Def: Låt H vara en delgrupp till en grupp G. För varje element $g \in G$ definierar vi en vänster respektive höger sidoklass genom

vänster $gH = \{x \in G;\ x = gh \text{ för något } h \in H\}$

höger $Hg = \{x \in G;\ x = hg \text{ för något } h \in H\}$

Ex: $H = \{id, (123), (132)\} \leq S_3$

$(12)H = \{(12), (23), (13)\}$ $\quad H \simeq C_3$

$(13)H = \{(13), (12), (23)\}$

$(23)H = \{(23), (13), (12)\}$

$(123)H = \{(123), (132), id\} = H$

$S_3 = H \cup (12)H = (123)H \cup (23)H$

Sats: $g_1H = g_2H$ eller $g_1H \cap g_2H = \emptyset$

bevis: Relationen $xRy \Leftrightarrow x^{-1}y \in H$ är en ekvivalensrelation och sidoklasserna är ekvivalensklasser.

Lagranges sats: Om G är en ändlig grupp, $|G| = n$, och H är en delgrupp av ordning m, så gäller $m \mid n$.

Ex: $|\{id, (123), (132)\}| = 3$, $|S_3| = 6$ och $3 \mid 6$.

Bevis: $|g_1H| = |g_2H| = m$ för $x \in g_1H$ ($x = g_1h$)

så gäller $g_2g_1^{-1}x = g_2g_1^{-1}g_1h = g_2h$.

Motsvarande om $x \in g_2H$.

Då sidoklasserna är disjunkta kan G skrivas som en union av ett antal lika stora delar.

Alltså $n = |G| =$ (antalet vänster sidoklasser) $\cdot |H|$

dvs $m \mid n$.

delgruppens index, $|G:H|$

Speciellt. (G ändlig grupp)

Sats: Låt $g \in G$, $|G| = n$, då delar g's ordning n.

bevis: $\langle g \rangle = \{e, g, \ldots, g^{m-1}\}$ $g^m = e$ en cyklisk delgrupp.

$m = |\langle g \rangle| = g$'s ordning $\Rightarrow m \mid n$

Ex: U_7 : $|U_7| = 6$

$\{1,2,3,4,5,6\}$

$* =$.

$2, 2^2 = 4, 2^3 = 8 = 1$

$\Rightarrow 2$ har ordning 3.

1	har ordning 1
2	ordning 3
3	ordning 6
4	ordning 3
5	ordning 6
6	ordning 2

Om $SGD(m,n)=1$ så gäller $C_m \times C_n \simeq C_{mn}$. Vi vet att $(\mathbb{Z}_m,+) \simeq C_m$, $(\mathbb{Z}_n,+) \simeq C_n$, $(\mathbb{Z}_{mn},+) \simeq C_{mn}$

