17-11-200

Wiederholung

1) Sei $\operatorname{ord}(a) = n$. Dann gilt

$$a^k = e \iff k \in n\mathbb{Z}$$

$$\langle a \rangle = \langle e, a, \dots, a^{n-1} \rangle$$

2) $c = ggt(a,b)$ $\quad a, b \in \mathbb{Z}$

$a \neq 0$ oder $b \neq \emptyset$

$\langle a, b \rangle \leq_g \mathbb{Z}$ ist zyklisch und es gilt

$\langle a, b \rangle = \langle ggt(a,b) \rangle \Rightarrow ggt(a,b) = xa + yb$

3) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$; $\mathbb{Z}_n^* := \{\bar{x} \in \mathbb{Z}_n : \bar{x}$ invertierbar

$\bar{x} \in \mathbb{Z}_n$ invertierbar $\iff \exists \bar{y} \in \mathbb{Z}_n \; \bar{x}\bar{y} = \bar{1}$

$\Rightarrow \bar{x}$ invertierbar $\iff ggt(x,n) = 1$

Eulersche $\varphi(n) = |\mathbb{Z}_n^*| =$

$|\{\bar{x} \in \mathbb{Z}_n ; x$ ist teilerfremd zu $n\}|$

Berechnung von ggt(a,b)

Satz (Euklidischer Algorithmus)

Für Elemente $a, b \in \mathbb{Z} \setminus \{0\}$ betrachte man die Folge $z_0, z_1, \ldots \in \mathbb{Z}$ die induktiv gegeben ist durch:

$z_0 = a$

$z_1 = b$

$$z_{i+1} = \begin{cases} \text{der Rest der Division von} \\ z_{i-1} \text{ durch } z_i \text{ falls } z_i \neq \\ 0 \text{ sonst} \end{cases}$$

Dann gibt es einen Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Für dieses n gilt

$$z_n = \text{ggt}(a,b)$$

Beweis Übungsaufgabe

Beispiel

Seien $a = 625$ und $b = 160$

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

$r_0 = 625$

$r_1 = 160$

$r_2 = 145$ $\longleftarrow$ $i=1$ $\quad 625 = 3 * 160 + 145$

$r_3 = 15$ $\longleftarrow$ $i=2$ $\quad 160 = 1 * 145 + 15$

$r_4 = 10$ $\longleftarrow$ $i=3$ $\quad 145 = 9 * 15 + 10$

$r_5 = 5$ $\longleftarrow$ $i=4$ $\quad 15 = 1 * 10 + 5$

$r_6 = 0$ $\longleftarrow$ $i=5$ $\quad 10 = 2 * 5 + 0$

$\Rightarrow \quad ggT(625, 160) = 5$

Berechnung der Koeffizienten x und y

$$ggt(a,b) = x\,a + y\,b$$

$$5 = x \cdot 625 + y \cdot 160$$

Berechnung von x und y durch sukzessives Einsetzen der entsprechenden Werte r_i aus der Folge $r_0, r_1, \dots,$ des Eukl. Alg.

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

$i=1$; $625 = 3 * 160 + 145 \Rightarrow 145 = 625 - 3 * 160$

$i=2$; $160 = 1 \cdot 145 + 15 \Rightarrow 15 = 160 - 145$

$= 160 - 625 + 3 * 160$

$= -625 + 4 * 160$

$i=3$; $145 = 9 * 15 + 10 \Rightarrow 10 = 10 * 625 - 39 * 160$

$i=4$; $15 = 10 + 5 \Rightarrow 5 = -11 * 625 + 43 * 160$

$$ggt(625,160) = 5 = -11 * 625 + 43 * 160$$

Satz

(i) Ist $n \in \mathbb{N}$ und $m \in \mathbb{Z}$ und $ggT(n,m) = 1$ } Satz von Euler

$$\boxed{m^{\varphi(n)} \equiv 1 \bmod n}$$

(ii) Ist $p \in \mathbb{N}$ Primzahl u. $m \in \mathbb{Z}$

dann gilt $\boxed{m^p \equiv m \bmod p}$ (Fermat)

(iii) G Gruppe u. $|G| = p$ Primzahl } G zyklisch

(iv) G Gruppe, U, V endl. Untergrp von G. Sind die Ordnungen von U und V teilerfremd dann ist $U \cap V = \{e\}$.

Beweis

(i) $\varphi(n) = |\mathbb{Z}_n^*|$

m teilerfremd zu n $\Big)$

$\overline{m} \in \mathbb{Z}_n$ ist invertierbar

d.h. $\overline{m} \in \mathbb{Z}_n^*$

$\overline{m}^{|\mathbb{Z}_n^*|} = \overline{1} \Leftrightarrow \overline{m}^{\varphi(n)} = \overline{1}$

$\Leftrightarrow m^{\varphi(n)} \equiv 1 \bmod n$ □

(ii) (Fermat) $m^p \equiv m \bmod p$

p prim $\Rightarrow \varphi(p) = p-1$

$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$

Fall 1: $ggt(m,p) = 1 \Rightarrow$ (Satz v. Euler)

$m^{p-1} \equiv 1 \bmod p \iff$

$\exists_{x \in \mathbb{Z}}$ $m^{p-1} - 1 = x \cdot p \Rightarrow$

$m^p - m = m \cdot x \cdot p$ (Multipl. mit m)

$\Leftrightarrow m^p \equiv m \bmod p$