[Thm. Euler] $m \geq 1$, $\forall a \in \mathbb{Z}_m^*$, $a^{\phi(m)} \equiv 1 \bmod m$ $\quad \phi(m) = |\mathbb{Z}_m^*|$ $\quad p^0 = p-1$, $\phi(p^e) = p^e - p^{e-1}$

[Corol. Fermat] $p \geq 2$, prim, $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$

[Criteriul lui Euler] $a \in QR_p \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$ $\quad a \equiv x^2 \bmod p$

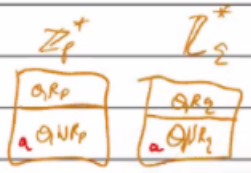
$a \in QNR_p \iff a^{\frac{p-1}{2}} \equiv -1 \bmod p$ $\quad a \in QR_p$

[Thm. Wilson] p prim $\iff (p-1)! \equiv -1 \bmod p$ $\quad QR_p = \{1^2, 2^2, (3^2)_p, (4^2)_p, (5^2)_p, (6^2)_p\}$

Simbolul Legendre $\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a \\ 1, & p \nmid a \text{ și } a \in QR_p \\ -1, & p \nmid a \text{ și } a \in QNR_p \end{cases}$ $\quad a \in \mathbb{Z}_p - \mathbb{Z}_p^*$; $a \in \mathbb{Z}_p^*$

Regulile de calcul pentru simb. Legendre

1. $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ $\quad \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$ $\quad 5 \bmod 3 = 2$ $\quad 5 \equiv 2 \bmod 3$
2. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{cases}$
5. $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8 \end{cases}$ $\quad 1 \mid 7$; $3 \mid 5$



Simbolul Jacobi $\left(\frac{a}{m}\right) = \begin{cases} 1, & m = 1 \\ \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}, & \text{altfel} \end{cases}$ $\quad \left(\frac{a}{m}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = (-1)(-1) = 1$

$1 \not\Rightarrow a \in QR_m$; $-1 \not\Rightarrow a \in QNR_m$ ✓ $\quad m = pq$, p, q prime dist.

$a \in \mathbb{Z}_m^* \setminus QR_m$

unde $m = p_1^{e_1} \cdots p_k^{e_k}$, $p_i \neq p_j$, prime

Ecuatia $ax^2+bx+c \equiv 0 \bmod p$ are
- 2 rădăcini în $\mathbb{Z}_p$, dacă $\Delta \equiv y^2 \bmod p$, $y \in \mathbb{Z}$, $p \nmid y$
- 1 rădăcină în $\mathbb{Z}_p$, dacă $\Delta \equiv 0 \bmod p$
- 0 rădăcini altfel

$\Delta = b^2-4ac$

$x = \frac{-b \pm \sqrt{\Delta}}{2a}$

$x^2 \equiv 1 \bmod p$ < sol. 1, sol. $p-1$

$x^2 \equiv 1 \bmod p_1 \cdots p_k \Rightarrow 2^k$ sol. în $\mathbb{Z}_{p_1 \cdots p_k}$

Ex. Calculati solutia sistemului

$$\begin{cases} x \equiv 9 \bmod 12 \\ x \equiv 3 \bmod 18 \\ x \equiv 1 \bmod 10 \end{cases}$$

$12 = 2^2 \cdot 3$: $x \equiv 1 \bmod 4$, $x \equiv 0 \bmod 3$ ($(7)_4 = 7 \bmod 4 = 3$, $(5)_4 = 1$)

$18 = 2 \cdot 3^2$: $x \equiv 1 \bmod 2$, $x \equiv 3 \bmod 9$ ($(7)_2 = 1$, $(5)_2 = 1$)

$10 = 2 \cdot 5$: $x \equiv 1 \bmod 2$, $x \equiv 1 \bmod 5$

$\Rightarrow x \equiv 1 \bmod 4$, $x \equiv 3 \bmod 9$, $x \equiv 1 \bmod 5$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$c_1 = 45 \equiv 1 \bmod 4$, $x_1 = 1$ (mod 4: $5 \cdot 9$)

$c_2 = 4 \cdot 5 = 20$, $x_2 = 6$ (mod 9: $4 \cdot 9 \equiv 36$)

$c_3 = 4 \cdot 9 \equiv 36$, $x_3 = 1$

$45 x_1 \equiv 1 \bmod 4$

$1 \cdot x_1 \equiv 1 \bmod 4$

$20 x_2 \equiv 3 \bmod 9$

$2 \cdot x_2 \equiv 3 \bmod 9$

$36 x_3 \equiv 1 \bmod 5$

$1 \cdot x_3 \equiv 1 \bmod 5$

CRT conditie: $\forall i, j, (m_i, m_j) = 1$

$[12, 18, 10] = 180 = m$

$x = (c_1 \cdot x_1 + c_2 \cdot x_2 + c_3 \cdot x_3) \bmod 180$

$x = (45 \cdot 1 + 20 \cdot 6 + 36 \cdot 1) \bmod 180 = 201 \bmod 180 = 21$ Vf ✓

Ex3. Calculati simbolurile:

a) $\left(\frac{82}{17}\right) \overset{2}{=} \left(\frac{41}{17}\right) \cdot \left(\frac{2}{17}\right) \overset{5a}{=} 1 \cdot \left(\frac{7}{17}\right) \overset{66}{=} \left(\frac{17}{7}\right) \overset{1}{=} \left(\frac{3}{7}\right) \overset{6a}{=} -\left(\frac{7}{3}\right) \overset{1}{=} -\left(\frac{1}{3}\right) \overset{3}{=} -1$

