Eigenschap: $S \subset \mathbb{N}$, $S \neq \emptyset$, dan heeft S een kleinste element

Gevolg: Als $a, b \in \mathbb{Z}$, $b \neq 0$, dan $\exists!$ q, r met $a = q \cdot b + r$, $0 \le r < |b|$

Vbd: $a = 18$, $b = 7$: $18 = 2 \cdot 7 + 4$

Bewijs: $S = \{a - qb \mid q \in \mathbb{Z},\ a - qb \ge 0\}$ merk op $S \neq \emptyset$, $r = \min(x \in S)$

$r \in S \Rightarrow r \ge 0$. stel $b > 0$ en $r \ge b$

dan $0 \le r - b = a - qb - b = a - b(q+1) \in S$

maar $r - b > r$ $\lightning$

Uniciteit: stel $a = q_1 b + r_1$, $0 \le r_1 < |b|$

$= q_2 b + r_2$, $0 \le r_2 < |b|$ $r_1 \ge r_2$

$\Rightarrow (q_2 - q_1) b = r_1 - r_2 \Rightarrow b$ deelt $r_1 - r_2$ $\quad 0 \le r_1 - r_2 < |b|$

$\Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \Rightarrow q_1 - q_2 = 0$

Gevolg 2: Als $\text{ggd}(a,b) = d$, dan $\exists x, y \in \mathbb{Z}$: $ax + by = d$, $a, b \neq 0$

Vbd: $a = 12$, $b = 15$, $d = 3$: $3 = -1 \cdot 12 + 1 \cdot 15$

Bewijs: $S = \{ax + by \mid ax + by \ge 1,\ x, y \in \mathbb{Z}\}$, definieer $d = \min(z \in S)$

(i) d deelt a en b, stel d deelt niet a, $a = qd + r$, $0 < r < d$

$r = a - qd = a - q(ax + by)$

$= a(1 - qx) - qby$ $\lightning$ dus d deelt a en zo <u>ook b</u>

stel g deelt a en b, $d = ax + by \Rightarrow g$ deelt d

Vraag: x en y uniek? Nee!

Hoe te berekenen? Euclidisch algoritme

Eigenschap: p deelt $a \cdot b$, p priemgetal, dan $p \mid a$ of $p \mid b$

Bewijs: stel $p \nmid a$, dan $\text{ggd}(p, a) = 1$ en dus $1 = ax + py$

$b = abx + bpy$, $p \mid ab$ en $p \mid bpy \Rightarrow p \mid b$

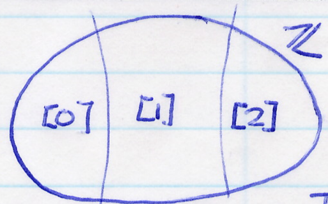
Eigenschap: $\mathbb{Z}_3 = \{[0], [1], [2]\}$

$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, 3, -3, 6, -6, \ldots\}$

$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{1, -2, 4, 7, \ldots\}$

$[2] = \{2 + 3k \mid k \in \mathbb{Z}\} = \{2, -1, 5, -4, \ldots\}$

$[3] = \{3 + 3k \mid k \in \mathbb{Z}\} = [0]$



$\mathbb{Z} = [0] \cup [1] \cup [2]$

en $[0] \cap [1] = \emptyset$

$[0] \cap [2] = \emptyset$

$[1] \cap [2] = \emptyset$

Partitie

partitie: opdeling van een verzameling in disjuncte deelverzamelingen

$\leftrightarrow$ equivalentierelatie

notatie: in $\mathbb{Z}_3$: $a \sim b \Leftrightarrow 3 \mid a - b$

$\sim$ heet equivalentierelatie op X indien:

$\forall x \in \mathcal{X}: x \sim x$ reflexiviteit

$\forall x,y \in \mathcal{X}: x \sim y \Rightarrow y \sim x$ symmetrie

$\forall x,y,z \in \mathcal{X}: x \sim y, y \sim z \Rightarrow x \sim z$ transitiviteit

$[o]$: equivalentieklasse met representant o

$\sim$ op $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

$(a,b) \sim (c,d) \Leftrightarrow ad = bc$

$\Leftrightarrow a/b = c/d$