$C_{1,2}$

<u>Grupuri</u>

$$(G, \cdot, 1)\text{-grup} \iff \begin{cases} \forall x,y,z \\ (xy)z = x(yz) \\ \text{asociativ} \\ \\ \forall x \quad x\cdot 1 = 1\cdot x = x \\ \text{el. neutru} \\ \\ \forall x \ \exists y \quad xy = 1 \\ \text{inversul } y = x^{-1} \end{cases}$$

$$\left.\begin{array}{l} 1 \in H \subseteq G \\ (H, \cdot|_H, 1)\text{-grup} \end{array}\right| \begin{array}{l} H \text{ subgrup} \\ \text{al lui } G \end{array} \qquad H \leq G$$

$$x, y \in G : \left.\begin{cases} xH = yH \\ \quad \text{sau} \\ xH \cap yH = \emptyset \end{cases}\right] \Rightarrow \left(\begin{array}{l} G \text{ finit} \\ H \leq G \end{array} \Rightarrow |H| \,\big|\, |G| \right)$$

<u>Exemplu</u> A mulțime

$$S(A) = \{ f : A \to A \mid f \text{ bijectivă} \}$$

$(S(A), \circ, 1_A)$ - grup
grupul de permutări al lui A

$$|A| = n \Rightarrow (S_n, \circ, 1_n)$$

$$|S_n| = n!$$

Cayley: G - grup $\Rightarrow G \leq S(G)$

$g \in G \rightsquigarrow f_g : G \to G$, $f_g(x) = g \cdot x$ (în grup)

$\Rightarrow f_g$ bijectivă, $f_1 = id$, $f_g \cdot f_h = f_{gh}$

$g(hx) = (gh)x$

$f_{g_1} = f_{g_2} \Rightarrow f_{g_1}(1) = f_{g_2}(1) \Rightarrow g_1 = g_2$

$G \to S(G)$
injectivă

Permutări: $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

$x \in G$

$\langle x \rangle$ = cel mai mic subgrup al lui G care conține x

$= \{x^k \mid k \in \mathbb{Z}\}$

G finit $\Rightarrow |\langle x \rangle| \,\big|\, |G|$

$\langle x \rangle$ grup ciclic finit

$|\langle x \rangle| = \min\{n \mid x^n = 1, n > 0\} = ord(x)$

$\forall x \in G$
$ord(x) \mid |G|$

$\forall x, y \in G \quad xy = yx$

$H \leq G$ $\quad x \in G$ $\quad$ clase la stânga
$\quad xH$ $\quad$ ale lui H

$\{xH \mid x \in G\}$ partiție disjunctă a lui $G \Rightarrow |H| \,\big|\, |G|$

<u>Def</u>: $\forall x \in G \quad xHx^{-1} = H$

$H \trianglelefteq G$ subgrup normal

$\Rightarrow \{xH\}_{x\in G}$ grup $G/_H$

G comutativ $\Rightarrow$ $\forall$ subgrup este normal

- grup ciclic generat de 1 element de ordin infinit:

$(\mathbb{Z}, +, 0)$ comutativ $\Rightarrow$ orice subgrup este normal

- $n \cdot \mathbb{Z} \trianglelefteq \mathbb{Z} \rightsquigarrow \mathbb{Z}/_{n}\mathbb{Z}$ singurul grup ciclic de ordin n

$\mathbb{Z} \xrightarrow{\text{mod } n} n\mathbb{Z}$

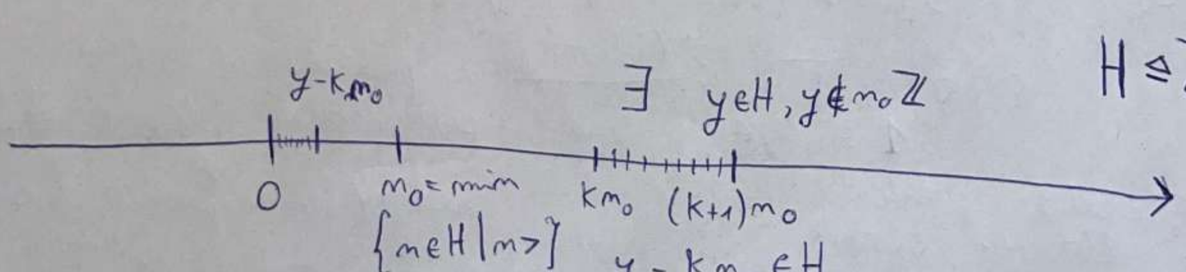
$x \longrightarrow x \text{ mod } n$

$H \leq \mathbb{Z} \quad (+, 0)$

$n_0 = \min \{x \in H \mid x > 0\} > 0$

$n_0 \in H \qquad H = n_0\mathbb{Z}$

$\exists\ y \in H, y \notin n_0\mathbb{Z}$ $\qquad H \trianglelefteq \mathbb{Z}$



$y - kn_0 \in H$

$\mathbb{Z}/_{m}\mathbb{Z} = \langle \hat{1} \rangle = \mathbb{Z}_m$ $\quad \hat{2} \bmod 7 + \hat{5} \bmod 7 = \hat{0} \bmod 7$

finite commutative
group with m elements, $\hat{1} = 1 \bmod m$

$m > 0$; $\mathbb{Z}_m$

$\mathcal{G}_m = \{ x \in \mathbb{Z}_m \mid \langle x \rangle = \mathbb{Z}_m \}$ generators of $\mathbb{Z}_m$

