Grundlagen der theoretischen Informatik

Vorlesung 10:
Zahlentheorie

Zahlentheorie

Definition

$a \in \mathbb{Z}$ ist ein *Teiler (osztó)* von $b \in \mathbb{Z}$ (Notation: $a|b$), wenn $\exists c \in \mathbb{Z}$ so dass $ac = b$.

Definition

Für $a, b \in \mathbb{Z}^+$ ist $c \in \mathbb{Z}^+$ der *größte gemeinsame Teiler (lnko)* (Notation: $ggT(a, b)$), wenn $c|a$, $c|b$ und für jedes $d \in \mathbb{Z}^+$ mit $d|a$ und $d|b$ gilt, dass $d|c$.

Definition

Für $a, b \in \mathbb{Z}^+$ ist $c \in \mathbb{Z}^+$ das *kleinste gemeinsame Vielfache (lkkt)* (Notation: $kgV(a, b)$), wenn $a|c$, $b|c$ und für jedes $d \in \mathbb{Z}^+$ mit $a|d$ und $b|d$ gilt, dass $c|d$.

Definition

$a \in \mathbb{Z}$, $a > 1$ ist eine *Primzahl*, wenn es keine positiven Teiler außer 1 und a hat.

Definition

$a, b \in \mathbb{Z}^+$ sind *teilerfremd (relatív prímek)*, wenn $ggT(a, b) = 1$.

Satz (Division mit Rest)

Für alle $a, b \in \mathbb{Z}^+$ existieren $q, r \in \mathbb{N}$ eindeutig so dass $a = qb + r$ und $0 \leq r \leq b - 1$. q, r können in Polynomialzeit bestimmt werden.

Euklidischer Algorithmus

Input: $a, b \in \mathbb{Z}^+$, $a > b$.
Output: $ggT(a, b)$.
Ablauf:

$$a = q_1 b + r_1; 0 < r_1 < b$$

$$b = q_2 r_1 + r_2; 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3; 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-1} = q_{n+1} r_n + r_{n+1}; 0 < r_{n+1} < r_n$$

$$r_n = q_{n+2} r_{n+1} + 0$$

$ggT(a, b) = r_{n+1}$.

Der euklidische Algorithmus terminiert in Polinomzeit und liefert den größten gemeinsamen Teiler.

Beispiel: $ggT(1392, 1170) = ?$

$$1392 = 1 \cdot 1170 + 222$$

$$1170 = 5 \cdot 222 + 60$$

$$222 = 3 \cdot 60 + 42$$

$$60 = 1 \cdot 42 + 18$$

$$42 = 2 \cdot 18 + 6$$

$$18 = 3 \cdot 6 + 0$$

$ggT(1392, 1170) = 6$

Lemma

Jede ganze Zahl ≥ 2 kann als das Produkt von Primzahlen aufgeschrieben werden.

Beweis. Vollständige Induktion bzgl. $|z|$. Die Behauptung ist klar wenn $|z| = 2$. Nehmen wir an, dass die Aussage schon für Zahlen $|z| \leq k$ bewiesen wurde. Sei $|z| = k + 1$.
Wenn z eine Primzahl ist, dann sind wir fertig.
Wenn z nicht eine Primzahl ist, dann gibt es zwei ganze Zahlen a, b mit $ab = z$ und $2 \leq |a|, |b| \leq k$. Laut Induktionsbedingung existieren Produkte $a = \prod p_i$, $b = \prod q_j$. Dann $z = ab = \prod p_i \prod q_j$ ist ein Produkt von Primzahlen.

Definition (kanonische Form, Primfaktorzerlegung)

$n \in \mathbb{Z}$, $n \geq 2 \Rightarrow n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, wobei $p_1, \dots, p_k$ verschiedene Primzahlen sind und $\alpha_i > 0$ für jedes $i = 1, \dots, k$.

Bemerkung. Wir kennen keinen effizienten Algorithmus für die Bestimmung der Primfaktoren einer Zahl.

