Satz (10.5) $\mathbb{Z}_m^*$ bzw. $(\mathbb{Z}/m\mathbb{Z})^*$

$$\mathbb{Z}_m^* = \{ x \mid 0 \leq x \leq m-1,\ ggT(x,m) = 1 \}$$

$|\mathbb{Z}_m^*| = \varphi(m)$ Eulersche φ-Funktion

Beweis: $x \in \mathbb{Z}_m^* \Leftrightarrow$ ex. y mit $x \cdot y = 1$ in $\mathbb{Z}_m$

$\Updownarrow$

$m \mid x \cdot y - 1$

Falls $ggT(x,m) = 1$, dann $a, b \in \mathbb{Z}$ mit $ax + bm = 1$

$-m \cdot b = ax - 1$

Für y kann man den Rest von a bei Division durch m wählen

bzw. in $\mathbb{Z}/m\mathbb{Z}$: $\bar{x}^{-1} = \bar{a}$

Falls $ggT(x,m) \neq 1$, dann $ggT(x,m) \mid x \cdot y$ in $\mathbb{Z}_m$

daher $xy \neq 1$ □

Bem: falls $p \neq 2$ Primzahl, dann ist $\mathbb{Z}_{p^n}^*$ zyklisch

$\mathbb{Z}_m$: $ggT(a,m) = 1 \iff a \in \mathbb{Z}_m^*$

$\iff$ a erzeugt $(\mathbb{Z}_m, +)$

Abbildung $x \mapsto x \cdot a$ ist additive Gruppenhomomorphismus
(Distributivgesetz!)

Falls bijektiv, dann Gruppen<u>iso</u>morphismus, nämlich Multiplikation mit a^{-1}

$\Downarrow$

Bild eines erzeugenden Elements muss wieder ein Erzeuger sein
z.B. 1

Falls nicht bijektiv, dann nicht surjektiv (da $\mathbb{Z}_m$ endlich), in diesem Fall a

dann ist $a \cdot 1 = a$ auch kein Erzeuger

und nicht injektiv (da $\mathbb{Z}_m$ endlich),

also $\ker(x \mapsto x \cdot a)$ nicht trivial

d.h. es existiert $y \neq 0$ (in $\mathbb{Z}_m$) mit $y \cdot a = 0$

Somit: a ist Nullteiler und kann kein Inverses haben!

$a \in \mathbb{Z}_m$: entweder $a \in \mathbb{Z}_m^*$

oder a ist Nullteiler

$\Downarrow$

$$a \cdot \underbrace{\frac{m}{ggT(m,a)}}_{\neq 0 \text{ in } \mathbb{Z}_m, \text{ falls } ggT(m,a) \neq 1} = 0 \quad \text{in } \mathbb{Z}_m$$

Satz 10.6

(a) Satz von Euler

$$a^{\varphi(m)} = 1 \quad \text{in } \mathbb{Z}_m \text{ für } ggT(a,m) = 1$$

(bzw. $m \mid a^{\varphi(m)} - 1$ in $\mathbb{Z}$)

(b) Spezialfall: „kleiner Satz von Fermat"

$m = p$ Primzahl: $a^{p-1} = 1$ in $\mathbb{Z}_p$ für $p \nmid a$

(bzw. $p \mid a^{p-1} - 1$)

Beweis: Satz von Lagrange für $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$!

Bem: • Falls $ggT(a,m) \neq 1$, gilt i.a. der Satz von Euler nicht:

$$m^{\varphi(m)} = 0 \quad \text{in } \mathbb{Z}_m$$

• kl. Fermat: $a^{p-1} = 1$ in $\mathbb{Z}_p$ falls $p \nmid a$

(Mathematiker schreiben meist: $a^{p-1} \equiv 1 \pmod p$)

also $\underline{a^p \equiv a \pmod p}$ gilt für alle a !

