Euklidischer Algorithmus

Ermitteln des größten gemeinsamen Teilers mit Euklid:

```
function ggT(m, n)
begin
        if m = 0 then return n
        else return ggT(n mod m, m) fi
end
```

Hierbei ist $m \geq 0$ und $n \geq 0$ vorausgesetzt.

Man sieht leicht, dass die folgende Gleichheit gilt:

$$ggT(n \bmod m, m) = ggT(m, n)$$

Denn jeder Teiler von m und n teilt auch $n \bmod m$, und jeder Teiler von m und $n \bmod m$ teilt auch n.

Daraus folgt unmittelbar die Korrektheit des Algorithmus.

(Die Termination des Algorithmus ist klar, da die Zahlen immer kleiner werden.)

Beispiele

Wir illustrieren die Arbeit des Euklidischen Algorithmus bei der Berechnung des ggT von 68 und 171:

$$\begin{aligned} 171 &= 2 \cdot 68 + 35 \\ 68 &= 1 \cdot 35 + 33 \\ 35 &= 1 \cdot 33 + 2 \\ 33 &= 16 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 171 &= 3 \cdot 68 - 33 \\ 68 &= 2 \cdot 33 + 2 \\ 33 &= 16 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Rechts die Variante mit negativen Zahlen – der ggT ist 1 und wird in beiden Varianten korrekt berechnet.

Zur Übung berechnen wir noch $ggT(210, 78)$:

$$\begin{aligned} 210 &= 2 \cdot 78 + 54 \\ 78 &= 1 \cdot 54 + 24 \\ 54 &= 2 \cdot 24 + 6 \\ 24 &= 4 \cdot 6 + 0 \end{aligned}$$

Also: $ggT(210, 78) = 6$

Lemma von Bézout

Das Lemma von Bézout besagt, dass man $ggT(m,n)$ immer als Linearkombination von m und n darstellen kann:

Lemma: Für alle $m, n \in \mathbb{Z}$ existieren $a, b \in \mathbb{Z}$, so dass

$$ggT(m,n) \;=\; am + bn$$

Beweis: Es sei ohne Einschränkung $m > n > 0$.

Mit Euklids Algorithmus erhalten wir Reste $r_0 > r_1 > \cdots > r_k$, so dass $r_0 = m$, $r_1 = n$, $r_k = 0$, $r_{k-1} = ggT(m,n)$ und für alle $1 \leq i < k$:

$$r_{i-1} = q_i r_i + r_{i+1}$$

Damit ist r_{k-1} eine Linearkombination von r_{k-2} und r_{k-3}, und man kann induktiv schließen, dass r_{k-1} auch eine Linearkombination von $r_1 = n$ und $r_0 = m$ ist. Da aber $r_{k-1} = ggT(m,n)$ ist, erhalten wir die Behauptung.

Zwei Aufgaben

Aufgabe 1.1: Zeige, dass $\log_{10}(p) \notin \mathbb{Q}$ für beliebige Primzahl p.

Lösung: Wir führen einen Widerspruchsbeweis.
Angenommen, $\log_{10}(p) = \frac{a}{b}$ mit $a, b \in \mathbb{N}$.
Dann folgt: $p^b = (10^{\log_{10}(p)})^b = 10^a = 2^a \cdot 5^a$.
Damit müssten sowohl 2, als auch 5 Teiler von p^b, und damit von p sein, ein Widerspruch, da ja p eine Primzahl ist!

Aufgabe 1.2:

a) Berechne $x, y \in \mathbb{Z}$ mit $ggT(35, 56) = x \cdot 35 - y \cdot 56$.

b) Und jetzt dasselbe für $x, y \in \mathbb{N}$.

Bitte selbst lösen. Zur Kontrolle die Ergebnisse: $7 = (-3) \cdot 35 - (-2) \cdot 56$
und $7 = 53 \cdot 35 - 33 \cdot 56$.

Eindeutige Primfaktorzerlegung

Die folgende Aussage ist eine Folge von Bézout's Lemma:

$$ggT(n, m_1) = 1 \ \wedge \ ggT(n, m_2) = 1 \quad \Longrightarrow \quad ggT(n, m_1 m_2) = 1$$

Denn: Aus $an + bm_1 = 1 = cn + dm_2$ folgt

$$1 = (an + bm_1)(cn + dm_2) = (anc + bm_1 c + adm_2)n + bd(m_1 m_2)$$

Also ist jeder Teiler von n und $m_1 m_2$ auch Teiler der 1, d.h. $ggT(n, m_1 m_2) = 1$.

