

Elementare Zahlentheorie

Prof. Dr. Hansen

16. Juni 2004

Inhaltsverzeichnis

1	Zahlen	3
1.1	Die natürlichen Zahlen \mathbb{N}	3
1.2	Die ganzen Zahlen \mathbb{Z}	5
1.3	Die rationalen Zahlen \mathbb{Q}	6
1.4	Die reellen Zahlen \mathbb{R}	6
2	Teilbarkeit und Primzahlen	7
2.1	Allgemeines und Definitionen	7
2.2	Bemerkungen zur Primzahlverteilung	18
2.3	Primzahlen in arithmetischen Progressionen	24
2.4	Primzahlen als Werte von Polynomen	25
2.5	Eulersche φ -Funktion	28
3	Kongruenzen und Restklassenringe	31
3.1	Allgemeines und Definitionen	31
3.2	Anwendung des Satzes von FERMAT-EULER in der Kryptographie	37
3.3	Satz von WILSON	38
3.4	Satz von EULER	40
3.5	Primfaktorzerlegung in $\mathbb{Z}[i]$	43
3.6	Chinesischer Restsatz	48
3.7	Polynomkongruenzen	49
4	Fibonacci-Zahlen	53
5	Zahlentheoretische Funktionen	56
5.1	Allgemeines und Definitionen	56
5.2	Anwendung auf die Eulersche φ -Funktion.	59
6	Prime Restklassen	60
6.1	Allgemeines	60
6.2	Primitivwurzeln zu Primzahlen	60
6.3	Quadratisches Reziprozitätsgesetz	66

1 Zahlen

1.1 Die natürlichen Zahlen \mathbb{N}

Die Menge der natürlichen Zahlen ist durch die *Peano-Axiome* charakterisiert:

- 1) 0 ist eine natürliche Zahl
- 2) Jede natürliche Zahl n hat genau einen Nachfolger n^+ .
- 3) 0 hat keinen Vorgänger, d.h. $\nexists n$ mit $n^+ = 0$.
- 4) Jede natürliche Zahl n außer 0 hat genau einen Vorgänger.
- 5) Ausgehend von 0 erhält man als Nachfolger alle natürlichen Zahlen.

Wir betrachten die Menge der natürlichen Zahlen \mathbb{N} mit

$$\mathbb{N} := \{0, 1, 2, \dots\} \text{ (d.h.: } 1 := 0^+, 2 := 1^+ \text{ usw.)}$$

Es sei $N^* := \mathbb{N} \setminus \{0\}$. Die Eigenschaft (5) schreibt sich formal so:

$$(M \subset \mathbb{N}, 0 \in M, (n \in M \Rightarrow n^+ \in M)) \Rightarrow M = \mathbb{N}$$

Sie ist äquivalent zum Prinzip der vollständigen Induktion:

Hat die Zahl 0 eine Eigenschaft (E) und hat mit n auch jeweils n^+ die Eigenschaft (E), dann haben alle natürlichen Zahlen die Eigenschaft (E).

Dies wird nicht nur in Beweisen verwandt, sondern auch zur rekursiven Definition. Salopp: Ist für 0 etwas definiert, und $\forall n \in \mathbb{N}$ auch etwas für n^+ definiert, so auch für alle natürlichen Zahlen.

Beispiel 1.1 (Definition der Addition). Für $m \in \mathbb{N}$ sei

$$\begin{aligned} m + 0 &:= m \\ m + n^+ &:= (m + n)^+ \end{aligned}$$

Damit sind alle Rechenregeln für natürliche Zahlen beweisbar.

- 1) Assoziativgesetz: $(k + m) + n = k + (m + n)$

Beweis.

$$(k + m) + 0 = k + m = k + (m + 0)$$

Sei $n \in \mathbb{N}$ mit

$$(k + m) + n = k + (m + n)$$

Dann ist

$$\begin{aligned}(k+m) + n^+ &= ((k+m) + n)^+ = (k + (m+n))^+ \\ &= k + (m+n)^+ = k + (m+n^+)\end{aligned}$$

□

2) Kommutativgesetz: $m+n = n+m$

Beweis. (1) $n+0 = 0+n$:

$$0+0 = 0+0$$

$$n+0 = 0+n \Rightarrow n^++0 = n^+ = (n+0)^+ = (0+n)^+ = 0+n^+$$

(2) $n+1 = 1+n$:

$$0+1 = 1+0$$

$$n+1 = 1+n \Rightarrow n^++1 = (n^+)^+ = (n+1)^+ = (1+n)^+ = 1+n^+$$

(3) $m+n = n+m$:

$$m+0 = 0+m$$

$$\begin{aligned}m+n = n+m &\Rightarrow m+n^+ = (m+n)^+ = (n+m)^+ = n+(m+1) \\ &= n+(1+m) = (n+1)+m = n^++m\end{aligned}$$

□

3) Kürzungsregel: $k+n = m+n \Rightarrow k=m$

Beispiel 1.2 (Definition der Multiplikation).

$$m \cdot 0 := 0$$

$$m \cdot n^+ := m \cdot n + m$$

Lemma 1.1. Sei $n \in \mathbb{N}, I \subset A_n$. Dann gibt es $k \in \mathbb{N}$, Bij. $f: A_k \rightarrow I$. Stets ist $k \leq n$.

21.10.03

Beweis. Basteln.

□

Satz 1.2. Sei M Menge, $k, n \in \mathbb{N}$ und $f: A_n \rightarrow M, g: A_k \rightarrow M$ Bijektionen. Dann ist $k=n$.

Beweis. Es ist $f^{-1} \circ g: A_k \rightarrow A_n (= I)$ als Verknüpfung von Bijektionen eine Bijektion. Nach Lemma ist $k \leq n$. Die Relation $n \leq k$ folgt aus Symmetrie der Voraussetzungen. $\Rightarrow n=k$. □

Definition 1.1. Eine Menge M heißt *endlich*, wenn es $n \in \mathbb{N}$ und Bijektion $f : A_n \rightarrow M$ gibt. Dabei heißt die eindeutig bestimmte Zahl n die *Anzahl der Elemente* von M oder Kardinalität, geschrieben: $\#M$, $|M|$

Satz 1.3. Jede Teilmenge \widetilde{M} einer endlichen Menge M ist endlich mit $\#\widetilde{M} \leq \#M$.

Beweis. Zu $n := \#M$ ex. Bijektion $f : A_n \rightarrow M$. Dann ist $I := f^{-1}(\widetilde{M})$ Teilmenge von A_n . Also existiert eine Bijektion $g : A_k \rightarrow I$, $n \geq k \in \mathbb{N}$. somit haben wir mit $f \circ g : A_k \rightarrow \widetilde{M}$ eine Bijektion, d.h. \widetilde{M} ist endlich und $\#\widetilde{M} = k \leq n = \#M$. \square

Definition 1.2. Eine Menge, die nicht endliche Menge ist, heißt *unendliche* Menge.

Satz 1.4. \mathbb{N} ist unendliche Menge.

Beweis. Annahme: \mathbb{N} ist endliche Menge. Wegen $A_n \subset \mathbb{N}$ ist dann $n \leq \#\mathbb{N}$ für alle $n \in \mathbb{N}$. Für $n = \#\mathbb{N} + 1$ Widerspruch. \square

Satz 1.5. Sei M eine Menge. Dann gilt: M ist genau dann unendliche Menge, wenn es eine Bijektion von M auf eine echte Teilmenge gibt.

Beweis. Übung. \square

1.2 Die ganzen Zahlen \mathbb{Z}

Wie kommt man von \mathbb{N} nach \mathbb{Z} ?

Nimm \mathbb{N}^2 und baue Äquivalenzrelation: $(k, m) \sim (k', m')$, falls $k + m' = k' + m$. Äquivalenzklassen seien $[(k, m)]$.

Definition 1.3 (Addition).

$$[(k, m)] + [(l, n)] := [(k + l, m + n)]$$

Definition 1.4 (Multiplikation).

$$[(k, m)][(l, n)] := [(kl + mn, kn + lm)]$$

Definition 1.5. Für $n \in \mathbb{N}$:

$$-n := [(0, n)]$$

$\mathbb{Z} := \{[(k, m)] : k, m \in \mathbb{N}\}$ mit $+\cdot$ ist Ring.

23.10.03

1.3 Die rationalen Zahlen \mathbb{Q}

Problem k/m nicht möglich für alle $k, m \in \mathbb{Z}$.
Betrachte $\mathbb{Z} \times \mathbb{Z}^*$ mit Äquivalenzrelation (!)

$$(k, m) \sim (l, n), \text{ falls } kn = lm$$

$\frac{k}{m} := [(k, m)]$ (Äquiv.klasse) ($k \in \mathbb{Z}, m \in \mathbb{Z}^*$)

$$\begin{aligned}\frac{k}{m} + \frac{k'}{m'} &:= \frac{km' + k'm}{mm'} \\ \frac{k}{m} \cdot \frac{k'}{m'} &:= \frac{kk'}{mm'}\end{aligned}$$

Die Operationen sind wohldefiniert!

$$k, k' \in \mathbb{Z} : \frac{k}{1} + \frac{k'}{1} = \frac{k+k'}{1}$$

Daher identifizieren wir k mit $\frac{k}{1}$.

$$m \cdot \frac{k}{m} = \frac{m}{1} \cdot \frac{k}{m} = \frac{mk}{1m} = \frac{k}{1} = k$$

$$\frac{k}{m} \cdot \frac{m}{k} = \frac{km}{mk} = 1$$

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$

Und \mathbb{Q} ist kommutativer Körper.

1.4 Die reellen Zahlen \mathbb{R}

Konstruktion analog Analysis II.

2 Teilbarkeit und Primzahlen

2.1 Allgemeines und Definitionen

Definition 2.1. $d \in \mathbb{Z}$ heie *Teiler* von $a \in \mathbb{Z}$, falls $v \in \mathbb{Z}$ existiert mit $dv = a$. In Zeichen: $d \mid a$. Falls d kein Teiler von a : $d \nmid a$. Ist $d \neq 0$ Teiler von a , so ist v in $dv = a$ eindeutig.

Beispiel 2.1. $3 \mid 12, -8 \mid 72, -11 \mid -99, 4 \nmid 7, 17 \mid 0, 0 \mid 0$

$\forall a \in \mathbb{Z}, \forall n \in \mathbb{N}^* : (a - 1) \mid (a^n - 1)$, denn $(a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1) = a^n - 1$

Bemerkung 2.1. $d \mid a \iff dx - a = 0$ hat Lsung in \mathbb{Z} .

Definition 2.2. $a \in \mathbb{Z}$ *gerade*, falls $2 \mid a$, *ungerade*, falls $2 \nmid a$.

Rechenregeln 2.2. 1) $a \mid a$

2) $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$

3) $(a \mid b \wedge c \mid d) \Rightarrow ac \mid bd$

4) $(a \mid b \wedge a \mid c) \Rightarrow \forall x, y \in \mathbb{Z} : a \mid bx + cy$

5) $\forall d \in \mathbb{Z} : d \mid 0$. aber

Satz 2.3. Sei $a \in \mathbb{Z}^*$, $d \mid a$. Dann:

$$1 \leq |d| \leq |a|$$

Insbes. hat a nur endl. viele Teiler.

Beweis. Sei $a = dv$ mit $d, v \in \mathbb{Z}$, also $|a| = |d||v|$. Wegen $a \neq 0$ sind auch $d, v \neq 0$. Somit $|d| \geq 1, |v| \geq 1$, also

$$|a| = |d||v| \geq |d| \geq 1$$

Schlielich: $\{d \in \mathbb{Z} : 1 \leq |d| \leq |a|\}$ hat $|2a|$ Elemente. □

Klar: a und $-a$ haben dieselben Teiler:

$$dv = a \iff d(-v) = -a$$

Auch gilt $d \mid a \iff -d \mid a$:

$$dv = a \iff (-d)(-v) = a$$

Satz 2.4 (Division mit Rest). Seien $a \in \mathbb{N}, b \in \mathbb{N}^*$. Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$a = qb + r$$

mit $0 \leq r < b$. (q „Quotient“, r Rest). Ist $a \geq 0$, so ist $q \geq 0$.

Beweis. $A = \{r \in \mathbb{N} : \exists q \in \mathbb{Z} \text{ mit } a = qb + r\}$ Dann $a \in A$ wegen $a = 0b + a$. Sei r kleinstes Element von A (\exists , da $A \subset \mathbb{N}, A \neq \emptyset$). Annahme: $r \geq b$. Dann $\exists r' \in \mathbb{N}$ mit $b + r' = r$. Sicher ist $r' < r$, da $b \neq 0$. Es gibt

$$q \in \mathbb{Z} \text{ mit } a = qb + r = (q + 1)b + r',$$

sodaß also $r' \in A$. Widerspruch (Statt \mathbb{Z} kann man wohl an geeigneten Stellen auch \mathbb{N} verwenden.)

Eindeutigkeit: $qb + r = a = q'b + r' \Rightarrow (q - q')b = r - r'$, $b \mid r - r'$ Falls $r - r' \neq 0$, so folgt $b \leq |r - r'|$. Wegen $0 \leq r < b$ und $0 \leq r' < b$ ist aber $|r - r'| < b$. Also $r - r' = 0$, $r = r'$, $qb = q'b$, $q = q'$ \square

Beweis. [2nd Flavour] $A = \{r \in \mathbb{N} : \exists q \in \mathbb{Z} \text{ mit } a = qb + r\}$. Ist $a \geq 0$, so ist $a \in A$ ($q = 0$).

Ist $a \leq 0$ so ist $r := a - ab = a(1 - b) \in A$ ($q = a$), denn $a = ba + r$ und $r \geq 0$ wegen $a \leq 0, 1 - b \leq 0$

...

Ist $q < 0$, so ist $a = qb + r \leq -b + r < 0$. Also $q \geq 0$, falls $a \geq 0$. \square

Beispiel 2.2 (für Bestimmung von größtem gemeinsamen Teiler von 1692 und 294).

$$1692 = 5 \cdot 294 + 222$$

$$294 = 1 \cdot 222 + 72$$

$$222 = 3 \cdot 72 + 6$$

$$72 = 12 \cdot 6 + 0$$

6 ist ggT, und obige Rechnung gibt $x, y \in \mathbb{Z}$ mit $6 = x \cdot 1692 + y \cdot 294$

$$\begin{aligned} 6 &= 222 - 3 \cdot 72 \\ &= 222 - 3(291 - 222) \\ &= 4 \cdot 222 - 3 \cdot 294 \\ &= 4(1692 - 5 \cdot 294) - 3 \cdot 294 \\ &= 4 \cdot 1692 - 23 \cdot 294 \end{aligned}$$

Satz 2.5 (Euklidischer Algorithmus). Seien $a, b \in \mathbb{N}^*$ mit $a > b$. Wir setzen $a_0 = a, a_1 = b$. Ist $n \in \mathbb{N}$ und sind $a_n, a_{n+1} \in \mathbb{N}^*$ definiert, so sei a_{n+2} der Rest von a_n bei Division durch a_{n+1} :

$$a_n = q_n a_{n+1} + a_{n+2}$$

Wir erhalten: $a_0 > a_1 > \dots > a_{N+1} = 0$ mit $N \in \mathbb{N}, N \leq a_0$. Es ist a_N ggT von a und b . Schreibweise: $\text{ggT}(a, b)$ oder kurz: (a, b) , und

$$(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = \{ax + by | x, y \in \mathbb{Z}\}$$

Insbesondere: (a, b) ist kleinste Zahl in \mathbb{N}^* , die ganzzahlige Kombination von a und b ist. Jeder Teiler von a und b ist Teiler von (a, b) .

Beweis. Wegen

$$a_n = q_n a_{n+1} + a_{n+2}$$

mit $q_n \in \mathbb{Z}$ ist für alle $0 \leq n \leq N$

$$a_n\mathbb{Z} + a_{n+1}\mathbb{Z} = a_{n+1}\mathbb{Z} + a_{n+2}\mathbb{Z}$$

Insbesondere ist

$$a\mathbb{Z} + b\mathbb{Z} = a_0\mathbb{Z} + a_1\mathbb{Z} = a_N\mathbb{Z} + a_{N+1}\mathbb{Z} = a_N\mathbb{Z}$$

Sei nun d Teiler von a, b . Wegen $a_N \in a\mathbb{Z} + b\mathbb{Z}$ ist d auch Teiler von a_N , erst recht $d \leq a_N$.

Wegen $a, b \in a_N\mathbb{Z}$ ist a_N Teiler von a, b .

Daraus folgt: a_N ist ggT von a, b : $(a, b) = a_N$. Jeder Teiler von a, b ist Teiler von (a, b) ,

$$(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

Auch ist klar:

$$(a, b) = \min(\mathbb{N}^* \cap (a\mathbb{Z} + b\mathbb{Z})) \quad \square$$

Korollar 2.6. Für alle $a, b \in \mathbb{N}^*$ ist $(ma, mb) = m(a, b)$.

Sind $a, b, d \in \mathbb{N}^*$ und ist $d | a, d | b$, so ist

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$$

Beweis.

$$\begin{aligned} (ma, mb) &= \min(\mathbb{N}^* \cap \{ma\mathbb{Z} + mb\mathbb{Z}\}) \\ &= m \cdot \min(\mathbb{N}^* \cap \{a\mathbb{Z} + b\mathbb{Z}\}) \\ &= m(a, b) \end{aligned}$$

Dann gilt weiter:

$$(a, b) = \left(d\frac{a}{d}, d\frac{b}{d}\right) = d \left(\frac{a}{d}, \frac{b}{d}\right) \quad \square$$

Korollar 2.7. Sind $a, b, c \in \mathbb{N}^*$, mit $c | ab$ und $(c, b) = 1$, dann gilt $c | a$.

Beweis.

$$\begin{aligned}(ab, ac) &= a(b, c) \\ &= a\end{aligned}$$

$c \mid ab$ und $c \mid ac$, dann folgt: $c \mid a$. □

$\frac{ab}{(a,b)} = \text{kgV}(a, b)$ kleinstes gemeinsames Vielfaches von a und b . Dies teilt jedes gemeinsame Vielfache von a, b .

Definition 2.3. $p \in \mathbb{N}$ heißt *Primzahl*, falls

- 1) $p > 1$
- 2) p besitzt keine echten Teiler, d.h. $p = ab, a, b \in \mathbb{N} \Rightarrow (a = 1 \vee b = 1)$

Es sei \mathbb{P} die Menge aller Primzahlen:

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}$$

Satz 2.8 (Existenz). *Jede natürliche Zahl $a > 1$ besitzt kleinsten Teiler $t > 1$; dieser ist Primzahl.*

Beweis. $T = \{t \in \mathbb{N} \mid t > 1, t \mid a\}$. $a \in T$, damit ist T nichtleer und es gibt ein kleinstes $t \in T$. Wäre $t \notin \mathbb{P}$, so gäbe es Teiler t' von t mit $1 < t' < t$. Dann $t' \mid a, t' \in T$. Widerspruch! □

Schon mit einer Primzahl kann man unendlich viele Zahlen gewinnen, z.B. mit 2:

$$2, 4, 8, \dots, 2^n, \dots$$

Satz 2.9 (von Euklid). \mathbb{P} ist unendliche Menge.

Genauer:

Seien $q_1, q_2, q_n \in \mathbb{P}$. Dann ist der kleinste Teiler $t > 1$ der Zahl

$$q_1 \cdot q_2 \cdots q_n + 1$$

eine Primzahl, die von allen q_1, \dots, q_n verschieden ist.

Beweis. Nach vorigem Satz: t ist Primzahl.

Annahme: $t \in \{q_1, \dots, q_n\}$.

Dann $t \mid q_1 \cdots q_n$. Wegen $t \mid q_1 \cdots q_n + 1$, also auch $t \mid 1, t = 1$. Widerspruch zu $t > 1$. □

Bemerkung 2.10. $\sum_{n=1}^{\infty} \frac{1}{n^2} < \infty$ (Summe ist $\frac{\pi^2}{6}$). Schärfer (von Euler): $\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty!$ (Beweis: mit eind. Primzerlegung später)

Es ist offen, ob $\{p \in \mathbb{P} \mid p + 2 \in \mathbb{P}\}$ unendlich ist!

Einfach: $\forall N \in \mathbb{N} \exists N$ aufeinander folgende Zahlen, die keine Primzahlen sind: $k \mid (N + 1)! + k$ für alle $2 \leq k \leq N + 1$

Beispiel 2.3. $60 = 2 \cdot 2 \cdot 3 \cdot 5$, $2, 3, 5 \in \mathbb{P}$
 $30\,031 = 59 \cdot 509$ (Div. durch $k \leq \sqrt{30031}$...)

Allgemein?

Satz 2.11. *Jede natürliche Zahl $a \geq 1$ besitzt Prim(faktor)zerlegung:*

$$a = p_1 p_2 \cdots p_n, \quad p_i \in \mathbb{P}$$

Beweis. Vollst. Ind. nach a :

$a = 1$ klar (leeres Produkt).

$a \rightarrow a + 1$: $t > 1$ kleinster Teiler von $a + 1$, $\Rightarrow a + 1 = tk$ mit $k \in \mathbb{N}$. Dann $k \leq a$. Also ex. $p_1, \dots, p_n \in \mathbb{P}$ mit $k = p_1 \cdots p_n$, nach Annahme, so daß also $a + 1 = t \cdot p_1 \cdots p_n$ \square

Eindeutigkeit? Dazu:

Lemma 2.12. *Seien $a, b \in \mathbb{N}^*$, $p \in \mathbb{P}$ und $p \mid ab$. Dann ist $p \mid a$ oder $p \mid b$.*

Beweis. Mit Folgerung 2 aus EUKLIDischem Algorithmus: $p \nmid b \Rightarrow (p, b) = 1 \Rightarrow p \mid a$ (da $p \mid ab$). \square

Korollar 2.13. *Sind $a_1, a_2, \dots, a_n \in \mathbb{N}^*$ und ist $p \in \mathbb{P}$ mit $p \mid a_1 \cdots a_n$, so gibt es $j \in \{1, \dots, n\}$ mit $p \mid a_j$.*

Beweis. Ind. nach n : $n = 0$ (oder 1): Nichts zu zeigen.

$n \rightarrow n + 1$: $p \mid a_1 \cdots a_n \cdot a_{n+1}$

$\Rightarrow p \mid a_1 \cdots a_n$ oder $p \mid a_{n+1}$

$\Rightarrow (\exists j \in \{1, \dots, n\}$ mit $p \mid a_j$) oder $p \mid a_{n+1}$. \square

Bemerkung 2.14. Für jedes $p \in \mathbb{N}$ mit $p > 1$ sind äquivalent (Primeigenschaft):

1) $p \in \mathbb{P}$

2) Sind $a, b \in \mathbb{Z}$ mit $p \mid ab$, so ist $p \mid a$ oder $p \mid b$.

Beweis. (i) \Rightarrow (ii): Voriges Lemma, falls $ab \in \mathbb{N}^*$. Sonst trivial.

