Algorithmus von Euklid

ggT(a,b):

$$a = q_1 \cdot b + r_1$$
$$b = q_2 \cdot r_1 + r_2$$
$$\vdots$$
$$r_{n-1} = q_* \cdot r_n + 0$$

ggT$(a,b) = r_n$

Multiplikativ Inverses x^{-1} in $\mathbb{Z}/n\mathbb{Z}$

$x \cdot x^{-1} \equiv 1 \bmod n$

Beispiel mit $x=31$ und $n=245$: Gesucht ist $31 \cdot x \equiv 1 \bmod 245 \Leftrightarrow 31 \cdot x + 245 \cdot y \equiv 1$

$245 = 7 \cdot 31 + 28$	$= -9 \cdot 31 + 10 \cdot (245 - 7 \cdot 31)$	$= 10 \cdot 245 \boxed{-79} \cdot 31$	$\uparrow$
$31 = 1 \cdot 28 + 3$	$= 28 - 9 \cdot (31 - 1 \cdot 28)$	$= -9 \cdot 31 + 10 \cdot 28$	$\uparrow$
$28 = 9 \cdot 3 + 1$	$1 = 28 - 9 \cdot 3$		$\uparrow$

$-79 \equiv 166$

166 ist das multiplikativ Inverse von 31 in $\mathbb{Z}/245\mathbb{Z}$

Kleinstes gemeinsames Vielfaches kgV(a,b)

ggT$(a,b) \cdot$ kgV$(a,b) = a \cdot b$

Beispiel:

$$\text{kgV}(120,315) = \text{kgV}(2^3 \cdot 3 \cdot 5, 3^2 \cdot 5 \cdot 7)$$
$$= 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$$

Berechne $ax+by=c$ mit $x,y \in \mathbb{Z}$

1. Berechne ggT(a,b) = ggT$(-a,b)$
2. Falls ggT$(a,b) \nmid c$, dann unlösbar.
   Satz.
   $$\forall a,b \in \mathbb{N}.\ \forall x,y \in \mathbb{Z}.\ \exists z \in \mathbb{Z}.\ x \cdot a + y \cdot b = z \cdot \text{ggT}(a,b)$$
3. Berechne Bezout-Koeffizienten: ggT$(a,b) = a \cdot x' + b \cdot y'$
   Falls ggT$(a,b) \neq 1$, dann
   $$\frac{a}{\text{ggT}(a,b)} \cdot x + \frac{b}{\text{ggT}(a,b)} \cdot y = \frac{c}{\text{ggT}(a,b)}$$
4. Berechne Partikularlösung, angenommen $ax' + by' = 1 = \text{ggT}(a,b)$
   $$q \cdot \text{ggT}(a,b) = c$$
   $$\Rightarrow a \cdot (q \cdot x') + b \cdot (q \cdot y') = q \cdot ggT(a,b) = c$$
   $$\Rightarrow (x_0, y_0) = (q \cdot x', q \cdot y') \text{ist Partikularlösung}$$
5. Berechne alle Lösungen: $\mathcal{L} = (x_o + t \cdot b, y_0 - t \cdot a) | t \in \mathbb{Z}$
   Löse nach t:
   $$x_0 + t \cdot b \geq 0$$
   $$y_0 - t \cdot a \geq 0$$

Beispiel: $6x + 4y = 14$:

1. ggT$(6,4) = 2 = 1 \cdot 6 + y' \cdot 4$
2. $2 | 14 \rightarrow$ lösbar
3. $q \cdot 2 = 14$, also $q = 7$
   Partikularlösung $(7 \cdot 1, 7 \cdot (-1)) = (7, -7)$
4. Lösungsmenge
   $$\mathcal{L} = \{(7 + (4/2) \cdot t, -7 + (4/2) \cdot t) \mid t \in \mathbb{Z}\}$$