$(\mathbb{Z}_{12}, +, 0)$ $\quad 8 \in \mathbb{Z}_{12}$

$\langle 8 \rangle = \{8, 4, 0\} \simeq \mathbb{Z}_3$, $\quad$ 8 is not a generator of $\mathbb{Z}_{12}$

$\gcd(12, 8) = 4$

$x \in \mathbb{Z}_m = \{0, 1, \dots, m-1\}$

$\langle x \rangle = \mathbb{Z}_m \iff \gcd(x, m) = 1$

$|\mathcal{G}| = \{ x \in \{0, \dots, m-1\} \mid \gcd(x, m) = 1 \}$

$|\mathcal{G}| = \varphi(m)$

Euler's Totient Function

S_m ; $\varepsilon : S_m \to (\{-1, 1\}, \cdot, 1)$

$\varepsilon(\sigma) = \prod\limits_{1 \le i < j \le m} \frac{\sigma(i) - \sigma(j)}{i - j}$ signature of the permutation; $\operatorname{Ker} \varepsilon \trianglelefteq S_m$

σ : odd , even
$\varepsilon(\sigma) = -1$, $\varepsilon(\sigma) = 1$

$\operatorname{Ker} \varepsilon$ = set of even permutations = A_m

odd permutations: transpositions (i, j) $\quad A_m$, $|A_m| = \frac{m!}{2}$

Theorem: Every $\sigma \in S_n$ is a product of $\leq n-1$ many transpositions. (this representation is not commutative, and not unique)

$\sigma \in S_n$

If $\sigma(1) \neq 1$; $(1, \sigma(1))$

$\tau = (1, \sigma(1))\, \sigma$ has 1 as a fixed point

If $\tau(2) \neq 2$; $(2, \tau(2))$

$(2, \sigma(2))\, \tau = (2, \tau(2))\, (1, \sigma(1))\, \sigma$ has 1 and 2 as fixed points

(goes on, $\leq n-1$ times)

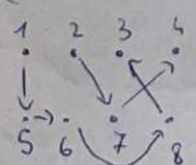
$()_1 ()_2 ()_3 \cdots ()_{n-1}\, \sigma = id$ $\qquad (i\ j)(i\ j) = id$

$\sigma = ()_{n-1} ()_{n-2} \cdots ()_1$

Theorem: Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. (this representation is commutative and unique)

$a_1, \dots, a_k$ pair-wise disjointed $\qquad (a_1, a_2, \dots, a_k)$ $\qquad \frac{k!}{k} = (k-1)!$ many cyclic permutations with k elements

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 2 & 6 & 8 & 4 & 3 \end{pmatrix} = (1, 5, 6, 8, 3)(2, 7, 4)$$



<u>Prove</u> : $(k, k+1) = (1,2,\dots,n)^{k-1} (1,2) (1,2,\dots,n)^{1-k}$

$(i,j) = (j-1, j)(j-2, j-1)\dots(i+1, i+2)(i, i+1)(i+1, i+2)\dots$
$\dots (j-2, j-1)(j-1, j)$

if $i<j$ the telescopic identity

$\Rightarrow \forall n \quad S_n = \langle (1,2), (1,2,\dots,n) \rangle$

$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3)\dots(a_{k-1}, a_k)$

<u>Rings</u>: $(R, +, \cdot, 0, 1)$ ring $\Leftrightarrow \begin{cases} (R,+,0) \text{ commutative group} \\ \forall x,y,z \quad (xy)z = x(yz) \\ \qquad x\cdot 1 = 1\cdot x = x \end{cases}$

$\left\| \begin{array}{l} x(y+z) = (x\cdot y) + (x\cdot z) \\ (y+z)x = (y\cdot x) + (z\cdot x) \end{array} \right.$

if moreover $xy = yx$ we speak about a commutative ring.
(Exception : rings of matrices, which are not commutative)

I ideal $\Leftrightarrow (I, +, 0) \subseteq (R, +, 0)$
$\forall x \in R \ \forall y \in I \quad xy \in I$

$(\mathbb{Z}, +, \cdot, 0, 1)$ ring $\quad n\mathbb{Z}$ additive subgroups, also bilateral ideals

$\underbrace{\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n}_{\text{cyclic groups}}$ and rings $(\underbrace{\mathbb{Z}_n, +, \cdot}_{\text{mod } n}, 0, 1)$ the finite cyclic rings operations with ideals:

$n\mathbb{Z} + m\mathbb{Z} = \gcd(n,m)\mathbb{Z}$ alternative def. of $\gcd(n,m)$

$n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(n,m)\mathbb{Z}$ $\operatorname{lcm}(n,m)$ = least common multiple

R ring, $R^* = \{x \in R \mid \exists y \in R,\ xy = 1\}$
units of the ring, build a commutative group with multiplication.