(ii) \Rightarrow (i): Ann.: $p \notin \mathbb{P}$. Dann ex. $a, b \in \mathbb{N}$, $a \geq 2, b \geq 2$ mit $p = ab$. Wegen $a < p$ ist $p \nmid a$, wegen $b < p$ ist $p \nmid b$. Aber $p \mid ab$. \square

Satz 2.15. *Die Primzerlegung einer jeden natürlichen Zahl $a \geq 1$ ist bis auf Reihenfolge der Faktoren eindeutig. Genauer: $a = p_1 \cdots p_n = q_1 \cdots q_m \Rightarrow m = n$ und die q_i sind eine Permutation der p_j .*

Beweis. Ind. nach n : $n = 0$: $a = 1, m = 0 = n$.

$n \rightarrow n + 1$:

$$p_1 \cdots p_n p_{n+1} = q_1 \cdots q_l$$

$\Rightarrow p_{n+1} \mid q_1 \cdots q_l. \Rightarrow \exists j \in \{1, \dots, l\} : p_{n+1} \mid q_j$

$\Rightarrow p_{n+1} = q_j$. OBdA: $j = l \Rightarrow \exists m \in \mathbb{N} : l = m + 1$. Es folgt (Div. durch p_{n+1})

$$p_1 \cdots p_n = q_1 \cdots q_m$$

Nach Annahme: $n = m$, also $n + 1 = m + 1 = l$ und $q_1 \dots q_n$ sind permutierte $p_1 \dots p_n$. \square

Definition 2.4 (Kanonische Darstellung):

$$a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

mit pw. verschiedenen $p_i \in \mathbb{P}$, $m_j \in \mathbb{N}$

Satz 2.16 (Teilbarkeitskriterium). Sei $a \in \mathbb{N}^*$ mit kan. Primzerlegung

$$a = \prod_{i=1}^r p_i^{m_i}$$

Dann ist

$$T := \left\{ \prod_{i=1}^r p_i^{\mu_i} \mid 0 \leq \mu_i \leq m_i \forall 1 \leq i \leq r \right\}$$

die Menge aller Teiler von a .

4.11.03

Beweis. 1) $0 \leq \mu_j \leq m_j \Rightarrow$

$$a = (p_1^{\mu_1} \cdots p_r^{\mu_r})(p_1^{m_1-\mu_1} \cdots p_r^{m_r-\mu_r})$$

Also ist $p_1^{\mu_1} \cdots p_r^{\mu_r}$ Teiler von a .

2) Sei t Teiler von a . Dann ex. $v \in \mathbb{N}$ mit $tv = a$. Zusammensetzen von Primzerlegungen von t und v ergibt Primzerlegung von a , also (nach Umordnen der Faktoren) $p_1^{m_1} \cdots p_r^{m_r}$. Daraus folgt, daß

$$t = p_1^{\mu_1} \cdots p_r^{\mu_r}$$

mit $0 \leq \mu_j \leq m_j$. □

Korollar 2.17. Seien $a, b \in \mathbb{N}^*$. Wir haben Darstellungen

$$a = \prod_{i=1}^r p_i^{m_i}$$

$$b = \prod_{j=1}^r p_j^{n_j}$$

mit $p_i \in \mathbb{P}$, $m_j, n_j \in \mathbb{N}$.

$$(a, b) = \text{ggT}(a, b) = \prod_{i=1}^r p_i^{\min(m_i, n_i)}$$

$$\text{kgV}(a, b) = \prod_{i=1}^r p_i^{\max(m_i, n_i)}$$

(Man sieht erneut: $\text{ggT}(a, b) \text{kgV}(a, b) = ab$, weil $\min(m_j, n_j) + \max(m_j, n_j) = m_j + n_j$)

Korollar 2.18. Für jedes $a \in \mathbb{N}^*$ eindeutige Darstellung

$$a = n^2 \cdot q_1 \cdots q_k$$

mit $n \in \mathbb{N}^*$ und verschiedenen $q_1 \dots q_k \in \mathbb{P}$.

Beweis. $a = \prod_{i=1}^r p_i^{m_i}$ mit verschiedenen $p_1 \dots p_r \in \mathbb{P}$. Es ist

$$m_j = 2\mu_j + \nu_j$$

mit $\mu_j \in \mathbb{N}, \nu_j \in \{0, 1\}$. Dann mit

$$n := \prod_{i=1}^r p_i^{\mu_i}$$

$a = n^2 \prod_{i=1}^r p_i^{\nu_i} = n^2 q_1 \cdots q_k$ mit $k \leq r$. Eindeutigkeit: (klar). □

Definition 2.5. $q_1 \dots q_k$ heißt quadratfreier Kern von a . (1, falls a Quadrat)

Beweis (für $\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty$ (EULER, 1707–1782)). Wir nehmen nun an: $\sum_{p \in \mathbb{P}} \frac{1}{p} < \infty$. Dann folgt auch: $\prod_{p \in \mathbb{P}} (1 + \frac{1}{p})$ konvergent.

$$\prod_{j=1}^m \left(1 + \frac{1}{p_j}\right) \leq e^{\sum_{j=1}^m \frac{1}{p_j}} \leq e^{\sum_{p \in \mathbb{P}} \frac{1}{p}} < \infty$$

$(1 + x \leq \sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x$ für $x \geq 0$)

$\mathbb{P} = \{p_1, p_2, \dots\}$ mit $p_1 < p_2 < \dots$ $k = n^2 \cdot \prod_{j=1}^r p_{i_j}$

$$\left(1 + \frac{1}{p_1}\right) \left(1 + \frac{1}{p_2}\right) \cdots \in \mathbb{N}$$

Daher ist

$$\sum_{k=1}^{\infty} \frac{1}{k} \leq \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right) \prod_{p \in \mathbb{P}} \left(1 + \frac{1}{p}\right) < \infty$$

Dann wäre auch die harmonische Reihe konvergent! □

Korollar 2.19. Für die Anzahl $\tau(a)$ der Teiler von $a = \prod_{i=1}^r p_i^{m_i}$ gilt

$$\tau(a) = (m_1 + 1)(m_2 + 1) \cdots (m_r + 1)$$

(rechte Seite ist $\#\prod_{j=1}^r \{0, 1, \dots, m_j\}$) $\tau(a)$ ist genau dann ungerade, wenn a ein Quadrat ist. ($\tau(a)$ ungerade $\iff m_1, \dots, m_r$ gerade!) Außerdem: $(a, b) = 1 \implies \tau(ab) = \tau(a)\tau(b)$ (Primzerlegungen von a und b haben kein q^ν , $q \in \mathbb{P}, \nu > 0$ gemeinsam)

Beispiele 2.4. 1) $5040 = 2^4 3^2 5 \cdot 7 \implies \tau(5040) = 5 \cdot 3 \cdot 2 \cdot 2 = 60$ (Schon PLATON wußte das)

2) $m_1 = \dots = m_r = 1 \Rightarrow \tau(a) = 2^r$ (CARDANO 1537)

Bemerkung 2.20. Für das Produkt $P(a)$ aller Teiler von a gilt:

$$(P(a))^2 = a^{\tau(a)}$$

Beweis. $f : d \mapsto \frac{a}{d}$ ist Bijektion von T auf sich. Daher ist

$$(P(a))^2 = \left(\prod_{d \in T} d \right) \left(\prod_{d \in T} f(d) \right) = \prod_{d \in T} (df(d)) = \prod_{d \in T} a = a^{\tau(a)} \quad \square$$

Beispiel 2.5. $a = 25 = 5^2$, $\tau(a) = 3$, $a^{\tau(a)} = a^3 \Rightarrow P(25) = a^{\frac{3}{2}} = 5^3 = 125 = 1 \cdot 5 \cdot 25$

Summe aller pos. Teiler von $a \in \mathbb{N}^*$:

$$\sigma(a) := \sum_{d|a} d$$

z.B.: $\sigma(6) = 1 + 2 + 3 + 6 = 12$

$\sigma(15) = 1 + 2 + 3 + 5 + 15 = 24$

$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$

DESCARTES 1638: $\sum_{d|p^m, d < p^m} d = \frac{p^{m+1} - 1}{p - 1}$ für $p \in \mathbb{P}$

WALLIS kannte 1658:

Satz 2.21. Ist $a = \prod_{i=1}^r p_i^{m_i}$ kanonische Primzerlegung von $a \in \mathbb{N}^*$, so ist

$$\sigma(a) := \sum_{d|a, d \geq 0} d = \prod_{j=1}^r \frac{p_j^{m_j+1} - 1}{p_j - 1}.$$

Insbesondere ist σ multiplikativ, d.h.

$$(a, b) = 1 \Rightarrow \sigma(ab) = \sigma(a)\sigma(b).$$

Beweis.

$$\begin{aligned} \sigma(a) &= \sum_{\substack{0 \leq i \leq r \\ 0 \leq \mu_i \leq m_i}} p_1^{\mu_1} \cdots p_r^{\mu_r} \\ &= \prod_{j=1}^r \sum_{\mu_j=0}^{m_j} p_j^{\mu_j} \\ &= \prod_{j=1}^r \frac{p_j^{m_j+1} - 1}{p_j - 1} \end{aligned}$$

(Zusatz: da bei Primdarstellung von a und b keine Primzahl gemeinsamer Faktor.) \square

Beispiele 2.6. 1) $a = 72 = 2^3 \cdot 3^2 \Rightarrow \sigma(a) = \frac{2^{3+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} = 15 \cdot 13 = 195$

$$2) a = 97 = 97^1 \Rightarrow \sigma(a) = \frac{97^2-1}{97-1} = 97 + 1 = 98$$

$$3) \sigma(p^m) = \frac{p^{m+1}-1}{p-1} = p^m + \underbrace{\frac{p^m-1}{p-1}}_{\text{DESCARTES}}$$

Definition 2.6. $a \in \mathbb{N}^*$ heißt *vollkommen*, falls

$$\sum_{d|a, d \neq a} d = a,$$

d.h. $\sigma(a) = 2a$.

Beispiel 2.7. 6, 28, ...??

Fragen:

1) \exists ungerade vollkommene Zahl? Offene Frage! Man weiß: Es gibt keine, die kleiner ist als 10^{50} . Jede ungerade vollkommene Zahl hat mindestens acht verschiedene Primfaktoren.

(klar, daß p^m , $p \in \mathbb{P}$ ungerade, nicht vollkommen ist: $\sigma(p^m) - p^m = \frac{p^m-1}{p-1} < p^m$)

2) Gibt es unendlich viele gerade Zahlen, die vollkommen sind? Offene Frage! klar:

$$\sigma(2^m) = \frac{2^{m+1}-1}{2-1} = 2^{m+1} - 1 = 2 \cdot 2^m - 1$$

Sei $a \in \mathbb{N}^*$, gerade, also $a = 2^{k-1}u$, $u \in \mathbb{N}^*$ ungerade, $k \geq 2$. Dann ist

$$\begin{aligned} \sigma(a) &= \sigma(2^{k-1}u) = \sigma(2^{k-1})\sigma(u) = (2^k - 1)\sigma(u) \\ 2a &= 2^k u = (2^k - 1)u + u \end{aligned}$$

Es sei $c := \frac{u}{2^k-1}$. Damit ist $\sigma(a) = 2a$ genau dann, wenn

$$\sigma(u) = u + c$$

Ist $u = 2^k - 1$ und u Primzahl, so ist $c = 1$ und $\sigma(u) = u + 1 = u + c$, also a vollkommen. Sei umgekehrt a vollkommen, also $\sigma(u) = u + c$. Insbesondere $c \in \mathbb{N}$, wegen $c(2^k - 1) = u$ also $c | u$, $1 \leq c < u$ wegen $2^k - 1 \geq 2^2 - 1 = 3$. Wäre $c > 1$, so wäre $\sigma(u) \geq u + 1 + c > u + c$. Unmöglich! Also $c = 1$.

Hätte u Teiler d mit $1 < d < u$, so wäre $u + 1 = \sigma(u) \geq u + 1 + d$. Unmöglich. Also ist u Primzahl, $u = 2^k - 1$

Somit gezeigt:

Satz 2.22. Sei $a \in \mathbb{N}^*$ gerade. Dann sind äquivalent:

1) a ist vollkommen.

2) $a = 2^{k-1}(2^k - 1)$ mit $k \in \mathbb{N}, k \geq 2$ und $2^k - 1$ Primzahl.

Definition 2.7. Falls $M_n := 2^n - 1$ Primzahl, so heißt sie *MERSENNEsche Primzahl*.

Bemerkung 2.23. M_n in Binärdarstellung: $\underbrace{1 \dots 1}_n$

Bemerkung 2.24. $k \notin \mathbb{P} \Rightarrow 2^k - 1 \notin \mathbb{P}$.

Beweis. Sei $k = st$ mit $s, t \in \mathbb{N}$, $s, t \geq 2$. Dann ist $1 < 2^s - 1 < 2^k - 1$ und

$$2^s - 1 \mid (2^s)^t - 1 = 2^k - 1 \quad \square$$

Beispiel 2.8 (für vollkommene Zahlen). $k = 2$: $2^2 - 1 = 3$ Primzahl, $2^{2-1} \cdot 3 = 6$ vollkommen.

$k = 3$: $2^3 - 1 = 7$ prim, $2^{3-1} \cdot 7 = 28$ vollkommen.

$k = 5$: $2^5 - 1 = 31$ prim, $2^4 \cdot 31 = 496$ vollkommen.

$k = 7$: $2^7 - 1 = 127$ prim, $2^6 \cdot 127 = 8128$ vollkommen.

$k = 11$: $2^{11} - 1 = 2047 = 23 \cdot 89 \notin \mathbb{P}$

$\#\{k \in \mathbb{N} : 2 \leq k \leq 20\,000, 2^k - 1 \in \mathbb{P}\} = 24$

1984: $2^{132049} \in \mathbb{P}$ ($\approx 40\,000$ Stellen)

1987: $2^{216091} - 1 \in \mathbb{P}$

1995: GIMPS (**G**reat **I**nternet **M**ersenne **P**rime **S**earch)

Test von LUCAS-LEHMER (1930): Sei (u_n) definiert durch

$$u_1 = 4, u_{n+1} = u_n^2 - 2$$

und es sei p Primzahl, $p > 2$. dann: $M_p := 2^p - 1 \in \mathbb{P} \Rightarrow M_p \mid u_{p-1}$

$$\sum_{k=1}^M \frac{1}{k} \approx \ln M \approx 9\,000\,000\,000$$

$$\sum_{p \leq M, p \in \mathbb{P}} \approx \ln \ln M \approx 7 \ln 10 \approx 16$$

Frage: Gibt es $c > 0 \forall a \in \mathbb{N}^* : \sigma(a) \leq ca$? Nein!

Satz 2.25. $\forall n \in \mathbb{N}^* :$

$$\frac{\sigma(n!)}{n!} \geq \sum_{j=1}^n \frac{1}{j} \approx \ln n$$

Beweis.

$$\sigma(a) = \sum_{d \mid a} d = \sum_{d \mid a} \frac{a}{\frac{a}{d}}$$

$$\Rightarrow \sigma(n!) \geq \sum_{j=1}^n \frac{n!}{j} \Rightarrow \frac{\sigma(n!)}{n!} \geq \sum_{j=1}^n \frac{1}{j} \quad \square$$

Primzerlegung von $n!$ ist leicht, wenn Primzahlen bis n bekannt.

Satz 2.26. Potenz, mit der $p \in \mathbb{P}$ in Primzerlegung von $n!$ vorkommt, ist

$$e_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

($\lfloor x \rfloor$ größte ganze Zahl $\leq x$, $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$, falls $p^k > n$.) (LEGENDRE, CHEBYSHEV)

Beweis. $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$. Daher: $p \mid p, p \mid 2p, \dots$ ($\left\lfloor \frac{n}{p} \right\rfloor$ Faktoren)

$p^2 \mid p^2, p^2 \mid 2p^2, \dots$ ($\left\lfloor \frac{n}{p^2} \right\rfloor$ Faktoren)

$p^k \mid p^k, p^k \mid 2p^k, \dots$ ($\left\lfloor \frac{n}{p^k} \right\rfloor$ Faktoren) □

Wie findet man *alle* Primzahlen $\leq n$? Sieb des ERATOSTHENES:

- 1) Man schreibe alle nat. Zahlen bis n hin.
- 2) Man markiere 2 und streiche alle Vielfachen von 2.
- 3) Markiere k , die erste nicht-markierte Zahl, und streiche alle Vielfachen von k .
- 4) Man führe Schritt 3) aus, solange es nicht-markierte Zahl $k \leq \sqrt{n}$ ($\iff k^2 \leq n$) gibt.
- 5) Dann sind die markierten und die nicht gestrichenen Zahlen $\leq n$ Primzahlen.

FERMATsche Primzahlen sind von der Form $2^s + 1$. Für welche s hat man eine Chance, daß $2^s + 1$ Primzahl ist?

Satz 2.27. Nur, wenn $s = 2^k$!

Beweis. Seien $s = 2^k v$, $v > 1$, $2 \nmid v$, $t := 2^k$. Dann ist

$$(-1)^v = -1, \quad 1 + 2^s = 1 - (-2^t)^v.$$

Wegen $1 - x^n = (1 - x)(1 + x + \dots + x^{n-1})$ ist (mit $x = -2^t$, $n = v$)

$$1 + 2^s = (1 + 2^t) \left(1 - 2^t + 2^{2t} - \dots + 2^{(v-1)t} \right)$$

Aber $1 + 2^t > 1$, der andere Faktor aber auch. Also ist diese Zahl faktorisiert. □

FERMAT (1601–1665) vermutete: 2^{2^t} Primzahl für $t = 0, 1, 2, 3, 4, \dots$. Aber: $2^{32} + 1$ hat 641 als Teiler. Bisher keine weitere FERMATschen Primzahlen bekannt.

GAUSS (1777–1855) hat bewiesen:

Satz 2.28. Sei $m \geq 3$ ungerade natürliche Zahl. Dann sind äquivalent:

- 1) Reguläres m -Eck kann mit Zirkel und Lineal konstruiert werden.
- 2) m ist quadratfreies Produkt FERMATscher Primzahlen.

2.2 Bemerkungen zur Primzahlverteilung

Für jedes reelle $x \geq 0$ sei $\pi(x)$ die Anzahl aller Primzahlen unterhalb von x :

$$\pi(x) := \#\{p \in \mathbb{P} : p \leq x\} = \sum_{p \leq x} 1$$

(bei der Summe wie bei späteren Produkten bezeichne p immer eine Primzahl, d.h. wir lassen den Zusatz $p \in \mathbb{P}$ unter Summen- bzw. Produktzeichen weg).

Gestützt auf Tabellen für Primzahlen formulierte GAUSS (1777–1855) bereits 1792 die folgende Aussage:

Satz 2.29 (Großer Primzahlsatz).

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Ein vollständiger Beweis dafür wurde erst 1896, also fast 100 Jahre später, gleichzeitig und unabhängig voneinander durch J. HADAMARD (1865–1963) und C. DE LA VALLÉE-POUSSIN (1866–1962) gegeben. Entscheidendes Hilfsmittel war dabei die RIEMANNSche Zetafunktion

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s > 1)$$

in Verbindung mit (eindimensionaler) Funktionentheorie, d.h., der Theorie komplexer Funktionen einer komplexen Veränderlichen. Den Zusammenhang zwischen ζ und Primzahlen sieht man an der Identität

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

Diese Identität folgt sofort aus der Formel

$$\frac{1}{1 - \frac{1}{p^s}} = \sum_{m=0}^{\infty} \left(\frac{1}{p^m}\right)^s$$

(geometrische Reihe) und der Beziehung

$$\sum_{\substack{p_1, \dots, p_r \in \mathbb{P} \text{ verschieden} \\ m_1, \dots, m_r \in \mathbb{N}}} \left(\frac{1}{p_1^{m_1} \cdots p_r^{m_r}}\right)^s = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

wobei die letzte Gleichheit auf dem Existenz- und Eindeigkeitssatz für die Primzerlegung beruht.

Erst 1949 fanden P. ERDŐS und A. SELBERG eine „elementaren“, d.h. ohne Funktionentheorie geführten Beweis.

Den ersten echten Beitrag zum Beweis des großen Primzahlsatzes leistete im Jahre 1850 P. L. CHEBYSHEV (1821–1894), indem er bewies, daß für alle hinreichend großen x gilt

$$a \frac{x}{\ln x} < \pi(x) < A \frac{x}{\ln x}, \quad (2.1)$$

und zwar für $a \approx 0,89$ und $A \approx 1,1$. Er zeigte außerdem, daß der Limes des Quotienten von $\pi(x)$ und $x/\ln x$, wenn er existiert, gleich 1 sein muß.

Unser Ziel wird es sein, eine Abschätzung der Form (2.1) zu zeigen, und zwar mit $a \approx 0,69$ und $A \approx 1,4$. Zusätzlich wollen wir beweisen, daß es für jedes $n \in \mathbb{N}^*$ eine Primzahl p gibt, für die $n < p \leq 2n$ ist (BERTRANDSches Postulat).

Der Schlüssel dazu ist das folgende Lemma, wobei (2.2) die obere Abschätzung und (2.4) die untere Abschätzung von $\pi(x)$ liefern wird. Die genaue Form von (2.3) ist für den Beweis des BERTRANDSchen Postulats erforderlich.

Lemma 2.30. 1) Für alle natürlichen Zahlen $n \geq 1$ ist

$$\prod_{n+2 \leq p \leq 2n+1} p \leq \binom{2n+1}{n}. \quad (2.2)$$

2) Für alle natürlichen Zahlen $n > 2$ gilt

$$\binom{2n}{n} = \prod_{p < 2n} p^{\alpha_p} \quad (2.3)$$

mit $p^{\alpha_p} \leq 2n$, insbesondere

$$\binom{2n}{n} \leq (2n)^{\pi(2n)}, \quad (2.4)$$

und $\alpha_p \in \{0, 1\}$ für alle $\sqrt{2n} < p < 2n$.

Genauer ist $\alpha_p = 1$ für alle $n < p < 2n$, aber $\alpha_p = 0$ für alle $\frac{2}{3}n < p \leq n$.

Beweis. Sei $n \in \mathbb{N}$. Sei p Primzahl und zunächst $n+1 < p \leq 2n+1$. Es ist

$$\binom{2n+1}{n} = \frac{(2n+1)!}{n!(n+1)!} \in \mathbb{N},$$

wobei p Teiler von $(2n+1)!$, aber kein Teiler von $n!$ oder $(n+1)!$ ist. Daher kommt p in der Primfaktorzerlegung von $\binom{2n+1}{n}$ vor, und es folgt (2.2).

Sei nun $n \geq 3$. Es ist

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{\alpha_p}$$

mit

$$\alpha_p = \sum_{k \geq 1} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Dabei ist jeder Summand als natürliche Zahl mit

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2$$

entweder 0 oder 1. Überdies sind die Summanden Null, wenn $p^k > 2n$ ist. Daher ist

$$\alpha_p \leq \max\{k : p^k \leq 2n\}, \quad p^{\alpha_p} \leq 2n.$$

Damit folgt schon (2.4).

