wenn wir zu Restklassen modulo 37 übergehen:

  $$\overline{35 \cdot 40 \cdot 374} = \overline{-2} \cdot \overline{3} \cdot \overline{10 \cdot 37 + 4} = \overline{-6} \cdot (\overline{10} \cdot \overline{0} + \overline{4}) = \overline{-24} = \overline{13}.$$

  Da $0 \leqslant 13 < 37$, ist der gesuchte Rest 13.

- Ist $929^{38} - 94^9$ durch 93 teilbar? Rechnen wir modulo 93, dann erhalten wir: $\overline{929} = \overline{-1}$ und $\overline{94} = \overline{1}$. (Denn $929-(-1) = 930$ und $94-1 = 93$ sind offensichtlich durch 93 teilbar). Also folgt $929^{38} - 94^9 \equiv (-1)^{38} - 1^9 \equiv 0$ mod 93. Die Antwort lautet also: Ja, $93 | (929^{38} - 94^9)$.

- Wie lautet die letzte Ziffer der Zahl 3^{51}? Die letzte Ziffer ist der Rest bei Division durch 10. Wir rechnen daher modulo 10: Zunächst bemerken wir, dass $\overline{3^2} = \overline{9} = \overline{-1}$. Da $51 = 2 \cdot 25 + 1$, folgt $3^{51} = 3 \cdot (3^2)^{25} \equiv 3 \cdot (-1)^{25}$. Weil 25 ungerade ist, haben wir $(-1)^{25} = -1$, also $\overline{3^{51}} = \overline{-3} = \overline{7}$. Die letzte Ziffer ist also 7.

- Wie lauten die zwei letzten Ziffern der Zahl 7^{2020}? Wir interessieren uns also für den Rest bei Division durch 100. Zuerst bemerken wir, dass $7^4 = 49 \cdot 49 = (50-1)(50-1) = 50^2 - 2 \cdot 50 + 1$, also $\overline{7^4} = \overline{1}$ modulo 100. Außerdem ist $2020 = 4 \cdot 505$, also $7^{2020} = (7^4)^{505}$. Es folgt also $7^{2020} \equiv 1^{505} \equiv 1 \mod 100$. Die letzten beiden Ziffern sind also 01.

- Behauptung: Falls $n \in \mathbb{N}$ gerade ist, gilt $3 \nmid 2^n + 1$. Beweis: Modulo 3 ist $\overline{2} = \overline{-1}$, also $\overline{2^n} = \overline{(-1)^n}$. Da n gerade ist, haben wir $(-1)^n = 1$. Damit folgt $\overline{2^n + 1} = \overline{1 + 1} = \overline{2} \neq \overline{0}$ (da $3 \nmid 2 - 0$), was zu beweisen war.

- Sei $n \in \mathbb{N}$, $n \geqslant 4$. Man bestimme die letzte Ziffer der Zahl $1! + 2! + 3! + \ldots + n!$. Für $k \geqslant 5$ ist $k!$ durch 10 teilbar, denn im Produkt $k! = k \cdot (k-1) \cdots 5 \cdot 4 \cdot 2 \cdot 1$ kommen in diesem Fall 5 und 2 als Faktoren vor. Diese Summanden $k!$ fallen also alle in die Restklasse $\overline{0}$ modulo 10. Übrig bleibt die Restklasse von $1! + 2! + 3! + 4!$. Diese ist $\overline{1} + \overline{2} + \overline{6} + \overline{24} = \overline{9} + \overline{4} = \overline{-1} + \overline{4} = \overline{3}$. Die letzte Ziffer ist also 3.

Lineare Kongruenzen

Wir untersuchen jetzt, wann eine Gleichung mit einer unbekannten Restklasse modulo n lösbar ist, und wie man alle Lösungen findet. Die einfachsten Gleichungen sind *lineare* Gleichungen, von der Form $\overline{a} \cdot \overline{x} = \overline{b}$, wobei $\overline{a}$ und $\overline{b}$ gegeben sind und nach $\overline{x}$ gelöst werden soll, oder, was dasselbe ist: $ax \equiv b \mod n$. Die Lösungsmenge lässt sich vollständig beschreiben. Dabei spielen der Satz von Bézout und der Algorithmus von Euklid eine wesentliche Rolle.

Satz 9. *Seien $a, b, n \in \mathbb{Z}$, $n \neq 0$ und $d := ggT(a, n)$. Die Kongruenz*

$$ax \equiv b \mod n$$

hat keine Lösungen wenn $d \nmid b$. Falls $d \mid b$, gibt es genau d verschiedene Restklassen von Lösungen modulo n.

Beweis. Angenommen, $x \in \mathbb{Z}$ sei eine Lösung von $ax \equiv b \mod n$. Dann gilt per Definition $n|(ax - b)$. Da $d|n$ und $d|a$, folgt $d|b$. Es kann also keine Lösungen geben, wenn $d \nmid b$.

Nehmen wir jetzt an, $d|b$. Mit Satz 3 (Bézout) finden wir $u, v \in \mathbb{Z}$ mit $ua + vn = d$. Da $d|b$, ist $\frac{b}{d} \in \mathbb{Z}$. Multiplizieren wir die Gleichung $ua + vn = d$ mit $\frac{b}{d}$, erhalten wir $\frac{b}{d}ua + \frac{b}{d}vn = b$, also $a \cdot \frac{b}{d}u \equiv b \mod n$. Wir haben also eine Lösung gefunden, nämlich $x = \frac{b}{d}u \in \mathbb{Z}$. Schließlich wollen wir zeigen, dass es modulo n genau d verschiedene Lösungen gibt:
Fall 1: $d = 1$. Dann ist $ua + vn = 1$, also $ua \equiv 1 \mod n$. Wenn nun x eine beliebige Lösung von $b \equiv ax$ ist, folgt $ub \equiv uax \equiv x$, wodurch die Restklasse von x modulo n eindeutig bestimmt ist.
Fall 2: $d \geqslant 2$. Da d einerseits a und n teilt (per Definition von d) und anderseits b teilt (nach Annahme), haben wir $a = a'd$, $b = b'd$, $n = n'd$ für bestimmte $a', b', n' \in \mathbb{Z}$, und $\mathrm{ggT}(a', n') = 1$. Sei jetzt x eine beliebige Lösung von $ax \equiv b \mod n$. Das bedeutet per Definition, dass $ax - b = nk$ für ein $k \in \mathbb{Z}$. Durch Einsetzen erhalten wir: $a'dx - b'd = n'dk$. Kürzen wir d (das geht, weil $d \neq 0$), folgt $a'x - b' = n'k$, also ist x eine Lösung der Kongruenz $a'x \equiv b' \mod n'$ mit $d' := \mathrm{ggT}(a', n') = 1$. Nach Fall 1 gibt es genau eine einzige Restklasse modulo n', die diese Kongruenz erfüllt. Diese muss die Restklasse von x sein: $\{\ldots, x - 2n', x - n', x, x + n', x + 2n', \ldots\}$. Die Restklasse modulo n' zerfällt also in genau d verschiedene Restklassen modulo n, nämlich $\overline{x + kn'}$ für $k \in \{0, \ldots, d - 1\}$. (Denn $\overline{dn'} = \overline{n} = \overline{0}$ modulo n.) $\square$

