HC 5
A&S

$|H|$ deelt $|G|$
i.h.b. $|g|$ deelt $G$
$g^{|G|} = e$
Toepassing: (kleine Fermat) $a^p = a \bmod p$, $p$ priem
immers in $U(p)$ geldt $x^{p-1} = 1 \bmod p$ dus $a^p = a \cdot a^{p-1} = a \bmod p$
Vb.d: $\{(x,y) \mid x \in \mathbb{Z}_2, y \in \mathbb{Z}_3\}$ is een groep m.b.t. $(+,+)$
$(x_1,y_1) + (x_2,y_2) = (\underbrace{x_1+x_2}_{\in \mathbb{Z}_2}, \underbrace{y_1+y_2}_{\in \mathbb{Z}_3})$

$e = (0,0)$, $-(x,y) = (-x,-y)$
associativiteit: $(x_1,y_1) + ((x_2,y_2) + (x_3,y_3)) = ((x_1,y_1)+(x_2,y_2)) + (x_3,y_3)$
$|G| = 2 \cdot 3 = 6$ $|(1,1)| = 6 \Rightarrow G$ cyclisch
$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3$
↑ directe som
Als $(G_i, *_i)$, $i = 1..n$ groepen, $G = G_1 \oplus G_2 \oplus \dots \oplus G_n$ directe som
$* = (*_1, *_2, \dots *_n)$
Vb.d: $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_m} = G$ $(\mathbb{Z}_3 \oplus \mathbb{Z}_9)$
$G$ is cyclisch $\Leftrightarrow$ $kgv(n_1, n_2, \dots n_m) = n$ $|G| = n_1 n_2 \dots n_m = n$
$\Leftrightarrow$ $ggd(n_i, n_j) = 1$, $i \neq j$ cyclisch
St: $G$ eindig en commutatief dan $G = \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_m}$ voor zekere $n_1 \dots n_m$
V.b.d: $G = \mathbb{Z}_5 \oplus U(10)$, $(x,y) \in G$. $(x \in (\mathbb{Z}_5, +)(y \in (U(10), \cdot)$

## Chinese reststelling

$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3} \sim \mathbb{Z}_n$, $n = n_1 n_2 n_3$ als $ggd(n_i, n_j) = 1$, $i \neq j$
isomorfisme $\varphi: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}$
$\varphi(k) = (k \bmod n_1, k \bmod n_2, k \bmod n_3)$
- $\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2)$
- injectief en surjectief

dus $\forall (k_1,k_2,k_3) \in \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}$ bestaat er precies één $k \in \mathbb{Z}_n$
zdd. $k = k_1 \bmod n_1 = k_2 \bmod n_2 = k_3 \bmod n_3$
Vraag: Hoe $k$ te construeren?
Antw: Huiswerk
Ook geldt: Als $ggd(s,t) = 1$ dan $U(s \cdot t) \sim U(s) \oplus U(t)$
Vb.d: $U(15) \sim U(5) \oplus U(3)$
ook hier $\varphi(k) = (k \bmod s, k \bmod t)$

**RSA:** $p, q$ priemgetallen

$n = p \cdot q$, $m = (p-1)(q-1)$

kies $e$ zdd $ggd(e,m) = 1$ $(e \in U(m))$

bepaal $d$ zdd $ed = 1 \bmod m$

kies $M \in U(n)$ (dus $M$ niet deelbaar door $p$ of $q$)

$R = M^e \bmod n$.

| $e$ en $n$ publiek |
|---|
| $d$ geheim |

$R^d = (M^e)^d$

$= M^{ed} = M^{1+k \cdot m} = M \cdot (M^m)^k = M \cdot (1)^k$

$= M \bmod n$

$U(n) = U(p) \oplus U(q)$

$|U(n)| = |U(p)| \cdot |U(q)|$

$= (p-1)(q-1)$

dus $x \in U(n) \Rightarrow x^m = 1 \bmod n$

**Ringen:** $(R, +, *)$

(i) $(R, +)$ is groep, commutatief

(ii) $\forall a,b,c \in R$: $a(bc) = (ab)c$ associatief

(iii) $\forall a,b,c \in R$: $a(b+c) = ab + ac$

$(b+c)a = ba + ca$

$R$ kan $1 \in R$ hebben: $1 \cdot a = a \cdot 1 = a$

V.b.d: • $R = (\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, *)$ $(\mathbb{C}, +, *)$ niet elke ring heeft alle inversen

• $R = (2\mathbb{Z}, +, \cdot)$ $(\mathbb{Z}_6, +*)$ $(\mathbb{Z}_7, +, *)$

Er geldt:

$0 \cdot a = (0+0) \cdot a$

$= 0 \cdot a + 0 \cdot a$

$\Rightarrow \underbrace{0 \cdot a + -0 \cdot a}_{0} = 0 \cdot a + \overbrace{0 \cdot a + -0 \cdot a}^{0}$

$= 0 \cdot a + 0 = 0 \cdot a$