Außerdem erhalten wir, daß α_p für $p > \sqrt{2n}$ höchstens 1 ist. Offensichtlich ist

$$\alpha_p = 1 - 2 \cdot 0 = 1$$

für alle $n < p \leq 2n$ (wegen $n > 2$ ist $n > \sqrt{2n}$).

Bleibt zu zeigen, daß

$$\alpha_p = 0 \quad \text{für alle } \frac{2}{3}n < p \leq n.$$

Sei also $\frac{2}{3}n < p \leq n$. Wegen $n \geq 3$ ist dann $p \geq 3$, also $p^2 \geq 3p > 2n$, aber $n < 2p \leq 2n$. Daher ist $\alpha_p = 2 - 2 = 0$. \square

Beispiele 2.9.

$$\begin{aligned} \binom{26}{13} &= 2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23, \\ \binom{28}{14} &= 2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23, \\ \binom{30}{15} &= 2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29 : \end{aligned}$$

Für $n = 13, 14, 15$ liegen 11 und 13 im Bereich zwischen $\frac{2}{3}n$ und n , können also nicht als Faktoren auftreten, während 17, 19 vorkommen müssen und zusätzlich 29 für $n = 15$. Die Größe der in Lemma 2.30 auftretenden Binomialkoeffizienten läßt sich sehr leicht kontrollieren (auch ohne STIRLINGSche Formel), wobei der Faktor $2n$, um den sich die linke von der rechten Seite der Abschätzung unterscheidet, für unsere Betrachtungen gänzlich unerheblich sein wird.

Lemma 2.31. *Für alle $n \in \mathbb{N}^*$ ist*

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

Beweis. Es ist

$$4^n = 2^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \leq (1+1) + \sum_{k=1}^{2n-1} \binom{2n}{k} \leq 2n \binom{2n}{n}$$

und

$$2 \binom{2n+1}{n} = \binom{2n+1}{n} + \binom{2n+1}{n+1} \leq \sum_{n=0}^{2n+1} \binom{2n+1}{k} = 2^{2n+1}. \quad \square$$

Satz 2.32. Für alle $x \geq 1$ ist

$$\prod_{p \leq x} p \leq 4^x.$$

Beweis. Wegen $\pi(x) = \pi([x])$ und $4^{[x]} \leq 4^x$ brauchen wir die Behauptung nur für $x \in \mathbb{N}^*$ zu beweisen. Für $n \in \{1, 2\}$ ist $\prod_{p \leq n} p \leq 2 \leq 4^n$. Sei $n \in \mathbb{N}$, $n \geq 2$ und $\prod_{p \leq m} p \leq 4^m$ für alle $1 \leq m \leq n$. Ist n ungerade, so ist $n+1$ als gerade Zahl keine Primzahl, also

$$\prod_{p \leq n+1} p = \prod_{p \leq n} p \leq 4^n \leq 4^{n+1}.$$

Sei also n gerade. Dann ist $n = 2m$ mit $m \in \mathbb{N}^*$, $m+1 \leq n$. Nach Lemma 2.30 und Lemma 2.31 folgt

$$\prod_{m+2 \leq p \leq 2m+1} p \leq \binom{2m+1}{m+1} \leq 4^m,$$

also nach Induktionsannahme

$$\prod_{p \leq n+1} p = \prod_{p \leq m+1} p \prod_{m+2 \leq p \leq 2m+1} p \leq 4^{m+1} 4^m = 4^{n+1}.$$

□

Satz 2.33. Es ist

$$\limsup_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leq 2 \ln 2 < 1.4. \quad (2.5)$$

Genauer: Für alle $x > 1$ und $0 < \varepsilon < 1$ ist

$$\frac{\pi(x)}{\frac{x}{\ln x}} \leq \frac{\ln 4}{1-\varepsilon} + \frac{\pi(x^{1-\varepsilon}) \ln x}{x} \leq \frac{\ln 4}{1-\varepsilon} + x^{-\varepsilon} \ln x \quad (2.6)$$

und

$$\pi(x) \leq (4 \ln 2) \frac{x}{\ln x}. \quad (2.7)$$

Beweis. Wegen

$$(x^{1-\varepsilon})^{\pi(x) - \pi(x^{1-\varepsilon})} \leq \prod_{x^{1-\varepsilon} < p \leq x} p \leq 4^x$$

ist

$$(1-\varepsilon)(\pi(x) - \pi(x^{1-\varepsilon})) \ln x \leq x \ln 4,$$

woraus mit Division durch $(1-\varepsilon)x$ die erste Ungleichung in (2.6) folgt. Wegen der trivialen Beziehung $\pi(x^{1-\varepsilon}) \leq x^{1-\varepsilon}$ ergibt sich auch die zweite Ungleichung in (2.6). Da $\lim_{x \rightarrow \infty} x^{-\varepsilon}/(\ln x) = 0$ folgt (2.5).

Um (2.7) zu zeigen, bemerken wir zunächst, daß für alle $1 < x \leq 16$

$$\pi(x) \leq x \leq \frac{\ln 16}{\ln x} x = (4 \ln 2) \frac{x}{\ln x}.$$

Für alle $x \geq 16$ (sogar schon für alle $x \geq 8$) ist

$$\pi(x) \leq \frac{x}{2}. \quad (2.8)$$

Denn es ist $\pi(16) = 6 = (16/2) - 2$ und stets $\pi(x+2) - \pi(x) \leq 1$, weil jede zweite Zahl*- gerade und damit keine Primzahl ist. Damit erhalten wir

$$\pi(x) \leq \frac{x}{2} \leq (4 \ln 2) \frac{x}{\ln x} \quad \text{für alle } 16 \leq x \leq 2^8 = 256.$$

Um (2.7) auch für alle $x \geq 256$ zu erhalten, bemerken wir, daß die Funktion

$$f : x \mapsto x^{-\varepsilon} \ln x \quad (2.9)$$

wegen $f'(x) = (-\varepsilon \ln x + 1)x^{-\varepsilon-1}/(\ln x)^2$ für $x \geq e^{1/\varepsilon}$ fallend (und für $1 < x \leq e^{1/\varepsilon}$ steigend) ist.

Wir wählen nun $\varepsilon = 1/3$ und $x_0 = 2^6 = 64$. Dann ist $x_0 \geq e^3 = e^{1/\varepsilon}$ und $x_0^{1-\varepsilon} = (2^6)^{2/3} = 2^4 = 16$, also für alle $x \geq x_0$

$$\frac{\pi(x^{1-\varepsilon}) \ln x}{x} \leq \frac{1}{2} x^{-\varepsilon} \ln x \leq \frac{1}{2} x_0^{-\varepsilon} \ln x_0 = \frac{1}{2} 2^{-2} 6 \ln 2 = \frac{3}{4} \ln 2.$$

Wegen $(\ln 4)/(1-\varepsilon) = 3 \ln 2$ folgt damit aus (2.6), daß (2.7) für alle $x \geq 64$ gilt. \square

Satz 2.34. *Es ist*

$$\liminf_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} \geq \ln 2 > 0,69. \quad (2.10)$$

Genauer: Für alle $x \geq 3$ ist

$$\pi(x) \geq \ln 2 \frac{x}{\ln x} - 2 \quad (2.11)$$

und

$$\pi(x) \geq \frac{\ln 2}{2} \frac{x}{\ln x}. \quad (2.12)$$

Beweis. Sei $x \geq 3$ und $m = 2n$ die kleinste gerade Zahl mit $m \geq x$. Dann ist selbstverständlich $\pi(x) + 1 \geq \pi(m)$. Nach Lemma 2.30 und Lemma 2.31 ist

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\pi(2n)},$$

also $2^m/m \leq m^{\pi(m)}$, $m \ln 2 - \ln m \leq \pi(m) \ln m$, d.h.

$$\ln 2 \frac{m}{\ln m} - 1 \leq \pi(m).$$

Dabei ist $\frac{x}{\ln x} \leq \frac{m}{\ln m}$ und $\pi(m) \leq \pi(x) + 1$.

Also folgt (2.11) und daraus sofort (2.10). Ist $x \geq 3$, so ist $2\pi(x) \geq \pi(x) + 2$. Daher gilt auch (2.12). \square

Bemerkungen 2.35. 1. Ungleichung (2.12) gilt sogar für alle $x \geq 2$: Sei $g(x) := \frac{\ln 2}{2} \frac{x}{\ln x}$. Dann ist $g(2) = 1$ und $g(3) = \frac{\ln 2^3}{\ln 3^2} < 1$. Da g auf $[2, e]$ fällt und auf $[e, 3]$ steigt (siehe die Diskussion zu (2.9)), ist also

$$\pi(x) = 1 \geq g(x) = \frac{\ln 2}{2} \frac{x}{\ln x} \quad \text{für alle } x \in [2, 3].$$

2. Es ist leicht, den Faktor auf der rechten Seite von (2.12) wesentlich näher an $\ln 2$ zu bringen, z.B. auf $\frac{15}{16} \ln 2$ für $x \geq 5$, $\frac{13}{14} \ln 2$ für $x \geq 3$: Für alle $x \geq 113$ ist $\pi(x) \geq 30$, also

$$\frac{16}{15} \pi(x) \geq (\pi(x) + 2) \geq \ln 2 \frac{x}{\ln x}.$$

Für alle $2^7 = 128 \geq x \geq 64$ ist

$$\frac{15}{16} \ln 2 \frac{x}{\ln x} \leq \frac{15}{16} \ln 2 \frac{128}{7 \ln 2} = \frac{120}{7} \leq 18 = \pi(61) \leq \pi(x),$$

für alle $64 \geq x \geq 32$ ist

$$\frac{15}{16} \ln 2 \frac{x}{\ln x} \leq \frac{15}{16} \ln 2 \frac{64}{6 \ln 2} = 10 = \pi(29) \leq \pi(x),$$

für alle $32 \geq x \geq 16$ ist

$$\frac{15}{16} \ln 2 \frac{x}{\ln x} \leq \frac{15}{16} \ln 2 \frac{32}{5 \ln 2} = 6 = \pi(13) \leq \pi(x),$$

für alle $8 \geq x \geq 5$ ist

$$\frac{15}{16} \ln 2 \frac{x}{\ln x} \leq \frac{15}{16} \ln 2 \frac{8}{3 \ln 2} = \frac{5}{2} < \pi(5) \leq \pi(x),$$

für alle $5 \geq x \geq 3$ ist

$$\frac{13}{14} \ln 2 \frac{x}{\ln x} \leq \frac{13}{14} \ln 2 \frac{5}{\ln 5} < 2 \leq \pi(x).$$

Nach empirischer Verifikation für $n < 3\,000\,000$ vermutete J. BERTRAND (1822 – 1900), daß es für jedes $n \in \mathbb{N}^*$ eine Primzahl zwischen n und $2n$ gibt. Dieses BERTRANDSche Postulat wurde erstmals 1850 durch CHEBYSHEV bewiesen. Der hier gegebene Beweis (der auch die Aussagen von Lemma 2.30 und Lemma 2.31 sowie Satz 2.32 enthält) stammt im wesentlichen von ERDŐS (veröffentlicht 1932, als er 19 Jahre alt war). Er war nur am Ende etwas länger, weil nicht die Ungleichung $\pi(x) \leq x/2$ benutzt wurde.

Satz 2.36 (Bertrandsches Postulat). *Für alle $n \in \mathbb{N}^*$ gibt es eine Primzahl p mit $n < p \leq 2n$.*

Beweis. Die Primzahlen

$$2, 3, 5, 7, 13, 23, 43, 83, 163,$$

von denen jede kleiner ist als das Doppelte der Vorhergehenden, zeigen, daß die Behauptung richtig ist für alle $1 \leq n < 163$ (LANDAUS Trick).

Sei also $n \geq 163$ und nehmen wir an, daß es kein $p \in \mathbb{P}$ mit $n < p \leq 2n$ gibt. Nach Lemma 2.30 und Lemma 2.31 ist dann

$$\frac{4^n}{2n} \leq (2n)^{\frac{1}{2}\sqrt{2n}} 4^{2n/3},$$

also

$$2^{2n/3} \leq (2n)^{\frac{1}{2}\sqrt{2n}+1}.$$

Dabei ist $\frac{1}{2}\sqrt{2n} + 1 < \frac{2}{3}\sqrt{2n}$ wegen $1 < 16/6 \leq \sqrt{2n}/6$. Somit ist

$$\frac{2}{3}n \ln 2 < \frac{2}{3}\sqrt{2n} \ln(2n),$$

d.h.

$$(2n)^{-\frac{1}{2}} \ln(2n) > \frac{\ln 2}{2} \tag{2.13}$$

Wegen $256 > e^2$ ist aber

$$(2n)^{-\frac{1}{2}} \ln(2n) \leq 256^{-\frac{1}{2}} \ln(256) = \frac{1}{16} \cdot 8 \ln 2 = \frac{\ln 2}{2}$$

im Widerspruch zu (2.13). □

Primzahlsatz $\Rightarrow \forall \varepsilon > 0 \exists n_0 \forall n \geq n_0 : p_{n+1} \leq p_n + \varepsilon p_n$.

Verschärfung: $\forall \delta > \delta_0 \exists c > 0 :$

$$p_{n+1} \leq p_n + cp_n^\delta$$

Werte für $\delta_0 (< 1)$: $\frac{3299}{3300}$ (1933 HOHEISEL), $\frac{5}{8}$ (1940 INGHAM), $\frac{3}{5}$ (1969 MONTGOMERY), $\frac{7}{12}$ (1972 HUXLEY)

$\Rightarrow \exists n_0 \forall n \geq n_0 : \text{Es gibt Primzahl } p \text{ mit } n^3 < p < (n+1)^3$. Offen für Quadratzahlen (würde erst für $\delta_0 < \frac{1}{2}$ folgen).

2.3 Primzahlen in arithmetischen Progressionen

Zum Beispiel:

Sätzchen 2.37. *Es gibt unendlich viele Primzahlen der Form $3n + 2$, $n \in \mathbb{N}$.*

Beweis. 1) Jede Primzahl außer 3 hat entweder Form $3n + 1$ oder Form $3n + 2$.

Dabei ist (für $k_j \in \mathbb{N}$)

$$\prod_{j=1}^l (3k_j + 1) = 3K + 1 \text{ mit } K \in \mathbb{N}$$

Wegen $(3k + 1)(3m + 1) = 3 \underbrace{(3km + k + m)}_{\in \mathbb{N}} + 1$ triviale Induktion nach l .

2) Seien $p_1, \dots, p_r \in \mathbb{P}$ mit $p_i = 3n_i + 2, n_i \in \mathbb{N}$. Betrachte

$$a = 3p_1 p_2 \dots p_r - 1 = 3(p_1 p_2 \dots p_r - 1) + 2$$

Keine der Primzahlen p_1, \dots, p_r teilt a (denn $p_i \nmid 1$). Alle Faktoren in Primzerlegung von a sind von p_1, \dots, p_r verschieden. Wegen (1) können nicht alle Faktoren Form $3n + 1$ haben. Also ex. weitere Primzahl p der Form $3n + 2$. \square

Allgemeine Frage: $q \in \mathbb{N}^*, r \in \mathbb{N}$: Ex. unendlich viele Primzahlen der Form $qn + r$? – Sicher nicht, falls q und r nicht teilerfremd sind! 1837 zeigte G. P. L. DIRICHLET (1805–1859) den

Satz 2.38 (Primzahlsatz für arithmetische Progressionen). *Seien $q, r \in \mathbb{N}^*$ teilerfremd. Dann gibt es in der arithmetischen Progression*

$$q + r, 2q + r, 3q + r, \dots$$

unendlich viele Primzahlen.

Es gibt einfache Beweise für gewisse Spezialfälle, aber bisher ist kein elementarer Beweis für den allgemeinen Satz gefunden.

2.4 Primzahlen als Werte von Polynomen

Satz 2.39 (Dirichlet). *Seien $a_0, a_1 \in \mathbb{Z}$, $x \mapsto a_0 + a_1 x$ hat für unendlich viele $x \in \mathbb{Z}$ Werte in \mathbb{P} .*

EULER: Für $h(x) = x^2 - x + 41$ sind $h(0), h(1), \dots, h(40) \in \mathbb{P}$.

LEGENDRE: Für $l(x) = x^2 + x + 41$ sind $l(0), l(1), \dots, l(39) \in \mathbb{P}$. (folgt aus „EULER“ wegen $l(x) = h(x + 1)$).

Später: Wegen $l(-x) = h(x)$ sind auch $l(-1), l(-2), \dots, l(-40) \in \mathbb{P}$. Folgerung: Für $g(x) = l(x - 40) = x^2 - 79x + 1601$ sind $g(0), g(1), \dots, g(79) \in \mathbb{P}$.

Frage: Gibt es Polynome mit Grad ≥ 1 mit $f \in \mathbb{Z}[x]$ mit $f(\mathbb{N}) \subset \mathbb{P}$? Nein!

Lemma 2.40. *Sei $f \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$, $b = f(a) \neq 0$*

$$\Rightarrow f(a + b^2) = f(a)c \text{ mit } \text{ggT}(f(a), c) = 1$$

Beweis. $f(x) = (x - a)g(x) + f(a)$ mit $g(x) \in \mathbb{Z}[x]$. Insbesondere gilt

$$f(a + b^2) = b^2 g(a + b^2) + f(a) = f(a)(f(a)g(a + b^2) + 1), \quad (f(a), c) = 1.$$

\square

Satz 2.41. *Sei $f(x) = \sum_{i=0}^r a_i x^i$ mit $a_i \in \mathbb{Z}, r \geq 1, a_r > 0$. Dann existiert für jedes $i \in \mathbb{N}$ ein $n_i \in \mathbb{N}$, sodaß $f(n_i)$ mindestens i verschiedene Primfaktoren hat.*

Beweis. $\exists x_0 \geq 4 \forall x \geq x_0 : f(x) > \frac{1}{2} a_r x^r$. Wähle $n_1 > x_0$ beliebig. Wegen $f(n_1) > 2$ hat $f(n_1)$ mindestens einen Primfaktor. Sei $i \geq 1$ und $n_i > x_0$, so daß $f(n_i)$ mindestens i Primfaktoren hat. Setze

$$n_{i+1} = n_i + (f(n_i))^2$$

Dann ist

$$f(n_{i+1}) > \frac{1}{2} a_r \underbrace{n_{i+1}^r}_{\geq n_{i+1}} \geq \frac{1}{2} a_r f(n_i) f(n_i).$$

Dabei ist

$$\frac{1}{2} a_r f(n_i) \geq 1,$$

da $\underbrace{f(n_i)}_{i \text{ Primfaktoren}} \geq 2$. Somit $f(n_{i+1}) > f(n_i)$. Nach Lemma

$$f(n_{i+1}) = f(n_i)c$$

mit $(f(n_i), c) = 1$. Dabei $c > 1$ wegen $f(n_{i+1}) > f(n_i)$. Nach Induktionsannahme hat $f(n_i)$ mindestens i verschiedene Primfaktoren. Durch c kommt mindestens ein weiterer für $f(n_{i+1})$ hinzu. \square

Welche Primzahlen als Werte von $x^2 + y^2$ mit $x, y \in \mathbb{N}$?

Satz 2.42 (Euler). *Eine Primzahl p ist genau dann Summe von zwei Quadratzahlen x^2, y^2 mit $x, y \in \mathbb{N}$, wenn p gleich 2 ist oder bei Division durch 4 den Rest 1 hat.*

Beweis. Eine Richtung leicht: Sei $p > 2$, $p = x^2 + y^2$ mit $x, y \in \mathbb{N}$. x, y können nicht beide gerade sein, da sonst p durch 4 teilbar. x, y können auch nicht beide ungerade sein, da sonst p durch 2 teilbar. Also etwa x gerade, y ungerade: $x = 2k, y = 2m + 1$ mit $k, m \in \mathbb{N}$. Dann

$$p = x^2 + y^2 = 4(k^2 + m^2 + m) + 1$$

(Der Rest fehlt...)

\square

GOLDBACHSche Vermutung: Jede gerade Zahl größer als zwei ist Summe von zwei Primzahlen.

Satz 2.43 (Großer Fermatscher Satz). *Die Gleichung $x^n + y^n = z^n$ mit $n > 2$ hat keine Lösungen mit $x, y, z \in \mathbb{Z}$ mit $xyz \neq 0$.*

Satz 2.44. *Seien $a, b, c \in \mathbb{N}^*$. Dann sind äquivalent:*

1) $a^2 + b^2 = c^2$ (a, b, c pythagoräisches Tripel: a, b Katheten, c Hypothense eines rechtwinkligen Dreiecks)

2) Es gibt $s, u, v \in \mathbb{N}^*$ mit $(u, v) = 1$, so daß

$$a = 2suv \quad b = s(u^2 - v^2) \quad c = s(u^2 + v^2)$$

oder

$$a = s(u^2 - v^2) \quad b = 2suv \quad c = s(u^2 + v^2)$$

(Grundtripel, falls $s = 1$)

Beweis. 2)⇒1):

$$a^2 + b^2 = 4s^2u^2v^2 + s^2(u^4 - 2u^2v^2 + v^4) = s^2(u^4 + 2u^2v^2 + v^4) = c^2$$

(Bemerkung: Verschiedene u, v ergeben verschiedene Tripel)

1)⇒2): a, b beide ungerade? Wenn ja, dann $2 \mid c^2$, $2 \mid c$, $4 \mid c^2$, außerdem $a = 2k + 1$, $b = 2m + 1$:

$$a^2 + b^2 = 4(k^2 + k + m^2 + m) + 2$$

$4 \nmid a^2 + b^2$. Widerspruch! ⚡

Sei zunächst $(a, b) = 1$. Dann sind nicht a und b gerade. Also oBdA a gerade, b ungerade. $a = 2a_0, a_0 \in \mathbb{N}^*$. Dann c^2 ungerade, also c ungerade.

$$a_1 := \frac{c+b}{2} \in \mathbb{N}^*, \quad a_2 := \frac{c-b}{2} \in \mathbb{N}^*.$$

Wegen $a^2 = c^2 - b^2 = (c+b)(c-b)$ folgt

$$a_0^2 = a_1 a_2$$

Es ist $(a_1, a_2) = 1$: Wegen $(a, b) = 1$ sind auch $(b, c) = 1$ ($p \in \mathbb{P}, p \mid b, p \mid c \Rightarrow p \mid c^2 - b^2 \Rightarrow p \mid a^2 \Rightarrow p \mid a$; $c = a_1 + a_2, b = a_1 - a_2$) Daher

$$a_1 = u^2, \quad a_2 = v^2$$

mit $u, v \in \mathbb{N}^*$. Wir erhalten

$$c = a_1 + a_2 = u^2 + v^2, \quad b = a_1 - a_2 = u^2 - v^2, \quad a^2 = 4a_0^2 = 4u^2v^2$$

□

Bemerkung 2.45. 1) $x^{nm} + y^{mn} = z^{mn} \iff (x^m)^n + (y^m)^n = (z^m)^n$

2) $n \in \mathbb{N}, n > 2 \Rightarrow (\exists p \in \mathbb{P}, p > 2, p \mid n) \vee (4 \mid n \text{ (} n = 2^k \text{ mit } k \geq 2))$

3) (1)+(2)⇒ GFS richtig für alle $n > 2$, falls richtig für $n = 4$ und $n = p \in \mathbb{P}, p > 2$.