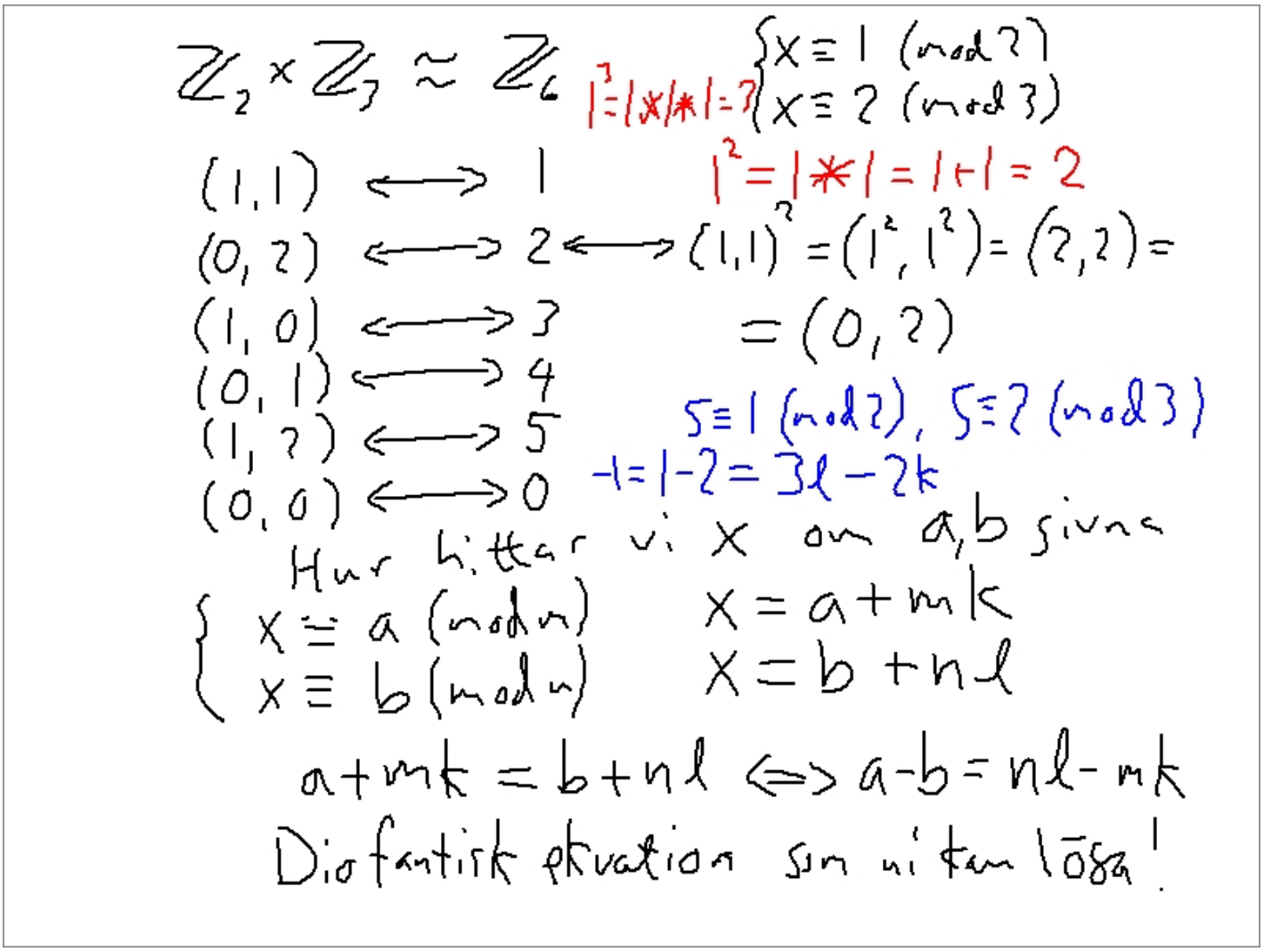
$\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$. Antag $x \in \mathbb{Z}_{mn}$

Vilket par (a,b) svara det mot?

$x = 1^x$ 1 svarar mot $(1,1)$ så 1^x svarar mot $(1,1)^x = (1^x, 1^x) = (a,b)$ där

$x \equiv a \pmod m$ $(0 \leq a < m)$

$x \equiv b \pmod n$ $(0 \leq b < n)$


$\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$
$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$
$1^3 = 1*1*1 = 2$
$1^2 = 1*1 = 1+1 = 2$
$(1,1) \longleftrightarrow 1$
$(0,2) \longleftrightarrow 2 \longleftrightarrow (1,1)^2 = (1^2, 1^2) = (2,2) =$
$(1,0) \longleftrightarrow 3 \quad = (0,2)$
$(0,1) \longleftrightarrow 4$
$(1,2) \longleftrightarrow 5$
$(0,0) \longleftrightarrow 0$
$5 \equiv 1 \pmod 2, \ 5 \equiv 2 \pmod 3$
$-1 = 1-2 = 3l - 2k$
Hur hittar vi x om a, b givna
$\begin{cases} x \equiv a \pmod n \\ x \equiv b \pmod n \end{cases}$
$x = a + mk$
$x = b + nl$
$a + mk = b + nl \Leftrightarrow a - b = nl - mk$
Diofantisk ekvation som vi kan lösa!

Ringar

Def: En ring är en mängd R med två operationer $+, \cdot$ som uppfyller

R1: $(R, +)$ är en abelsk grupp.

R2: $r_1 \cdot r_2 \in R$, $(r_1 r_2) r_3 = r_1 (r_2 r_3)$

Det finns ett element $1 \in R$ sådant att $r \cdot 1 = 1 \cdot r = r$.