$\mathbb{Z}_n^* = \{x \mid \exists y \quad xy = 1\} = \{x \mid \gcd(x,n) = 1\} = \mathcal{G}(\mathbb{Z}_n, +, \circ)$
additive generator = multiplicative unit

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ $\quad 5^2 = 25 \bmod 12 = 1$
$\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ $\quad 7^2 = 49 \bmod 12 = 1$
$\quad 11^2 = 121 \bmod 12 = 1$

Chinese Remainder Theorem: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$; $p_1, \dots, p_k$ primes

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$
$$k^{\epsilon} \rightsquigarrow (k \bmod p_1^{\alpha_1}, k \bmod p_2^{\alpha_2}, \dots, k \bmod p_k^{\alpha_k})$$
isomorphism of rings

Warning: $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \not\simeq \mathbb{Z}/25\mathbb{Z}$
all elements have order 1 or 5 $\quad \exists x,\ \operatorname{ord}(x) = 25$

$\gcd(m,n) = 1 \Rightarrow \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ goes until you reach the prime-powers
$\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

$\varphi(n) = \left|\{x \in \{0, \dots, n-1\} \mid \gcd(n, x) = 1\}\right|$ Euler's Totient Function

$\gcd(n, m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$

$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha - 1}$

p prime

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$
$$= p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right)$$

Euler: $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$

$\operatorname{ord}(x) \mid \operatorname{ord}(G) \quad (x \in G)$

$G = \mathbb{Z}_n^*$, $\operatorname{ord}(G) = \varphi(n)$

$a \in \mathbb{Z}_n^* \; (\Leftrightarrow \gcd(a, n) = 1)$

$\boxed{a^{\varphi(n)} \equiv 1 \bmod n}$ Euler's Theorem

$\gcd(m, n) = 1$, $m < n$? $m^{-1} \in \mathbb{Z}_n$ $\quad m \cdot m^{-1} \equiv 1 \bmod n$
modular inverse

$\gcd(17, 100) = 1$

$100 = 5 \cdot 17 + 15$
$17 = 1 \cdot 15 + 2$
$15 = \cancel{7} \cdot 2 + 1$

$1 = 15 - 7 \cdot 2 = 15 - 7 \cdot (17 - 15) = 8 \cdot 15 - 7 \cdot 17 =$

$= 8 \cdot (-5) \cdot 17 - 7 \cdot 17 = -47 \cdot 17 = 53 \cdot 17$

Extended Euclid Algorithm $\Rightarrow \cancel{17^{-1} = 53}$

$17^{-1} \bmod 100 = 53$

$\boxed{\text{Chinese Remainder Theorem (effective version)}}$

$m_1, \dots, m_\lambda \geq 2$; $\gcd(m_i, m_j) = 1 \quad (i \neq j)$

we know the remainders $x \bmod m_i = a_i \quad i = 1, \dots, \lambda$

$M = m_1 \cdot m_2 \cdot \dots \cdot m_\lambda$

$M_i = \dfrac{M}{m_i} \qquad x = \sum_{i=1}^{\lambda} a_i M_i y_i \bmod M$

$y_i = M_i^{-1} \bmod m_i$

$$\begin{cases} x = 5 \bmod 7 \\ x = 3 \bmod 11 \\ x = 10 \bmod 13 \end{cases}$$

$M = 1001$

$M_1 = 11 \cdot 13 = 143, \quad y_1 = 143^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5$

$M_2 = 7 \cdot 13 = 91, \quad y_2 = 91^{-1} \bmod 11 = 3^{-1} \bmod 11 = 4$

$M_3 = 7 \cdot 11 = 77, \quad y_3 = 77^{-1} \bmod 13 = 12^{-1} \bmod 13 = 12$

$x = (5 \cdot 143 \cdot 5 + 3 \cdot 91 \cdot 4 + 10 \cdot 77 \cdot 12) \bmod 1001$

$= 894$

Fast exponentiation

$$b = \sum_{b_i \in \{0,1\}} b_i \cdot 2^i$$

$$a^b = a^{\sum b_i \cdot 2^i} = \prod_{b_i = 1} a^{2^i}$$

<u>Theorem</u> : $(\mathbb{Z}_m^*, \cdot, 1)$

cyclic $\Leftrightarrow m \in \{2, 4, p^\alpha, 2p^\alpha\}$ p. odd primes, $\alpha \geq 1$

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ $\quad 9 - 3 = 3^2 - 3^1$

$2^n \bmod 9$: 2, 4, 8, 7, 5, 1

$\Rightarrow \mathbb{Z}_9^\times$ cyclic $= \langle 2 \bmod 9 \rangle$