Beweis. von FERMAT für $n = 4$:

Ann.: $\exists x, y, z \in \mathbb{N}^*$ mit $x^4 + y^4 = z^4 = (z^2)^2$. Dann existiert minimales $m \in \mathbb{N}^*$, zu dem es $x, y \in \mathbb{N}^*$ gibt mit $x^4 + y^4 = m^2$. Insbesondere $(x, y) = 1$. Sei etwa x^2 gerade, y^2 ungerade. Nach vorigem Satz existieren $u, v \in \mathbb{N}^*$ mit $(u, v) = 1$:

$$x^2 = 2uv, \quad y^2 = u^2 - v^2, \quad m = u^2 + v^2$$

Wegen $y^2 + v^2 = u^2$ existieren $r, s \in \mathbb{N}^*$ mit $(r, s) = 1$,

$$v = 2rs, \quad y = r^2 - s^2, \quad u = r^2 + s^2$$

(y ungerade!) Wir erhalten $x^2 = 2uv = 4rs(r^2 + s^2)$,

$$\left(\frac{x}{2}\right)^2 = rs(r^2 + s^2)$$

mit $\frac{x}{2} \in \mathbb{N}^*$. Die Zahlen $r, s, r^2 + s^2$ sind paarweise teilerfremd. Daher sind $r, s, r^2 + s^2$ Quadrate:

$$r = x_1^2, s = y_1^2, r^2 + s^2 = m_1^2$$

mit $x_1, y_1, m_1 \in \mathbb{N}^*$. Es folgt

$$x_1^4 + y_1^4 = m_1^2$$

Nun ist aber

$$m = u^2 + v^2 > u^2 = (r^2 + s^2)^2 = m_1^4 \geq m_1.$$

Also $m > m_1$. Widerspruch! □

$p = 3$: EULER. E. KUMMER (1810–1893): bis $p < 643$. Mit Computer: bis $p < 25000$.
Fälle:

1) $p \nmid xyz$. Mit Computer bis 253 747 889. Auch für $n = 2$ keine Lösung mit $xyz \neq 0$.

2) $p \mid xyz$

2.5 Eulersche φ -Funktion

(1760 von L. EULER eingeführt).

$$\forall a \in \mathbb{N}^* : \varphi(a) := \#\{j \in \mathbb{N}^* \mid j \leq a, (j, a) = 1\}$$

a	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(a)$	1	1	2	2	4	2	6	4	6	4	10	4

Satz 2.46 (Teilersummenformel). $\forall a \in \mathbb{N}^* : \sum_{d|a} \varphi(d) = a$

Beweis. Sei $d \mid a$, $T(d) := \{x \in \mathbb{N}^* : x \leq a, (x, a) = d\}$. Dann

$$\bigcup_{d|a} T(d) = \{1, 2, \dots, a\}$$

Klar: Für $d' \neq d$ ist $T(d') \cap T(d) = \emptyset$. Somit ist

$$a = \sum_{d|a} \#T(d)$$

Sei $d \mid a$. Dann ist

$$T(d) = \left\{ qd \mid q \in \mathbb{N}^*, q \leq \frac{a}{d}, (qd, a) = d \right\}$$

wegen $(qd, a) = d \iff (q, a/d) = 1$ gilt

$$\#T(d) = \# \left\{ q \in \mathbb{N}^* \mid q \leq \frac{a}{d}, (q, a/d) = 1 \right\} = \varphi(a/d)$$

Es folgt

$$a = \sum_{d|a} \varphi(a/d) = \sum_{d|a} \varphi(d)$$

□

Beispiel 2.10. $a = 12$:

$$\sum_{d|12} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$

Lemma 2.47. Seien $a, b \in \mathbb{N}^*$, $(a, b) = 1$. Dann $d \mid ab \iff d = d_1 d_2$ mit $d_1 \mid a$ und $d_2 \mid b$. Dabei d_1, d_2 eindeutig durch d bestimmt.

Beweis. „ \Leftarrow “: Trivial.

„ \Rightarrow “: Wir haben Primzerlegungen

$$a = \prod_{i=1}^r p_i^{m_i}, \quad b = \prod_{j=1}^s q_j^{n_j}$$

mit paarweise verschiedenen p_i, q_i . Sei $d \mid ab$, also

$$d = \prod_{i,j=1}^{r,s} p_i^{\mu_i} q_j^{\nu_j}$$

mit $0 \leq \mu_i \leq m_i$ und $0 \leq \nu_j \leq n_j$. Daher $d = d_1 d_2$ mit

$$d_1 = \prod_{i=1}^r p_i^{\mu_i}, \quad d_2 = \prod_{j=1}^s q_j^{\nu_j}$$

Annerns geht dat nich! (sic!)

$$d = \tilde{d}_1 \tilde{d}_2, \tilde{d}_1 \mid a, \tilde{d}_2 \mid b \Rightarrow (\tilde{d}_1 \mid d, \tilde{d}_2 \mid d) \Rightarrow \tilde{d}_1 = \prod_{i=1}^r p_i^{\tilde{\mu}_i}, \tilde{d}_2 = \prod_{i=1}^s p_i^{\tilde{\nu}_i}$$

Also $\tilde{\mu}_i = \mu_i, \tilde{\nu}_j = \nu_j \forall i, j$. □

Satz 2.48. 1) φ ist multiplikativ: $\forall a, b \in \mathbb{N}^*$ mit $(a, b) = 1$ ist $\varphi(ab) = \varphi(a)\varphi(b)$.

$$2) \varphi(a) = a \prod_{p|a} \left(1 - \frac{1}{p}\right)$$

Beweis. 1) Vollständige Induktion nach $n = ab$:

$$n = 1: a = b = 1, \varphi(ab) = \varphi(1) = 1 \cdot 1 = \varphi(a)\varphi(b)$$

Sei $n \geq 2$ und die Behauptung richtig für alle $a, b \in \mathbb{N}^*$ mit $ab < n$. Seien $a, b \in \mathbb{N}^*$ mit $a, b = n$. Es ist nach Lemma

$$\sum_{d_1|a, d_2|b} \varphi(d_1 d_2) = \sum_{d|ab} \varphi(d) = ab = \sum_{d_1|a} \varphi(d_1) \sum_{d_2|b} \varphi(d_2) = \sum_{d_1|a, d_2|b} \varphi(d_1)\varphi(d_2)$$

Nach IA ist dabei $\varphi(d_1 d_2) = \varphi(d_1)\varphi(d_2)$, falls $d_1 d_2 < n = ab$. Nur für $d_1 = a$ und $d_2 = b$ ist $d_1 d_2 = ab$. Aus obiger Gleichheit folgt daher, daß auch

$$\varphi(ab) = \varphi(a)\varphi(b)$$

2) Sei $1 \leq j \leq p^m, p \in \mathbb{P}, m \in \mathbb{N}^*$. Dann ist

$$(j, p^m) \neq 1 \iff p | j$$

und

$$\{j \in \mathbb{N}^* : 1 \leq j \leq p^m, p | j\} = \{qp : 1 \leq q \leq p^{m-1}\}.$$

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

Für $a = p_1^{m_1} \cdots p_r^{m_r}$ (mit verschiedenen p_i) ist also

$$\varphi(a) = \prod_{i=1}^r \varphi(p_i^{m_i}) = \prod_{i=1}^r (p_i^{m_i} - p_i^{m_i-1}) = \prod_{i=1}^r p_i^{m_i} \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

□

Beispiel 2.11. $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \Rightarrow \varphi(2100) = (2^2 - 2^1)(3^1 - 3^0)(5^2 - 5^1)(7^1 - 7^0) = 2 \cdot 2 \cdot 20 \cdot 6 = 480$

3 Kongruenzen und Restklassenringe

3.1 Allgemeines und Definitionen

Lemma 3.1. Seien $a, b \in \mathbb{Z}, m \in \mathbb{N}^*$. Dann sind äquivalent:

- 1) a, b haben bei Division durch m denselben Rest.
- 2) $m \mid a - b$.
- 3) $\frac{a-b}{m} \in \mathbb{Z}$

Beweis. $\exists! q_j \in \mathbb{Z}, r_j \in \mathbb{N}: a = q_1 m + r_1, b = q_2 m + r_2, 0 \leq r_j \leq m - 1$

(1) \Rightarrow (2): $r_1 = r_2 \Rightarrow a - b = (q_1 - q_2)m$

(2) \iff (3): trivial

(2) \Rightarrow (1): $qm + 0 = a - b = (q_1 - q_2)m + (r_1 - r_2) \Rightarrow r_1 = r_2$ falls $r_1 \geq r_2$. Falls $r_1 < r_2$ betrachte $b - a$. \square

Definition 3.1. Sei $m \in \mathbb{N}^*$. Dann heißen $a, b \in \mathbb{Z}$ kongruent modulo m , geschrieben

$$a \equiv b \pmod{m} \text{ kurz: } a \equiv b (m),$$

falls $m \mid a - b$.

Beispiel 3.1. $17 \equiv 1 \pmod{4}, 15 \equiv -1 \pmod{4}$

Bemerkung 3.2. „ $\equiv \cdot (m)$ “ ist Äquivalenzrelation ($(a - c = (a - b) + (b - c))$). (Mathematikhistorisch die erste, die man betrachtet hat.)

Rechenregeln 3.3. $a' \equiv a (m), b' \equiv b (m) \Rightarrow a' \pm b' \equiv a \pm b (m)$

Beweis.

$$(a' \pm b') - (a \pm b) = (a' - a) \pm (b' - b)$$

$$a'b' - ab = (a' - a)b' + a(b' - b) \in m\mathbb{Z} \quad \square$$

Beispiel 3.2. 1) $2^{2^5} + 1 \notin \mathbb{P}$, da $641 \mid 2^{32} + 1$.

$$641 = 5 \cdot 128 + 1 \Rightarrow 5 \cdot 2^7 \equiv -1 (641)$$

$$\Rightarrow 5^4 \cdot 2^{28} \equiv 1 (641). \quad 641 = 625 + 16 = 5^4 + 2^4 \Rightarrow 5^4 \equiv -2^4 (641) \Rightarrow (-2^4)2^{28} \equiv 1 (641) \iff -2^{32} \equiv 1 (641) \iff 641 \mid 2^{32} + 1$$

- 2) $47 \mid 2^{23} - 1 =: M_{23}: 2^5 = 32 \equiv -15 (47) \Rightarrow 2^{10} \equiv (-15)^2 \equiv -10 (47)$
 $\Rightarrow 2^{20} \equiv 100 \equiv 6 (47) \Rightarrow 2^{20} \cdot 8 \equiv 48 \equiv 1 (47)$
 $\Rightarrow 2^{23} - 1 \equiv 0 (47)$

Aus den Rechenregeln für Kongruenzen folgt, daß $\mathbb{Z}/m\mathbb{Z}$ = Menge aller Äquivalenzklassen, explizit:

$$\{x + m\mathbb{Z} \mid x \in \mathbb{Z}\} = \{x + m\mathbb{Z} \mid x \in \mathbb{N}, x \leq m - 1\}$$

ein kommutativer Ring mit 1 ist:

$$(x + m\mathbb{Z}) + (y + m\mathbb{Z}) = (x + y) + m\mathbb{Z},$$

und $\#\mathbb{Z}/m\mathbb{Z} = m$. Wenn man will, kann man mit den Repräsentanten $0, 1, \dots, m - 1$ rechnen.

Beispiel 3.3. Symmetrie = Kommutativität

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Tabelle 3.1: Additionstafel, Multiplikationstafel für $m = 2$

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \qquad \begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}$$

Tabelle 3.2: Additionstafel, Multiplikationstafel für $m = 4$

Trivialerweise: $a \equiv b \pmod{m}, d \mid m \Rightarrow a \equiv b \pmod{d}$

Lemma 3.4. $m_1, m_2 \geq 1, v = \text{kgV}(m_1, m_2), a, b \in \mathbb{Z}$

$$a \equiv b \pmod{m_1} \text{ und } a \equiv b \pmod{m_2} \iff a \equiv b \pmod{v}$$

„ \Leftarrow “: trivial wg. oben.

„ \Rightarrow “: $m_1 \mid a - b, m_2 \mid a - b \Rightarrow \text{kgV}(m_1, m_2) \mid a - b$

Spezialfall: Gilt $(m_1, m_2) = 1$, so sind äquivalent

1) $a \equiv b \pmod{m_1}$ und $a \equiv b \pmod{m_2}$

2) $a \equiv b \pmod{m_1 m_2}$

Korollar 3.5. $m_1, \dots, m_r \geq 1, m_i$ paarweise teilerfremd.

$$a \equiv b \pmod{m_j} \forall j \iff a \equiv b \pmod{\left(\prod_{i=1}^r m_i\right)}$$

Beweis. „ \Leftarrow “: trivial. . .

„ \Rightarrow “: $a \equiv b(m_1 m_2)$ laut Spezialfall, $a \equiv b((m_1 m_2) m_3)$ laut Spezialfall. \square

Spezialfall: $m = \prod_{i=1}^r \underbrace{p_i^{n_i}}_{m_i}$, $a \equiv b(m) \iff a \equiv b(p_i^{n_i}) \forall i$

Bemerkung 3.6. $2 \cdot 2 \equiv 0(4)$, die Kürzungsregel gilt also nicht in Restklassenringen.

Satz 3.7 (Kürzungsregel).

$$(a, m) = 1, ab \equiv ac(m) \Rightarrow b \equiv c(m)$$

Scheinbar allgemeiner:

$$(a, m) = 1, a' \equiv a(m), ab \equiv a'c(m) \Rightarrow b \equiv c(m)$$

Beweis. $ab \equiv ac(m), a(b - c) \equiv 0(m)$, d.h. $m \mid a(b - c)$, also $m \mid (b - c)$. \square

Korollar 3.8. *Es sei $m = p$ eine Primzahl. Dann gilt*

- 1) $ab \equiv 0(p) \Rightarrow a \equiv 0(p)$ oder $b \equiv 0(p)$
- 2) Zu jedem $a, a \not\equiv 0(p) \exists b$ mit $ab \equiv 1(p)$

Beweis. 1) Angenommen $a \not\equiv 0(p)$. Dann ist $(a, p) = 1$. $ab \equiv a0 \Rightarrow b \equiv 0(p)$

- 2) Zu jedem $x \in \{0, 1, \dots, p - 1\}$ gibt es genau ein

$$\underbrace{f(x)}_{\text{Rest bei Division durch } p} \in \{0, 1, \dots, p - 1\}$$

mit $ax \equiv f(x)(p)$. Wegen Kürzungsregel ist f injektiv. Jede injektive Abbildung einer endlichen Menge in sich selbst ist surjektiv, also bijektiv (Schubfachprinzip). Insbesondere gibt es b mit $f(b) = 1$. \square

Satz 3.9. $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\iff m$ ist eine Primzahl.

Beweis. „ \Leftarrow “: Laut Korollar gibt es multiplikative Inverse.

„ \Rightarrow “: Wäre m keine Primzahl, so gäbe es Zerlegung $m = m_1 m_2, 1 < m_1, m_2 < m, m_1 m_2 \equiv 0(m)$. Damit ist $\mathbb{Z}/m\mathbb{Z}$ kein Körper. \square

Erinnerung: Ist p prim, $1 \leq k \leq p - 1$, so ist p ein Teiler von $\binom{p}{k}$

Satz 3.10. p prim, $n \geq 1$. $a \equiv b(p^n)$

Behauptung: $a^p \equiv b^p(p^{n+1})$. Ist zusätzlich $p > 2$ oder $n > 1$ sowie $a \not\equiv b(p^{n+1})$, so gilt $a^p \not\equiv b^p(p^{n+2})$.

Beweis. $a = b + cp^n$. Also gilt

$$a^p = \sum_{i=0}^p \binom{p}{i} b^{p-i} (cp^n)^i.$$

Es gelte nun $n > 1$ oder $p > 2$:

$$a^p \equiv b^p + \binom{p}{1} b^{p-1} cp^n + cp^{np} (p^{n+2}).$$

$np \geq n + 2$. Z.z.: $b^{p-1} cp^{n+1} \not\equiv 0 \pmod{p^{n+2}}$, also z.z.: $p \nmid cb^{p-1}$. Angenommen: $p \mid c$, dann wäre $a \equiv b \pmod{p^{n+1}}$, oder $p \mid b^{p-1}$. \square

$9 \mid a \iff 9 \mid \text{Quersumme}(a)$ Allgemeiner: $g \in \mathbb{N}$, $g \geq 2$. $a \in \mathbb{N}$ habe die g -adische Entwicklung, d.h.

$$a = \sum_{\nu=0}^n a_{\nu} g^{\nu} \quad a_{\nu} \in \{0, \dots, g-1\}$$

Definition 3.2. $Q_g(a) = \sum_{\nu=0}^n a_{\nu}$ heißt g -adische Quersumme von a .
 $Q'_g(a) = \sum_{\nu=0}^n (-1)^{\nu} a_{\nu}$ heißt g -adische alternierende Quersumme von a .

Satz 3.11. $a \equiv Q_g(a) (g-1)$, $a \equiv Q'_g(a) (g+1)$

Beweis.

$$\begin{aligned} g &\equiv 1 \pmod{g-1} \\ g^{\nu} &\equiv 1 \pmod{g-1} \\ a &= a_0 g^0 + \dots + a_n g^n \\ \Rightarrow a &\equiv \sum_{i=0}^n a_i \pmod{g-1} \\ g &\equiv -1 \pmod{g+1} \\ g^{\nu} &\equiv (-1)^{\nu} \pmod{g+1} \end{aligned}$$

und so weiter und so fort. \square

Beispiel 3.4. 1) $Q_{10}(a) \equiv a \pmod{9} \Rightarrow (9 \mid Q_{10}(a) \Rightarrow 9 \mid a)$

2) Was ist der Rest von 3794 modulo 11, d.h., Division durch 11: $Q'_{10}(3794) = 4 - 9 + 7 - 3 = -1$

Korollar 3.12.

$$\begin{aligned} Q_g(a \dagger b) &\equiv Q_g(a) \dagger Q_g(b) \pmod{g-1} \\ Q'_g(a \dagger b) &\equiv Q'_g(a) \dagger Q'_g(b) \pmod{g+1} \end{aligned}$$

Beweis.

$$\begin{aligned} Q_g(a \cdot b) &\equiv a \cdot b \pmod{g-1} \\ &\equiv Q_g(a) \cdot Q_g(b) \end{aligned} \quad \square$$

Beispiel 3.5. ISB-Nummern: Es gibt Ziffern a_j , $j \in \{0 \dots 9\}$, $a_j \in \{1 \dots 9\}$, sowie $a_{10} \in \{0, \dots, 9, A\}$. Es gilt die Prüfbedingung (P): $\sum_{\nu=1}^9 \nu a_\nu \equiv a_{10} \pmod{11}$

Satz 3.13 (Euler-Fermatscher Satz, „kleiner Fermat“). *Es gilt: $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$. Insbesondere: $m = p$ prim, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.*

Beweis. 1) $m = 1$: trivial.

$m = p$: prim.

$$\begin{aligned} (a+b)^p &\equiv a^p + b^p \pmod{p} \\ (a_1 + \dots + a_n)^p &\equiv a_1^p + \dots + a_n^p \pmod{p} \end{aligned}$$

Speziell: $n = a$, $a_j = a \forall j$. OBdA $a > 0$.

$$a^{2p} \equiv a \cdot a^p \pmod{p}$$

mit Kürzungsregel: $a^{p-1} \equiv 1 \pmod{p}$

2) $m = p^k$: $\varphi(m) = p^k - p^{k-1}$, $p\varphi(p^k) = p^{k+1} - p^k = \varphi(p^{k+1})$. Induktion über k : $k = 1$ erledigt.

$$a^{\varphi(p^k)} \equiv 1 \pmod{p^k} \Rightarrow a^{p\varphi(p^k)} \equiv 1^p \pmod{p^{k+1}}$$

3) $m = \prod_{i=1}^r \underbrace{p_i^{\alpha_i}}_{m_i}$ Primfaktorzerlegung.

$$\varphi(m) = \varphi\left(\prod_i m_i\right) = \prod_i \varphi(m_i)$$

wegen m_i pw. teilerfremd. Insbes. $\varphi(m_j) \mid \varphi(m)$. Wir wissen $a^{\varphi(m_j)} \equiv 1 \pmod{m_j} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m_j} \forall j$

m_1, \dots, m_r pw. teilerfremd $\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$.

Zweiter Beweis:

$(a, m) = 1 \exists x, y : 1 = xa + ym \Rightarrow 1 \equiv xa \pmod{m}$

$m > 1$ Setze $n := \varphi(m)$. x_1, \dots, x_n seien die m teilerfremden Zahlen in $\{1, \dots, m\}$. a gegeben, $(a, m) = 1$. Division mit Rest ergibt $ax_\nu = q_\nu m + r_\nu$, und wir erhalten Reste r_1, \dots, r_n $0 < r_\nu \leq m-1$.

Beh. $r_j \neq r_l$ für $j \neq l$. Sonst $(ax_\nu, m) = 1$,

$$a(x_j - x_l) = m(q_j - q_l) \Rightarrow m \mid a(x_j - x_l) \Rightarrow m \mid x_j - x_l$$

Widerspruch, weil $|x_j - x_l| < m$. Aus $ax_\nu = q_\nu m + r_\nu$ ergibt sich, daß r_ν, m teilerfremd. Schubfachprinzip: $\{x_1, \dots, x_n\} = \{r_1, \dots, r_n\}$.

$ax_\nu \equiv r_\nu \pmod{m}$ $1 \leq \nu \leq n$, multipliziere diese n Kongruenzen zusammen

$$(ax_1) \cdot \dots \cdot (ax_n) \equiv r_1 \dots r_n \equiv a^n x_1 \dots x_n \pmod{m}$$

\Rightarrow Kürzen, da teilerfremd: $a^n \equiv 1 \pmod{m}$. □

Anwendung/Erläuterung: $(a, m) = 1$. Suche Lösung von $ax + ym = 1$, z.B. $x = a^{\varphi(m)-1}$, $y = -\frac{a^{\varphi(m)}-1}{m} \in \mathbb{Z}$

Beispiel 3.6. $a^{12} \equiv 1 \pmod{13}$; $10^6 \equiv 1 \pmod{13}$, denn

$$1001 = 910 + 91 \Rightarrow 1000 \equiv -1 \pmod{13} \Rightarrow 1000^2 \equiv 1 \pmod{13}$$

Korollar 3.14. Seien $a, m \in \mathbb{N}^*$ mit $(a, m) = 1$, und $m = m_1 m_2 \dots m_r$ mit paarweise teilerfremden m_i . Dann ist bereits

$$a^l \equiv 1 \pmod{m} \text{ für } l = \text{kgV}(\varphi(m_1), \dots, \varphi(m_r))$$

Beweis. („bereits“, da $\varphi(m_j) \mid \varphi(m) \forall j$, also $l \leq \varphi(m)$.)

