§ 6: PRIMZAHLEN UND TEILER

6.1. Bedeutung in der Informatik

Wichtige Algorithmen in der Kryptographie (z.B. RSA-Algorithmus) beruhen auf grundlegenden Ergebnissen der Zahlentheorie:
Es ist einfach, zwei große Primzahlen zu multiplizieren, aber schwierig, eine große Zahl schnell in ihre Primfaktoren zu zerlegen

6.2. Division mit Rest

Zu jeder Zahl $a \in \mathbb{Z}$ und jeder Zahl $b \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$a = qb + r, \qquad 0 \leq r < b$$

Wir nennen q den Quotienten und r den Rest der Division von a durch b.
a heißt Dividend, b ist der Divisor.

Beweis: Betrachte Fall $a \geq 0$. Sei q die größte ganze Zahl mit $qb \leq a$. Dann gibt es ein $r \geq 0$ mit $a = qb + r$. Ferner gilt $r < b$, denn andernfalls wäre q nicht maximal gewesen.
Den Fall $a < 0$ zeigt man analog. $\square$.

Besonders interessant ist der Fall $r = 0$ und die Erweiterung $b \in \mathbb{Z} \setminus \{0\}$:

6.3. Def.: Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Wir sagen, b teilt a ($b \mid a$), wenn es ein $q \in \mathbb{Z}$ gibt mit $a = qb$.
In diesem Fall heißt b Teiler von a.
Falls b kein Teiler von a ist, schreiben wir $b \nmid a$
Eine natürliche Zahl $p > 1$ heißt Primzahl („ist prim"), wenn sie nur die trivialen Teiler $\pm p, \pm 1$ besitzt
Zahlen, die nicht prim sind, heißen zusammengesetzt.

6.4. Beispiele

a) $-7 \mid 63$, denn $63 = (-9)(-7)$
b) 11 ist prim.
c) 35 ist zusammengesetzt: $35 = 5 \cdot 7$

Folgende Teilbarkeitseigenschaften sind leicht zu zeigen.

6.5. Satz (Teilbarkeitsregeln)

a) Aus $c \mid b$ und $b \mid a$ folgt $c \mid a$.
(Bsp.: $3 \mid 12$ und $12 \mid 24 \Rightarrow 3 \mid 24$).
b) Aus $b_1 \mid a_1$ und $b_2 \mid a_2$ folgt $b_1 b_2 \mid a_1 a_2$.
(Bsp.: $2 \mid 4$ und $7 \mid 21 \Rightarrow 14 \mid 84$)
c) Aus $b \mid a_1$ und $b \mid a_2$ folgt $b \mid \alpha a_1 + \beta a_2 \quad \forall \alpha, \beta \in \mathbb{Z}$.
(Bsp.: $3 \mid 6$ und $3 \mid 9 \Rightarrow 3 \mid (2 \cdot 6 + 3 \cdot 9)$)
d) Aus $a \mid b$ und $b \mid a$ folgt $|a| = |b|$.

6.6. Satz (Fundamentalsatz der Zahlentheorie)

Jede nat. Zahl $n > 1$ ist als Produkt endlich vieler (nicht notwendig verschiedener) Primzahlen darstellbar (Primzahlfaktorisierung). Diese Zerlegung ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis: siehe z.B. Brill: Math. f. Informatiker, S. 60-63.

Beispiel: $84 = 2^2 \cdot 3 \cdot 7$ ist eine Primzahlfaktorisierung.

6.7. Primzahlfaktorisierung großer Zahlen ist aufwändig. Ein einfaches (nicht sehr effizientes) Verfahren zur Primzahlfaktorisierung ist das Sieb des Erathostenes:

- Um zu prüfen, ob n prim ist, genügt es für jede Primzahl $p \le \sqrt{n}$ zu testen, ob $p \mid n$.
- Findet man einen Teiler p, setzt man das Verfahren mit $\frac{n}{p}$ fort.

6.8. Beispiel

Zur Primzahlfaktorisierung von 84 genügt es, alle Primzahlen $\le \sqrt{84} \approx 9.17$ zu testen, d.h. $2, 3, 5, 7$.

Wegen $7 \mid 84$, fährt man mit $\frac{84}{7} = 12$ fort

Hier müssen nur noch die Faktoren 2,3 getestet werden

$\frac{12}{3} = 4$

$4 = 2 \cdot 2$

$\Rightarrow 84 = 2^2 \cdot 3 \cdot 7$

6.9. Def.: Sind $a, b, d \in \mathbb{Z}$ und gilt $d | a$ und $d | b$, so heißt d gemeinsamer Teiler von a und b.

Wenn für jeden anderen gemeinsamen Teiler c von a und b gilt $c | d$, dann heißt d größter gemeinsamer Teiler (ggT, engl. gcd: greatest common divisor).

$$d = \operatorname{ggT}(a, b).$$

6.10. Beispiel

$\operatorname{ggT}(84, 66) = 6$, denn 84 und 66 haben die Primfaktorzerlegung

$$84 = 2^2 \cdot 3 \cdot 7$$
$$66 = 2 \cdot 3 \cdot 11$$

ggT ist Produkt der gemeinsamen Faktoren 2 und 3.