Satz (Fundamentalsatz der Arithmetik)

Jede ganze Zahl ≥ 2 kann als das Produkt von Primzahlen aufgeschrieben werden. Welche Primzahlen darin vorkommen und wie oft eine gegebene Primzahl darin vorkommt ist eindeutig, die Reihenfolge der Primzahlen nicht.

Satz

Sei die kanonische Form von a: $a = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$. Sei $b|a$. Dann ist $b = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k}$, wobei $0 \leq \beta_i \leq \alpha_i$ für jedes $i = 1, \dots, k$.

Sei $n \in \mathbb{Z}^+$. $d(n)$ bezeichnet die Anzahl der positiven Teiler von n.

Satz

Sei die kanonische Form von n: $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$. Dann ist $d(n) = (\alpha_1 + 1) \cdot \dots \cdot (\alpha_k + 1)$.

Beweis. Die Anzahl den Teilern von n ist gleich die Anzahl den $\beta_1, \dots, \beta_k$ Folgen mit $0 \leq \beta_i \leq \alpha_i, \forall i$.

Satz

Seien $a = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ und $b = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k}$, wobei einige α_is oder β_is auch 0 sein können. Dann ist

$ggT(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot \dots \cdot p_k^{\min\{\alpha_k, \beta_k\}}$,

$kgV(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdot \dots \cdot p_k^{\max\{\alpha_k, \beta_k\}}$.

Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis. Nehmen wir indirekt an, dass die Behauptung nicht wahr ist. Sei p die grösste Primzahl. $P = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p + 1$ ist teilerfremd mit $2, 3, \dots, p$. Aber P hat eine kanonische Form, so sie soll ein Primteiler grösser als p haben. Das ist ein Widerspruch.

Satz

Es gibt beliebig große Lücken zwischen nacheinanderfolgenden Primzahlen.

Definition

p und $p + 2$ sind *Primzahlenzwillinge*, wenn sie beide Primzahlen sind.

Es ist unklar, ob es unendlich viele Primzahlenzwillinge gibt.

Kongruenzen

Definition

Seien $a, b, m \in \mathbb{Z}$, $m > 1$. a und b sind *kongruent (kongruens) modulo* m (Notation: $a \equiv b \ (mod \ m)$), wenn $m|a - b$.

Bemerkung: Eine andere äquivalente Definition ist die folgende: $a \equiv b \ (mod \ m)$, wenn ganze Zahlen q_1, q_2, r existieren, so dass $0 \leq r \leq m - 1$ und $a = q_1 m + r$ und $b = q_2 m + r$.

Satz

Wenn $a \equiv b \ (mod\ m)$ und $c \equiv d \ (mod\ m)$, dann gilt:
(1) $a + c \equiv b + d \ (mod\ m)$;
(2) $a - c \equiv b - d \ (mod\ m)$ und
(3) $ac \equiv bd \ (mod\ m)$.

Satz

Sei $ac \equiv bc \ (mod\ m)$, $d = ggT(c, m)$. Dann gilt:
$a \equiv b \ (mod\ \frac{m}{d})$.

Definition

Lineare Kongruenz: $ax \equiv b \ (mod\ m)$.
Hier x ist eine Variable und $a,\ b,\ m$ sind ganze Zahlen.
Alle Lösungen sollen ganz sein!!!!

Beispiel 1: $2x \equiv 3 \ (mod\ 5)$
Die Lösungen sind $\ldots,\ -6,\ -1,\ 4,\ 9,\ 14, \ldots$.
Oder: $x \equiv 4 \ (mod\ 5)$.