Satz: Sei $n \in \mathbb{N}$ und $n > 0$. Dann lässt sich n eindeutig darstellen als

$$n = \prod_{p \text{ Primzahl}} p^{n_p}$$

Dabei ist $n_p \neq 0$ genau dann, wenn p Teiler von n ist.

Beweis

Für $n = 1$ existiert nur die Darstellung $1 = \prod p^0$, d.h. $n_p = 0$ für alle Primzahlen p.
Sei nun $n > 1$, dann existiert eine Primzahl p, die n teilt.
Nach Induktionsvoraussetzung hat n/p eine Primfaktorzerlegung, also auch n, da es $p \cdot (n/p)$ ist. Zu zeigen bleibt die Eindeutigkeit:

Angenommen, es gibt zwei verschiedene Primfaktorzerlegungen von n, etwa

$$\prod p^{n_p} = \prod p^{n'_p}$$

dann dividieren wir beide Seiten durch gemeinsame Primteiler, bis es keine solchen mehr gibt. Nun haben wir zwei Produkte von Primzahlen, wobei keine Primzahl auf beiden Seiten vorkommt. Andererseits können beide Produkte nicht leer sein, ihr Wert ist also größer als 1. Ein beliebiger Primteiler des einen Produkts teilt aber nach der Folgerung aus Bézout's Lemma das andere Produkt nicht, da er keine der darin enthaltenen Primzahlen teilt, und folglich auch nicht deren Produkt.

Das ist ein Widerspruch, da beide Seiten gleich sind!

Modulare Arithmetik

Wir rechnen mit den sogenannten *Restklassen:*

Es sei $n \in \mathbb{N}$, $n \geq 1$. Betrachte für $k \in \mathbb{Z}$ die Menge $k + n\mathbb{Z}$:

$$k + n\mathbb{Z} = \{\ldots, k-2n, k-n, k, k+n, k+2n, k+3n, \ldots\}$$

Beachte: $(k + n\mathbb{Z}) \cap (\ell + n\mathbb{Z}) \neq \emptyset \iff k + n\mathbb{Z} = \ell + n\mathbb{Z} \iff n \mid (k - \ell)$

Wir definieren die Äquivalenzrelation $\equiv \pmod{n}$ durch

$$k \equiv \ell \mod n \iff k \in \ell + n\mathbb{Z}$$

Man überprüfe, dass das wirklich eine Äquivalenzrelation ist.

Zur Beachtung: Das ist zu unterscheiden von der Informatik-spezifischen Notation bei der durch $k \bmod n$ die eindeutig bestimmte nichtnegative Zahl kleiner als n gemeint ist, die in $k + n\mathbb{Z}$ liegt.

Restklassenring $\mathbb{Z}/n\mathbb{Z}$

Aus den Restklassen bilden wir den *Restklassenring* $\mathbb{Z}/n\mathbb{Z}$:

Addition:

$$(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) = k + \ell + n\mathbb{Z}$$

Für diese Definitionen ist jeweils die Wohldefiniertheit zu prüfen. (Bitte selbst machen.)

Multiplikation:

$$(k + n\mathbb{Z}) \cdot (\ell + n\mathbb{Z}) = k \cdot \ell + n\mathbb{Z}$$

Die Gültigkeit der Ringaxiome ist leicht nachzuweisen.

Die *multiplikative Gruppe* in $\mathbb{Z}/n\mathbb{Z}$ besteht aus den invertierbaren Elementen (bzgl. der Multiplikation), bezeichnet mit $(\mathbb{Z}/n\mathbb{Z})^*$.

Die Elemente von $(\mathbb{Z}/n\mathbb{Z})^*$ werden auch als *Einheiten* im Ring $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.