Gibt es schnelle Algorithmen zur Bestimmung des ggT?

Hierzu benötigen wir einen Hilfssatz (Lemma)

6.11. Lemma (Eigenschaften des ggT)

Seien $a, b, q \in \mathbb{Z}$. Dann gilt:

a) $d = \operatorname{ggT}(a, b) \iff d = \operatorname{ggT}(b, a - qb)$

b) Ist $a = qb$, so gilt $b = \operatorname{ggT}(a, b)$

Beispiel:

a) $6 = \operatorname{ggT}(84, 66) \iff 6 = \operatorname{ggT}(66, 84 - 1 \cdot 66) = \operatorname{ggT}(66, 18)$.

b) $84 = 7 \cdot 12 \Rightarrow 12 = \operatorname{ggT}(84, 12)$.

Beweis:

a) Wir zeigen nur „$\Rightarrow$" („$\Leftarrow$" geht ähnlich)

Sei $d = ggT(a,b)$

Aus $d|a$ und $d|b$ folgt mit 6.5(c): $d \mid a-qb$.

Also ist d gemeinsamer Teiler von b und $a-qb$.

Um zu zeigen, dass d auch größter gem. Teiler ist, betrachten wir weiteren gem. Teiler c und zeigen $c|d$:

$$\left.\begin{array}{l} c|b \Rightarrow c|qb \\ c|a-qb \end{array}\right\} \Rightarrow c|(a-qb)+qb$$

$$\left.\begin{array}{r} \text{d.h. } c|a \\ \text{nach Vor.: } c|b \end{array}\right\} \Rightarrow c|d \text{ da } d = ggT(a,b)$$

b) Prüfe Def. des ggT für b nach:

Aus $a = qb$ folgt: $b|a$.

Wegen $b|b$ ist b gemeins. Teiler von a und b (nach 6.5.(c)).

Sei c weiterer gem. Teiler von a und b: $c|a$, $c|b$

Wegen $c|b$ ist $b = ggT(a,b)$. □

Dieses Lemma bildet die Grundlage des Euklidischen Algorithmus'.

6.12. Satz (Euklidischer Algorithmus zur Berechnung des ggT)

Für die natürl. Zahlen $a > b$ setzen wir $r_0 := a$, $r_1 := b$ und berechnen folgende Divisionen mit Rest:

$$\begin{array}{ll} r_0 = q_0 r_1 + r_2 & (0 < r_2 < r_1) \\ r_1 = q_1 r_2 + r_3 & (0 < r_3 < r_2) \\ \vdots & \vdots \\ r_{n-2} = q_{n-2} r_{n-1} + r_n & (0 < r_n < r_{n-1}) \\ r_{n-1} = q_{n-1} r_n & \end{array}$$

Dann ist $r_n = ggT(a,b)$.

6.13. Beispiel

Ges.: $ggT(133, 91)$

Euklid. Alg.:
$$133 = 1 \cdot 91 + 42$$
$$91 = 2 \cdot 42 + 7$$
$$42 = 6 \cdot 7$$

Also ist $7 = ggT(133, 91)$.

6.14. Beweis von Satz 6.12

Die Reste $r_j > 0$ werden in jedem Schritt echt kleiner.
$\Rightarrow$ Algorithmus terminiert nach endlich vielen Schritten mit Rest 0.

Für $ggT(a,b) = ggT(r_0, r_1)$ gilt nach Lemma 6.11 (a):

$$ggT(r_0, r_1) = ggT(r_1, \underbrace{r_0 - q_0 r_1}_{r_2}) = ggT(r_1, r_2)$$

$$ggT(r_1, r_2) = ggT(r_2, \underbrace{r_1 - q_1 r_2}_{r_3}) = ggT(r_2, r_3)$$

$$\vdots$$

$$ggT(r_{n-2}, r_{n-1}) = ggT(r_{n-1}, \underbrace{r_{n-2} - q_{n-2} r_{n-1}}_{r_n}) = ggT(r_{n-1}, r_n).$$

und somit $ggT(a,b) = ggT(r_{n-1}, r_n)$.

Da $r_{n-1} = q_{n-1} r_n$, folgt mit Lemma 6.11 (b):

$$r_n = ggT(r_{n-1}, r_n)$$

und daher $r_n = ggT(a,b)$. $\square$