Grundlagen der theoretischen Informatik

Übung 10

22. November 2018.

Theorie

Def: $a \in \mathbb{Z}$ ist ein *Teiler* von $b \in \mathbb{Z}$ (Notation: $a|b$), wenn $\exists c \in \mathbb{Z}$ so dass $ac = b$. Für $a, b \in \mathbb{Z}^+$ ist $c \in \mathbb{Z}^+$ der *grösste gemeinsame Teiler* (Notation: $ggT(a, b)$), wenn $c|a$, $c|b$ und für jedes $d \in \mathbb{Z}^+$ mit $d|a$ und $d|b$ gilt, dass $d|c$. Für $a, b \in \mathbb{Z}^+$ ist $c \in \mathbb{Z}^+$ das *kleinste gemeinsame Vielfache* (Notation: $kgV(a, b)$), wenn $a|c$, $b|c$ und für jedes $d \in \mathbb{Z}^+$ mit $a|d$ und $b|d$ gilt, dass $c|d$. $a \in \mathbb{Z}$, $a > 1$ ist eine *Primzahl*, wenn es keine positiven Teiler auSSer 1 und a hat. $a, b \in \mathbb{Z}^+$ sind *teilerfremd*, wenn $ggT(a, b) = 1$.

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

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

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

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

$$\vdots$$

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

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

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

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

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.

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

Behauptung: 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 $i = 1, \dots, k$.

Korollar: Sei $n \in \mathbb{Z}^+$. $d(n)$ bezeichnet die Anzahl der positiven Teiler von n. Sei die kanonische Form von n: $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$. Dann ist $d(n) = (\alpha_1 + 1) \cdot \dots \cdot (\alpha_k + 1)$.

Behauptung: 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: Es gibt unendlich viele Primzahlen.

Def: Seien $a, b, m \in \mathbb{Z}$, $m > 1$. a und b sind *kongruent (kongruens) modulo* m (Notation: $a \equiv b \ (mod\ m)$), wenn $m|a - b$. Äquivalente Definition: $a \equiv b \ (mod\ m)$, 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) $a - c \equiv b - d \ (mod\ m)$; (3) $ac \equiv bd \ (mod\ m)$.
Sei $ac \equiv bc \ (mod\ m)$, $d = ggT(c, m)$. Dann gilt: $a \equiv b \ (mod\ \frac{m}{d})$.

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
$x_0 + \frac{m}{ggT(a,m)}$
$x_0 + 2\frac{m}{ggT(a,m)} \dots$
$x_0 + (ggT(a, m) - 1)\frac{m}{ggT(a,m)}$.

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 $a = \frac{a}{d}$, $b = \frac{b}{d}$, $m = \frac{m}{d}$.

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

Von x_0 können alle Lösungen kalkuliert werden.

Übungen

1. Für welche Primzahlen p werden (a) $p + 10$ und $p + 14$; (b) $p^2 + 2$; (c) $p^2 + 4$ und $p^2 + 6$ Primzahlen sein?
2. Beweisen Sie, dass das Produkt von 6 beliebigen aufeinanderfolgenden Zahlen mit 720 teilbar ist.
3. Beweisen Sie, dass alle positive ganze n Zahlen in Form $n = k^2 \cdot l$ aufgeschrieben werden können, wo k und l positive ganze Zahlen sind und l hat keine Quadratzahl Teiler ausser 1.
4. Berechnen Sie $ggT(372, 504)$ und $ggT(612, 834)$.
5. Öröm és boldogság: ma van Dzsenifer születésnapja. Ezért matek és földrajz helyett Britnivel, a barátnőjével plázába mentek okostelefont nézni. Kipróbálták a legújabb, facebookon agyonlájkolt, minden eddiginél okosabb születésnapi appot és megállapították, hogy Dzsenifernek feltétlenül vennie kell egy rózsaszín szelfibotot a jóképű eladótól, ugyanis ma (2015-ben) az életkora osztója az aktuális évszámnak. Márpedig az app szerint ilyenkor különösen sok szerencse éri a horoszkópokban kellőképpen jártas beavatottakat. Meg tudjuk-e mondani a fizetős appra történő regisztráció nélkül, hogy legutóbb mikor történt ez meg és hogy legközelebb mikor fog ismét bekövetkezni Dzsenifer életében ez a csodálatos, születésnapi konstelláció?
6. Beweisen Sie, dass es unter 5 beliebigen aufeinanderfolgenden Zahlen eine solche gibt, die mit der 4 anderen teilerfremd ist.
7. Welche ist die kleinste solche Zahl n, die $d(n) = 12$ Teiler hat und $3 \nmid n$?
8. Wie viele solche positive ganze Zahlen gibt es, die der Teiler von mindestens einem der Zahlen $n = 2^3 \cdot 7^5 \cdot 11^2$ und $m = 2^5 \cdot 5^3 \cdot 7 \cdot 13$ sind?
9. Sei $n = \Pi_{i=1}^{k} p_i^{\alpha_i}$ die kanonische Form von der positiven ganzen Zahl n. Wie viel ist $\sum_{d|n} \frac{1}{d}$? (V '99) Wie viel ist $\prod_{d|n} \frac{1}{d}$?
10. Welche ist die kleinste positive ganze Zahl n, für welcher $d(n)$ mit 10 teilbar ist?
11. Wie viele positive Teiler haben 10! und $n = \binom{12}{6}$? (pZH '15)
12. Beweisen Sie, dass der Rest bei der Division um 9 einer beliebigen Zahl n und ihrer Quersumme (die Summe der Ziffern) die selbe sind.
13. Was ist der Regel der Division um 8 im Zahlensystem 9?
14. Lösen Sie die folgende lineare Kongruenzen: (a) $202x \equiv 157(203)$, (b) $14x - 4 \equiv 80(21)$, (c) $49^{49}x \equiv 3(15)$. (d) $155x \equiv 7(352)$, (e) $122x \equiv 5(166)$, (f) $122x \equiv 6(166)$.
15. Dzsúlió már régóta gyűjt nagy álmára, hogy volt barátnője, Vanessza mobiltelefonon őrzött arcképét a bicepszére tetováltassa. Legjobb barátja, Rodzser tanácsára, míg össze nem jön az ehhez szükséges 35000 forint, átváltja az ezer forintosokban tartott megtakarítását euróra, amit a Rodzser által ajánlott Rikárdótól (az ismeretségre tekintettel) szuperkedvezményes 330 Ft-os árfolyamon vesz meg. Miután Rikárdó centekkel nem foglalkozik, Dzsúliónak éppen 140 Ft marad a megtakarításából, amiből Rodzserrel közösen lottószelvényt vesznek azzal, hogy a nyereményt majd felezik. Hány euró boldog birtokosának mondhatja magát Dzsúlió a sikeres tranzakció után?
16. Ura születésnapjára Tűzvirág egy 77 gyönggyel díszített, mangalicabőr tokot varrt Vérbulcsú ivótülkéhez. Annyira elégedett volt az eredménnyel, hogy Vérbulcsú hagyományőrző dorombegyüttesének minden tagját is ugyanilyen tokkal lepte meg, hogy jól mutasson a csapat a tarsolylemezek mellett csüngő tülkökkel amikor fellépnek Dobogókőn a táltosünnep 50 személyes központi jurtájában. Mivel a kínai boltban százasával árulják a gyöngyöket, 7 gyöngy kimarad, melyekkel Tűzvirág a hétköznapi pártáját ékesítette. Hányan dorombolnak Vérbulcsú zenekarában? (ZH '15)