Bemerkung. Der Beweis zeigt nicht nur die Aussage des Satzes, sondern beschreibt auch, wie man die Lösungen von

$$ax \equiv b \mod n$$

explizit findet, falls b durch $d = \mathrm{ggT}(a, n)$ teilbar ist. Man findet nämlich zuerst (mit Euklids Algorithmus) $u, v \in \mathbb{Z}$ mit $ua + vn = d$ und definiert

$$a' := \frac{a}{d}, \qquad b' := \frac{b}{d}, \qquad n' := \frac{n}{d}$$

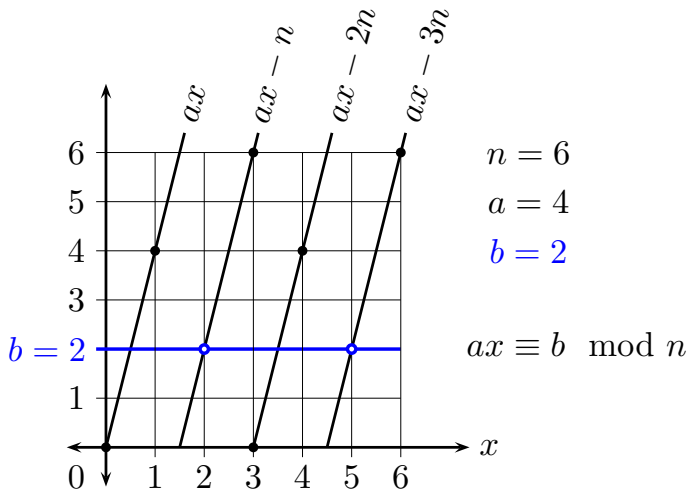
Dann ist $ua' + vn' = 1$; wie in Fall 1 des Beweises können wir $x := ub'$ setzen und haben eine erste Lösung gefunden. Die d Restklassen von Lösungen sind dann (gemäß Fall 2 des Beweises) die folgenden d Restklassen modulo n.

$$\overline{x}, \quad \overline{x + n'}, \quad \overline{x + 2n'}, \quad \overline{x + 3n'}, \quad \ldots, \quad \overline{x + (d-1)n'}.$$

Beispiel. $(a, b, n) = (4, 2, 6)$. Dann ist $d = \mathrm{ggT}(a, n) = 2 = (-1) \cdot 4 + 1 \cdot 6$. Wir können also $u := -1$ und $v := 1$ wählen. Außerdem $(a', b', n') = (2, 1, 3)$, also $x = -1$ und es gibt die 2 Lösungen

$$\overline{-1} = \overline{5} \qquad \text{und} \qquad \overline{-1 + n'} = \overline{-1 + 3} = \overline{2} \quad \text{(modulo 6)}.$$

Das Beispiel ist in der folgenden Skizze illustriert.



Bemerkung. Eine Lösung $\overline{x}$ von $\overline{a} \cdot \overline{x} = \overline{b}$ kann man interpretieren als eine Art "Quotient" $\frac{\overline{b}}{\overline{a}}$. Satz 9 beschreibt also die Teilbarkeit von Elementen in $\mathbb{Z}/n\mathbb{Z}$. Wir haben allerdings gesehen, dass es (anders als zum Beispiel in $\mathbb{Q}$), nicht immer einen solchen Quotienten gibt, und wenn einer existiert, ist er im Allgemeinen nicht eindeutig – ein Gegensatz zur Teilbarkeit in $\mathbb{Z}$.

Die folgende Aussage folgt direkt aus Satz 9.

Korollar 1. *Falls a und n teilerfremd sind, bilden die Lösungen $x \in \mathbb{Z}$ der Kongruenz $ax \equiv b \mod n$ eine einzige Restklasse modulo n.*

Beweis. Dies ist der Fall $d = 1$ im Satz 9. □

Beispiele.

- Die Kongruenz $7x \equiv 4 \mod 12$ hat eine einzige Restklasse von Lösungen (da 7 und 12 teilerfremd sind), nämlich die Restklasse $\overline{x} = \overline{4}$, da $\overline{7} \cdot \overline{4} = \overline{28} = \overline{24 + 4} = \overline{4}$ modulo 12.

- Die Kongruenz $10x \equiv 6 \mod 12$ hat zwei Restklassen von Lösungen (da $d = \mathrm{ggT}(10, 12) = 2$ und $d|6$). Wir können als erste Lösung $x = 3$ nehmen (da $10 \cdot 3 = 30 \equiv 6 \mod 12$). Die allgemeine Lösung ist dann von der Form $x + kn' = 3 + 6k$, wobei $k \in \mathbb{Z}$. Diese Lösungen bilden zwei Restklassen modulo 12, nämlich $\overline{3}$ und $\overline{9}$.

Das letzte Beispiel lädt dazu ein, beide Seiten der Kongruenz $10x \equiv 6$ durch 2 zu teilen, um die Gleichung zu vereinfachen. Aber Vorsicht! Zum Beispiel gilt $8 \cdot 2 \equiv 5 \cdot 2 \mod 6$, aber $8 \not\equiv 5 \mod 6$. Wir können also den Faktor 2 in dieser Kongruenz nicht kürzen – jedenfalls nicht, ohne den *Modul* (hier die Zahl 6) zu verändern. Der folgende Satz zeigt, wie sich Kongruenzen richtig kürzen lassen, indem der Modul angepasst wird.

Satz 10 (Kürzen von Kongruenzen)**.** *Seien $a, b, c, n \in \mathbb{Z}$, $c \neq 0$, und sei $d := ggT(c, n)$. Dann gilt:*

$$ac \equiv bc \mod n \quad \Longleftrightarrow \quad a \equiv b \mod \frac{n}{d}$$

Beweis. "⇐": Aus $a \equiv b \mod \frac{n}{d}$ folgt $a - b = \frac{n}{d}m$ für ein $m \in \mathbb{Z}$. Multiplizieren mit c gibt $ac - bc = n(\frac{c}{d}m)$. Da $d|c$, folgt $\frac{c}{d}m \in \mathbb{Z}$, also $ac \equiv bc \mod n$.
"⇒": Aus $ac \equiv bc \mod n$ folgt $(a-b)c = nk$ für ein $k \in \mathbb{Z}$, also $(a-b)\frac{c}{d} = \frac{n}{d}k$. Da $d = \mathrm{ggT}(c, n)$, gibt es $u, v \in \mathbb{Z}$ mit $uc + vn = d$, also $\frac{c}{d}u + \frac{n}{d}v = 1$. Es folgt: $\frac{n}{d}ku = (a - b)\frac{c}{d}u = (a - b)(1 - \frac{n}{d}v) = (a - b) - \frac{n}{d}v(a - b)$. Also $a - b = \frac{n}{d}(ku + v(a - b))$ und damit $a \equiv b \mod \frac{n}{d}$, da $(ku + v(a - b)) \in \mathbb{Z}$. □

Siebente Vorlesung – Der Restsatz

"Ich denke mir eine Zahl zwischen 1 *und* 100*. Durch* 3 *geteilt hat sie den Rest* 2*, durch* 4 *geteilt den Rest* 1 *und durch* 5 *geteilt den Rest* 3*."*

In der letzten Vorlesung haben wir gesehen, wie lineare Kongruenzen der Form $ax \equiv b \mod n$ nach x gelöst werden können. Jetzt untersuchen wir *simultane lineare Kongruenzen*. Das Rätsel lässt sich wie folgt fomulieren: Gesucht ist eine ganze Zahl x, welche die drei Kongruenzen erfüllt:

$$x \equiv 2 \mod 3, \qquad x \equiv 1 \mod 4, \qquad x \equiv 3 \mod 5$$

Der folgende Satz, der unter dem Namen *Chinesischer Restsatz* bekannt ist, beschreibt die Lösungen solcher simultanen Kongruenzen.

Satz 11 (Restsatz)**.** *Seien $n_1, n_2, \ldots, n_k \geqslant 1$ paarweise teilerfremde natürliche Zahlen, $n := n_1 \cdot \ldots \cdot n_k$, und seien $a_1, \ldots, a_k$ beliebige ganze Zahlen. Dann bilden die Lösungen $x \in \mathbb{Z}$ der simultanen Kongruenzen*

$$x \equiv a_1 \mod n_1, \qquad x \equiv a_2 \mod n_2, \quad \ldots, \quad x \equiv a_k \mod n_k$$

eine einzige Restklasse modulo n.

Beweis. Wir definieren m_i als das Produkt der n_j mit $j \neq i$. Mit anderen Worten: $m_i := n_1 \cdot \ldots \cdot n_{i-1} \cdot n_{i+1} \cdot \ldots \cdot n_k = \frac{n}{n_i}$. Da jeder der Faktoren n_j teilerfremd zu n_i ist, sind auch m_i und n_i teilerfremd.