Wichtige Eigenschaften

Für den Ring $\mathbb{Z}/n\mathbb{Z}$ und seine Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ gilt:

Satz: a) $(\mathbb{Z}/n\mathbb{Z})^* = \{k + n\mathbb{Z} \mid ggT(k,n) = 1\}$

b) $\mathbb{Z}/n\mathbb{Z}$ ist Körper, gdw. n ist Primzahl

c) $x \mapsto kx$ auf $\mathbb{Z}/n\mathbb{Z}$ bijektiv, gdw. $ggT(k,n) = 1$

Beweis: a) k ist invertierbar genau dann, wenn ein a existiert mit $ak \equiv 1 \bmod n$, also genau dann, wenn a und b existieren mit $ak = 1 + bn$, also genau dann, wenn 1 eine Linearkombination von k und n ist, also genau dann, wenn k und n teilerfremd sind.

b) $\mathbb{Z}/n\mathbb{Z}$ ist Körper genau dann, wenn alle $k \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ invertierbar sind, also genau dann, wenn alle k mit $1 \leq k < n$ teilerfremd zu n sind, also genau dann, wenn n eine Primzahl ist.

c) Wenn $ggT(k,n) = 1$ ist, hat k ein Inverses, d.h. $x \mapsto kx$ hat eine Umkehrabbildung. Also ist die Abbildung bijektiv.
Wenn aber $ggT(k,n) = m > 1$, dann ist $k \cdot n/m = 0 = k \cdot 0$, d.h. die Abbildung ist nicht injektiv, da $0 < n/m < n$, also $n/m \neq 0$.

Ein zentrales Lemma

Lemma: Es seien m, n zwei teilerfremde ganze Zahlen.
Die folgende Abbildung π ist surjektiv:

$$\pi\colon\ \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

Zwischen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ wird dadurch eine bijektive Abbildung induziert:

$$(x \bmod mn) \mapsto (x \bmod m, x \bmod n)$$

Die erste Aussage besagt, dass für $ggT(m, n) = 1$ zwei gleichzeitige Kongruenzen in $\mathbb{Z}$ immer lösbar sind, d.h. $\forall a, b \in \mathbb{Z}\ \exists x \in \mathbb{Z}$, so dass $x \equiv a \bmod m$ und $x \equiv b \bmod n$.

Die zweite Aussage bedeutet, dass die Abbildung surjektiv bleibt, wenn man sich auf die Zahlen $\{0, \ldots, mn - 1\}$ beschränkt. In diesem Fall wird die Abbildung sogar injektiv, also ist sie bijektiv.

Beweis des Lemmas

Wir beginnen mit der ersten Aussage, der Surjektivität von π:

Zu gegebenen ganzen Zahlen y und z suchen wir eine ganze Zahl x, so dass $\pi(x) = (y + m\mathbb{Z}, z + n\mathbb{Z})$ gilt.

Per Definition ist $\pi(x) = (x + m\mathbb{Z}, x + n\mathbb{Z})$. Zu zeigen ist also, dass es eine ganze Zahl x gibt, so dass $x + m\mathbb{Z} = y + m\mathbb{Z}$ und $x + n\mathbb{Z} = z + n\mathbb{Z}$, d.h. m teilt $x - y$ und n teilt $x - z$.

Da m und n teilerfremd sind, gibt es a, b mit $am + bn = 1$.

Wir wählen $x = zam + ybn$ und überprüfen, dass diese Zahl tatsächlich unsere Bedingungen erfüllt.

$$x - y = zam + y(bn - 1) = zam - yam = (za - ya)m$$
$$x - z = z(am - 1) + ybn = -zbn + ybn = (yb - zb)n$$

Also ist m Teiler von $x - y$ und n Teiler von $x - z$, wie verlangt.

Beweis (Forts.)

Nun fehlt noch der Beweis, dass die Einschränkung auf $\mathbb{Z}/mn\mathbb{Z}$ bijektiv ist.

1. Injektivität:

Sei $(x + m\mathbb{Z}, x + n\mathbb{Z}) = (y + m\mathbb{Z}, y + n\mathbb{Z})$, d.h. m teilt $x - y$ und n teilt $x - y$.
Da m und n teilerfremd sind, teilt auch mn die Differenz $x - y$.
Aber das bedeutet, dass in $\mathbb{Z}/mn\mathbb{Z}$ die Gleichheit $x = y$ gilt.

2. Surjektivität:

Sowohl der Urbildbereich $\mathbb{Z}/mn\mathbb{Z}$, wie auch der Bildbereich $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ haben mn Elemente. Bei endlichen gleichgroßen Bereichen ist aber jede injektive Abbildung automatisch auch surjektiv.

Damit ist die Bijektivität gezeigt.