• gilt nicht bei Euler $m = 8$, $\varphi(m) = 4$, $a = 4$

$$a^{\varphi(m)} \cdot a = 4^5 \equiv 0 \pmod 8$$

$$a = 4 \not\equiv 0 \pmod 8$$

große Zahl $2011 \mod 1009$?

$$2345^{2011} \pmod{1009} \quad ?$$

$$2345^{1009} \equiv 2345 \pmod{1009}$$

$$\left.\begin{aligned} 2345^{2011} &\equiv 2345^{1009+1002} \\ &\equiv 2345^{1009} \cdot 2345^{1002} \\ &\equiv 2345^{1003} \end{aligned}\right\} \bmod 1009$$

---

auch ohne Euler bzw kl. Fermat

$x^y \bmod m$ $\quad x, y$ sind groß

zum Ausrechnen alle nicht nur x-Produkte und Reste

$$\underbrace{\text{Rest}\left(\text{Rest}(x^2)\cdot\text{Rest}(x^2)\right)}_{=\text{Rest}(x^4)}$$

$\text{Rest}\left(\text{Rest}(X\cdot X)\cdot X\right)\ldots$

noch besser: Binärdarstellung ausnutzen:

Anwendung Primzahltest

$n \in \mathbb{N}$ Frage: Ist n Primzahl?

- Algorithmus aus der Definition:

  teste für Zahlen $2, 3, 4, 5, \ldots, \lfloor \sqrt{n} \rfloor$

  ob sie Teiler von n sind

  im wesentlichen $\sqrt{n}$ viele Divisionen | dauert zu lange!

- Fermat-Test: für ausgewählte Testzahlen: gilt der kleine Satz von Fermat?

  man wählt „zufälliges" $a < n$

  und überprüft, ob $a^{n-1} \equiv 1 \pmod{n}$

  - falls es nicht gilt, ist n keine PZ
  - falls es gilt, kann n PZ sein, muss aber nicht!

- Es gibt sogenannte Carmichael-Zahlen n
  - keine Primzahlen
  - der kleine Satz von Fermat gilt trotzdem für alle a mit $\gcd(a,n)=1$

  Kleinste Carmichael-Zahl ist 561

- Kleine Kontrolle über die „Wahrscheinlichkeit", dass n Pz, wenn der Test mehrfach bestanden wird.

- Bessere Tests beruhen aber dennoch auf dem kleinen Satz von Fermat!

Anwendung: public key-Verschlüsselung
RSA-Verfahren

Singh
The Code Book
Geheime Nachrichten
(oder so ähnlich)

S Sender, E Empfänger

E wählt 2 große, „unbekannte" Primzahlen p, q $(p \neq q)$

$n = p \cdot q$

$\varphi(n) = (p-1) \cdot (q-1)$

E wählt ein „zufälliges" zu $\varphi(n)$ teilerfremde Zahl e

z.B. nicht $\varphi(n) - 1$

e und n werden öffentlich gemacht
p, q und $\varphi(n)$ bleiben geheim

S will Nachricht schicken

Nachricht wird geschickt durch Zahlen in $\mathbb{Z}_n$ kodiert

$(a_1, \ldots, a_k)$

und die verschlüsselte Nachricht $(a_1^e, \ldots, a_k^e)$

in $\mathbb{Z}_n$ ausgerechnet. — wird versendet

E rechnet d (= e^{-1} in $\mathbb{Z}_n^*$ aus (euklidischer Algorithmus)

und berechnet dann $((a_1^e)^d, \ldots, (a_k^e)^d)$ in $\mathbb{Z}_n$

Behauptung: $(a^e)^d = a$ in $\mathbb{Z}_n$

$$a^{e \cdot d} = a^{l \cdot \varphi(n) + 1} = \left(a^{\varphi(n)}\right)^l \cdot a$$

Falls a teilerfremd zu n; Satz von Euler

$$a^{\varphi(n)} = 1 \text{ in } \mathbb{Z}_n$$

Falls a nicht teilerfremd zu n:

Unterfall 1: $a = 0$: $a^{e \cdot d} = 0^{e \cdot d} = 0 = a$

Unterfall 2: $p \mid a$, $q \nmid a$

$a = k \cdot p$ — $p \mid a^{e \cdot d}$, also $p \mid (a^{e \cdot d} - a)$

— a teilerfremd zu q

$a^{\varphi(q)} \equiv 1 \pmod q$ $\quad \varphi(q) = (q-1) \mid \varphi(n)$

also $a^{\varphi(n)} \equiv 1 \pmod q$

$a^{l \cdot \varphi(n) + 1} \equiv a \pmod q$

d.h. $q \mid a^{ed} - a$

Unterfall 3: $p \nmid a$, $q \mid a$

analog

zusammen

$p \cdot q \mid a^{ed} - a$

d.h. $a^{ed} \equiv a \pmod{n = p \cdot q}$