($(17)_8 = 1$; $(17)_4 = 1$)

b) $\left(\frac{111}{991}\right) =$

$-\left(\frac{-1}{p}\right) \overset{4b}{=} -(-1) = 1$

↓ +q

$= -(1) = -1$

c) $\left(\frac{41}{163}\right) =$

Regula de calcul pentru simb. Legendre

1. $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) \overset{a}{=} \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{cases}$ (b)
5. $\left(\frac{2}{p}\right) \overset{a}{=} \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8 \end{cases}$ (b)
6. $\left(\frac{q}{p}\right) \overset{a}{=} \begin{cases} -\left(\frac{p}{q}\right), & p \equiv_4 q \equiv_4 3 \\ \left(\frac{p}{q}\right), & p \equiv_4 1 \text{ sau } q \equiv_4 1 \end{cases}$ (b)

Legea reciprocitatii

Ordine de mărime

$g: \mathbb{N} \to \mathbb{R}_+$

$O(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \exists c > 0, \exists m_0 \in \mathbb{N}, \forall m \geq m_0 : f(m) \leq c \cdot g(m) \}$

$\Omega(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \exists c > 0, \exists m_0 \in \mathbb{N}, \forall m \geq m_0 : f(m) \geq c \cdot g(m) \}$

$\Theta(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \exists c_1, c_2 > 0, \exists m_0 \in \mathbb{N}, \forall m \geq m_0 : c_1 g(m) \leq f(m) \leq c_2 \cdot g(m) \}$

$o(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \forall c > 0, \exists m_0 \in \mathbb{N}, \forall m \geq m_0 : f(m) < c \cdot g(m) \}$

Ex 5 Dem. că

Dacă $f(m) = O(h_1(m))$ și $g(m) = O(h_2(m))$ atunci $f(m) + g(m) = O(\max\{h_1(m), h_2(m)\})$

$\exists c > 0, \exists m_0 \in \mathbb{N}, \forall m \geq m_0 : f(m) + g(m) \leq c \cdot \max\{h_1(m), h_2(m)\}$

$c = ?$

$f(m) = O(h_1(m)) \Rightarrow \exists c_1 > 0, \exists m_0' \in \mathbb{N}, \forall m \geq m_0' : f(m) \leq c_1 \cdot h_1(m)$

$g(m) = O(h_2(m)) \Rightarrow \exists c_2 > 0, \exists m_0'' \in \mathbb{N}, \forall m \geq m_0'' : g(m) \leq c_2 \cdot h_2(m)$

$$f(m) + g(m) \leq c_1 \cdot h_1(m) + c_2 \cdot h_2(m) \leq c_1 \cdot \max\{h_1(m), h_2(m)\} + c_2 \cdot \{h_1(m), h_2(m)\}$$

$$\leq \underbrace{(c_1 + c_2)}_{c} \cdot \max\{h_1(m), h_2(m)\}$$

Ex1

$$(S)\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \end{cases}$$

a) Demonstrați că sistemul (S) are soluție dacă și numai dacă $b_1 \equiv b_2 \bmod (m_1, m_2)$, unde $(m_1, m_2) \neq 1$. (cmmdc)

b) Dacă are soluție, atunci ea este unică modulo $[m_1, m_2]$ (cmmmc)

c) Rezolvați următorul sistem utilizând demonstrațiile anterioare

$$\begin{cases} x \equiv 31 \bmod 50 \\ x \equiv 16 \bmod 35 \end{cases}$$

b) Contradicție presp: α_1, α_2 sol. dist. mod $[m_1, m_2]$

$$\left.\begin{array}{l} \alpha_1 \equiv b_1 \bmod m_1 \\ \alpha_2 \equiv b_1 \bmod m_1 \end{array}\right\} \Rightarrow \alpha_1 \equiv \alpha_2 \bmod m_1$$

$$\alpha_1 = \alpha_2 \bmod m_2$$

$$\Downarrow$$

$$\alpha_1 = \alpha_2 \bmod [m_1, m_2]$$

$$\Leftarrow \begin{cases} \alpha_1 \equiv b_2 \bmod m_2 \\ \alpha_2 \equiv b_2 \bmod m_2 \end{cases}$$

c) $x \equiv 31 \bmod 50 \Rightarrow 50 \mid x-31 \Rightarrow x-31 = 50y \Rightarrow x = 50y + 31$

$50y + 31 \equiv 16 \bmod 35 \Rightarrow 35 \mid 50y + 31 - 16 \Rightarrow 50y + 15 = 35z$

$\Downarrow$

$50y \equiv 20 \bmod 35$ (a, b, c)

$\rightarrow 50y - 35z = 20$

y