$$\mathbb{Z}_n = \{0, 1, ..., n-1\}$$

$+$

$\cdot$

Satz:

$r, n \in \mathbb{N}$. Ein $r \in \mathbb{Z}_n$ ist invertierbar bez. der Multiplikation, wenn $ggT(r, n) = 1$
(d.h. r und n teilerfremd)

Beweis:

"$\Rightarrow$" Sei $r \in \mathbb{Z}_n$ invertierbar, d.h. es ex. ein $x \in \mathbb{Z}_n$ mit $r \cdot x = 1$ (in $\mathbb{Z}_n$) ($r \cdot x \equiv 1 \; mod \; n$)

Das bedeutet: $n|(rx - 1)$

Also gibt es ein $s \in \mathbb{Z}$ mit $n \cdot s = rx - 1$ (in $\mathbb{Z}$)

$1 = rx - ns$

Wäre nun ein $d > 1$ ein gemeinsamer Teiler von r und n, so würde gelten: $d|(rx - ns)$ also $d|1$ $\underset{\text{Widerspruch}}{\lightning}$ zu $d > 1$.

Also gilt: $ggT(r, n) = 1$

"$\Leftarrow$" Gilt $ggT(r, n) = 1$ Dann existieren ganze Zahlen x, y:

$\boxed{rx + ny = 1}$

(Satz vom 8.11.): kleinste positive ganzz. LK von r und $n = ggT(r, n)$

$rx - 1 = ny$

D.h. $n|(rx - 1)$

$\Leftrightarrow rx \equiv 1 (mod \; n)$

$\Leftrightarrow r \cdot \underset{\text{Rest bei der Division von } x \; mod \; n \in \{0,1,...,r-1\}}{(x \; mod \; n)} = 1$ (in $\mathbb{Z}_n$)

Also r invertierbar $\square$

Beispiel:

1) $n = 7$, $r = 2$, r invertierbar:

   $2 \cdot 4 = 1$ (in $\mathbb{Z}_7$)

2) $n = 8$, $r = 6$, $ggT(6, 8) = 2$

   Es gibt kein Inverses Element zu 6

$6 \cdot 1 = 6 \quad 6 \cdot 3 = 2 \quad 6 \cdot 5 = 6$

$6 \cdot 2 = 4 \quad 6 \cdot 4 = 0 \quad 6 \cdot 6 = 4$

(in $\mathbb{Z}_8$) $\qquad 6 \cdot 7 = 2$

Lemma (Kürzungsregel)

Seien $a, n \in \mathbb{N}$.

Ist $ggT(a, n) = 1$, so folgt für alle $x, y \in \mathbb{Z}$:

$$ax \equiv ay \; mod \; n \Rightarrow x \equiv y \; mod \; n$$

Erinnerung: in $\mathbb{Z}/\mathbb{Q}/\mathbb{R}$:

$ax = ay \overset{\text{Teilen durch } a}{\Rightarrow} x = y \quad a \neq 0$

Beweis:

1) Aus $ax \equiv ay \; mod \; n$ folgt:

   $n|a(x-y)$.

   Weil $ggT(n, a) = 1$, gilt: $n|(x-y)$

   d.h. $x \equiv y \; mod \; n \quad \square$

2) $ax \equiv ay$ (in $\mathbb{Z}_n$)

   Multiplizieren beider Seiten mit a^{-1} liefert (in $\mathbb{Z}_n$)

   $1 \cdot x = a^{-1} \cdot ax = a^{-1} \cdot ay = 1 \cdot y = y$

   x^{II}

($\underset{\text{ohne Beschränkung der Allgemeinheit}}{\text{o.B.d.A.}} : x, y \in \{0, 1, ..., n-1\}$)

$\equiv_n$ ist Äquivalenzrelation:

$$r \in \{0, 1, ..., n-1\} : [r] \ni x, \; x \equiv r \; mod \; n$$

$ax \equiv ar(mod \; n)$

Beispiel:

$2 \cdot 3 \equiv 4 \cdot 3 \; mod \; 6 \not\Rightarrow 2 \equiv 4 \; mod \; 6$

$(ggT(6, 3) = 3)$

Primzahlen

def.

Eine nat. Zahl $p(\in \mathbb{N}),\ p \geq 2$, heißt prim oder eine Primzahl, falls die einzigen positiven Teiler von p nur 1 und p selbst sind. Mit P bezeichnet man die Menge der Primzahlen.