$\forall j : a^{\varphi(m_j)} \equiv 1 \pmod{m_j}$, $\varphi(m_j) \mid l$

$$\Rightarrow \forall j : a^l \equiv 1 \pmod{m_j} \iff a^l \equiv 1 \pmod{m_1 \dots m_r}$$

da m_i paarweise teilerfremd. □

Beispiel 3.7. $m = 15 = 3 \cdot 5$, $\varphi(3) = 2$, $\varphi(5) = 4$, $\text{kgV}(\varphi(3), \varphi(5)) = 4 < 8$

Nach Satz ist $11^4 \equiv 1 \pmod{15}$. Nicht optimal: $11^2 = 121 \equiv 1 \pmod{15}$!

Weiteres

Korollar 3.15. Sei $a \in \mathbb{N}^*$, $p \in \mathbb{P}$, $p > 2$, $p \nmid a$. Dann gilt entweder

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$$

oder

$$a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$$

Beweis. $s := \frac{1}{2}(p-1) \in \mathbb{N}^*$

$$(a^s - 1)(a^s + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}$$

$\Rightarrow a^s - 1 \equiv 0 \pmod{p}$ oder $a^s + 1 \equiv 0 \pmod{p}$. Nicht beides kann gelten, da sonst $1 \equiv -1 \pmod{p}$, aber $p > 2$. □

Bemerkung 3.16. „kleiner FERMATScher Satz“ (d.h. $a^{p-1} \equiv 1 \pmod{p}$ für alle $a \in \mathbb{N}^*$ mit $p \nmid a$) charakterisiert nicht Primzahlen! Denn (ohne Beweis!) für $m = 561 = 3 \cdot 11 \cdot 17$ ist

$$a^{560} \equiv 1 \pmod{561} \quad \forall a \in \mathbb{N}^* \text{ mit } (a, 561) = 1.$$

Lemma 3.17. Sei $p \in \mathbb{P}$, $p > 2$, und seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$ mit $p \nmid b$ und $a^p \equiv b^p \pmod{p^{n+1}}$. Dann ist $a \equiv b \pmod{p^n}$

Beweis. Trivial für $a = b$. Sei also $a \neq b$. Sicher ist $a^p \equiv b^p \pmod{p}$ wegen $p \mid p^{n+1}$. Wegen $p \nmid b$ also auch $p \nmid a$. Somit $a^{p-1} \equiv 1 \equiv b^{p-1} \pmod{p}$. Es folgt

$$(a - b)b^{p-1} = a^p - b^p - a(a^{p-1} - b^{p-1}) \equiv 0 \pmod{p} = 0b^{p-1}$$

$b^{p-1} \not\equiv 0 \pmod{p} \Rightarrow a - b \equiv 0 \pmod{p}$. Wegen $a \neq b$ ist $a \not\equiv b \pmod{p^r}$ wenn r hinreichend groß ist. Daher gibt es $\max r \in \mathbb{N}^*$ mit $a \equiv b \pmod{p^r}$. Nach früherem Satz folgt

$$a^p \equiv b^p \pmod{p^{r+1}}, \quad a^p \not\equiv b^p \pmod{p^{r+2}}$$

Somit $a^p \equiv b^p \pmod{p^k} \iff k \leq r + 1$. Nach Voraussetzung ist $a^p \equiv b^p \pmod{p^{n+1}}$, also $n + 1 \leq r + 1, n \leq r$. Daher $a \equiv b \pmod{p^n}$ wegen $p^n \mid p^r$. \square

3.2 Anwendung des Satzes von Fermat-Euler in der Kryptographie

W. DIFFEE, M. HELLMANN: "New directions in cryptography" (publiziert 1976); 1978: R. L. RIVEST, A. SHAMIR, L. ADLEMAN: "A method for obtaining digital signatures and public-key cryptosystems"
„RSA-System“:

Happy $2^2 \cdot 3 \cdot 167!$

- 1) Empfänger teilt aller Welt $m, s \in \mathbb{N}^*$ mit.
- 2) Sender verschlüsselt die nach irgendeinem (bekanntem) Verfahren als $a \in \mathbb{N}^*$ dargestellte Nachricht, indem er Rest r bei Division von a^s durch m berechnet.
- 3) Sender schickt r an Empfänger, auch öffentlich.

Bedingungen: $1 < a < \min\{p \in \mathbb{P} : p \mid m\}, 1 < s < \varphi(m), (\varphi(m), s) = 1$ Empfänger kennt $\varphi(m)$, andere können es nicht berechnen, z. B. durch $m = pq$ mit großen $p, q \in \mathbb{P}$ ($\geq 10^{100}$). Es ist

$$\begin{aligned} \varphi(m) &= (p-1)(q-1) \\ &= (p-1)(m/p-1) \\ &= (m/q-1)(q-1) \end{aligned}$$

also Kenntnis von $\varphi(m)$ etwa gleichwertig mit Kenntnis von p, q .

Entschlüsseln: $\exists t, n \in \mathbb{Z} : 1 = ts - n\varphi(m)$; oBdA $t > 0$ (addiere Vielfache des kgV($s, \varphi(m)$) zu beiden Termen), dann

$$r^t \equiv (a^s)^t = a^{n\varphi(m)+1} = a(a^{\varphi(m)})^n \equiv a \pmod{m}$$

Also: a Rest von r^t bei Division durch m .

3.3 Satz von Wilson

Frage: Gegeben $a, b, c, m \in \mathbb{Z}$. Wann existiert $x_0 \in \mathbb{Z}$ mit $ax_0 + c \equiv b \pmod{m}$? („Lineare Kongruenz“:

$$ax + c \equiv b \pmod{m}, \quad (3.1)$$

x Variable)

Klar, daß oBdA: $c = 0$. (Ersetze b durch $b - c$)

Lemma 3.18. Sei $x_0 \in \mathbb{Z}$ Lösung von (3.1). Dann ist

$$\{x_0 + z : z \in \mathbb{Z}, az \equiv 0 \pmod{m}\}$$

Gesamtheit aller Lösungen von (3.1).

Beweis. Klar (z. B. $ax \equiv b \pmod{m} \Rightarrow a(x - x_0) \equiv b - b \equiv 0 \pmod{m}$, $x = x_0 + (x - x_0)$). \square

Lemma 3.19. Seien $a, b, m \in \mathbb{Z}$, $d = (a, m) \neq 0$. Dann sind äquivalent:

1) $ax \equiv b \pmod{m}$ ist lösbar in \mathbb{Z}

2) $d \mid b$

Gilt (2) und ist x_0 Lösung von $ax \equiv b \pmod{m}$, so ist

$$\left\{ x_0 + \frac{m}{d}v \mid v \in \mathbb{Z} \right\}$$

Gesamtheit aller Lösungen von $ax \equiv b \pmod{m}$.

Beweis. Wir wissen $d\mathbb{Z} = a\mathbb{Z} + m\mathbb{Z}$.

(1) \Rightarrow (2): Wähle $x_0 \in \mathbb{Z}$ mit $ax_0 \equiv b \pmod{m}$. Dann ex. $y_0 \in \mathbb{Z}$ mit $ax_0 + my_0 = b$, also $b \in a\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, also $d \mid b$.

(2) \Rightarrow (1): Sei d ein Teiler von b , also $b \in d\mathbb{Z} = a\mathbb{Z} + m\mathbb{Z}$. Dann ex. $x_0, y_0 \in \mathbb{Z}$ mit

$$b = ax_0 + my_0,$$

also $ax_0 \equiv b \pmod{m}$.

Gelte jetzt (2) und sei $x_0 \in \mathbb{Z}$ mit $ax_0 \equiv b \pmod{m}$. Nach vorigem Lemma zu zeigen: für $z \in \mathbb{Z}$ ist

$$az \equiv 0 \pmod{m} \iff \exists v \in \mathbb{Z} : z = \frac{m}{d}v.$$

Sei $\hat{a} = \frac{a}{d}$, $\hat{m} = \frac{m}{d}$ ($\hat{a}, \hat{m} \in \mathbb{Z}$). Es gilt

$$az \equiv 0 \pmod{m} \iff m \mid az \iff \hat{m} \mid \hat{a}z \stackrel{(\hat{m}, \hat{a})=1}{\iff} \hat{m} \mid z \iff \exists v \in \mathbb{Z} : z = \hat{m}v \quad \square$$

Korollar 3.20. $a, b, m \in \mathbb{Z}$, $(a, m) = 1 \Rightarrow ax \equiv b \pmod{m}$ lösbar.

Beispiel 3.8. $8x \equiv -4 \pmod{12}$. $(8, 12) = 4$, $4 \mid -4$, \Rightarrow lösbar, 1 ist Lösung. Alle Lösungen sind dann von der Form $1 + 3\mathbb{Z}$, z. B. 1, 4, 7, 10.

Allgemein:

Satz 3.21. Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^*$, $d := (a, m) \mid b$. Dann hat $ax \equiv b \pmod{m}$ in \mathbb{Z} genau d mod m inkongruente Lösungen. Genauer:

1) Sei x_0 Lösung von $ax \equiv b \pmod{m}$,

$$x_j := x_0 + j \frac{m}{d} \quad (0 \leq j \leq d-1).$$

Dann sind x_0, x_1, \dots, x_{d-1} d paarweise modulo m inkongruente Lösungen von $ax \equiv b \pmod{m}$.

2) Jede Lösung von $ax \equiv b \pmod{m}$ ist kongruent zu einem x_j , $0 \leq j \leq d-1$.

Beweis. 1) Nach Lemma: $ax_j \equiv b \pmod{m} \forall 0 \leq j \leq d-1$. Dann ist

$$0 < x_j - x_k = (j - k) \frac{m}{d} < m,$$

also $x_k \not\equiv x_j \pmod{m}$.

2) Sei $z \in \mathbb{Z}$ Lösung von $ax \equiv b \pmod{m}$. Nach Lemma ist $z = x_0 + \frac{m}{d}v$ mit $v \in \mathbb{Z}$. Sei r Rest von v bei Division durch d :

$$v = qd + r, \quad q, r \in \mathbb{Z}, 0 \leq r < d.$$

Dann ist $z \equiv x_0 + r \frac{m}{d} = x_r \pmod{m}$ (da $\frac{m}{d}qd \equiv 0 \pmod{m}$) □

Lemma 3.22 (Heiratslemma). Sei $p \in \mathbb{P}$, $p \geq 5$, $K = \{n \in \mathbb{N} : 2 \leq n \leq p-2\}$,

$$E = \{(a, a') : a, a' \in K, aa' \equiv 1 \pmod{p}\}$$

Dann gilt:

1) $\forall a \in K \exists! a' \in K : (a, a') \in E$.

2) $(a, a') \in E \Rightarrow (a', a) \in E$.

3) $(a, a') \in E \Rightarrow a \neq a'$.

Beweis. 1) $a \in K, p \in \mathbb{P} \Rightarrow \exists a' \in \{0, 1, \dots, p-1\}$ mit $aa' \equiv 1 \pmod{p}$. $a' = 0$? $0 \cdot a = 0 \not\equiv 1 \pmod{p}$. $a' = 1$? $a \not\equiv 1 \pmod{p}$. $a' = p-1$? $a(p-1) \equiv 1 \pmod{p} \Rightarrow 0 \equiv ap \equiv a+1 \pmod{p}$ Widerspruch, da $3 \leq a+1 \leq p-1$. Also $a' \in K$.

2) trivial.

3) $a^2 \equiv 1 \pmod{p} \Rightarrow (a+1)(a-1) \equiv 0 \pmod{p} \Rightarrow a+1 \equiv 0 \pmod{p}$ oder $a-1 \equiv 0 \pmod{p}$. Für $a \in K$ ist aber $a \not\equiv \pm 1 \pmod{p}$. □

Korollar 3.23. $(p-2)! \equiv 1 \pmod{p}$

Beweis. $p = 2: 0! = 1$

$p = 3: 1! = 1$

$p \geq 5: (p-2)! = \prod_{a \in K} a = \prod_{\text{Paare } (a, a') \in E} aa' \equiv \prod 1 = 1$. Im ersten Produkt stehen $(p-2) - 2 + 1 = p-3$ Faktoren, im zweiten $\frac{p-3}{2}$ Faktoren. \square

Beispiel 3.9. $p = 7, K = \{2, 3, 4, 5\}, 2 \cdot 4 = 8 \equiv 1 \pmod{7}, 3 \cdot 5 = 15 \equiv 1$
 $2 \cdot 3 \cdot 4 \cdot 5 = (2 \cdot 4)(3 \cdot 5) \equiv 1$

Satz 3.24 (von Wilson). $\forall p \in \mathbb{P}: (p-1)! \equiv -1 \pmod{p}$

Beweis.

$$(p-1)! = (p-2)!(p-1)$$

$$(p-2)! \equiv 1 \pmod{p}$$

$$p-1 \equiv -1 \pmod{p} \quad \square$$

Bemerkung 3.25.

- 1) 1770 von E. WARING (1736–1798) bewiesen, der den Satz SIR JOHN WILSON zugeschrieben hat. Aber: Wahrscheinlich kannte LEIBNIZ die Aussage auch schon.
- 2) Der Satz charakterisiert Primzahlen.

3.4 Satz von Euler

Lemma 3.26. Sei $p = 2n + 1$ ungerade Primzahl. Dann gilt

$$(n!)^2 \equiv (-1)^{n+1} \pmod{p}$$

Insbesondere $((2k)!)^2 \equiv -1 \pmod{p}$, falls $p = 4k + 1, k \in \mathbb{N}$ und $((2k+1)!)^2 \equiv 1 \pmod{p}$, falls $p = 4k + 3, k \in \mathbb{N}$

Beweis. $2n = p - 1, 2n - 1 = p - 2, \dots, n + 1 = p - n$

$$\Rightarrow (p-1)! = (2n)! = n!(n+1)(n+2) \dots (2n-1)(2n)$$

$$= n!(p-1)(p-2) \dots (p-n)$$

$$\equiv n!(-1)^n n! \pmod{p}$$

$$-1 \equiv (n!)^2 (-1)^n \pmod{p} \quad \text{Satz v. WILSON}$$

$$(-1)^{n+1} \equiv (n!)^2 \pmod{p} \quad \square$$

Anwendung:

Satz 3.27 (Euler 1749). Für alle $p \in \mathbb{P}$ äquivalent:

- 1) $\exists a, b \in \mathbb{N}: a^2 + b^2 = p$
- 2) $p = 2$ oder $p \equiv 1 \pmod{4}$ ($p = 4k + 1$)

Dabei $\{a, b\}$ eindeutig ($a \neq b$ für $p \neq 2$)!

Beweis. (1) \Rightarrow (2): Schon gezeigt: $p > 2$: Entweder $a \equiv 0$ (2), $b \equiv 1$ (2) oder umgekehrt
 $\Rightarrow a^2 + b^2 \equiv 1$ (4)

(2) \Rightarrow (1): $2 = 1^2 + 1^2$.

Sei $2 < p \in \mathbb{P}, p \equiv 1$ (4). Dann existiert $k \in \mathbb{N}$: $p = 4k + 1$. Somit folgt nach Lemma

$$((2k)!)^2 \equiv -1 \pmod{p}$$

Mit $u := (2k)!$ also $u^2 \equiv -1 \pmod{p}$. Rest ist elegant zu machen, falls man weiß, daß in $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ eindeutige Primzerlegung gilt (bis auf Einheiten). (Indiz: $a^2 + b^2 = (a + ib)(a - ib), p = \pi\bar{\pi}, \pi, \bar{\pi} \in \mathbb{Z}[i] \mid \pi \mid p, \bar{\pi} \mid p \Rightarrow \pi = \bar{\pi}$)

$$\begin{aligned} p^2 &= p\bar{p} = \pi\bar{\pi}\pi\bar{\pi} = \pi\bar{\pi}\pi\bar{\pi} \in \mathbb{Z}[i] \cap \mathbb{R} = \mathbb{Z} \\ &\Rightarrow \pi\bar{\pi} = \pi\bar{\pi} = p = \pi\bar{\pi} \Rightarrow \pi = \bar{\pi} \end{aligned}$$

Aber...)

Elementar: Betrachte alle Paare $(x, y) \in \mathbb{Z}$ mit $0 \leq x \leq \lfloor \sqrt{p} \rfloor, 0 \leq y \leq \lfloor \sqrt{p} \rfloor$. Das sind $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ Paare (x, y) . Daher gibt es zwei verschiedene solcher Paare (x, y) , für die $ux - y \pmod{p}$ gleich ist.

Wähle $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ mit $(x_1, y_1) \neq (x_2, y_2), x_i, y_i \in [0, \lfloor \sqrt{p} \rfloor]$ mit

$$ux_1 - y_1 \equiv ux_2 - y_2 \pmod{p}$$

Für $x_0 := x_1 - x_2, y_0 = y_1 - y_2$ ist dann

$$ux_0 \equiv y_0 \pmod{p}, \quad (x_0, y_0) \neq (0, 0)$$

Es folgt

$$-x_0^2 \equiv (ux_0)^2 \equiv y_0^2 \pmod{p}$$

D. h.

$$x_0^2 + y_0^2 \equiv 0 \pmod{p} < 2p$$

Dabei ist

$$0 < x_0^2 + y_0^2$$

wegen $|x_0| \leq \lfloor \sqrt{p} \rfloor, |y_0| \leq \lfloor \sqrt{p} \rfloor$, mindestens eine strikte Ungleichung, da $x_1 \neq y_1$ oder $x_2 \neq y_2$. Somit

$$x_0^2 + y_0^2 = p$$

Eindeutigkeit: Sei

$$p = x^2 + y^2 = u^2 + v^2$$

mit $x, y, u, v \in \mathbb{N}, 0 < x < y < \sqrt{p}, 0 < u < v < \sqrt{p}$. Zu zeigen: $x = u, y = v$. Wir beweisen

$$p \mid xv - yu$$

Dann wegen

$$0 \leq |xv - yu| < p$$

sicher

$$0 = xv - yu, \quad \frac{x}{y} = \frac{u}{v}$$

$$y^2 \left(\left(\frac{x}{y} \right)^2 + 1 \right) = x^2 + y^2 = p = u^2 + v^2 = v^2 \left(\left(\frac{u}{v} \right)^2 + 1 \right)$$

$\Rightarrow y^2 = v^2 \Rightarrow y = v$. Dann auch $x = u$.

$$(xv - uy)(xv + yu) = x^2v^2 - y^2u^2 = (p - y^2)v^2 - y^2u^2 = pv^2 - y^2(u^2 + v^2) = p(v^2 - y^2)$$

$p \mid xv - yu$ oder $p \mid xv + yu$

Noch z. z.: $p \nmid xv + yu$. Annahme: $p \mid xv + yu$. Es ist

$$0 < xv + yu < 2p,$$

dann gilt $xv + yu = p$.

$$p^2 = (x^2 + y^2)(u^2 + v^2) = \underbrace{(xv + yu)^2}_{=p^2} + (xu - yv)^2 \quad (\forall x, y, u, v \in \mathbb{R})$$

$\Rightarrow xu - yv = 0$. Widerspruch wegen $xu < yv$ ($0 < x < y, 0 < u < v$). □

Korollar 3.28. Sei $n \in \mathbb{N}$, $n = p_1 p_2 \dots p_m$, $p_j \in \mathbb{P}$, kein p_j sei von der Form $4k + 3$. Dann ist n Summe von zwei Quadraten natürlicher Zahlen.

Beweis. $p_j = a_j^2 + b_j^2$ mit $a_j, b_j \in \mathbb{N}$. Also ist n ein Produkt von Quadratsummen; also wiederum Quadratsumme. □

Satz 3.29. Sei $n \in \mathbb{N}^*$. Dann sind äquivalent:

- 1) $\exists a, b \in \mathbb{N} : n = a^2 + b^2$.
- 2) In der Primfaktorzerlegung von n treten Faktoren der Form $4k + 3$ mit gerader Vielfachheit auf.

Beweis. (2) \Rightarrow (1): $n = p_1 \dots p_m s^2$ mit $p_j = 4k + 1$, $k \in \mathbb{N}$. Dann gibt es $a, b \in \mathbb{N}$ mit

$$p_1 \dots p_m = a^2 + b^2$$

so daß $n = (as)^2 + (bs)^2$

(1) \Rightarrow (2): $d := (a, b)$

$$\hat{a} := \frac{a}{d}, \quad \hat{b} := \frac{b}{d}$$

Dann gilt

$$d^2(\hat{a}^2 + \hat{b}^2) = d^2\hat{a}^2 + d^2\hat{b}^2 = a^2 + b^2 = n.$$

Mit $\hat{n} := \frac{n}{d^2}$ ist $\hat{n} = \hat{a}^2 + \hat{b}^2$.

Annahme: $\exists q \in \mathbb{P}$, $q \equiv 3 \pmod{4}$, $q \mid n$, q mit ungerader Vielfachheit. In d^2 kommt q mit gerader Vielfachheit vor. Also kommt q in \hat{n} mit ungerader Vielfachheit vor. Also $q \mid \hat{n}$.

Falls $q \mid \hat{a}$, dann $q \mid \hat{n} - \hat{a}^2 = \hat{b}^2$, $q \mid \hat{b}$. Widerspruch zu $(\hat{a}, \hat{b}) = \frac{1}{d}(a, b) = 1$. Also $q \nmid \hat{a}$.
Dann existiert $u \in \mathbb{Z}$ mit

$$\hat{a}u \equiv \hat{b} \pmod{q}.$$

Wegen $q \mid \hat{n}$ ist dann

$$0 \equiv \hat{n} = \hat{a}^2 + \hat{b}^2 \equiv \hat{a}^2(1 + u^2) \pmod{q}$$

Noch einmal wegen $q \nmid \hat{a}$: $q \mid u^2 + 1$. Daher: $q = c^2 + d^2$ für gewisse $c, d \in \mathbb{N}$, also $q \neq 3$ (4). Widerspruch. \square

Beispiel 3.10. 3, 7, 15, 23 nicht Summen von zwei Quadraten. Summe von 3 Quadraten?
 $3 = 1^2 + 1^2 + 1^2$

Satz 3.30 (Gauß 1801). $\forall n \in \mathbb{N}^*$ sind äquivalent:

1) $\exists a, b, c \in \mathbb{N} : a^2 + b^2 + c^2 = n$

2) $n = 4^r(8s + 7)$ mit $r, s \in \mathbb{N}$.

