§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 leicht, zwei große Primzahlen zu multiplizieren, aber schwierig, eine große Zahl schnell in ihre Primfaktoren zu zerlegen.

6.2. Satz und Definition (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

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

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 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 ähnlich. □

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 ($b|a$) wenn es eine ganze Zahl q 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 ("p ist prim") wenn sie nur die trivialen Teiler $\pm p, \pm 1$ besitzt. Zahlen, die nicht prim sind, heißen zusammengesetzt.

Bem.: In 3.6 haben wir gesehen, dass es unendlich viele Primzahlen gibt.

6.4. Beispiele

a) $-7 \mid 63$, denn $(-7)(-9) = 63$

b) 11 ist prim. c) 35 ist zusammengesetzt: $35 = 5 \cdot 7$.

Folgende Teilbarkeitseigenschaften sind leicht zu zeigen:

6.5. Satz (Teilbarkeitsregeln)

a) Aus $c|b$ und $b|a$ folgt $c|a$
(Bsp.: $3|12$ und $12|24 \Rightarrow 3|24$)

b) Aus $b_1|a_1$ und $b_2|a_2$ folgt $b_1 b_2 | a_1 a_2$
(Bsp.: $2|4$ und $7|21 \Rightarrow 14|84$)

c) Aus $b|a_1$ und $b|a_2$ folgt $b | \alpha a_1 + \beta a_2 \quad \forall \alpha, \beta \in \mathbb{Z}$.
(Bsp.: $3|6$ und $3|9 \Rightarrow 3|(2 \cdot 6 + 3 \cdot 9)$)

d) Aus $a|b$ und $b|a$ folgt $|a| = |b|$.

6.6. Satz (Fundamentalsatz der Zahlentheorie)

Jede natürliche 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 Brill: Math. f. Informatiker, S. 60 - 63.

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

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

- Um zu prüfen, ob n prim oder zusammengesetzt ist, genügt es, für jede Primzahl $p \leq \sqrt{n}$ zu testen, ob $p \mid n$.
- Findet man einen Teiler p, kann man das Verfahren mit n/p fortsetzen.

6.8. Beispiel:

Zur Primzahlfaktorisierung von 84 genügt es, alle Primzahlen $\leq \sqrt{84} \approx 9{,}17$ zu testen, d.h. 2, 3, 5, 7

Wegen $7 \mid 84$, fällt man mit Fakt. von $84/7 = 12$ fort

Hier müssen nur noch die Fakt. 2, 3 getestet werden

$12/3 = 4$

$4 = 2 \cdot 2$.

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

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):

$$c = ggT(a,b).$$

Bsp.: $ggT(84,66) = 6$, denn 84 und 66 haben die Primfaktorzerl.

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

ggT ist Produkt der gemeins. Faktoren 2 und 3.

Gibt es schnelle Algorithmen zur Bestimmung des ggT? Hierzu benötigen wir einen Hilfssatz (Lemma).

6.10. Lemma (Eigenschaften des ggT)

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

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

b) Ist $a = qb$, so gilt $b = ggT(a,b)$.

Beispiel:

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

b) Ist $84 = 7 \cdot 12 \Rightarrow 12 = ggT(84, 12)$

Beweis

(a) Wir zeigen nur „⇒". („⇐" geht ähnlich)

Sei $d = ggT(a,b)$.

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

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

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

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

$$\left.\begin{array}{l} c \mid a \\ c \mid b \end{array}\right\} \Rightarrow c \mid d$$

da $d = ggT(a,b)$

(b) Prüfe Def. des ggT für b nach:

Aus $a = qb$ folgt $b \mid a$. Wegen $b \mid b$ ist b gemeins. Teiler von a und b.

Ist c weiterer gem. Teiler von a und b gilt $c \mid a$ und $c \mid b$.

Wegen $c \mid b$ ist $b = ggT(a,b)$. □

Dieses Lemma bildet die Grundlage des Euklidischen Algorithmus!

6.11 Satz (Euklidischer Algorithmus)

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

$$r_0 = q_0 r_1 + r_2 \qquad (0 < r_2 < r_1)$$

$$r_1 = q_1 r_2 + r_3 \qquad (0 < r_3 < r_2)$$

$$\vdots$$

$$r_{n-2} = q_{n-2} r_{n-1} + r_n \qquad (0 < r_n < r_{n-1})$$

$$r_{n-1} = q_{n-1} r_n$$

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

6.12. Beispiel

$ggT(133, 91)$

$$133 = 1 \cdot 91 + 42$$
$$91 = 2 \cdot 42 + 7$$
$$42 = 6 \cdot 7$$

$7 = ggT(133, 91)$.

6.13. Warum liefert der Euklidische Algorithmus den ggT?

Beweis von Satz 6.11:

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

Falls $ggT(a,b) = ggT(r_0, r_1)$ ex., gilt nach Lemma 6.10.(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 6.10.(b):

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

und somit $r_n = ggT(a,b)$.

□