R3: $r_1 (r_2 + r_3) = r_1 r_2 + r_1 r_3$

$(r_1 + r_2) r_3 = r_1 r_3 + r_2 r_3$.

Ex: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$

Ett element r kallas inverterbart om det har en multiplikativ invers, dvs det finns ett element $s \in R$ så att $rs = sr = 1$.

Sats: Mängden av inverterbara element i en ring, $U(R)$, bildar en grupp med avseende på operationen $\cdot$.

bevis: som för U_m.

Ex: $U(\mathbb{Z}_n) = U_n$, $U(\mathbb{Z}) = \{1, -1\}$

Ex: Booleska algebran $\mathbb{B}_n$ är en ring. (Övn: verifiera axiomen!)

Kroppar (Field)

En **kropp**, F, är en ring där multiplikationen är kommutativ ($ab = ba$) och alla element utom 0 har en multiplikativ invers, dvs $U(F) = F \setminus \{0\}$

Ex: $\mathbb{Q}$ (rationella talen), $\mathbb{R}$, $\mathbb{C}$ (komplexa talen) kroppar men $\mathbb{Z}$ är ingen kropp

Ex: I allmänhet är $\mathbb{Z}_m$ inte någon kropp men om m är ett primtal blir det en kropp.
Vi har ju att $|U(\mathbb{Z}_m)| = \phi(m)$
men $|\mathbb{Z}_m \setminus \{0\}| = m-1$ så $\mathbb{Z}_m$ är en kropp precis då $\phi(m) = m-1$, dvs då m är ett primtal.

Om p är ett primtal blir $U(\mathbb{Z}_p) = U_p$ blir cyklisk. Hur hittar man en generator?

Ex: Hitta en cyklisk generator i $U(\mathbb{Z}_{17})$. $|U(\mathbb{Z}_{17})| = 16$

Lösn: $\phi(17) = 16 = 2^4$. Elementen har alltså ordning 1, 2, 4, 8, eller 16.

Vi börjar undersöka potenser av 2. 2, 4, 8, 16, 15, 13, 9, 1

så 2 har ordning 8.

$\langle 2 \rangle = \{1, 2, 4, 8, 9, 13, 15, 16\}$

$\langle 2 \rangle$ är en delgrupp av ordning 8 så elementen som ingår har ordningar som delar 8.

Antalet generatorer ges av $\phi(16)$ för elementens ordning delar 16. Antalet generatorer blir så

$$\phi(16) = 16 - \phi(8) - \phi(4) - \phi(2) - \phi(1)$$
$$= 16 - (8 - \phi(4) - \phi(2) - \phi(1)) - \phi(4) - \phi(2) - \phi(1)$$
$$= 16 - 8 = 8 \text{ st.}$$

Vi har redan strukit 8 element som ej kan vara generatorer så övriga är generatorer.

Tex: 3. Övn: Testa att 3 har ordning 16.

Ex: Hitta en/cy klisk generator i $U(\mathbb{Z}_{41})$.

Lösn: $\phi(41) = 40 = 2^3 \cdot 5$. Elementen i $U(\mathbb{Z}_{41})$ har ordningar 1, 2, 4, 5, 8, 10, 20 eller 40. Vi testar med 2

$\langle 2 \rangle = \{1, 2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21\}$

$|\langle 2 \rangle| = 20$. Antalet generatorer är

$\phi(40) = 40 - \frac{40}{2} - \frac{40}{5} + \frac{40}{10} = 40 - 20 - 8 + 4 = 16$ st

men $40 - 20 - 16 = 4$ så vi får inte alla ännu. Vi försöker med 3.

$$\langle 3 \rangle = \{1, 3, 9, 27, 40, 38, 32, 14\}$$

$$|\langle 3 \rangle| = 8$$

Fortfarande ingen generator

men $MGM(8, 20) = \frac{8 \cdot 20}{SGD(8,20)} = 40$.

så $6 = 2 \cdot 3$ har ordning 40.

Ex: Antag att $x \cdot y = 0$ i F
och visa att då är
$x = 0$ eller $y = 0$

Lösn: Om x inte är noll
så är x inverterbar. Vi får
då $x^{-1}(xy) = x^{-1} \cdot 0$
$\Rightarrow y = 0$