23.12.21

Donnerstag, 21. Dezember 2023 12:02

Korollar 152 Sind $a, b \in \mathbb{Z}$ teilerfremde Zahlen, so gibt es ein $\tilde{a} \in \{0, \ldots, b-1\}$, so dass gilt:

$$a \cdot \tilde{a} \equiv 1 \ (b)$$

Beweis $ggT(a,b) = 1 \overset{\text{Satz 150}}{\Rightarrow} \exists a', b' \in \mathbb{Z} : 1 = a \cdot a' + b \cdot b'$

Falls $a' > b$ ist: $a' = q \cdot b + r$, $r \in \{0, \ldots, b-1\}$.

$\Rightarrow 1 = a \cdot a' + b \cdot b' = a \cdot (q \cdot b + r) + b \cdot b' =$

$= ar + aqb + b \cdot b' = ar + b(\underbrace{aq + b'}_{\in \mathbb{Z}})$

Wähle $\tilde{a} := r$. Dann $a \cdot \tilde{a} \equiv 1 \ (b)$

Falls $a' \leq b$, dann wähle $\tilde{a} := a'$ $\square$

Primzahlen

Sei $n \in \mathbb{N}$, $n \geq 2$, $\mathbb{Z}_n := \{[0]_n, \ldots, [n-1]_n\} \hat{=}$

$\hat{=}$ Menge der Restklassen auf $\mathbb{Z}$ bei Division mit Rest durch n. Also $[a]_n = \{a + k \cdot n \mid k \in \mathbb{Z}\}$ und a heißt <u>Repräsentant</u> der Restklasse $[a]_n$.

Man kann auf $\mathbb{Z}_n$ eine Addition "+" und eine

Man kann auf $\mathbb{Z}_n$ eine Addition "+" und eine Multiplikation "·" einführen:

$$[a]_n + [b]_n := [a+b]_n \quad , \quad [a]_n \cdot [b]_n := [a \cdot b]_n$$

Hier muss man die Unabhängigkeit von der Wahl der Repräsentanten zeigen (machen wir nicht)

Es gilt: $[a]_n = [b]_n \iff [a-b]_n = [0]_n$

$\iff \{ k \cdot n + (a-b) \mid k \in \mathbb{Z} \} = \{ k \cdot n + 0 \mid k \in \mathbb{Z} \}$

$\iff \exists\, l \in \mathbb{Z} : l \cdot n + a - b = 0$

$\iff \exists\, l \in \mathbb{Z} : a = b - ln$

$\iff a \equiv b \mod n \qquad (a \equiv b \ (n))$

Beispiel 153 $\quad \mathbb{Z}_4 = \{0, 1, 2, 3\}$ (Abkürzung: $1 = [1]_4$)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$2 \in \mathbb{Z}_4$ hat kein multiplikatives Inverses

Der ggT charakterisiert die Existenz multiplikativer Inversen in $\mathbb{Z}_n$:

Inversen im $\mathbb{Z}_n$:

Satz 154 $[a]_n \in \mathbb{Z}_n$. Es sind äquivalent:

$\exists a' \in \mathbb{Z} : [a]_n \cdot [a']_n = [1] \iff ggT(a,n) = 1$

Beweis „$\Leftarrow$" $ggT(a,n) = 1 \overset{K152}{\Longrightarrow} \exists a' \in \mathbb{Z} : a \cdot a' \equiv 1 (n)$

$\Rightarrow [1]_n = [a \cdot a']_n = [a]_n \cdot [a']_n$

„$\Rightarrow$" Zeige: jeder gemeinsame Teiler von a und n teilt die 1 ($\Rightarrow ggT(a,n) = 1$). Sei nach Vor. $[a]_n \cdot [a']_n = [1]_n \Rightarrow a \cdot a' \equiv 1 \ (n) \Rightarrow \exists q \in \mathbb{Z}$: $a \cdot a' = q \cdot n + 1 \Rightarrow 1 = a \cdot a' - qn$. Sei $d \in \mathbb{Z}$ mit $d | a$ und $d | n$, also $d \cdot k = a$ und $d \cdot k' = n$, also $1 = dka' - qdk' = d(\overbrace{ka' - qk'}^{\in \mathbb{Z}})$

also $d | 1$ $\square$

Es sei K eine Menge mit Addition „+" und Multiplikation „$\cdot$". Das neutrale Element der Addition sei 0, das der Multiplikation sei 1. Man nennt K einen <u>Körper</u>, falls $(K, +)$ und $(K \setminus \{0\}, \cdot)$

abelsche Gruppen sind und die Distributivgesetze gelten. Als Faustregel: man kann in Körpern genauso rechnen wie im $\mathbb{R}$ oder $\mathbb{Q}$. ($\mathbb{R}$ und $\mathbb{Q}$ sind Körper). Die Bedingung $\circledast$ bedeutet insbesondere, dass jedes Element aus $K \setminus \{0\}$ ein multiplikatives Inverses hat.