Beispiel 1: (PZH2017) $21x \equiv 35 \ (mod\ 68)$
Nach Dividierung mit 7: $3x \equiv 5 \ (mod\ 68)$
$5 \equiv -63 \ (mod\ 68)$: $3x \equiv -63 \ (mod\ 68)$
Nach Dividierung mit 3: $x \equiv -21 \ (mod\ 68)$

Satz

Lineare Kongruenz $ax \equiv b \ (mod \ m)$ ist lösbar genau dann wenn $ggT(a, m)|b$. Wenn x_0 eine Lösung ist, dann sind alle Lösungen modulo m die folgende:

x_0

$x_0 + \frac{m}{ggT(a,m)}$

$x_0 + 2\frac{m}{ggT(a,m)} \ldots$

$x_0 + (ggT(a, m) - 1)\frac{m}{ggT(a,m)}$.

Euklidischer Algorithmus für Lineare Kongruenzen

Input: Lineare Kongruenz $ax \equiv b \ (mod \ m)$

Output: Alle Lösungen wenn sie existieren. Sondern der Algorithmus bestimmt dass es keine Lösung gibt.

Ablauf:

(1) Berechnung von $ggT(a, m) = d$.

(2a) Falls $d \not| b$: es gibt keine Lösung, der Algorithmus terminiert.

(2b) Falls $d|b$: seien $a = \frac{a}{d}$, $b = \frac{b}{d}$, $m = \frac{m}{d}$.

(3)

$$
\begin{array}{lll}
(A) & mx \equiv 0 \ (mod \ m) & \\
(B) & ax \equiv b \ (mod \ m) & \text{sei } m = q_1 a + r_1 \\
(1) & (A) - q_1(B) & \text{sei } a = q_2 r_1 + r_2 \\
(2) & (B) - q_2(1) & \text{sei } r_1 = q_3 r_2 + r_3 \\
\vdots & \vdots & \vdots \\
 & x \equiv x_0 \ (mod \ m) &
\end{array}
$$

Von x_0 können alle Lösungen kalkuliert werden.

Der euklidische Algorithmus terminiert in Polinomzeit.

Beispiel: $21x \equiv 35 \ (mod\ 68)$

$$
\begin{array}{cc}
(A) & 68x \equiv 0 \ (mod\ 68) \\
(B) & 21x \equiv 35 \ (mod\ 68) \qquad 68 = 3 \cdot 21 + 5 \\
(A) - 3 \cdot (B) & 68x - 3 \cdot 21x \equiv 0 - 3 \cdot 35 \ (mod\ 68) \\
(1) & 5x (\equiv -105) \equiv -37 \ (mod\ 68) \qquad 21 = 4 \cdot 5 + 1 \\
(B) - 4 \cdot (1) & 21x - 4 \cdot 5x \equiv 35 - 4 \cdot (-37) \ (mod\ 68) \\
(2) & x (\equiv 183) \equiv 47 \ (mod\ m)
\end{array}
$$

Definition Eulersche φ-Funktion

Für $m \in \mathbb{Z}$, $m > 1$ bezeichne $\varphi(m)$ die Anzahl ganzer Zahlen in $\{1, 2, \ldots, m\}$, die zu m teilerfremd sind.

Beispiele:

$\varphi(12) = 4$	Mit 12 sind die folgende Zahlen teilerfremd: 1, 5, 7, 11.
$\varphi(11) = 10$	11 ist eine Primzahl, alle positive ganze Zahlen sind mit 11 teilerfremd.

Bemerkung: Falls p eine Primzahl ist, dann ist $\varphi(p) = p - 1$.

Satz (Euler-Fermat)

Seien $a, m \in \mathbb{Z}$, $m > 1$, $ggT(a, m) = 1$. Dann gilt:
$a^{\varphi(m)} \equiv 1(\mod m)$.

Satz (kleiner Satz von Fermat)

Sei p eine Primzahl, $a \in \mathbb{Z}$ beliebig. Dann gilt:
$a^p \equiv a(\mod p)$.

Satz

Sei die kanonische Form von n: $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$. Dann ist
$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = n \cdot (1 - \frac{1}{p_1}) \cdot \dots \cdot (1 - \frac{1}{p_k})$.

Beispiel: $12 = 2^2 \cdot 3$.
$\varphi(12) = (2^2 - 2) \cdot (3 - 1) = 4$