Mit Korollar 1 folgt daraus, dass die Kongruenz $m_i x \equiv 1 \mod n_i$ eine einzige Restklasse $\overline{\ell_i}$ modulo n_i als Lösungsmenge hat – es gilt also $m_i \ell_i \equiv 1 \mod n_i$. Wir betrachten jetzt die Zahl

$$x := a_1 m_1 \ell_1 + a_2 m_2 \ell_2 + \ldots + a_k m_k \ell_k$$

und behaupten, dass x eine Lösung der simultanen Kongruenzen ist. Es genügt nämlich zu überprüfen, dass $x \equiv a_i \mod n_i$ für jedes $i \in \{1, \ldots, k\}$. Dazu bemerken wir, dass $n_i | m_j$ für alle $i \neq j$, also $a_j m_j \ell_j \equiv 0 \mod n_i$, woraus folgt, dass $x \equiv a_i m_i \ell_i \equiv a_i \cdot 1 \equiv a_i \mod n_i$.

Natürlich folgt sofort, dass die ganze Restklasse $\overline{x}$ modulo n aus Lösungen der simultanen Kongruenzen besteht, denn aus $y \equiv x \mod n$ folgt, dass $y \equiv x \equiv a_i \mod n_i$ für jedes $i \in \{1, \ldots, k\}$.

Es bleibt zu zeigen, dass $\overline{x}$ die *einzige* Restklasse von Lösungen ist. Angenommen, $y \in \mathbb{Z}$ sei irgend eine Lösung der simultanen Kongruenzen, also $y \equiv a_i \equiv x \mod n_i$ für alle i. Das bedeutet, dass $n_i | (y - x)$ für alle i. Da die n_i paarweise teilerfremd sind, folgt daraus, dass $n | (y - x)$, also folgt $\overline{y} = \overline{x}$. $\square$

Bemerkung. Ähnlich wie bei Satz 9 zeigt der Beweis nicht nur die Aussage des Satzes, sondern liefert auch einen Lösungsalgorithmus für solche simultanen Kongruenzen.

Beispiel. Im einleitenden Beispiel am Anfang des Kapitels,

$$x \equiv 2 \mod 3, \qquad x \equiv 1 \mod 4, \qquad x \equiv 3 \mod 5,$$

sind $(n_1, n_2, n_3) = (3, 4, 5)$ und $(a_1, a_2, a_3) = (2, 1, 3)$. Also $n = 3 \cdot 4 \cdot 5 = 60$ und $(m_1, m_2, m_3) = (4 \cdot 5, 3 \cdot 5, 3 \cdot 4) = (20, 15, 12)$. Als Nächstes benötigen wir Lösungen der Kongruenzen $m_i x \equiv 1 \mod n_i$. Für $i = 1$ haben wir $20x \equiv 1 \mod 3$. Wir können zum Beispiel $\ell_1 = 2$ als Lösung nehmen, denn $20 \cdot 2 - 1 = 39$ ist durch 3 teilbar. Ähnlich für $i = 2$, $15x \equiv 1 \mod 4$, wo wir $\ell_2 = -1$ wählen können und für $i = 3$, $12x \equiv 1 \mod 5$, wo $\ell_3 = -2$ eine mögliche Wahl ist. Damit haben wir

$$x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot (-1) + 3 \cdot 12 \cdot (-2) = -7.$$

Natürlich würde eine andere Wahl für ℓ_1, ℓ_2, ℓ_3 zu einem anderen Wert für x führen. Aber dessen Restklasse modulo 60 wird unabhängig von der Wahl immer dieselbe sein (das ist Teil des Beweises von Satz 11). Die Lösungsmenge ist also die Restklasse von -7 modulo 60.

$$\overline{-7} = \{\ldots, -127, -67, -7, 53, 113, 173, 233, \ldots\}$$

Bemerkung. In Satz 11 (Restsatz) haben wir ausschließlich Systeme linearer Kongruenzen der Form $x \equiv a_i \mod n_i$ betrachtet. Hat man es mit einem System allgemeiner linearer Kongruenzen der Form $a_i x \equiv b_i \mod n_i$ zutun, kann man diese mithilfe von Satz 9 zuerst einzeln lösen und die Lösungen als Restklasse (modulo einem Teiler von n_i) darstellen. Damit lässt sich das Problem auf Satz 11 zurückführen.

Beispiel. Betrachten wir die simultanen Kongruenzen

$$3x \equiv 6 \mod 12, \qquad 3x \equiv 1 \mod 5, \qquad 2x \equiv 5 \mod 7$$

Die erste Kongruenz $3x \equiv 6 \mod 12$ hat 3 verschiedene Restklassen von Lösungen modulo 12, nämlich $\overline{2}, \overline{6}$ und $\overline{10}$. Deren Vereinigung ist genau die Restklasse $\overline{2}$ modulo 4. Wir können die erste Kongruenz also durch die äquivalente Kongruenz $x \equiv 2 \mod 4$ ersetzen. Die zweite Kongruenz,

$3x \equiv 1 \mod 5$, hat genau die Lösungen $x = 2 + 5k$, mit $k \in \mathbb{Z}$, was genau die Lösungsmenge von $x \equiv 2 \mod 5$ ist. Die dritte Kongruenz $2x \equiv 5 \mod 7$ hat schließlich die Lösungen $x = -1 + 7k$ für $k \in \mathbb{Z}$, also können wir sie durch die Kongruenz $x \equiv -1 \mod 7$ ersetzen. Insgesamt haben wir das Kongruenzsystem zurückgeführt auf das System

$$x \equiv 2 \mod 4, \qquad x \equiv 2 \mod 5, \qquad x \equiv -1 \mod 7,$$

welches wir mithilfe von Satz 11 (Restsatz) lösen können (denn 4, 5 und 7 sind paarweise teilerfremd).

Beispiel. Wenn die n_i in Satz 11 nicht teilerfremd sind, kann es vorkommen, dass die simultanen Kongruenzen $x \equiv a_i \mod n_i$ überhaupt keine Lösung haben, wie das folgende Beispiel zeigt:

$$x \equiv 3 \mod 9, \qquad x \equiv 2 \mod 6$$

Ist $x \in \mathbb{Z}$ eine Lösung der ersten Kongruenz $x \equiv 3 \mod 6$, so folgt, dass x durch 3 teilbar ist. Dann kann aber x keine Lösung der zweiten Kongruenz sein. Das Problem liegt hier darin, dass 9 und 6 den gemeinsamen Teiler 3 haben; beide Kongruenzen machen also Aussagen über die Restklasse von x modulo 3 – in diesem Fall sind es widersprüchliche Aussagen.

Falls es jedoch keine Widersprüche zwischen den einzelnen Kongruenzen einer simultanen Kongruenz gibt, können diese durch ein äquivalentes System von Kongruenzen ersetzt werden, bei dem die n_i paarweise teilerfremd sind. Damit lässt sich die Lösung wieder auf Satz 11 (Restsatz) zurückführen.

$2 \cdot 2 \cdot 2$. Vorlesung – Repetitionsstunde

3^2. Vorlesung – Primzahlen und Quadrate

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
mod 4	2	3	1	3	3	1	1	3	3	1	3	1	1	3	3	1	3

$$5 = 1^2 + 2^2 \qquad 13 = 2^2 + 3^2 \qquad 17 = 1^2 + 4^2 \qquad 29 = 2^2 + 5^2$$

$$37 = 1^2 + 6^2 \qquad 41 = 4^2 + 5^2 \qquad 53 = 2^2 + 7^2$$

Was fällt auf? Die Primzahlen $p \equiv 1 \mod 4$ scheinen sich als Summe zweier Quadrate darstellen zu lassen – eine besondere Eigenschaft, die nicht jede natürliche Zahl hat: Zum Beispiel kommen für $7 = a^2 + b^2$ nur a, b mit $1 \leqslant a, b \leqslant 2$ in Frage (weil $3^2 = 9$ bereits zu groß ist), aber weder $1^2 + 1^2$, noch $1^2 + 2^2$, noch $2^2 + 2^2$ ist gleich 7. Daher lässt sich 7 nicht als Summe zweier Quadratzahlen darstellen.