Stellenwertsysteme

Dezimalsystem → b-System Beispiel: 521 zur Basis 3:

$$521 = 201022_{(3)}$$

$521 = 173 \cdot 3 +$	$2 \uparrow$
$173 = 57 \cdot 3 +$	$2 \uparrow$
$57 = 19 \cdot 3 +$	$0 \uparrow$
$19 = 6 \cdot 3 +$	$1 \uparrow$
$6 = 2 \cdot 3 +$	$0 \uparrow$
$2 = 0 \cdot 3 +$	$2 \uparrow$

Dezimalbruchentwicklung

Bestimme Art der Dezimalbruchentwicklung (endlich, rein- oder gemischtperiodisch) von $\frac{n}{m}$

1. Bruch vollständig kürzen. (explizit hinschreiben!)
2. Faktorisiere Nenner

   Satz. *Ein Bruch $\frac{n}{m}$ mit $m < n$ und* ggT$(m,n) = 1$ *hat*

   ***endliche* Dezimalbruchentwicklung** *mit s Stellen, wenn $n = 2^a \cdot 5^b$ mit $s = \max(a,b)$*
   ***reinperiodische* Dezimalbruchentwicklung** *mit Periodenlänge s, wenn* ggT$(n,10) = 1$ *mit $s = \min(s,n) \mid (10^s - 1)$*
   ***gemischtperiodische* Dezimalbruchentwicklung** $0{,}p_1 \ldots p_t \overline{q_1 \ldots q_s}$, *wenn $n = n_1 \cdot n_2$ mit $n_1, n_2 > 1$ und* $\min(t, n_1) \mid 10^t$, ggT$(n_2, 10) = 1$ *und s als Periodenlänge von $\frac{1}{n_2}$*

Periodische Zahl als Bruch

Beispiel: Stelle $0{,}\overline{0456}$ als Bruch dar.

Mit $z = 456$ und der Periodenlänge $s = 4$

$$0{,}\overline{0456} = \frac{456}{10^s - 1} = \frac{456}{9999}$$

Kettenbruchdarstellung

Beispiel: Kettenbruchdarstellung von $\frac{162}{355}$

$$162 = \boxed{0} \cdot 355 + 162$$
$$355 = \boxed{5} \cdot 162 + 7$$
$$31 = \boxed{4} \cdot 7 + 3$$
$$7 = \boxed{2} \cdot 3 + 1$$
$$3 = \boxed{3} \cdot 1 + 0$$

$$\frac{162}{355} = 0 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{3}}}}}$$

φ, Euler, Fermat

Satz (von Euler)**.** *Seien a,m teilerfremd, dann* $a^{\varphi(m)} \equiv 1 \bmod m$

Korollar (vom kleinen Fermat)**.** *Für $a \in \mathbb{N}$, p prim, gilt:* $a^p \equiv a \bmod p$

Für Primzahlen $p,n \geq 1$

$$\varphi(p^n) = p^{n-1} \cdot (p-1)$$

Für $\text{ggT}(a,b) = 1$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

Satz (eulersche φ-Funktion)**.**

$$\varphi(n) = \Pi_{p|n} p^{k_p - 1}(p-1)$$

Beispiel: $\varphi(72) = \varphi(2^3 \cdot 3^2) = 2^{3-1} \cdot (2-1) \cdot 3^{2-1} \cdot (3-1) = 24$

a^b in $\mathbb{Z}/m\mathbb{Z}$ Wenn a,m teilerfremd: $a^{\varphi(m)} \equiv 1$

Generell: Fast Modular Exponentation

Beispiel: $7^{19} \bmod 17$

$19 = 10011_{(2)}$

$1 \Rightarrow 1^2$	$\cdot 7 \bmod 17 \equiv$	7
$0 \Rightarrow 7^2$	$\bmod 17 \equiv$	15
$0 \Rightarrow 15^2$	$\bmod 17 \equiv$	4
$1 \Rightarrow 4^2$	$\cdot 7 \bmod 17 \equiv$	17
$1 \Rightarrow 10^2$	$\cdot 7 \bmod 17 \equiv$	$\boxed{3}$