$P = \{2, 3, 5, 7, 11, 13, 17, 19, ...\}$

$4 = 2 \cdot 2$ ist keine Primzahl

$6 = 2 \cdot 3$ -||-

Zahlen, die sich als Produkt von zwei oder mehr Primzahlen(nicht notwendigerweise verschieden) schreiben lassen, heißen zusammengesetzt.

$8 = 2 \cdot 2 \cdot 2$

Bem:

2 ist die einzige gerade Primzahl.

Wie viele Primzahlen gibt es?

$$P \subseteq \mathbb{N} \begin{cases} \text{endlich viele} \\ \text{oder} \\ \text{abzählbar viele} \end{cases}$$

Satz (Euclid)

Es gibt unendlich viele Primzahlen.

Beweis: (durch Widerspruchsbeweis)

Angenommen, $|P| < \infty$.

Seien $p_1 < ... < p_n$ alle Primzahlen.

$$m := 1 + \prod_{i=1}^{N} p_i \, (= p_1 \cdot p_2 \cdot ... \cdot p_N + 1)$$

0. Beobacht. $\boxed{m \geq 2,\ m \in \mathbb{N}}$

$\boxed{\text{Beobachtung:}}\ \forall i : p_i \nmid m$

2 Fälle:

1. Fall: m ist durch keine nat. Zahl $2 \leq n < m$ teilbar $\Rightarrow m$ Primzahl $\lightning$ zu $(m > P_N)$

2. Fall: m ist durch eine nat. Zahl $n,\ 2 \leq n < m$ teilbar

Dann: betrachte

$$p = min\underbrace{\{n : n \in \mathbb{N},\ n \geq 2,\ n|m\}}_{\neq \emptyset\ \geq 2} < m$$

p muss nun selbst eine Primzahl sein!

(sonst gäbe es ein $q \in \mathbb{N},\ q > 1,\ q|p,\ q < p$)

Also: aus $\left.\begin{matrix} q|p \\ p|m \end{matrix}\right\} q|m \quad \lightning$ zur Definition p

Widerspruch zu Beobachtung 1.

D.h. unsere Annahme $|P| < \infty$ falsch. $\square$

Satz:

Ist $p \in P$ und sind $x_1, ..., x_n \in \mathbb{N}$, sodass

$$p| \prod_{i=1}^{n} x_i$$

so existiert ein $i \in [n] = \{1, ..., n\}$ mit $p|x_i$

Beweis: (Induktion)

$n = 1$ (trivial)

$n = 2$: $p|x_1 \cdot x_2$

Gilt $p \nmid x_1$, so haben: $ggT(p, x_1) = 1$

$\overset{\text{Lemma}}{\underset{\text{von 8.11}}{\Rightarrow}} p|x_2$

Induktionsschritt: $n \to n + 1$

Die Aussage $\boxed{A(n) : p| \prod_{i=1}^{n} x_i \Rightarrow \exists i \in [n] : p|x_i}$

z.z. $A(n) \Rightarrow A(n + 1)$

Seien $x_1, ..., x_{n+1} \in \mathbb{N}$.

Mit

$$X := \prod_{i=1}^{n} x_i \text{ gilt: } \prod_{i=1}^{n+1} x_i = x \cdot x_{n+1}$$

$$p|X \cdot x_{n+1} \overset{\text{Fall } n=2}{\Rightarrow} p|X \text{ oder } p|x_{n+1}$$

Im Fall $p|x_{n+1}$ sind wir fertig.

Falls

$$p|X = \prod_{i=1}^{n} x_i \overset{A(n)}{\Rightarrow} \exists i \in [n] : p|x_i$$

Also gilt: $A(n+1)$ $\square$

$n \in \mathbb{N},\ n > 1$

n hat Teiler, genauer: n lässt sich als Produkt von Primzahlen schreiben.

---

def.:

Ist $n \in \mathbb{N},\ p \in P$ und gilt $p|n$, so nennen wir p einen Primfaktor von n.

Satz: (Eindeutige Primfaktorzerlegung)

Jedes $n \geq 2,\ n \in \mathbb{N}$, hat eine eindeutige Schreibweise als Produkt von Primzahlen (bis auf die Ordnung der Primzahlen).