Dass dieses Muster nicht nur zufällig bei den ersten siebzehn Primzahlen auftritt, ist die Aussage des *Zwei-Quadrate-Satzes von Fermat*.

Satz 12 (Fermat)**.** *Jede Primzahl p mit der Eigenschaft $p \equiv 1 \mod 4$ lässt sich als Summe zweier Quadratzahlen darstellen.*

Den folgenden Beweis kann man im *Buch der Beweise* von Aigner und Ziegler nachlesen. Er wurde offenbar von Roger Heath-Brown 1971 entdeckt; die hier wiedergegebene "visuelle Version" wurde 2007 vom Moskauer Mathematiklehrer Alexander Spivak präsentiert.

Beweis. Sei p eine Primzahl der Form $p = 4n + 1$. Wenn $n = m^2$ eine Quadratzahl wäre, stünde da $p = 4m^2 + 1 = (2m)^2 + 1^2$, und wir hätten p bereits als Summe zweier Quadrate ausgedrückt. So leicht geht es nicht, denn es gibt keinen Grund, weshalb n ein Quadrat sein sollte. Aber wir nehmen diese Bemerkung zur Inspiration: Um etwas mehr Spielraum zu haben, ersetzen wir $m^2 = m \cdot m$ durch zwei unabhängige Variablen $x \cdot y$ und die 1 durch eine dritte Variable z.

$$p = 4xy + z^2$$

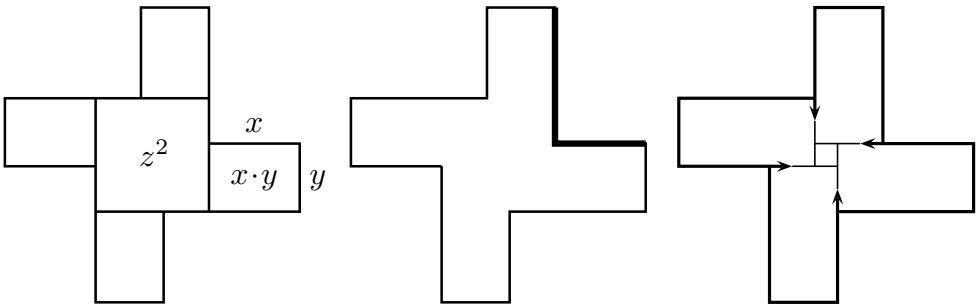
Falls es x, y, z gibt, welche diese Gleichung und zusätzlich $x = y$ erfüllen, bedeutet das, dass sich p als Summe zweier Quadrate schreiben lässt, nämlich

$$p = 4xx + z^2 = (2x)^2 + z^2$$

Wir interessieren uns also für die Menge der Lösungen:

$$\{(x, y, z) \in \mathbb{N}^3 \mid 4xy + z^2 = p\}$$

Zwei Lösungstripel kennen wir bereits, weil $p = 4n+1$; nämlich $(x, y, z) = (n, 1, 1)$ und $(x, y, z) = (1, n, 1)$. Jedes Lösungstripel (x, y, z) definiert eine Dachterrasse der gezeigten Form:



Um eine quadratische Platte der Seitenlänge z in der Mitte sind vier rechteckige Platten vom Format x mal y angelegt, und zwar so, dass die Seite der Länge y an der mittleren Platte anliegt, wie im linken Bild.

Die Dachterrasse hat die Gesamtfläche $4xy + z^2 = p$. Wir legen sie immer so an, dass das "L" oben rechts (fett gedruckt im mittleren Bild) mindestens so hoch wie breit ist. Das Bild rechts zeigt, dass dieselbe Dachterrasse immer durch zwei Lösungstripel $(x, y, z), (x', y', z')$ beschrieben wird (die mittlere Platte der Seitenlänge z' ist dort kleiner als im linken Bild).

Wann sind $(x, y, z) = (x', y', z')$? Genau dann, wenn das "L" gleich hoch wie breit ist, das heißt, wenn die Terrasse aussieht wie ein Schweizerkreuz. Aber dann ist $y = z$, also ist $p = 4xy + z^2$ durch z teilbar. Da p prim ist, muss in diesem Fall $z = 1$ sein, also auch $y = 1$. Wir erhalten also die Lösung, die wir schon kennen: $(n, 1, 1)$.

Jede solche Terrasse kann also auf zwei verschiedene Arten mit Platten belegt werden und entspricht daher zwei verschiedenen Lösungen – außer jene, die zur Lösung $(n, 1, 1)$ gehört. Daraus folgt, dass es insgesamt eine *ungerade* Zahl von Lösungen gibt.

Diejenigen Lösungen (x, y, z), für die $x \neq y$ ist, kommen aber ebenfalls in Paaren vor: Wenn (x, y, z) eine Lösung ist, dann offensichtlich auch (y, x, z). Die Zahl der übrigen Lösungen (x, y, z), für die $x = y$ ist, muss also ungerade sein, woraus folgt, dass es mehr als 0 davon gibt! □

Zehnte & elfte Vorlesung – Der kleine Fermat

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$2^n \mod 7$	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4	1	2
$3^n \mod 7$	1	3	2	6	4	5	1	3	2	6	4	5	1	3	2	6	4
$4^n \mod 7$	1	4	2	1	4	2	1	4	2	1	4	2	1	4	2	1	4
$5^n \mod 7$	1	5	4	6	2	3	1	5	4	6	2	3	1	5	4	6	2
$6^n \mod 7$	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1

Was fällt auf? Die Restklassen von a^n modulo 7 wiederholen sich immer nach 6 Schritten (eins weniger als 7), und zwar für jede Wahl der Basis a. Dieses Muster zeigt sich nicht nur zufällig bei Potenzen modulo 7, sondern lässt sich auf alle Primzahlen übertragen:

Satz 13 (Der kleine Satz von Fermat)**.** *Sei p eine Primzahl und a eine ganze Zahl mit $a \not\equiv 0 \mod p$. Dann gilt $a^{p-1} \equiv 1 \mod p$.*

Beweis. $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ sind alle Restklassen modulo p die es gibt, außer $\overline{0}$. Multiplizieren wir alle mit $\overline{a}$, erhalten wir die Restklassen $\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}$.

Wir zeigen jetzt, dass das genau dieselben Restklassen sind, nur vielleicht in einer anderen Reihenfolge: Da $a \not\equiv 0 \mod p$, ist $\mathrm{ggT}(a,p) = 1$. Nach Satz 9 (Lineare Kongruenzen) gibt es also ein $b \in \mathbb{Z}$ mit $\overline{ab} = \overline{1}$. Wären zwei Restklassen der zweiten Liste gleich, also $\overline{ua} = \overline{va}$ für zwei verschiedene $u, v \in \{1, 2, \ldots, p-1\}$, so folgte $\overline{u} = \overline{uab} = \overline{vab} = \overline{v}$, also $u = v$, Widerspruch. Es sind also $p-1$ verschiedene Restklassen, und keine davon ist $\overline{0}$ (sonst wäre $\overline{ua} = \overline{0}$ für ein $u \in \{1, 2, \ldots, p-1\}$, also $\overline{u} = \overline{uab} = \overline{0 \cdot b} = \overline{0}$, Widerspruch).