(ohne Beweis)

Beispiel 3.11. 7, 15, 23, Aber: $7 = 2^2 + 1^2 + 1^2 + 1^2$, $15 = 3^2 + 2^2 + 1^2 + 1^2$, $23 = 3^2 + 3^2 + 2^2 + 1^2$

Satz 3.31 (Legendre 1770). $\forall n \in \mathbb{N}^* \exists a, b, c, d \in \mathbb{N} :$

$$a^2 + b^2 + c^2 + d^2 = n$$

Beweis. mit Satz v. GAUSS: oBdA: $n = 4^r(8s + 7)$ (sonst $n = a^2 + b^2 + c^2 + 0^2$).
 $4 \nmid 8s + 6$ nach GAUSS

$$\begin{aligned} 8s + 6 = a^2 + b^2 + c^2 &\Rightarrow 8s + 7 = a^2 + b^2 + c^2 + 1^2 \\ &\Rightarrow n = 4^r(8s + 7) = (2^r a)^2 + (2^r b)^2 + (2^r c)^2 + (2^r)^2 \quad \square \end{aligned}$$

3.5 Primfaktorzerlegung in $\mathbb{Z}[i]$

$\mathbb{Z}[i] := \{x + iy : x, y \in \mathbb{Z}\}$ ($\mathbb{Z} \times \mathbb{Z}$ als Teilmenge von $\mathbb{R}^2 \cong \mathbb{C}$)

Allgemeiner: $(R, +, \cdot)$ kommutativer Ring mit 1 und nullteilerfrei. (weiteres Beispiel: Polynomring $\mathbb{K}[x]$, \mathbb{K} Körper)

Für $\omega \in \mathbb{C}$ sei

$$\mathbb{Z}[\omega] := \{a_0 + a_1\omega : a_0, a_1 \in \mathbb{Z}\}$$

Wir betrachten die Fälle

$$\omega = \sqrt{m}, \quad m \in \{-2, -1, 0, 2, 3\},$$

insbesondere ($m = -1$)

$$\mathbb{Z}[i] := \{a_0 + a_1 i : a_0, a_1 \in \mathbb{Z}\} \quad (\text{GAUSSsche ganze Zahlen})$$

$$\omega = \frac{1 + \sqrt{-m}}{2}, \quad m \in \{3, 7, 11\}$$

In all diesen Fällen ist $\omega^2 \in \mathbb{Z}[\omega]$ (klar für $\omega = \sqrt{m}$, für $\omega = \frac{1+\sqrt{-m}}{2}$ Übung), also $\mathbb{Z}[\omega]$ Ring bzgl. der üblichen Operationen $(+, \cdot)$ in \mathbb{C} .

Allgemeine Bezeichnungen: Ist R ein Integritätsbereich (d. h. kommutativer Ring mit Einselement 1 und nullteilerfrei ($\alpha, \beta \in R, \alpha\beta = 0 \Rightarrow \alpha = 0 \vee \beta = 0$)), so definiert man:

- 1) Für $\alpha, \beta \in R$ heißt α Teiler von β ($\alpha \mid \beta$), falls $\exists \gamma \in R$ mit $\alpha\gamma = \beta$.
- 2) $\varepsilon \in R$ heißt Einheit, falls $\varepsilon \mid 1$. (z. B. ± 1)
- 3) $\alpha, \beta \in R$ heißen assoziiert, $\alpha \sim \beta$, falls $\alpha \mid \beta$ und $\beta \mid \alpha$.
- 4) $\alpha \in R$ heißt unzerlegbar, falls $\alpha \neq 0$, α keine Einheit und gilt: $\alpha = \beta\gamma$ mit $\beta, \gamma \in R \Rightarrow \beta$ oder γ Einheit.
- 5) $\pi \in R$ heißt Primelement, falls gilt

$$\pi \mid \alpha\beta, \quad \alpha, \beta \in R \Rightarrow \pi \mid \alpha \text{ oder } \pi \mid \beta$$

(Weitere Ringe: $\mathbb{Q}, \mathbb{Z}, \mathbb{K}[x]$ Polynomring über Körper \mathbb{K})

Bemerkung 3.32. 1) $\varepsilon_1, \varepsilon_2$ Einheiten $\Rightarrow \varepsilon_1\varepsilon_2$ Einheit:

$$\varepsilon_j \delta_j = 1 \Rightarrow (\varepsilon_1\varepsilon_2)(\delta_1\delta_2) = (\varepsilon_1\delta_1)(\varepsilon_2\delta_2) = 1 \cdot 1 = 1$$

(Einheiten bilden Gruppen)

- 2) Sei $\alpha \in R$ unzerlegbar, $\beta \in R$ keine Einheit. Dann:

$$\beta \mid \alpha \iff \exists \text{ Einheit } \varepsilon : \beta\varepsilon = \alpha$$

- 3) $\pi \in R$ Primelement $\Rightarrow \pi$ unzerlegbar:

Seien $\beta, \gamma \in R$ mit $\pi = \beta\gamma$. Dann $\pi \mid \beta$ oder $\pi \mid \gamma$, etwa $\pi \mid \beta$, also $\beta = \pi\alpha$ mit $\alpha \in R$. Es folgt

$$1\pi = \beta\gamma = \pi\alpha\gamma$$

und daraus $1 - \alpha\gamma = 0$, d. h. γ Einheit.

Einheiten in \mathbb{Z} : ± 1 ; Einheiten in $\mathbb{Z}[i]$: $\pm 1, \pm i$. ($z \in \mathbb{Z}[i] \setminus \{0\} \Rightarrow |z| \geq 1 \Rightarrow$ Jede Einheit hat Betrag 1) Einheiten in $\mathbb{Z}[\sqrt{-2}]$: Nur ± 1 . Einheiten in $K[x]$: Jedes $a \in K^*$.

Lemma 3.33. 1) Für alle $k \in \mathbb{N}^*$ ist

$$M := \{z \mid z \in \mathbb{Z}[i], |z| \leq k\}$$

endlich.

2) Für alle $u, v \in \mathbb{Z}[i], v \neq 0$, existiert $w \in \mathbb{Z}[i]$ mit

$$|u - vw| < |v|$$

Beweis. $M \subset \{|x + yi| : x, y \in \mathbb{Z}, -k \leq x \leq k, -k \leq y \leq k\}$, $|\{ \quad \}| = (2k + 1)^2$
 $u/v \in \mathbb{C}$, Es ex. $w \in \mathbb{Z}[i]$ mit $|u/v - w| \leq 1/\sqrt{2}$, also

$$|u - vw| \leq \frac{|v|}{\sqrt{2}} < |v| \quad \square$$

Bemerkung 3.34. Ebenso für $\mathbb{Z}[\sqrt{-2}]$: $\frac{\sqrt{3}}{2} < 1$

Allgemeiner: R Integritätsbereich, außerdem $\eta : R \rightarrow \mathbb{R}_+$ mit:

1) $\eta(\alpha) = 0 \iff \alpha = 0$

2) $\forall k \in \mathbb{N} : \{\eta(\alpha) : \alpha \in R, \eta(\alpha) \leq k\}$ endliche Menge.

3) $\forall \alpha, \beta \in R, \beta \neq 0 \exists \gamma \in R :$

$$\eta(\alpha - \beta\gamma) < \eta(\beta)$$

Beispiel 3.12. 1) $R = \mathbb{Z}[\omega]$ mit $\omega = \sqrt{-m}, m = 1, 2$ oder $\omega = \frac{1+\sqrt{-m}}{2}, m = 3, 7, 11$
mit $\eta(\alpha) = |\alpha|$.

2) $R = \mathbb{K}[x]$, Polynomring über \mathbb{K} , mit $\eta(f) = \begin{cases} 0 & f = 0 \\ 2^{\deg(f)} & \text{sonst} \end{cases}$. Daraus folgt:
 $\eta(fg) = \eta(f)\eta(g)$

3) $R = \mathbb{Z}[\sqrt{m}], m = 2, 3$ oder $m = -1, -2$ mit

$$\eta(a_0 + a_1\sqrt{m}) := |a_0^2 - a_1^2m|$$

(Wohldefiniert!)

Beweis:

(1) $\eta(\alpha) = 0 \iff \alpha = 0$ (klar wg. Wohldefiniertheit)

(2) Trivial, wegen $\eta(R) \subset \mathbb{N}$

(3) Für $a_0 + a_1\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ sei

$$\eta(a_0 + a_1\sqrt{m}) := |a_0^2 - a_1^2m| \in \mathbb{Q}_+$$

η ist multiplikativ auf $\mathbb{Q}[\sqrt{m}]$:

$$\begin{aligned} (a_0 + a_1\sqrt{m})(b_0 + b_1\sqrt{m}) &= c_0 + c_1\sqrt{m} \\ c_0 &= a_0b_0 + a_1b_1m \\ c_1 &= a_1b_0 + a_0b_1 \end{aligned}$$

Dann:

$$(a_0^2 - a_1^2 m)(b_0^2 - b_1^2 m) = a_0^2 b_0^2 - (a_0^2 b_1^2 + a_1^2 b_0^2)m + a_1^2 b_1^2 m^2 \\ \stackrel{!}{=} c_0^2 - c_1^2 m$$

Somit

$$\eta(\alpha\beta) = \eta(\alpha)\eta(\beta) \quad \forall \alpha, \beta \in \mathbb{Q}[\sqrt{m}]$$

Seien $\alpha, \beta \in \mathbb{Z}[\sqrt{m}]$, $\beta = b_0 + b_1\sqrt{m} \neq 0$. Dann ist

$$\frac{\alpha}{\beta} = \frac{\alpha(b_0 - b_1\sqrt{m})}{b_0^2 - b_1^2 m} = c_0 + c_1\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$$

Es existieren $g_0, g_1 \in \mathbb{Z}$, so daß für $d_j := c_j - g_j$ gilt:

$$|d_j| \leq \frac{1}{2}$$

Sei $\gamma := g_0 + g_1\sqrt{m}$, $\rho := \alpha - \beta\gamma$ und $\delta := d_0 + d_1\sqrt{m}$. Dann

$$\gamma, \rho \in \mathbb{Z}[\sqrt{m}], \quad \delta \in \mathbb{Q}[\sqrt{m}],$$

$\rho = \beta\delta$, denn

$$\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \gamma = (c_0 - g_0 + (c_1 - g_1)\sqrt{m}) = \delta$$

Wegen $d_0^2 \leq \frac{1}{4}$ und $d_1^2 \leq \frac{1}{4}$ ist $\eta(\delta) = |d_0^2 - d_1^2 m| \leq \frac{3}{4} < 1$ für $m = 2, 3$.
($d_0^2, d_1^2 m \in [0, \frac{3}{4}]$), wie auch für $m = -1, -2$:

$$\eta(\delta) = d_0^2 + d_1^2 |m| \leq \frac{1}{4} + \frac{2}{4}$$

Daraus folgt

$$\eta(\rho) = \eta(\beta\delta) = \eta(\beta)\underbrace{\eta(\delta)}_{<1} < \eta(\beta)$$

Satz 3.35. Seien R, η wie oben. Dann gilt für alle $\pi \in R$: π unzerlegbar $\iff \pi$ Primelement.

Beweis. „ \Leftarrow “: schon gezeigt.

„ \Rightarrow “: Sei $\pi \in R$ unzerlegbar. Seien $\alpha\beta \in R$ mit $\pi \mid \alpha\beta$. Z.z.: $\pi \mid \alpha \vee \pi \mid \beta$

Sei

$$B := \{\tilde{\beta} \in R : \pi \mid \alpha\tilde{\beta}\}$$

Selbstverständlich $\pi, \beta \in B$. Wir wählen $\beta_0 \in B$ mit minimalem $\eta(\beta_0) > 0$. ($\{\eta(\tilde{\beta}) : \tilde{\beta} \in B, 0 < \eta(\tilde{\beta}) \leq \eta(\beta)\}$ ist endliche nicht-leere Menge). Wir behaupten: $B = R\beta_0$.

Klar: $R\beta_0 \subset B$: ($\pi \mid \alpha\beta_0 \Rightarrow \pi \mid \alpha\beta_0\gamma \forall \gamma \in R$)

Sei $\tilde{\beta} \in B$. Es existiert ein $\gamma \in R$ mit

$$\eta(\tilde{\beta} - \beta_0\gamma) < \eta(\beta_0) \tag{3.2}$$

Dabei gilt

$$\pi \mid \alpha\tilde{\beta} - \alpha\beta_0\gamma = \alpha(\tilde{\beta} - \beta_0\gamma),$$

also ist $\tilde{\beta} - \beta_0\gamma \in B$. Wegen Wahl von β_0 und (3.2) ist

$$\eta(\tilde{\beta} - \beta_0\gamma) = 0, \tilde{\beta} - \beta_0\gamma = 0,$$

also $\tilde{\beta} \in R\beta_0$

Wegen $\pi \in B$ existiert also $\gamma \in R$ mit

$$\pi = \beta_0\gamma.$$

Da π unzerlegbar, ist β_0 Einheit oder γ Einheit. Ist β_0 Einheit, so ist $\pi \mid \alpha$ wegen $\pi \mid \alpha\beta_0$ ($\beta_0\varepsilon = 1 \Rightarrow \pi \mid \alpha\beta_0\varepsilon = \alpha$). Ist γ Einheit, so ist $\pi \mid \beta$ wegen $\beta_0 \mid \beta$ ($\beta \in B$) ($\gamma\varepsilon = 1 \Rightarrow \pi\varepsilon = \beta_0\gamma\varepsilon = \beta_0, \pi \mid \beta_0$). \square

Korollar 3.36. In R mit η , außerdem η multiplikativ, $\eta(\alpha) \geq 1 \forall \alpha \in R^*$, gilt eindeutige Zerlegbarkeit in unzerlegbare Elemente. Genauer:

$\forall \alpha \in R^*$ keine Einheit, so \exists unzerlegbare $\pi_1, \dots, \pi_n \in R$ ($n \in \mathbb{N}^*$) mit $\alpha = \prod_i^n \pi_i$

Ist $\alpha = \prod_i^m \tilde{\pi}_i$ mit unzerlegbaren $\tilde{\pi}_i$, so ist $m = n$ und nach Umordnung $\tilde{\pi}_j = \varepsilon_j \pi_j$, ε_j Einheit.

Beweis. Korrektur: a) $0 \neq \eta(1) = \eta(1 \cdot 1) = \eta(1)\eta(1) \Rightarrow \eta(1) = 1$

b) ε Einheit $\Rightarrow \exists \gamma \in R : \varepsilon\gamma = 1$

$\Rightarrow \eta(\varepsilon)\eta(\gamma) = \eta(\varepsilon\gamma) = \eta(1) = 1 \Rightarrow \eta(\varepsilon) = 1$

c) Sei $\varepsilon \in R, \eta(\varepsilon) = 1$. wegen (iii) existiert $\gamma \in R$ mit

$$\eta(1 - \varepsilon\gamma) < \eta(\varepsilon) = 1$$

Dann folgt $1 - \varepsilon\gamma = 0$, ε Einheit.

Ende Korrektur.

Existenz: Angenommen, es existiert $\alpha \in R^*$, α keine Einheit, α nicht Produkt von unzerlegbaren Elementen. Wähle ein solches α mit minimalem $\eta(\alpha)$. α ist selbstverständlich zerlegbar. Also existieren $\beta, \gamma \in R$, keine Einheiten, mit

$$\alpha = \beta\gamma$$

Wegen $\eta(\beta)\eta(\gamma) = \eta(\alpha)$ und $\eta(\beta) > 1, \eta(\gamma) > 1$ ist $\eta(\beta) < \eta(\alpha)$ und $\eta(\gamma) < \eta(\alpha)$. Nach Wahl von α existieren unzerlegbare

$$\pi_1, \dots, \pi_k, \pi_{k+1}, \dots, \pi_m \in R$$

mit $\beta = \pi_1 \dots \pi_k, \gamma = \pi_{k+1} \dots \pi_m$, so daß also $\alpha = \beta\gamma = \prod_i \pi_i$ Widerspruch.

Eindeutigkeit: Seien $m, n \in \mathbb{N}^*$ und $\pi_1, \dots, \pi_n, \tilde{\pi}_1, \dots, \tilde{\pi}_m$ unzerlegbare Elemente in R mit $\prod_i \pi_i = \prod_i \tilde{\pi}_i$.

Zu zeigen: $m = n$, nach Umordnen: $\pi_j = \tilde{\pi}_j \varepsilon_j$, ε_j Einheit. Vollst. Induktion nach m :
 $m = 1$: $\pi_1 = \prod_i \tilde{\pi}_i = \tilde{\pi}_1 (\prod_{i>1} \tilde{\pi}_i) \Rightarrow n = 1, \pi_1 = \tilde{\pi}_1$
 $m \rightarrow m + 1$: $\prod_{i=1}^{m+1} \pi_i = \prod_{j=1}^n \tilde{\pi}_j \Rightarrow \pi_{m+1} \mid \prod_j \tilde{\pi}_j \Rightarrow \exists 1 \leq j \leq n : \pi_{m+1} \mid \tilde{\pi}_j$ oBdA:
 $j = n$.

Also existiert $\varepsilon_n \in R$: $\pi_{m+1} \varepsilon_n = \tilde{\pi}_n$. Dabei ε_n Einheit, da $\tilde{\pi}_n$ unzerlegbar. Außerdem folgt:

$$\prod_{i=1}^{m+1} \pi_i \varepsilon_n = (\varepsilon_n \tilde{\pi}_1) \prod_{i=2}^n \tilde{\pi}_i$$

$$\prod_{i=1}^m \pi_i = \varepsilon_1 \prod_{i=1}^{n-1} \tilde{\pi}_i$$

Nach Induktionsannahme: $m = n - 1$. Nach Umordnen: \exists Einheiten η_j

$$\eta_1 \varepsilon_n \tilde{\pi}_1 = \pi_1, \eta_2 \tilde{\pi}_2 = \pi_2, \dots, \tilde{\pi}_m \eta_m = \pi_m \quad \square$$

Bemerkung 3.37. Dies gilt nicht für $\mathbb{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

mit unzerlegbaren $2, 3, 1 \pm \sqrt{-5}$. $\Rightarrow 2, 3, 1 \pm \sqrt{-5}$ keine Primelemente.

Beweis. für Unzerlegbarkeit: Für

$$\alpha = a_0 + a_1 \sqrt{-5} \quad (a_0, a_1 \in \mathbb{Z})$$

sei

$$\eta(\alpha) = |a_0^2 + 5a_1^2|$$

Dann ist η multiplikativ (siehe früher!), $\eta(1) = 1$, $\eta(\alpha) > 1 \forall \alpha \in \mathbb{Z}[\sqrt{-5}] \setminus \{0, \pm 1\}$.
 Es ist $\eta(2) = 2^2 = 4$, $\eta(3) = 3^2 = 9$, $\eta(1 \pm \sqrt{-5}) = 1^2 + 1^2 \cdot 5 = 6$. Für jeden echten Teiler β einer dieser Zahlen $2, 3, 1 \pm \sqrt{-5}$ muß $\eta(\beta)$ echter Teiler von $4, 9, 6$ sein, also 2 oder 3. Aber in diesem Ring wird das nie und nimmer passieren. Schade. \square

3.6 Chinesischer Restsatz

Satz 3.38. Seien $m_1, \dots, m_r \in \mathbb{N}^*$ paarweise teilerfremd. Es sei

$$m := \prod_{i=1}^r m_i \text{ und } b_1, \dots, b_r \in \mathbb{Z}.$$

Dann gilt

1) Das System der simultanen Kongruenzen

$$x \equiv b_1 \pmod{m_1}, \dots, x \equiv b_r \pmod{m_r} \quad (3.3)$$

hat Lösung. Setzt man $a_j := \frac{m}{m_j}$ und wählt $x_j \in \mathbb{Z}$ mit

$$a_j x_j \equiv b_j \pmod{m_j}$$

so ist

$$x' := a_1 x_1 + \dots + a_r x_r$$

Lösung von (3.3)

2) Gesamtheit der Lösungen von (3.3) ist

$$x' + \mathbb{Z}m = \{x'' \in \mathbb{Z} : x'' \equiv x' \pmod{m}\}$$

Beweis. 1) Für alle $1 \leq j \leq r$ ist $(a_j, m_j) = 1$, also existiert $x_j \in \mathbb{Z}$ mit

$$a_j x_j \equiv b_j \pmod{m_j}.$$

Für $j \neq i$ ist $m_j \mid a_i$, also $a_i x_i \equiv 0 \pmod{m_j}$. Somit ist

$$x' \equiv a_j x_j \equiv b \pmod{m_j}$$

2) Für alle $c \in \mathbb{Z}$ und $1 \leq j \leq r$ ist

$$x' + cm \equiv x' \equiv b_j \pmod{m_j}$$

Ist umgekehrt x'' Lösung von (3.3), so ist $x'' - x' \equiv 0 \pmod{m_j}$ für alle $1 \leq j \leq r$, d.h. $m_j \mid x'' - x'$ für alle $1 \leq j \leq r$, also $m \mid x'' - x'$, $x'' - x' = cm$, $c \in \mathbb{Z}$. \square

Beispiel 3.13. $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 4 \pmod{5}$.

$$m = 2 \cdot 3 \cdot 5 = 30, \quad a_1 = 15, \quad a_2 = 10, \quad a_3 = 6$$

$$15x_1 \equiv 1 \pmod{2}, \quad 10x_2 \equiv 2 \pmod{3}, \quad 6x_3 \equiv 4 \pmod{5}.$$

$$x_1 = 1, \quad x_2 = 2, \quad x_3 = 4$$

$$\Rightarrow x' = 15 \cdot 1 + 10 \cdot 2 + 6 \cdot 4 = 59 \equiv -1 \pmod{30}$$

3.7 Polynomkongruenzen

Für $f \in \mathbb{Z}[x]$ und $b, m \in \mathbb{Z}$ fragen wir nach Lösungen der *Polynomkongruenz*

$$f(x) \equiv b \pmod{m}.$$

Selbstverständlich können wir wieder o.B.d.A. $b = 0$ annehmen. Eine ganze Zahl x_0 mit $f(x_0) \equiv 0 \pmod{m}$ wird dann auch *Wurzel der Polynomkongruenz* genannt.

Beispiel 3.14. 1) Für $p \in \mathbb{P}$ hat $x^{p-1} - 1 \equiv 0 \pmod{p}$ die $p-1$ nicht kongruenten Wurzeln $1, \dots, p-1$ (kleiner Fermatscher Satz).

2) $x^2 - 2 \equiv 0 \pmod{3}$ hat keine Lösung (man probiere 0, 1, 2).

- 3) $x^2 + 1 \equiv 0 \pmod{p}$ hat für jede Primzahl p der Form $4k + 1$, $k \in \mathbb{N}$, genau zwei nicht kongruente Wurzeln (z.B. $\pm(2k)!$), für Primzahlen $p = 4k + 3$ aber keine Lösung.
- 4) $x^4 - 1 \equiv 0 \pmod{16}$ hat die acht nicht kongruenten Wurzeln 1, 3, 5, 7, 9, 11, 13, 15, während $x^4 - 2 \equiv 0 \pmod{16}$ keine Lösung besitzt.

Bemerkung 3.39. 1) Ist $x_0 \in \mathbb{Z}$ eine Nullstelle von f , so ist für alle $m \in \mathbb{N}^*$ auch $f(x_0) \equiv 0 \pmod{m}$.