Korollar 155 Ist $p \in \mathbb{Z}$ eine Primzahl, dann ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper $\square$

Um zu zeigen dass es ∞-viele Primzahlen gibt, brauchen wir den Hauptsatz der Zahlentheorie:

Satz 156 (Primfaktorzerlegung) Jede Zahl $n \in \mathbb{N}$, $n \geq 2$, lässt sich als Produkt von Primzahlpotenzen schreiben, also $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$. Diese Darstellung ist eindeutig bis auf die Reihenfolge $\square$

Satz 157 Es gibt unendlich viele Primzahlen.

Satz 157 Es gibt unendlich viele Primzahlen.

Beweis Angenommen es gibt nur endlich viele, also $p_1 < p_2 < \dots < p_k$. Dann ist $n := p_1 \cdot \ldots \cdot p_k + 1 > p_k$ keine Primzahl. Nach Satz 156 gibt es eine Primzahl, die n teilt. Dann muss p eines der p_i sein, also $p = p_i$. Dann: $\mathbb{Z} \ni \frac{n}{p} = \frac{n}{p_i}$

$$= \frac{1}{p_i}\left(p_1 \cdot \ldots \cdot p_k + 1\right) = p_1 \cdot \ldots \cdot \hat{p_i} \cdot \ldots \cdot p_k + \frac{1}{p_i}$$

rausgekürzt

$$\frac{p_1 \cdot p_2 \cdot \ldots \cdot \cancel{p_i} \cdot \ldots \cdot p_k}{\cancel{p_i}}$$

$$\Rightarrow \frac{1}{p_i} \in \mathbb{Z}$$

$\Rightarrow p_i \mid 1$ im ↯ p_i ist Primzahl □

Beispiel 158 1) Mersenne-Primzahlen: $2^n - 1$, $n \in \mathbb{N}$, $n \geq 2$, 2) Fermat'sche Zahlen (1640): $2^{2^n} + 1$ sind für $n \in \{0,1,2,3,4\}$ Primzahlen. Für $n = 5$ nicht (Euler 1732). Für welche n sonst: unbekannt.

Bemerkung 159 (Primzahlsatz) Es sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Dann wächst $\pi(x)$ für $x \to \infty$

Primzahlen $\le x$. Dann wächst $\pi(x)$ für $x \to \infty$ wie $\frac{x}{\ln x}$ $\square$

Bemerkung 160 Sieb des Eratosthenes: notiere die natürlichen Zahlen aufsteigend.

2 3 4 5 6 7 8 9 10 11 12 13

Streiche Vielfache, die kleinste nicht-gestrichene Zahl ist eine Primzahl.

Teilbarkeitsregeln

Lemma 161 Es sei $a \equiv b\ (m)$ und $c \equiv d\ (m)$.

Dann gelten: $a + c \equiv b + d\ (m)$, $ac \equiv bd\ (m)$.

Beweis Es gelten: $a = k \cdot m + b$, $c = l \cdot m + d$ für gewisse $k, l \in \mathbb{Z}$. Dann $a + c = b + d + m\underbrace{(k+l)}_{\in \mathbb{Z}}$

also $a + c \equiv b + d\ (m)$. Weiter: $ac =$

$= a(lm + d) = alm + ad = alm + (km + b)d$

$= bd + dkm + alm = bd + m(dk + al)$

$\Rightarrow \quad ac \equiv bd \ (m) \quad \square$

Es sei $n \in \mathbb{N}$ dargestellt durch $n = \sum_{i=0}^{k} a_i \cdot 10^i =$

$= a_0 + 10 a_1 + 10^2 a_2 + \dots + 10^k a_k$. Also n hat die

Stellen $a_k a_{k-1} \dots a_0$. Zum Beispiel: $n = 324 =$

$= 3 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0$

Satz 1.62 Es sei $n = \sum_{i=0}^{k} a_i \, 10^i$, $a_i \in \{0, \dots, 9\}$

1) 10er-Regel: $10 \mid n \Leftrightarrow a_0 = 0$

2) 5er-Regel: $5 \mid n \Leftrightarrow a_0 \in \{0, 5\}$

3) 2er-Regel: $2 \mid n \Leftrightarrow a_0 \in \{0, 2, 4, 6, 8\}$

4) 4er-Regel: $4 \mid n \Leftrightarrow 4 \mid \underbrace{a_1 \cdot 10 + a_0}_{\text{Zahl aus letzten beiden Stellen}}$

5) 8er-Regel: $8 \mid n \Leftrightarrow$

$8 \mid a_2 \cdot 100 + a_1 \cdot 10 + a_0$

zu 1) $10 \mid 10^i \ \forall i \geq 1$: $10 \mid n \Leftrightarrow 10 \mid a_0$

$\Leftrightarrow a_0 = 0$

zu 4) $4 \mid 10^i \ \forall i \geq 2$: $4 \mid n \Leftrightarrow 4 \mid a_1 \cdot 10 + a_0$

6) 3er / 9er - Regel : $d \in \{3, 9\}$ Quersumme von n

$$d \mid n \iff d \mid Q(n) := \sum_{i=0}^{k} a_i$$

zu 6) Es gilt : $10 \equiv 1 \ (d) \overset{L161}{\Longrightarrow} 10^i \equiv 1^i \ (d)$

$$\Rightarrow n = \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i = Q(n) \mod d$$

$$\Rightarrow n \equiv Q(n) \ (d)$$

Also $d \mid n \iff d \mid Q(n)$