Die beiden Listen enthalten also genau dieselben Restklassen. Das bedeutet, das Produkt der Restklassen der zweiten Liste ist gleich dem Produkt der ersten:

$$a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a \quad \equiv \quad 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \qquad \mod p$$

Auf der linken Seite lässt sich a^{p-1} faktorisieren; wir erhalten also

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$$

Da $p \nmid (p-1)!$ (sonst würde p einen der Faktoren teilen, was nicht möglich ist), können wir die Kongruenz kürzen und erhalten $a^{p-1} \equiv 1 \mod p$. □

Korollar 2. *Ist p prim und $a \in \mathbb{Z}$ beliebig, dann gilt $a^p \equiv a \mod p$.*

Beweis. Falls $a \equiv 0 \mod p$ ist die Aussage klar erfüllt; falls $a \not\equiv 0 \mod p$, folgt sie aus Satz 13 durch Multiplikation mit a auf beiden Seiten. □

Fermats kleiner Satz hat große Auswirkungen: Damit lassen sich nämlich sehr effizient die Restklassen von großen Potenzen berechnen. Diese Methode spielt in der Verschlüsselung und Entschlüsselung von Nachrichten (Kartenzahlung übers Internet, E-Mails) eine wichtige Rolle.

Beispiel. Welcher Rest bleibt bei Division der Zahl 18^{113} durch 23? Da 23 eine Primzahl ist und $18 \not\equiv 0 \mod 23$, können wir Fermats kleinen Satz anwenden mit $p = 23$ und $a = 18$ und erhalten $18^{22} \equiv 1 \mod 23$. Statt die astronomisch große Zahl 18^{113} mit ihren 142 Dezimalstellen erst zu berechnen und dann durch 23 zu dividieren, genügt es, den Exponenten 113 durch 22 zu dividieren: $113 = 5 \cdot 22 + 3$. Die weitere Rechnung ist dann nicht mehr schwer: $18^{113} = (18^{22})^5 \cdot 18^3 \equiv 1^5 \cdot 18^3 \equiv (-5)^3 = -125 \equiv -10 \equiv 13 \mod 23$. Der gesuchte Rest ist also 13.

Der Kleine Fermat lässt sich auch als Primzahltest verwenden: Angenommen, wir möchten wissen, ob n eine Primzahl ist. Sobald wir eine ganze Zahl a finden mit der Eigenschaft $a^n \not\equiv a \mod n$, wissen wir, dass n keine Primzahl sein kann.

Umgekehrt kann man sich fragen, ob eine Zahl n, die jeden solchen Primzahltest besteht, tatsächlich eine Primzahl sein muss. Diese sehr verlockende Vermutung trifft allerdings nicht zu: $n = 561 = 3 \cdot 11 \cdot 17$ ist zwar keine Primzahl, aber man kann zeigen, dass $a^{561} \equiv a \mod 561$ für alle $a \in \mathbb{Z}$ gilt. Solche "Schein-Primzahlen" nennt man *Carmichael-Zahlen*. Sie treten zwar sehr viel seltener auf als Primzahlen – was den Test für praktische Anwendungen wie die Kryptographie nützlich macht – trotzdem gibt es unendlich viele davon (1912 vermutet von Carmichael; 1992 bewiesen von Alford, Granville und Pomerance).

Die Voraussetzung, dass p eine Primzahl sei, ist im kleinen Satz von Fermat wesentlich. Zum Beispiel ist $2^6 = 64 \not\equiv 2 \mod 6$. Trotzdem lässt sich der Satz auf den allgemeinen Fall von Kongruenzen modulo n anpassen, wobei n nicht unbedingt eine Primzahl ist: Im Beweis haben wir vor allem verwendet, dass $\mathrm{ggT}(a, p) = 1$. Die Bedingung $a \not\equiv 0 \mod p$ ersetzen wir also durch die Bedingung: $\mathrm{ggT}(a, n) = 1$. Der Exponent $p - 1$ kam dadurch zustande, dass es $p - 1$ Reste modulo p gibt, die zu p teilerfremd sind.

Definition 10 (Eulers φ-Funktion)**.** $\varphi(n)$ ist die Anzahl der Restklassen $\overline{c}$ modulo n, für die $\mathrm{ggT}(c, n) = 1$ gilt.

Beispiele.

- Die möglichen Reste modulo $n = 12$ sind $0, 1, 2, \ldots, 11$. Davon sind nur vier teilerfremd zu 12, nämlich $1, 5, 7$ und 11. Daher ist $\varphi(12) = 4$.
- Falls p eine Primzahl ist, gilt $\varphi(p) = p-1$, denn die Reste $1, 2, \ldots, p-1$ sind alle teilerfremd zu p.
- Hier sind die ersten fünfzehn Werte von Eulers Funktion:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Der folgende Satz von Euler ist die angedeutete Verallgemeinerung des kleinen Satzes von Fermat:

Satz 14 (Euler)**.** *Falls* $ggT(a, n) = 1$*, dann gilt* $a^{\varphi(n)} \equiv 1 \mod n$.

Beispiel. Wie lautet die letzte Ziffer der Zahl 3^{774}? Da 3 und 10 teilerfremd sind, können wir Eulers Satz auf $a = 3$ und $n = 10$ anwenden. Wir erhalten: $3^4 \equiv 1 \mod 10$, denn $\varphi(10) = 4$. Dividieren wir den Exponenten 774 durch 4, erhalten wir: $774 = 193 \cdot 4 + 2$, also $3^{774} = (3^4)^{193} \cdot 3^2 \equiv 1^{193} \cdot 3^2 \equiv 9 \mod 10$, also ist 9 die letzte Ziffer.

Lemma 8. *Für zwei verschiedene Primzahlen* p, q *gilt* $\varphi(pq) = (p-1)(q-1)$.

Beweis. Die positiven Teiler von pq sind $1, p, q, pq$. Ist $a \in \{0, 1, 2, \ldots, pq-1\}$ mit $\mathrm{ggT}(a, pq) \neq 1$, dann muss also a ein Vielfaches von p oder ein Vielfaches von q sein. Es gibt genau q Vielfache von p zwischen 0 und $pq - 1$, nämlich $0, p, 2p, 3p, \ldots, (q-1)p$. Genauso gibt es genau p Vielfache von q zwischen 0 und $pq-1$. Darunter gibt es eine einzige Zahl, die sowohl Vielfaches von p als auch Vielfaches von q ist, nämlich 0. Also gibt es unter den pq Restklassen modulo pq genau $p+q-1$ Restklassen $\overline{c}$, für die $\mathrm{ggT}(c, pq) \neq 1$. Daraus folgt: $\varphi(pq) = pq - (p + q - 1) = (p-1)(q-1)$. □

Die in den Beispielen genannte Gleichung $\varphi(p) = p - 1$ für Primzahlen p, und auch die Aussage des Lemmas lassen sich so verallgemeinern, dass aus der Primfaktorzerlegung einer natürlichen Zahl $n \geqslant 2$ recht einfach der Wert von Eulers Funktion, $\varphi(n)$, berechnet werden kann:

Satz 15 (Eigenschaften der φ-Funktion)**.**

(a) $\varphi(p^n) = p^n - p^{n-1}$ *für jede Primzahl* p *und jede natürliche Zahl* $n \geqslant 1$*.*

(b) $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ *für teilerfremde Zahlen* $m, n \in \mathbb{N}$*.*

Bemerkung. Für $n = 1$ reduziert sich Teil (a) auf die bereits erwähnte Gleichung $\varphi(p) = p - 1$. Falls m, n zwei verschiedene Primzahlen sind, erhalten wir daraus als Spezialfall von Teil (b) die Aussage von Lemma 8.

Beispiel. Die Zahl 200 hat die Primfaktorzerlegung $200 = 2^3 \cdot 5^2$. Da 2^3 und 5^2 teilerfremd sind, haben wir $\varphi(200) = \varphi(2^3 \cdot 5^2) = \varphi(2^3) \cdot \varphi(5^2)$, mit Teil (b) des Satzes. Mit Teil (a) folgt $\varphi(2^3) = 2^3 - 2^2 = 4$ und $\varphi(5^2) = 5^2 - 5^1 = 20$, also $\varphi(200) = 4 \cdot 20 = 80$.

Im nächsten Abschnitt schauen wir uns ein berühmtes Beispiel einer Anwendung elementarer Zahlentheorie an, welches einen bestimmten Aspekt des täglichen Lebens radikal verändert hat – fast 300 Jahre nachdem Fermat seinen Satz formuliert hat.