- 2) Es gibt ein $f \in \mathbb{Z}[x]$, so daß für alle $m \in \mathbb{N}^*$ die Polynomkongruenz $f(x) \equiv 0 \pmod{m}$ eine Wurzel besitzt, aber f keine Nullstelle in \mathbb{Z} hat (ohne Beweis).
- 3) Ein Polynom n -ten Grades hat höchstens n Nullstellen in \mathbb{Z} , es kann aber mehr Wurzeln für Polynomkongruenzen $f(x) \equiv 0 \pmod{m}$ geben (siehe Beispiel 4).

Satz 3.40. *Es sei*

$$f = a_0 + a_1x + \cdots + x^n \quad (n \in \mathbb{N}, a_i \in \mathbb{Z}).$$

Dann hat $f(x) \equiv 0 \pmod{p}$ für jede Primzahl p höchstens n inkongruente Lösungen in \mathbb{Z} .

Beweis. Die Behauptung folgt daraus, daß $\mathbb{Z}_p := \mathbb{Z}/\mathbb{Z}p$ ein Körper ist (und eine entsprechende Aussage allgemein für Körper gilt).

Wir können aber auch direkt mit vollständiger Induktion vorgehen: Für $n = 0$ haben wir $f(x) = 1 \not\equiv 0 \pmod{p}$. Sei nun $n \in \mathbb{N}^*$ und die Behauptung richtig für $n - 1$. Besitzt die Kongruenz $f(x) = a_0 + a_1x + \cdots + x^n \equiv 0 \pmod{p}$ keine Lösung, so haben wir nichts mehr zu zeigen. Besitzt sie eine Lösung $c \in \mathbb{Z}$, so ist für alle $x \in \mathbb{Z}$

$$f(x) \equiv f(x) - f(c) = \sum_{\nu=1}^n a_\nu (x^\nu - c^\nu) = (x - c)g(x) \pmod{p}$$

mit

$$g := \sum_{\nu=1}^n a_\nu (x^{\nu-1} + x^{\nu-2}c + \cdots + xc^{\nu-2} + c^{\nu-1}) \in \mathbb{Z}[x],$$

(wobei $a_n := 1$), so daß also

$$f(x) \equiv 0 \pmod{p} \iff (x \equiv c \pmod{p} \quad \text{oder} \quad g(x) \equiv 0 \pmod{p}).$$

Beachten wir, daß g die Form $b_0 + b_1x + \cdots + x^{n-1}$ mit $b_i \in \mathbb{Z}$ hat (in der g definierenden Summe tritt x^{n-1} nur bei $\nu = n$ auf!), so folgt nach Induktionsvoraussetzung, daß $g(x) \equiv 0 \pmod{p}$ höchstens $n - 1$ inkongruente Lösungen hat. Damit folgt die Behauptung für n . \square

Korollar 3.41. *Es sei p eine Primzahl und $d \in \mathbb{N}^*$ ein Teiler von $p - 1$. Dann hat $x^d - 1 \equiv 0 \pmod{p}$ genau d inkongruente Lösungen.*

Beweis. Sei $q \in \mathbb{N}^*$ mit $p - 1 = dq$. Dann hat

$$g := 1 + x^d + x^{2d} + \dots + x^{(q-1)d} \in \mathbb{Z}[x]$$

den Grad $p - 1 - d$. Es bezeichne l bzw. k die Anzahl der Lösungen von $x^d - 1 \equiv 0 \pmod{p}$ bzw. von $g(x) \equiv 0 \pmod{p}$ in $\{1, \dots, p - 1\}$. Nach dem vorigen Satz ist

$$0 \leq l \leq d \quad \text{und} \quad 0 \leq k \leq p - 1 - d. \quad (3.4)$$

Wir wissen, daß für alle $x \in \{1, \dots, p - 1\}$ gilt

$$(x^d - 1)g(x) = x^{p-1} - 1 \equiv 0 \pmod{p},$$

also

$$x^d - 1 \equiv 0 \pmod{p} \quad \text{oder} \quad g(x) \equiv 0 \pmod{p}.$$

Daraus folgt, daß

$$p - 1 \leq l + k \quad (3.5)$$

gilt (zunächst nur \leq , da gewisse x Lösungen beider Kongruenzen sein könnten). Wäre $l < d$, so wäre nach (3.4)

$$l + k < d + (p - 1 - d) = p - 1,$$

was (3.5) widerspricht. Also ist $l = d$ (und ebenso $k = p - 1 - d$). \square

Satz 3.42 (andere Formulierung von Satz 3.40). *Es sei p eine Primzahl und $f = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$, so daß $f(x) \equiv 0 \pmod{p}$ mehr als n inkongruente Lösungen hat. Dann sind alle Koeffizienten a_0, a_1, \dots, a_n durch p teilbar.*

Beweis. Nehmen wir an, daß es ein $1 \leq m \leq n$ gibt, so daß a_m nicht durch p teilbar ist. Es sei m die größte Zahl mit dieser Eigenschaft. Dann existiert ein $b \in \mathbb{Z}$ mit $a_mb \equiv 1 \pmod{p}$. Sei

$$g := a_0b + a_1bx + \dots + a_{m-1}bx^{m-1} + x^m.$$

Nach Satz 3.40 hat $g(x) \equiv 0 \pmod{p}$ höchstens m inkongruente Lösungen in \mathbb{Z} . Andererseits gilt für jedes $x \in \mathbb{Z}$ mit $f(x) \equiv 0 \pmod{p}$ sicher

$$g(x) \equiv a_0b + a_1bx + \dots + a_{m-1}bx^{m-1} + x^m \equiv f(x)b \equiv 0 \pmod{p}$$

(und von denen gibt es nach Voraussetzung mehr als n , also mehr als m inkongruente). Widerspruch! \square

Damit erhalten wir einen neuen Beweis für den *Satz von Wilson*:

Es sei p eine Primzahl. Das Polynom

$$f := (x - 1)(x - 2) \dots (x - (p - 1)) - (x^{p-1} - 1) \in \mathbb{Z}[x]$$

hat einen Grad, der strikt kleiner als $p - 1$ ist (die Terme mit Potenz $p - 1$ heben sich gegenseitig auf). Nach dem kleinen Satz von Fermat ist $f(x) \equiv 0 \pmod{p}$ für alle

$x \in \{1, \dots, p-1\}$. Nach dem eben bewiesenen Satz ist daher jeder Koeffizient von f durch p teilbar. Insbesondere ist also der konstante Term

$$(-1)^{p-1}(p-1)! + 1$$

durch p teilbar. Für $p \neq 2$ ist $(-1)^{p-1} = 1$ und damit

$$(p-1)! \equiv -1 \pmod{p}$$

(für $p = 2$ ist trivial $(p-1)! = 1 \equiv -1(p)$).

4 Fibonacci-Zahlen

Die Folge (F_n) der *Fibonacci-Zahlen* ist definiert durch

$$F_1 := F_2 := 1, \quad F_{n+2} := F_{n+1} + F_n \quad (n \in \mathbb{N}^*).$$

Erste Folgenglieder:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377

Mit Matrix $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ ist für alle $n \in \mathbb{N}$ (mit $F_0 := 0$)

$$\begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix} = A^{n+1} :$$

Für $n = 0$ ist die Behauptung trivial aufgrund der Definition von F_0, F_1, F_2 und A , der Induktionsschritt ergibt sich mit

$$\begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{n+2} + F_{n+1} & F_{n+2} \\ F_{n+1} + F_n & F_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n+3} & F_{n+2} \\ F_{n+2} & F_{n+1} \end{pmatrix}.$$

Der Schlüssel zu Eigenschaften der Folge (F_n) ist die Folgerung:

Satz 4.1. *Für alle $m \in \mathbb{N}^*$ und $n \in \mathbb{N}$ ist*

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

Beweis. Es ist

$$\begin{pmatrix} F_{m+n+2} & F_{m+n+1} \\ F_{m+n+1} & F_{m+n} \end{pmatrix} = A^{m+n+1} = A^m A^{n+1} = \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix} \begin{pmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{pmatrix}. \quad \square$$

Korollar 4.2. *Für alle $m, n \in \mathbb{N}^*$ gilt:*

- 1) F_n und F_{n+1} sind teilerfremd.
- 2) F_m ist ein Teiler von F_{mn} .
- 3) $(F_m, F_n) = F_{(m,n)}$.
- 4) Sind m, n teilerfremd, so ist $F_m F_n$ ein Teiler von F_{mn} .

5) m ist genau dann ein Teiler von n , wenn F_m ein Teiler von F_n ist.

Beweis. 1. Trivial für $n = 1$, Induktionsschluß mit

$$(F_{n+1}, F_{n+2}) = (F_{n+1}, F_n + F_{n+1}) = (F_{n+1}, F_n).$$

2. Trivial für $n = 1$, Induktionsschluß mit

$$F_{m(n+1)} = F_{mn+m} = F_{mn-1}F_m + F_{mn}F_{m+1}.$$

3. O.B.d.A. sei $n < m$. Wählen wir $q \in \mathbb{N}^*$ und $r \in \mathbb{N}$ mit $m = qn + r$ und $0 \leq r < n$, so ist

$$F_m = F_{qn+r} = F_{qn-1}F_r + F_{qn}F_{r+1}.$$

Dabei ist $F_n \mid F_{qn}$, wegen $(F_{qn-1}, F_{qn}) = 1$ also $(F_{qn-1}, F_n) = 1$ und damit

$$(F_m, F_n) = (F_n, F_r).$$

Fortfahren mit dem euklidischen Algorithmus ergibt mit $d := (m, n)$ schließlich

$$(F_m, F_n) = (F_d, F_0) = (F_d, 0) = F_d.$$

(4) und (5) folgen sofort aus (2) und (3). □

Satz 4.3. Für alle $n \in \mathbb{N}$ ist

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$

Beweis. Mit vollständiger Induktion folgt sofort, daß $F_n \leq 2^n$ für alle $n \in \mathbb{N}$. Daher ist die Potenzreihe

$$f(x) := \sum_{n=0}^{\infty} F_{n+1}x^n \tag{4.1}$$

für alle $x \in \mathbb{R}$ mit $|x| < 1/2$ konvergent. Wegen der Identität

$$1 + xf(x) + x^2f(x) = 1 + \sum_{n=1}^{\infty} F_n x^n + \sum_{n=2}^{\infty} F_{n-1} x^n = 1 + F_1 x + \sum_{n=2}^{\infty} F_{n+1} x^n = f(x)$$

ist offenbar

$$f(x) = \frac{1}{1 - x - x^2}.$$

Setzen wir

$$\alpha_{1,2} := \frac{1 \pm \sqrt{5}}{2},$$

so ist

$$1 - x - x^2 = (1 - \alpha_1 x)(1 - \alpha_2 x)$$

wegen $\alpha_1 + \alpha_2 = 1$ und $\alpha_1 \alpha_2 = -1$. Für alle $x \in \mathbb{R}$ mit $|x| < 1/2$ gilt also

$$f(x) = \frac{1}{\sqrt{5}} \left(\frac{\alpha_1}{1 - \alpha_1 x} - \frac{\alpha_2}{1 - \alpha_2 x} \right) = \frac{1}{\sqrt{5}} (\alpha_1^{n+1} - \alpha_2^{n+1}) x^n. \tag{4.2}$$

Aus (4.1) und (4.2) folgt nun sofort $F_n = (\alpha_1^n - \alpha_2^n)/\sqrt{5}$. □

Lucas-Folgen

a_1, a_2 gegeben,

$$a_{n+2} = a_{n+1} + a_n, \quad n > 0$$

Dann gilt:

$$a_{n+1} = a_1 F_{n-1} + a_2 F_n \quad n \geq 2$$

5 Zahlentheoretische Funktionen

5.1 Allgemeines und Definitionen

Jede Funktion $f : \mathbb{N}^* \rightarrow \mathbb{Q}$ heißt *zahlentheoretische Funktion*. Eine solche Funktion heißt *multiplikativ*, falls für teilerfremde $a, b \in \mathbb{N}^*$ stets gilt

$$f(ab) = f(a)f(b).$$

Beispiel 5.1. 1) $f = 0$.

2) $o(1) = 1, o(a) = 0$ für $a > 1$.

3) $e(a) := 1$.

4) $i(a) := a$.

5) $i_k(a) := a^k, k \in \mathbb{N}$ (es ist $i_0 = e, i_1 = i$).

6) $\tau(a) := \sum_{d|a} 1$.

7) $\sigma(a) := \sum_{d|a} d$.

8) $\sigma_k(a) := \sum_{d|a} d^k, k \in \mathbb{N}$ (siehe Satz 5.4/Folgerungen; es ist $\sigma_0 = \tau, \sigma_1 = \sigma$).

9) $\varphi(a) :=$ (Anzahl der zu a teilerfremden natürlichen Zahlen $j \in \{1, 2, \dots, a\}$).

Definition 5.1. Die DIRICHLET-Faltung von zwei zahlentheoretischen Funktionen f und g ist definiert durch

$$(f * g)(n) := \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{a \cdot b = n} f(a)g(b).$$

Satz 5.1. 1) $f * g = g * f$.

2) $(f * g) * h = f * (g * h)$.

3) $f * o = o * f = f$.

Beweis. (1) und (3) sind trivial. Weiter ist

$$(f * g) * h(n) = \sum_{d \cdot c = n} (f * g)(d)h(c) = \sum_{d \cdot c = n} \sum_{a \cdot b = d} f(a)g(b)h(c) = \sum_{a \cdot b \cdot c = n} f(a)g(b)h(c).$$

Ebenso ist

$$f * (g * h)(n) = \sum_{a \cdot b \cdot c = n} f(a)g(b)h(c). \quad \square$$

Lemma 5.2. Sind $f, g: \mathbb{N}^* \rightarrow \mathbb{Q}$ multiplikativ, so auch $f * g$.

Beweis. Seien $a, b \in \mathbb{N}^*$ teilerfremd. Dann ist

$$\begin{aligned} (f * g)(ab) &= \sum_{d|ab} f(d)g\left(\frac{ab}{d}\right) = \sum_{d_1|a, d_2|b} f(d_1 d_2)g\left(\frac{ab}{d_1 d_2}\right) \\ &= \sum_{d_1|a, d_2|b} f(d_1)f(d_2)g\left(\frac{a}{d_1}\right)g\left(\frac{b}{d_2}\right) = \sum_{d_1|a} f(d_1)g\left(\frac{a}{d_1}\right) \sum_{d_2|b} f(d_2)g\left(\frac{b}{d_2}\right) \\ &= (f * g)(a)(f * g)(b). \end{aligned}$$

Dabei haben wir benutzt, daß Teiler von a und b ebenfalls teilerfremd sind. \square

Definition 5.2. Die *Summatorfunktion* (*Teilersummenfunktion*) von $f: \mathbb{N} \rightarrow \mathbb{Q}$ ist definiert als $F := f * e$, d.h. durch

$$F(a) := \sum_{d|a} f(d),$$

Vorläufige Tabelle:

$$\begin{array}{cccc} f & e & i & i_k \\ F & \tau & \sigma & \sigma_k \end{array}$$

Die MÖBIUSSche μ -Funktion ist definiert durch

$$\mu(a) := \begin{cases} 0, & a \text{ nicht quadratfrei,} \\ (-1)^r, & a = p_1 \cdots p_r \text{ quadratfrei } (p_j \in \mathbb{P}). \end{cases}$$

Einige Werte:

$$\begin{array}{cccccccccccc} a & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \mu(a) & 1 & -1 & -1 & 0 & -1 & 1 & -1 & 0 & 0 & 1 & -1 & 0 \end{array}$$

Lemma 5.3. 1) μ ist multiplikativ.

2) $\mu * e = e * \mu = o$.

Beweis. 1. Sei $a \in \mathbb{N}^*$, $a = p_1^{m_1} \cdots p_r^{m_r}$ mit voneinander verschiedenen Primzahlen

$$p_1, \dots, p_r.$$

Zu zeigen:

$$\mu(a) = \mu(p_1^{m_1}) \cdots \mu(p_r^{m_r}). \quad (5.1)$$

Wenn es ein $1 \leq j \leq r$ gibt mit $m_j \geq 2$, so ist $\mu(a) = 0 = \mu(p_j^{m_j})$, also (5.1) sicher richtig. Ist hingegen $m_1 = \cdots = m_r = 1$, so ist

$$\mu(a) = (-1)^r = \mu(p_1) \cdots \mu(p_r).$$

2. Mit μ und e ist auch $\mu * e$ multiplikativ. Da o ebenfalls multiplikativ ist, brauchen wir also nur zu zeigen, daß für alle Primzahlen p und $m \in \mathbb{N}$ gilt

$$(\mu * e)(p^m) = o(p^m)$$

gilt. Nun ist aber sicherlich $\mu * e(1) = 1 = o(1)$ und für $m \geq 1$

$$(\mu * e)(p^m) = \sum_{j=0}^m \mu(p^j) = 1 + (-1) + 0 + \cdots + 0 = 0 = o(p^m). \quad \square$$

Satz 5.4 (Möbiusscher Umkehrsatz). Für alle $f, F: \mathbb{N}^* \rightarrow \mathbb{Q}_+$ sind äquivalent:

1) F ist Summatorfunktion von f :

$$F(a) = \sum_{d|a} f(d).$$

2) $f = F * \mu$, d.h.

$$f(a) = \sum_{d|a} \mu\left(\frac{a}{d}\right) F(d).$$

Beweis. Ist $F = f * e$, so ist

$$f = f * o = f * (e * \mu) = (f * e) * \mu = F * \mu.$$

Ist umgekehrt $F * \mu = f$, so ist

$$F = F * o = F * (\mu * e) = (F * \mu) * e = f * e. \quad \square$$

Korollar 5.5. Sei $f: \mathbb{N}^* \rightarrow \mathbb{Q}_+$ und F Summatorfunktion von f . Dann gilt:

1) f ist genau dann multiplikativ, wenn F multiplikativ ist.

2) Für alle Primzahlen p und alle $m \in \mathbb{N}^*$ ist

$$f(p^m) = F(p^m) - F(p^{m-1}).$$

Ist f multiplikativ, f nicht die Nullfunktion, so ist

$$f(p_1^{m_1} \cdots p_r^{m_r}) = \prod_{j=1}^r \left(F(p_j^{m_j}) - F(p_j^{m_j-1}) \right).$$

Beweis. 1. Ist f multiplikativ, so ist nach Lemma 5.2 auch $F = f * e$ multiplikativ, da e multiplikativ ist.

Ist F multiplikativ, so ist nach Lemma 5.2 auch $f = F * \mu$ multiplikativ, da μ multiplikativ ist.

2. Es ist

$$f(p^m) = (F * \mu)(p^m) = \sum_{i=0}^m F(p^{m-i}) \mu(p^i) = F(p^m) \cdot 1 + F(p^{m-1}) \cdot (-1).$$

Der Rest ist klar. □

5.2 Anwendung auf die Eulersche φ -Funktion.

Die Teilersummenformel

$$\sum_{d|a} \varphi(d) = a$$

besagt, daß i Summatorfunktion von φ ist. Da i multiplikativ ist, sehen wir erneut, daß φ multiplikativ ist und

$$\varphi(p_1^{m_1} \dots p_r^{m_r}) = \prod_{j=1}^r (p_j^{m_j} - p_j^{m_j-1}) = a \prod_{j=1}^r \left(1 - \frac{1}{p_j}\right)$$

gilt. Außerdem ist φ durch die Teilersummenformel charakterisiert: Ist f zahlentheoretische Funktion mit $\sum_{d|a} f(d) = a$, so ist $f = \varphi$.

Die MÖBIUSSche Umkehrformel ergibt

$$\varphi(a) = \sum_{d|a} \mu(d) i\left(\frac{a}{d}\right) = \sum_{d|a} \mu(d) \frac{a}{d}$$

oder auch

$$\frac{\varphi(a)}{a} = \sum_{d|a} \frac{\mu(d)}{d}.$$

Beispiel:

$$\begin{aligned} \varphi(120) &= 120 - \frac{120}{2} - \frac{120}{3} - \frac{120}{5} + \frac{120}{6} + \frac{120}{10} + \frac{120}{15} - \frac{120}{30} \\ &= 120 - 60 - 40 - 24 + 20 + 12 + 8 - 4 \\ &= 32. \end{aligned}$$

Für f und die Summatorfunktion F von f haben wir die Tabelle

f	μ	o	e	φ	i	$\frac{\mu}{i}$
F	o	e	τ	i	σ	$\frac{\varphi}{i}$

6 Prime Restklassen

6.1 Allgemeines

Sei $m \in \mathbb{N}$, $m \geq 2$. Die Restklassen

$$\bar{j} := j + \mathbb{Z}m, \quad j \in \{0, 1, \dots, m-1\}$$

sind die m Elemente des Rings $\mathbb{Z}_m = \mathbb{Z}/\mathbb{Z}m$:

$$\bar{j} \pm \bar{k} = \bar{l} \iff j \pm k \equiv l \pmod{m}, \quad \bar{j} \cdot \bar{k} = \bar{l} \iff j \cdot k \equiv l \pmod{m}.$$

Wir wissen, daß für alle $j \in \{1, \dots, m-1\}$ gilt:

$$\begin{aligned} (j, m) = 1 &\iff \exists k \in \{1, \dots, m-1\} : j \cdot k \equiv 1 \pmod{m} \\ &\iff \exists k \in \{1, \dots, m-1\} : \bar{j} \cdot \bar{k} = \bar{1} \\ &\iff \bar{j} \text{ ist Einheit in } \mathbb{Z}_m. \end{aligned}$$

Definition 6.1. Die Gruppe

$$\mathbb{Z}'_m := \{\bar{j} : j \in \{1, 2, \dots, m-1\}, \bar{j} \text{ Einheit in } \mathbb{Z}_m\}$$

heißt *prime Restklassengruppe*. Die Anzahl der Elemente in \mathbb{Z}'_m ist $\varphi(m)$.

(Die Standardschreibweise ist \mathbb{Z}_m^* ; wir können sie nicht benutzen, da wir generell $R^* := R \setminus \{0\}$ definiert haben.)

Beispiele 6.1. 1) $\mathbb{Z}'_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \{\bar{2}, \bar{2}^2, \bar{2}^3, \bar{2}^4\} = \{\bar{3}, \bar{3}^2, \bar{3}^3, \bar{3}^4\}$, aber $\mathbb{Z}'_5 \neq \{\bar{4}, \bar{4}^2, \bar{4}^3, \bar{4}^4\}$, weil $\bar{4}^2 = \bar{1}$.

2) $\mathbb{Z}'_{15} = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$, für alle $\bar{a} \in \mathbb{Z}'_{15}$ ist $\bar{a}^4 = \bar{1}$.

3) $\mathbb{Z}'_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, für alle $\bar{a} \in \mathbb{Z}'_8$ ist $\bar{a}^2 = \bar{1}$.

6.2 Primitivwurzeln zu Primzahlen

Für jede Primzahl p ist

$$\mathbb{Z}'_p = \mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\},$$

und wir wissen, daß für alle $x \in \{1, 2, \dots, p-1\}$ gilt

$$x^{p-1} \equiv 1 \pmod{p} \quad (\text{ bzw. } \bar{x}^{p-1} = \bar{1}).$$

Definition 6.2. Ordnung von $x \in \mathbb{Z}_p^*$ ist die kleinste Zahl $j \in \mathbb{N}^*$ mit

$$x^j \equiv 1 \pmod{p}.$$

Lemma 6.1. Sei $m \in \mathbb{N}^*$ und $x \in \mathbb{Z}_p^*$. Dann ist

$$x^m \equiv 1 \pmod{p} \iff m \text{ ist Vielfaches der Ordnung von } x.$$

Insbesondere ist die Ordnung von x ein Teiler von $p - 1$.