Bem.:

Primzahlen sind nicht notwendigerweise verschieden in dieser Darstellung von n

Beweis:

Sei N die kleinste nat. Zahl, für die der Satz nicht gilt. D.h. N lässt sich wie folgt darstellen:

$$N = \prod_{i=1}^{k} p_i \quad , p_1, ..., p_k \text{ Primzahlen}$$

$$N = \prod_{j=1}^{l} q_j \quad , q_1, q_{\tilde{j}}, q_l \text{ Primzahlen}$$

Wir schreiben $N = p_1 \cdot N'$, wobei

$$N' = \prod_{i=2}^{k} p_i$$

Da $p_1|N$ und $N = \prod_{j=1}^{l} q_j$ folgt:

$p_1|q_{\tilde{j}}$ für ein $\tilde{j}$ mit $1 \leq \tilde{j} \leq l$

$\underset{q_{\tilde{j}} \text{ prim}}{\Rightarrow} p_1 = q_{\tilde{j}}$

D.h.

$$N' = \prod_{i=2}^{k} p_i = \prod_{\substack{j=1 \\ j \pm \tilde{j}}}^{l} j_j < N$$

Nach der Definition von N, muss N' eine eindeutige Schreibweise als Produkt von Primzahlen besitzen.

$p_2, ..., p_k$

$q_1, q_2, ..., q_{\tilde{j}\cdot 1}, q_{\tilde{j+1}}, ..., q_l$

Wegen der Eindeutigkeit: $k = l$

und es gibt eine Bijektion zwischen den 'Beiden Zeilen'; Weil $p_1 = q_{\tilde{j}}$, besitzt auch N

Weil $p_1 = q_{\tilde{j}}$, sind $\prod_{i=1}^{k} p_i$ und $\prod_{j=1}^{l} q_j$, bis auf die Reihenfolge der Primzahlen identisch. $\lightning$ zur Eigenschaft von N $\square$

Bemerkung:

Ist $n \in \mathbb{N},\ n \geq 2$, so existieren verschiedene Primzahlen $p_1, ..., p_k \in P$ und natürliche Zahlen $l_1, ..., l_k \in \mathbb{N}$ mit:

$$\boxed{n = \prod_{i=1}^{k} p_i^{l_i} = p_1^{l_1} \cdot p_2^{l_2} \cdot ... \cdot p_k^{l_k}}$$

Beispiele:

$$\begin{aligned} 4 &= 2^2 \\ 6 &= 2 \cdot 3 \\ 8 &= 2^3 = 2 \cdot 2 \cdot 2 \\ 14 &= 2 \cdot 7 \end{aligned}$$

Seien $n, m \in \mathbb{N}$.

Mit Primfaktorzerlegungen:

$$n = \prod_{i=1}^{k} p_i^{l_i}$$

$$m = \prod_{j=1}^{k} p_j^{s_j}$$

$(l_i, s_j \in \mathbb{N}_0,\ p^0 := 1)$

Dann gilt:

$$ggT(n, m) = \prod_{i=1}^{k} p_i^{min(l_i, s_i)}$$

Beispiel:

$$\begin{aligned} n &= 2^2 \cdot 3^3 \cdot 5^7 \\ m &= 2 \cdot 3^4 \cdot 5^5 \\ ggT(n, m) &= 2 \cdot 3^3 \cdot 5^5 \end{aligned}$$

Euclidischer Algorithmus:

Seien $a, b \in \mathbb{N} \quad a \geq b$.

Ziel: berechne $ggT(a, b)$

Beobachtungen:

1) $b|a \Rightarrow ggT(a, b) = b$

2) $a = bt + r \Rightarrow ggT(a, b) = ggT(b, r)$

Beweis:

1) klar

2) jeder gemeinsame Teiler von a und b muss auch $r = a - bt$ teilen. Also $ggT(a, b) \leq ggT(b, r)$

Andererseits:

da jeder Teiler von b und r auch $a = bt + r$ teilt, gilt auch: $ggT(b, r) \leq ggT(a, b)$.

Insgesamt: $ggT(a, b) = ggT(b, r)$ $\square$

Algorithmus Euclid(a, b)

Eingabe: $a \geq b \geq 0$

Ausgabe: $ggT(a, b)$

```
If b=0 then return a
    else return Euclid(b, a mod b)
```

Falls $b = 0$ dann gibt a aus

sonst: gib Euclid$(b, a \ mod \ b)$ aus.

$$\begin{aligned}
&ggT(\underset{a}{348}, \underset{b}{124}) \\
&= ggT(124, \underbrace{348 \ mod \ 124}_{100}) \\
&= ggT(\underset{a}{124}, \underset{b}{100}) \\
&= ggT(100, \underset{\rightarrow 124 \ mod \ 100}{24}) \\
&= ggT(24, \underset{\rightarrow 100 \ mod \ 24}{4}) \\
&= ggT(4, \underset{b \rightarrow 24 \ mod \ 4}{0}) = 4
\end{aligned}$$

Durch 'Rückwärtsrechnen' findet man x und $y \in \mathbb{Z}$:

$\boxed{ax + by = ggT(a, b)}$