Die Rivest-Shamir-Adleman – Verschlüsselung (RSA)

In den 1970er Jahren haben diese drei Autoren ihre *Method for Obtaining Digital Signatures and Public-Key Cryptosystems* veröffentlicht und damit die abhörsichere öffentliche Kommunikation ermöglicht: zwei Menschen unterhalten sich über einen öffentlichen Kommunikationskanal (das heißt, jeder kann alle Nachrichten lesen oder abhören, die die beiden sich zusenden), und trotzdem bleiben die übermittelten Informationen geheim und ausschliesslich für die beiden verständlich – und das, ohne dass sich die beiden zuerst im Geheimen über eine Verschlüsselungsmethode geeinigt hätten.

Die Methode wird (mit einigen zusätzlichen Verbesserungen, auf die wir hier nicht eingehen) bis heute verwendet, unter anderem bei Transaktionen beim Einkaufen mit der Kreditkarte übers Internet, beim E-Banking, bei der E-Mail-Verschlüsselung und für Netzwerk-Übertragungsprotokolle. Die Information auf dem RFID-Chip im deutschen Reisepass ist ebenfalls mit der RSA-Methode verschlüsselt.

Die RSA-Methode. Sophia möchte Anna eine geheime Nachricht senden.

1. Anna wählt zwei verschiedene Primzahlen p, q. Sie berechnet $n := pq$ und $\varphi(n) = (p-1)(q-1)$. Dazu wählt sie $a \in \mathbb{N}$ teilerfremd zu $\varphi(n)$. Das Zahlenpaar (a, n) ist Annas *öffentlicher Schlüssel*. Dann findet sie ein $b \in \mathbb{N}$, so dass $ab \equiv 1 \mod \varphi(n)$. Diese Zahl b ist ihr *privater Schlüssel*.

2. Anna $\longmapsto (a, n) \longrightarrow$ Sophia (über den öffentlichen Kanal)

3. Sophia übersetzt ihre geheime Nachricht in eine Folge von natürlichen Zahlen $(c_1, \ldots, c_k)$ mit $c_i < n$ und berechnet $0 \leqslant r_1, \ldots, r_k < n$ so dass $r_i \equiv (c_i)^a \mod n$. Die Zahlenfolge $(r_1, \ldots, r_k)$ ist die verschlüsselte Nachricht.

4. Sophia $\longmapsto (r_1, \ldots, r_k) \longrightarrow$ Anna (über den öffentlichen Kanal)

5. Anna berechnet $0 \leqslant s_1, \ldots, s_k < n$ so dass $s_i \equiv (r_i)^b \mod n$. Da $ab \equiv 1 \mod \varphi(n)$, ist $ab - 1$ ein Vielfaches von $\varphi(n)$. Falls $\mathrm{ggT}(c_i, n) = 1$, sagt der Satz 14 (Euler), dass $(c_i)^{ab-1} \equiv 1 \mod n$. Daraus folgt:

$$s_i \equiv (r_i)^b \equiv ((c_i)^a)^b \equiv (c_i)^{ab} \equiv c_i \cdot (c_i)^{ab-1} \equiv c_i \cdot 1 \equiv c_i \mod n$$

   Sie hat also Sophias Nachricht entschlüsselt, denn $s_i = c_i$.
   Tatsächlich gilt $c_i^{ab} \equiv c_i \mod n$ immer, sogar wenn $\mathrm{ggT}(c_i, n) \neq 1$: Dazu überprüft man separat die Kongruenzen $c_i^{ab} \equiv c_i \mod p$ und $c_i^{ab} \equiv c_i \mod q$: Wenn $c_i \equiv 0 \mod p$, ist die Kongruenz $c_i^{ab} \equiv c_i \mod p$ offensichtlich erfüllt, weil beide Seiten kongruent 0 sind. Wenn dagegen $c_i \not\equiv 0 \mod p$, sagt Satz 13 (Kleiner Fermat), dass $c_i^{p-1} \equiv 1 \mod p$. Da $ab - 1$ ein Vielfaches von $\varphi(n) = (p-1)(q-1)$ ist, ist es auch ein Vielfaches von $(p-1)$, also folgt $c_i^{ab-1} \equiv 1 \mod p$ und deshalb $c_i^{ab} \equiv c_i \mod p$. Genauso zeigt man die Kongruenz modulo q.

Eine Spionin, die die Kommunikation abhört, könnte natürlich die Zahl n in ihre Primfaktoren p, q zerlegen, damit Annas privaten Schlüssel berechnen und somit Sophias Nachricht entschlüsseln.

Die Sicherheit der RSA-Methode beruht darauf, dass es mit den heute bekannten Methoden extrem aufwändig ist, die Primfaktorzerlegung einer großen Zahl zu berechnen (einige hundert Dezimalstellen genügen), während alle für Anna und Sophia nötigen Rechenoperationen dank des Algorithmus

von Euklid und des kleinen Satzes von Fermat mit einem Computer sehr effizient durchführbar sind.

Das folgende Beispiel illustriert die RSA-Methode (der Einfachheit halber mit unrealistisch kleinen Primzahlen).

Beispiel. Anna wählt $p = 11$, $q = 13$ und berechnet $n = pq = 143$ und $\varphi(n) = (p-1)(q-1) = 120$. Dazu wählt Anna $a = 17$. Der öffentliche Schlüssel ist also $(17, 143)$. Sophia möchte die geheime Nachricht

DACHTERRASSE

an Anna übermitteln. Öffentlich einigen sie sich, dass die Buchstaben des Alphabets wie folgt codiert sind:

A	B	C	$\cdots$	Y	Z
1	2	3	$\cdots$	25	26

Sophia definiert also $(c_1, \ldots, c_{12}) = (4, 1, 3, 8, 20, 5, 18, 18, 1, 19, 19, 5)$. Dann berechnet sie die Reste der Potenzen c_i^{17} bei Division durch 143, die sie an Anna sendet:

$$(r_1, \ldots, r_{12}) = (49, 1, 9, 112, 37, 135, 83, 83, 1, 2, 2, 135)$$

Zum Beispiel lässt sich der sechste Eintrag folgendermaßen berechnen: Wir schreiben zuerst $5^{17} = 5^{16} \cdot 5 = (((5^2)^2)^2)^2 \cdot 5 = (((25)^2)^2)^2 \cdot 5 = ((625)^2)^2 \cdot 5$. Dann wenden wir wiederholt Euklids Algorithmus an, um große Zahlen (zum Beispiel 625) durch ihre Reste bei Division durch 143 zu ersetzen:

$$5^{17} \equiv (53^2)^2 \cdot 5 \equiv (2809)^2 \cdot 5 \equiv 92^2 \cdot 5 \equiv 8464 \cdot 5 \equiv 27 \cdot 5 \equiv 135 \mod 143$$

Um Sophias Nachricht zu entschlüsseln, konstruiert Anna eine Zahl b mit $17 \cdot b \equiv 1 \mod 120$. Sie kennt sich mit solchen linearen Kongruenzen gut aus und weiss, wie das geht: $b = 113$. Dann berechnet sie die Reste der $(r_i)^{113}$ bei Division durch 143, et voilà: $(4, 1, 3, 8, 20, 5, 18, 18, 1, 19, 19, 5)$. Jetzt braucht sie nur noch im Alphabet abzuzählen.

Zwölfte & dreizehnte Vorlesung – Kettenbrüche

Nachdem bisher die ganzen Zahlen im Mittelpunkt standen, wollen wir jetzt am Beispiel der Kettenbrüche einen kurzen Ausflug zu den den rationalen und irrationalen Zahlen unternehmen.