Beweis. Sei j die Ordnung von x . Ist $q \in \mathbb{N}^*$, so ist selbstverständlich

$$x^{jq} = (x^j)^q \equiv 1^q = 1 \pmod{p}.$$

Sei also umgekehrt $m \in \mathbb{N}^*$ mit $x^m \equiv 1 \pmod{p}$. Dann existieren $q, r \in \mathbb{N}$, so daß $m = qj + r$ und $0 \leq r < j$ ist. Es folgt

$$x^r \equiv (x^j)^q x^r = x^m \equiv 1 \pmod{p}.$$

Nach Wahl von j ist $r = 0$, also j Teiler von m . □

Entsprechendes gilt für alle endlichen Gruppen:

Satz 6.2. Sei G eine endliche Gruppe, e das Einselement in G und k die Anzahl der Elemente in G . Für alle $a \in G$ ist dann $a^k = e$.

Für jedes $a \in G$ besteht die Menge aller $m \in \mathbb{N}^*$ mit $a^m = e$ aus den Vielfachen einer gewissen Zahl, die Ordnung von a genannt wird (und insbesondere ein Teiler von k ist).

Beweis. Wir werden den Satz nur für kommutative Gruppen benötigen und daher auch nur für solche beweisen. Wir gehen wie beim Beweis des kleinen Satzes von Fermat vor (der ein Spezialfall ist!): Es sei $G = \{x_1, x_2, \dots, x_k\}$ und $a \in G$. Dann ist auch $\{ax_1, ax_2, \dots, ax_k\} = G$. Bezeichnen wir das Produkt der Gruppenelemente x_1, x_2, \dots, x_k mit y , so ist also

$$a^k y = (ax_1)(ax_2) \dots (ax_k) = x_1 x_2 \dots x_k = y$$

und daher $a^k = e$. Der Rest des Beweises ergibt sich durch leichte Modifikation des Beweises von Lemma 6.1. □

Satz 6.3. Es sei p eine Primzahl und $d \in \mathbb{N}^*$ ein Teiler von $p - 1$. Dann existieren genau $\varphi(d)$ Zahlen in $\{1, 2, \dots, p - 1\}$ mit der Ordnung d .

Beweis. Es sei $\psi(d) := \#\{x \in \{1, 2, \dots, p - 1\} : p \text{ hat Ordnung } d\}$. Wir zeigen durch Induktion nach d , daß

$$\psi(d) = \varphi(d).$$

Induktionsanfang: Für $1 \leq x \leq p - 1$ ist $x^1 \equiv 1 \pmod{p}$ genau dann, wenn $x = 1$ ist. Also ist $\psi(1) = 1 = \varphi(1)$.

Induktionsschluß: Sei $d > 1$ und die Behauptung richtig für alle Teiler t von $p - 1$ mit $t < d$. Dann ist

$$\begin{aligned} d &= \#\{x \in \{1, \dots, p-1\}: x^d \equiv 1 \pmod{p}\} \\ &= \#\{x \in \{1, \dots, p-1\}: \text{Ordnung von } x \text{ ist Teiler von } d\} \\ &= \sum_{t|d} \psi(t) = \psi(d) + \sum_{t|d, t \neq d} \psi(t) = \psi(d) + \sum_{t|d, t \neq d} \varphi(t). \end{aligned}$$

Wegen $\sum_{t|d} \varphi(t) = d$ ist also auch $\psi(d) = \varphi(d)$. □

Korollar 6.4. *Es existieren genau $\varphi(p-1) \geq 1$ Zahlen $x \in \{1, 2, \dots, p-1\}$ mit der Eigenschaft: Modulo p gerechnet sind x^1, x^2, \dots, x^{p-1} die Zahlen $1, 2, \dots, p-1$ (jede solche x heißt Primitivwurzel zu p).*

Mit anderen Worten: \mathbb{Z}_p^ ist zyklisch, Anzahl der Erzeugenden ist $\varphi(p-1)$.*

Kleinste Primitivwurzeln $a \geq 1$ für Primzahlen $p \leq 53$:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$\varphi(p-1)$	1	1	2	2	4	4	8	6	10	12	8	12	16	12	22	24
a	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2

Beispiel 6.2. $p = 11$, $\varphi(10) = 4$:

2, 6, 7, 8 sind Primitivwurzeln:

Die Potenzen von 2 sind: 2, 4, 8, 5, 10, 9, 7, 3, 6, 1.

Die Potenzen von 6 sind: 6, 3, 7, 9, 10, 5, 8, 4, 2, 1.

Die Potenzen von 7 sind: 7, 5, 2, 3, 10, 4, 6, 9, 8, 1.

Die Potenzen von 8 sind: 8, 9, 6, 4, 10, 3, 2, 5, 7, 1.

Definition 6.3. $a \in \mathbb{Z}^*$ heißt *Primitivwurzel* von p , wenn $p-1$ die kleinste Zahl $j \in \mathbb{N}^*$ ist mit $a^j \equiv 1 \pmod{p}$.

Frage. Sei p Primzahl, $n \in \mathbb{N}^*$, $n \geq 2$. Ist \mathbb{Z}'_{p^n} zyklisch?

Die Anzahl der Elemente in \mathbb{Z}'_{p^n} ist $\varphi(p^n) = (p-1)p^{n-1}$. Also lautet die Frage:

Gibt es ein $a \in \mathbb{Z}^*$, so daß $(p-1)p^{n-1}$ das kleinste j ist mit $a^j \equiv 1 \pmod{p^n}$?

Bemerkung 6.5. 1) Primitivwurzeln für \mathbb{Z}_p^* sind nicht notwendig Primitivwurzeln für \mathbb{Z}'_{p^n} : So ist beispielsweise 7 Primitivwurzel für \mathbb{Z}_5^* wegen

$$7^1 \equiv 2 \pmod{5}, \quad 7^2 \equiv 4 \pmod{5}, \quad 7^3 \equiv 3 \pmod{5}, \quad 7^4 \equiv 1 \pmod{5},$$

aber bereits $7^4 \equiv 1 \pmod{25}$, während $\varphi(25) = 20$ ist.

2) \mathbb{Z}'_{2^3} ist nicht zyklisch (siehe früheres Beispiel).

Lemma 6.6. Sei $p \in \mathbb{P}$, $n \in \mathbb{N}^*$, a Primitivwurzel zu p und $\bar{a} \in \mathbb{Z}'_{p^n}$ Restklasse von a modulo p^n . Dann gilt für alle $\nu \in \mathbb{N}$:

$$\text{Ordnung von } \bar{a}^{p^\nu} \text{ ist } (p-1)p^{l_\nu} \text{ mit } 0 \leq l_\nu \leq n-1.$$

Beweis. Sei t diese Ordnung. Dann ist

$$a^{tp^\nu} = \left(a^{p^\nu}\right)^t \equiv 1 \pmod{p^n}.$$

Diese Kongruenz gilt erst recht modulo p . Nach Lemma 6.1 ist also $p-1$ ein Teiler von tp^ν . Weil $p-1$ und p^ν teilerfremd sind, folgt daraus, daß $p-1$ Teiler von t ist. Außerdem ist t nach Satz 6.2 Teiler von $(p-1)p^{l_\nu}$. Damit folgt die Behauptung. \square

Lemma 6.7. Sei $p \neq 2$ eine Primzahl und $c \in \mathbb{Z}$ eine Primitivwurzel für p^2 . Dann ist c eine Primitivwurzel für alle p^n , $n \in \mathbb{N}^*$.

Beweis. Wir benutzen

$$a \equiv 1 \pmod{p} \Rightarrow a^p \equiv 1 \pmod{p^2}, \quad (6.1)$$

$$a^p \equiv 1 \pmod{p^n} \Rightarrow a \equiv 1 \pmod{p^{n-1}} \quad (n \in \mathbb{N}, n \geq 2). \quad (6.2)$$

Wir bemerken zunächst, daß c auch Primitivwurzel zu p ist: Wäre $c^d \equiv 1 \pmod{p}$ mit $1 \leq d < p-1$, so wäre nach (6.1) auch $c^{dp} \equiv 1 \pmod{p^2}$ mit $dp < (p-1)p = \#\mathbb{Z}'_{p^2}$, was nach Voraussetzung falsch ist.

Sei $n \in \mathbb{N}$, $n > 2$ und $\bar{c} \in \mathbb{Z}'_{p^n}$ die Restklasse von c modulo p^n . Die Ordnung von \bar{c} ist $(p-1)p^l$ mit einem gewissen $0 \leq l \leq n-1$. Nehmen wir an, daß $l \leq n-2$ ist. Wegen $c^{(p-1)p^l} \equiv 1 \pmod{p^n}$ ist dann auch

$$c^{(p-1)p^{n-2}} \equiv 1 \pmod{p^n},$$

also nach $(n-2)$ -maliger Anwendung von (6.2) auch

$$c^{p-1} \equiv 1 \pmod{p^2}.$$

Dies steht im Widerspruch dazu, daß die Ordnung von c in \mathbb{Z}'_{p^2} gleich $(p-1)p$ ist. \square

Satz 6.8. Sei $p \neq 2$ Primzahl. Dann sind alle \mathbb{Z}'_{p^n} , $n \in \mathbb{N}^*$, zyklisch. Genauer gilt für jede a Primitivwurzel zu p :

- 1) $a^{p-1} \not\equiv 1 \pmod{p^2} \Rightarrow a$ ist Primitivwurzel für alle p^n .
- 2) $a^{p-1} \equiv 1 \pmod{p^2} \Rightarrow$ Es sind $a \pm p$ Primitivwurzeln für alle p^n .

Beweis. Nach Lemma 6.7 brauchen wir die Behauptungen nur für $n = 2$ zu zeigen.

1. Sei \bar{a} die Restklasse von a modulo p^2 . Nach Lemma 6.6 ist die Ordnung von \bar{a} entweder $p - 1$ oder $(p - 1)p$. Die Möglichkeit $p - 1$ ist aber ausgeschlossen, da $a^{p-1} \not\equiv 1 \pmod{p^2}$. Also ist die Ordnung von \bar{a} gleich $p(p - 1) = \varphi(p^2)$.

2. Mit a ist auch $b := a \pm p$ Primitivwurzel zu p , da $b \equiv a \pmod{p}$. Also reicht es zu zeigen, daß

$$b^{p-1} \not\equiv 1 \pmod{p^2}.$$

Es gilt

$$b^{p-1} = (a \pm p)^{p-1} \equiv a^{p-1} \pm (p-1)a^{p-2}p \equiv 1 \pm (p-1)pa^{p-2} \pmod{p^2},$$

wobei p weder Teiler von $p - 1$ noch von a^{p-2} ist (letzteres, da sonst a keine Primitivwurzel für p wäre). Daher ist $b^{p-1} \not\equiv 1 \pmod{p^2}$. \square

Beispiele 6.3. 1) $p = 5$: 2 ist Primitivwurzel zu 5 (früheres Beispiel).

Es ist $2^4 \not\equiv 1 \pmod{5^2}$. Also ist 2 Primitivwurzel für alle 5^n . 7 ist ebenfalls Primitivwurzel zu 5, aber $7^4 \equiv 1 \pmod{5^2}$, 7 nicht Primitivwurzel zu 5^2 , wohl aber ist $7 + 5 = 12$ Primitivwurzel für alle 5^n .

2) Schwieriger ist es, Primitivwurzeln a zu $p > 2$ zu finden mit $1 \leq a \leq p$, so daß a nicht Primitivwurzel zu p^2 ist (für $p = 467$ beispielsweise $a = 10$).

Wir wollen jetzt allgemein klären, für welche $m \in \mathbb{N}^*$ die Gruppe \mathbb{Z}'_m zyklisch ist.

Satz 6.9. Für alle ungeraden Primzahlen p und alle $n \in \mathbb{N}^*$ ist \mathbb{Z}'_{2p^n} zyklisch.

Genauer gilt dabei für jede Primitivwurzel c zu p^n :

$$c \text{ ungerade} \Rightarrow c \text{ ist Primitivwurzel zu } 2p^n.$$

$$c \text{ gerade} \Rightarrow c + p^n \text{ ist Primitivwurzeln zu } 2p^n.$$

Beweis. Sei zunächst c ungerade, also weder 2 noch p ein Teiler von c . Dann liegt die Restklasse \bar{c} von c modulo $2p^n$ in \mathbb{Z}'_{2p^n} . Sei t die Ordnung von \bar{c} . Dann gilt $c^t \equiv 1 \pmod{2p^n}$, also erst recht $c^t \equiv 1 \pmod{p^n}$, $\varphi(p^n) \mid t$. Wegen

$$\#\mathbb{Z}'_{2p^n} = \varphi(2p^n) = \varphi(2)\varphi(p^n) = \varphi(p^n)$$

ist auch t Teiler von $\varphi(p^n)$, also $t = \varphi(p^n)$, \bar{c} Primitivwurzel zu p^n .

Ist c gerade, so ist $c + p^n$ ungerade und Primitivwurzel zu p^n . Somit ist auch $c + p^n$ Primitivwurzel zu $2p^n$. \square

Wir wissen, daß $\mathbb{Z}'_2 = \{\bar{1}\}$ und $\mathbb{Z}'_4 = \{\bar{3}, \bar{3}^2\}$ zyklisch sind. Aber:

Lemma 6.10. Sei $n \in \mathbb{N}$, $n \geq 3$, $a \in \mathbb{Z}$ ungerade. Dann ist

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

Insbesondere ist \mathbb{Z}'_{2^n} nicht zyklisch.

Beweis. Betrachten wir zunächst den Fall $n = 3$: Es ist $a = 1 + 2b$ mit $b \in \mathbb{Z}$ also

$$a^2 = 1 + 4b(b+1) = 1 + 8c \quad \text{mit} \quad c = \frac{b(b+1)}{2} \in \mathbb{Z}.$$

Daraus folgt, daß

$$a^{2^{3-2}} = a^2 \equiv 1 \pmod{2^3}.$$

Gilt die behauptete Kongruenz für ein $n \geq 3$, dann auch für $n + 1$:

$$a^{2^{n-2}} \equiv 1 \pmod{2^n} \Rightarrow a^{2^{(n+1)-2}} \equiv \left(a^{2^{n-2}}\right)^2 \equiv 1 \pmod{2^{n+1}}.$$

Die weitere Behauptung folgt wegen $\varphi(2^n) = 2^{n-1} > 2^{n-2}$. □

Abschließend haben wir:

Satz 6.11. Für alle $m \in \mathbb{N}$, $m > 1$, sind äquivalent:

1) \mathbb{Z}'_m ist zyklisch.

2) $m = 2$ oder $m = 4$ oder $m = p^n$ oder $m = 2p^n$ mit $n \in \mathbb{N}^*$ und $p \in \mathbb{P} \setminus \{2\}$.

Beweis. (2) \Rightarrow (1): Bereits gezeigt.

(1) \Rightarrow (2): Sei $m = p_1^{n_1} \dots p_r^{n_r}$ die Primzerlegung von m und

$$l := \text{kgV}(\varphi(p_1^{n_1}), \dots, \varphi(p_r^{n_r})).$$

Sei $a \in \mathbb{N}^*$ mit $(a, m) = 1$ und \bar{a} die Restklasse von a in \mathbb{Z}'_m mit Ordnung $\varphi(m)$ (existiert, wenn \mathbb{Z}'_m zyklisch). Wegen

$$a^{\varphi(p_j^{n_j})} \equiv 1 \pmod{p_j^{n_j}},$$

also $a^l \equiv 1 \pmod{p_j^{n_j}}$ für alle $1 \leq j \leq r$ ist

$$a^l \equiv 1 \pmod{m}$$

und damit $l \geq \varphi(m) = \varphi(p_1^{n_1}) \dots \varphi(p_r^{n_r})$,

$$l = \varphi(p_1^{n_1}) \dots \varphi(p_r^{n_r}). \tag{6.3}$$

Ist $p \in \mathbb{P}$ ungerade, $n \in \mathbb{N}^*$, so ist $\varphi(p^n) = (p-1)p^{n-1}$ gerade. Wegen (6.3) können also in der Primfaktorzerlegung von m nicht zwei ungerade Primfaktoren vorkommen, d.h., es ist

$$m = 2^{n_1} p^{n_2}$$

mit ungeradem $p \in \mathbb{P}$ und $n_1, n_2 \in \mathbb{N}$, $n_1 + n_2 > 0$. Nach Lemma 6.10 ist $m = 2$ oder $m = 4$, falls $n_2 = 0$. Sei also $n_2 > 0$. Wäre $n_1 \geq 2$, so wäre $\varphi(2^{n_1}) = 2^{n_1-1}$ ein Vielfaches von 2 und $\varphi(p^{n_2})$ gerade im Widerspruch zu (6.3). Daher folgt $n_1 < 2$, $m = p^{n_2}$ oder $m = 2p^{n_2}$. □

6.3 Quadratisches Reziprozitätsgesetz

Definition 6.4. Sei $m \in \mathbb{N}$, $m > 1$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$.
 a heißt *quadratischer Rest modulo m (oder nach m)*, wenn es ein $x \in \mathbb{Z}$ gibt mit

$$x^2 \equiv a \pmod{m}.$$

Beispiel 6.4. $m = 9$.

1, 4, 7 sind quadratische Reste modulo 9:

$$1^2 \equiv 1 \pmod{9}, \quad 2^2 \equiv 4 \pmod{9}, \quad 4^2 \equiv 7 \pmod{9}.$$

2, 5, 8 sind keine quadratischen Reste modulo 9.

Definition 6.5. *LEGENDRESches Restsymbol* $\left(\frac{a}{p}\right)$, „ a nach p “, für $a \in \mathbb{Z}$, p Primzahl, die a nicht teilt:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{wenn } a \text{ quadratischer Rest modulo } p, \\ -1, & \text{sonst.} \end{cases}$$

Satz 6.12 (Eulersches Kriterium:). Für alle Primzahlen $p > 2$ und jede zu p prime ganze Zahl a ist

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

Beweis. Ist $x^2 \equiv a \pmod{p}$, so ist $(x, p) = 1$, also nach dem kleinen Satz von FERMAT (3.13)

$$1 \equiv x^{p-1} = (x^2)^{\frac{1}{2}(p-1)} \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Nach früherem Satz (3.41) existieren höchstens $(p-1)/2$ nicht kongruente a mit $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$.

Da \mathbb{Z}_p^* zyklisch ist, existieren andererseits $(p-1)/2$ nicht kongruente quadratische Reste: Sei $c \in \mathbb{Z}$ mit

$$\mathbb{Z}_p^* = \{c, c^2, c^3, \dots, c^{p-1}\}$$

und $1 \leq i \leq p-1$. Dann gibt es genau dann ein $1 \leq j \leq p-2$ mit

$$(c^j)^2 \equiv c^i \pmod{p},$$

wenn $i = 2j$ oder $i = 2j - (p-1)$, d.h., wenn i gerade ist. Dafür gibt es genau $(p-1)/2$ Möglichkeiten. \square

Das folgende Korollar wird auch *Erster Ergänzungssatz zum quadratischen Reziprozitätsgesetz* genannt.

Korollar 6.13. Für alle Primzahlen $p > 2$ ist

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

Bemerkung 6.14. Die Aussage des Korollars ist nur eine andere Formulierung der uns schon bekannten Tatsache, daß es für Primzahlen $p > 2$ genau dann ein $x \in \mathbb{Z}$ mit $p \mid x^2 + 1$ (d.h. mit $x^2 \equiv -1 \pmod{p}$) gibt, wenn $p \equiv 1 \pmod{4}$ ist.

Rechenregeln 6.15. Für alle zu $p \in \mathbb{P}$ primen $a, a' \in \mathbb{Z}$:

$$1) \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right), \text{ wenn } a \equiv a' \pmod{p}.$$

$$2) \left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{a'}{p}\right).$$

$$3) \left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right) \text{ für alle } c \in \mathbb{Z}^*.$$

Beweis. (1) ist trivial, (2) folgt aus dem EULERSchen Kriterium zusammen mit den Rechenregeln für Kongruenzen, und (3) folgt aus (2) wegen $\left(\frac{c}{p}\right)^2 = 1$. \square

Die folgenden Sätze geben wir ohne Beweis an. Zunächst den *Zweiten Ergänzungssatz zum quadratischen Reziprozitätsgesetz*:

Satz 6.16 (Lagrange 1775). Für alle Primzahlen $p > 2$ ist

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

M. a. W.:

2 ist genau dann quadratischer Rest modulo p , wenn p die Form $8k \pm 1$ hat.

Dann der Hauptsatz, den LEGENDRE 1785 entdeckt, aber nie vollständig bewiesen hat (GAUSS allein hat acht Beweise dafür gegeben):

Satz 6.17 (Quadratisches Reziprozitätsgesetz). Für alle ungeraden Primzahlen p, q ist

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

M. a. W.:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), \text{ wenn } p, q \text{ beide die Form } 4k + 3 \text{ haben,}$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), \text{ wenn } p \text{ und } q \text{ nicht beide die Form } 4k + 3 \text{ haben.}$$

Beispiele 6.5. 1) Ist 3 quadratischer Rest modulo 29? Nach Satz genau dann, wenn 29 quadratischer Rest modulo 3 ist. Nun ist $29 \equiv 2 \pmod{3}$, somit

$$\left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1,$$

also 3 kein quadratischer Rest modulo 29.

2) 35 ist quadratischer Rest modulo 281: Es ist

$$\left(\frac{35}{281}\right) = \left(\frac{5}{281}\right) \left(\frac{7}{281}\right), \quad \left(\frac{5}{281}\right) = \left(\frac{281}{5}\right), \quad \left(\frac{7}{281}\right) = \left(\frac{281}{7}\right),$$

wobei $281 \equiv 1 \pmod{5}$ und $281 \equiv 1 \pmod{7}$, also

$$\left(\frac{281}{5}\right) = \left(\frac{1}{5}\right) = 1, \quad \left(\frac{281}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

3) 65 ist quadratischer Rest modulo 307: Es ist

$$\left(\frac{65}{307}\right) = \left(\frac{5}{307}\right) \left(\frac{13}{307}\right) = \left(\frac{307}{5}\right) \left(\frac{307}{13}\right) = \left(\frac{2}{5}\right) \left(\frac{8}{13}\right) = \left(\frac{2}{5}\right) \left(\frac{2}{13}\right)^3,$$

wobei

$$\left(\frac{2}{5}\right) = (-1)^{\frac{25-1}{8}} = -1 \quad \text{und} \quad \left(\frac{2}{13}\right) = (-1)^{\frac{169-1}{8}} = -1,$$

also

$$\left(\frac{65}{307}\right) = (-1) \cdot (-1)^3 = 1.$$