Chinesischer Restesatz

$$x \equiv 5 \bmod 11$$
$$x \equiv 6 \bmod 14$$
$$x \equiv 7 \bmod 15$$

$m = 11 \cdot 14 \cdot 15$	$= 2310$
$q_1 = 14 \cdot 15$	$= 210$
$q_2 = 11 \cdot 15$	$= 165$
$q_3 = 11 \cdot 14$	$= 154$

in $\mathbb{Z}/11\mathbb{Z}$: $\overline{q_1} = \overline{210} = 1$ $\qquad \Rightarrow q_1' = 1$

in $\mathbb{Z}/14\mathbb{Z}$: $\overline{q_2} = \overline{165} = \overline{11}$ $\qquad \Rightarrow \overline{11} \cdot \underbrace{\overline{9}}_{\text{Inverses}} \equiv 1 \Rightarrow q_2' = 9$

in $\mathbb{Z}/15\mathbb{Z}$: $\overline{q_3} = \overline{154} = \overline{4}$ $\qquad \Rightarrow \overline{4} \cdot \overline{4} \equiv 1 \Rightarrow q_2' = 9$

$$\begin{aligned} x &= a_1 \cdot q_1 \cdot q_1' + \ldots \\ &= 5 \cdot 210 \cdot 1 + 6 \cdot 165 \cdot 9 + 7 \cdot 154 \cdot 4 \\ &= 14272 \equiv 412 \bmod 2310 \end{aligned}$$

Eindeutige Lösung $\overline{x} \equiv \overline{412}$

Teilbarkeitsregeln

Endstellenregeln

Satz. *Sei $t \mid 10^s$, dann gilt:*

$$z_n \ldots z_0 \equiv z_{s-1} \ldots z_0 \bmod t$$

Beispiel: $4 \mid 100$*:*

$$4 \mid 87954236 \Leftrightarrow 4 \mid 36$$

Quersummenregeln

Für $t \mid 9$:

$$z_n \ldots z_0 \equiv z_n + \cdots + z_0 \bmod t$$

Für $t \mid 99$:

$$z_n \ldots z_0 \equiv z_n z_{n-1} + \cdots + z_1 z_0 \bmod t$$

Beispiel: $11 \mid 21748 \Leftrightarrow 11 \mid (01 + 17 + 48) \Leftrightarrow 11 \mid 66$

Für $t \mid 11 = 10^1 + 1$

$$z_n \ldots z_0 \equiv \cdots - z_3 + z_2 - z_1 + z_0 \bmod t$$

Für $t \mid 101 = 10^2 + 1$

$$z_n \ldots z_0 \equiv \cdots - z_3 z_2 + z_1 z_0 \bmod t$$

Sonstiges

RSA – Verschlüsseln

1. Wähle p,q prim, $n = p \cdot q$
2. $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$
3. Wähle e teilerfremd zu $\varphi(n)$ (z.B. eine Primzahl)
4. Berechne multiplikativ Inverses d zu e in $\mathbb{Z}/\varphi(n)\mathbb{Z}$

Öffentlicher Schlüssel (n,e)

Privater Schlüssel (n,d)

$$c = m^e \bmod n$$

RSA – Entschlüsseln

$$m = c^d \bmod m$$

Berechnung mit chinesischem Restesatz:

1. $m = c \bmod p$ $m = c \bmod q$
2. $t_1 = c^{d \bmod \varphi(p)} \bmod p$ $t_2 = c^{d \bmod \varphi(q)} \bmod q$
3. $d_1 = p^{-1} \bmod q$ $d_2 = q^{-1} \bmod p$
4. $m = (d_1 \cdot p \cdot t_2 + d_2 \cdot q \cdot t_1) \bmod n$