Definition 11 (Endlicher Kettenbruch)**.** Seien $a_1, \ldots, a_n \geqslant 1$ positive ganze Zahlen und a_0 eine beliebige ganze Zahl. Der *Kettenbruch* $[a_0, a_1, a_2, \ldots, a_n]$ ist definiert als die folgende rationale Zahl:

$$[a_0, a_1, a_2, \ldots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

Beispiel.

$$[2,3,1,4] \;=\; 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}} \;=\; 2 + \cfrac{1}{3 + \cfrac{1}{\frac{5}{4}}} \;=\; 2 + \cfrac{1}{3 + \frac{4}{5}} \;=\; 2 + \cfrac{1}{\frac{19}{5}} \;=\; \frac{43}{19}$$

Ein Kettenbruch lässt sich also in einen einfachen Bruch umschreiben. Umgekehrt geht es auch:

Lemma 9. *Sind $a, b \in \mathbb{Z}$ mit $b \neq 0$, dann gilt $\frac{a}{b} = [q_1, q_2, \ldots, q_n]$, wobei die Zahlen $q_1, \ldots, q_n$ die Quotienten sind, die beim Anwenden von Euklids Algorithmus auf a und b entstehen.*

Beweis. Wenden wir den Algorithmus von Euklid auf a und b an:

$$\begin{array}{rcll}
a & = & q_1 b + r_1 & 0 \leqslant r_1 < b \\
b & = & q_2 r_1 + r_2 & 0 \leqslant r_2 < r_1 \\
r_1 & = & q_3 r_2 + r_3 & 0 \leqslant r_3 < r_2 \\
 & \vdots & & \vdots \\
r_{n-3} & = & q_{n-1} r_{n-2} + r_{n-1} & 0 \leqslant r_{n-1} < r_{n-2} \\
r_{n-2} & = & q_n r_{n-1} + 0 &
\end{array}$$

Teilen wir die erste Gleichung durch b, die zweite durch r_1, die dritte durch r_2, und so weiter, erhalten wir

$$\begin{aligned}
\frac{a}{b} &= q_1 + \frac{r_1}{b} = q_1 + \frac{1}{b/r_1} \\
\frac{b}{r_1} &= q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{r_1/r_2} \\
&\vdots \\
\frac{r_{n-3}}{r_{n-2}} &= q_{n-1} + \frac{r_{n-1}}{r_{n-2}} = q_{n-1} + \frac{1}{r_{n-2}/r_{n-1}} \\
\frac{r_{n-2}}{r_{n-1}} &= q_n
\end{aligned}$$

Rückwärts Einsetzen führt zur behaupteten Kettenbruchdarstellung. □

Bemerkung. Wenn der letzte Koeffizient eines Kettenbruchs $a_n = 1$ ist, steht unter dem zweitletzten Bruchstrich $a_{n-1} + 1$. Das bedeutet, dass sich der Kettenbruch vereinfachen lässt; die Darstellung einer rationalen Zahl als endlicher Kettenbruch ist also nicht eindeutig: $[a_0, a_1, \ldots, a_{n-1}, 1]$ beschreibt dieselbe rationale Zahl wie $[a_0, a_1, \ldots, a_{n-1} + 1]$. Man kann aber relativ leicht zeigen, dass dies die einzige Mehrdeutigkeit ist.

Unendliche Kettenbrüche

Wenn statt einer endlichen Liste von Koeffizienten eine unendliche Folge ganzer Zahlen $a_0, a_1, a_2, \ldots$ gegeben ist, wobei $a_i \geqslant 1$ für $i \geqslant 1$, können wir den folgenden Ausdruck betrachten

$$[a_0, a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

und ihn interpretieren als Grenzwert der Zahlenfolge $x_0 = a_0$, $x_1 = [a_0, a_1]$, $x_2 = [a_0, a_1, a_2]$, $\ldots$, $x_n = [a_0, a_1, \ldots, a_n]$. Tatsächlich konvergiert eine solche unendliche Folge von Kettenbrüchen immer gegen eine irrationale Zahl, und die Darstellung einer irrationalen Zahl als unendlicher Kettenbruch ist immer eindeutig. Die Beweise dieser Behauptungen sind nicht schwer; trotzdem verzichten wir hier darauf.

Satz 16. *Jeder unendliche Kettenbruch beschreibt eine irrationale Zahl.*

Damit können wir sehr leicht irrationale Zahlen konstruieren: Es genügt, eine unendliche Zahlenfolge zu wählen und den zugehörigen Kettenbruch zu betrachten.

Beispiele. Hier sind einige bekannte unendliche Kettenbrüche.

$$\sqrt{2} = [1, 2, 2, 2, 2, \ldots]$$

$$\frac{1+\sqrt{5}}{2} = [1, 1, 1, 1, 1, 1, 1, \ldots] \qquad \text{(Der goldene Schnitt)}$$

$$e = \sum_{n \geqslant 0} \tfrac{1}{n!} = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] \qquad \text{(Eulersche Zahl)}$$

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, \ldots] \quad \text{(kein erkennbares Muster)}$$

$$\pi = 3 + \cfrac{1^2}{6 + \cfrac{3^2}{6 + \cfrac{5^2}{6 + \cfrac{7^2}{6 + \cfrac{9^2}{6 + \ddots}}}}}$$

Die letzte Darstellung von π als "Kettenbruch" ist kein Kettenbruch im Sinne unserer Definition 11, da von 1 verschiedene Zähler auftreten. Sie widerspricht also nicht der oben behaupteten Eindeutigkeit.

Ein unendlicher Kettenbruch $[a_0, a_1, a_2, \ldots]$ wird (per Definition) durch die Folge seiner endlichen Teilkettenbrüche beliebig präzise angenähert, nämlich durch $a_0, [a_0, a_1], [a_0, a_1, a_2], \ldots, [a_0, a_1, a_2, \ldots, a_n], \ldots$
Zum Beispiel erhält man für den Kettenbruch der Zahl π die folgenden Näherungswerte:

$$3, \quad [3, 7] = \frac{22}{7}, \quad [3, 7, 15] = \frac{333}{106}, \quad [3, 7, 15, 1] = \frac{355}{113}, \quad \ldots$$

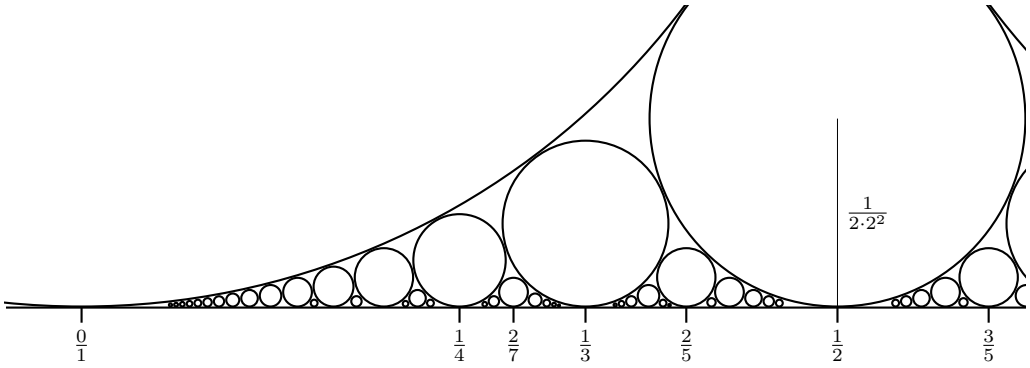
Der dritte Näherungsbruch ist $3.14150943\ldots$, stimmt also bereits bis zur vierten Stelle nach dem Komma mit dem Wert von π überein. Tatsächlich kann man zeigen, dass diese Näherungsmethode sehr effizient ist; unter allen

Folgen von rationalen Zahlen, die eine gegebene irrationale Zahl annähern, konvergiert die Folge der endlichen Teilkettenbrüche am schnellsten.

Wir zeigen jetzt eine sehr einfache geometrische Methode, um diese endlichen Teilkettenbrüche zu finden.

Die Kreispackung von Farey

Für jede rationale Zahl p/q in gekürzter Form[5] zeichnen wir in der Ebene einen Kreis vom Radius $1/2q^2$, der die Zahlengerade im Punkt p/q berührt. Dies führt zu folgendem Bild, der sogenannten *Kreispackung von Farey* [6].



Zu jeder rationalen Zahl gehört also genau ein Kreis, und je größer der Nenner, desto kleiner wird der zugehörige Kreis. Die Kreise, die zu ganzen Zahlen gehören, haben alle den Radius $\frac{1}{2}$.

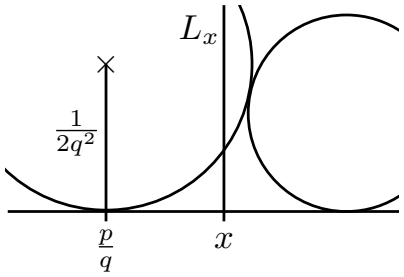
Lemma 10. *Die Kreise, die zu den (gekürzten) Brüchen $\frac{a}{b} \neq \frac{c}{d}$ gehören, berühren sich in einem Punkt, falls $ad - bc = \pm 1$. In diesem Fall gibt es genau einen weiteren Kreis, der die beiden berührt; nämlich den Kreis, der zum Bruch $\frac{a+c}{b+d}$ gehört. Andernfalls schneiden sich die beiden Kreise nicht.*

Die "falsche" Addition von zwei Brüchen $\frac{a}{b}$ und $\frac{c}{d}$, vor der in der Schule stets gewarnt wird, hat hier also eine Bedeutung: Der Bruch $\frac{a+c}{b+d}$ liegt "genau zwischen" $\frac{a}{b}$ und $\frac{c}{d}$, in dem Sinn, dass sich die drei zugehörigen Kreise paarweise berühren.

[5] Das heißt, p und q sind teilerfremde ganze Zahlen, und $q \geqslant 1$.

[6] Benannt nach John Farey, Geologe, 1766–1826.

Betrachten wir jetzt einen beliebigen Punkt x auf der Zahlengeraden, ziehen von x aus eine gerade Linie L_x senkrecht nach oben und schauen, welche Kreise der Gerade L_x am nächsten kommen. Durchquert L_x den Kreis, der zu einer rationalen Zahl p/q gehört, muss der Abstand von L_x zum Kreismittelpunkt kleiner sein als der Radius des Kreises. Da der Mittelpunkt genau über dem Punkt x auf der Zahlengerade liegt, folgt daraus, dass der Abstand zwischen x und p/q höchstens $1/2q^2$ beträgt:



$$\left| x - \frac{p}{q} \right| \leqslant \frac{1}{2q^2}$$

Die Zahl x wird in diesem Fall also sehr gut durch p/q approximiert.

Wir beschreiben jetzt, wie sich von der Gerade L_x und den Kreisen die Kettenbruchdarstellung einer Zahl x ablesen lässt: Wir wandern auf L_x von oben nach unten Richtung Zahlengerade und schauen stets, welcher Kreismittelpunkt uns am nächsten kommt. Dabei können wir immer nur diejenigen Punkte sehen, die auf unserer momentanen Höhe liegen. Mal liegt der nächste Kreismittelpunkt auf der rechten Seite von L_x, mal auf der linken; es wird also immer wieder vorkommen, dass wir unseren Blick von rechts nach links wenden (oder umgekehrt). Die Kreise *unmittelbar vor jedem Seitenwechsel* interessieren uns. Sie berühren die Zahlengerade bei bestimmten rationalen Zahlen; diese notieren wir in der Reihenfolge, in der sie uns auf unserer Reise begegnen: $x_0, x_1, x_2, \ldots$ Die erste Zahl in der Folge, x_0, ist die ganze Zahl, die x am nächsten liegt.

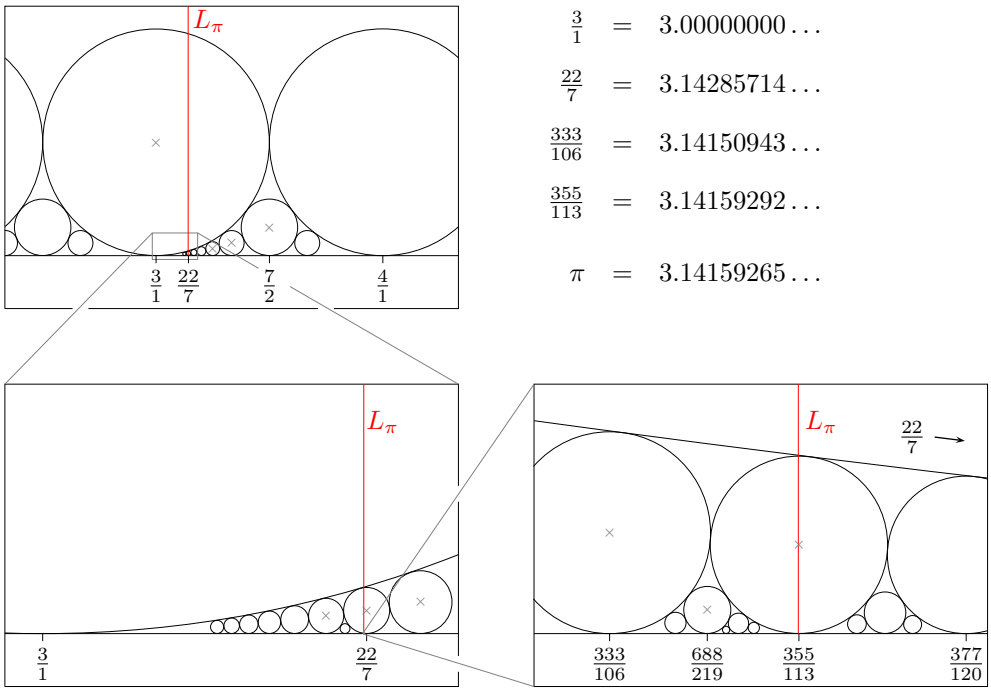
$$\begin{array}{rll} \text{Falls } x_0 < & x, & \text{dann} \\ & x & < x_1 \\ x_2 < & x & \\ & x & < x_3 \\ x_4 < & x & \\ & x & < x_5 \\ & \vdots & \end{array} \qquad \begin{array}{rll} \text{Falls} & x & < x_0, \text{ dann} \\ x_1 < & x & \\ & x & < x_2 \\ x_3 < & x & \\ & x & < x_4 \\ x_5 < & x & \\ & \vdots & \end{array}$$

Satz 17. *Falls x die Kettenbruchentwicklung $x = [a_0, a_1, a_2, a_3, a_4, \ldots]$ hat und $x_0, x_1, x_2, \ldots$ die Folge von rationalen Zahlen ist, die wir uns (wie oben beschrieben) notiert haben, dann gilt: $x_n = [a_0, a_1, \ldots, a_n]$.*

Beispiel. Als Beispiel betrachten wir die Zahl $\pi = 3.141592653589793\ldots$ Die Kreise, die der Geraden L_π am nächsten kommen, gehören zu den folgenden rationalen Zahlen (vergleiche mit der Abbildung weiter unten).

$$\frac{3}{1}, \quad \frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}, \quad \ldots$$

Wir erkennen die Näherungsbrüche von weiter oben wieder.



$$\begin{aligned}
\tfrac{3}{1} &= 3.00000000\ldots \\
\tfrac{22}{7} &= 3.14285714\ldots \\
\tfrac{333}{106} &= 3.14150943\ldots \\
\tfrac{355}{113} &= 3.14159292\ldots \\
\pi &= 3.14159265\ldots
\end{aligned}$$

Literatur

G.A. Jones, J.M. Jones: *Elementary Number Theory*
Springer-Verlag London, 1998, ISBN 978-3-540-76197-6.

M. Aigner, G. Ziegler: *Das Buch der Beweise*
Springer, 2018, ISBN: 978-3-662-57766-0.

I. Niven: *Irrational Numbers*
Mathematical Association of America, 1956, ISBN: 978-0-883-85011-4.

Version: 16. September 2020

GRIPS-Seite der Vorlesung:
`https://elearning.uni-regensburg.de/course/view.php?id=42327`