1) Det $\gcd(a,b) = ?$ și $u, v \in \mathbb{Z}$ a.î.

$u \cdot a + v \cdot b = \gcd(a,b)$

a) $a = 461$

$b = 153$

$461 = 153 \cdot 3 + 2$

$153 = 2 \cdot 76 + 1$

$2 = 1 \cdot 2 + 0$

$\gcd(461, 153) = 1$

$1 = 153 - 2 \cdot 76$

$1 = 153 - (461 - 153 \cdot 3) \cdot 76$

$= 153 - 461 \cdot 76 + 153 \cdot 228$

$= 153 \cdot 229 - 461 \cdot 76$

$1 = u \cdot 461 + v \cdot 153$

$u_1 = -76$

$v_1 = 229$

$461 : 1 = 461 \Rightarrow v = 229 + 461k$, $\forall k \in \mathbb{Z}$

$153 : 1 = 153 \Rightarrow u = -76 - 153k$

b) $a = 120$, $b = 23$

$120 = 23 \cdot 5 + 5$

$23 = 5 \cdot 4 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\gcd(120, 23) = 1$

$1 = 3 - 2 \cdot 1$

$1 = 3 - (5 - 3) = 3 - 5 + 3 \cdot 1 = 3 \cdot 2 - 5 \cdot 1 =$

$= (23 - 5 \cdot 4) \cdot 2 - 5 \cdot 1$

$= 23 \cdot 2 - 5 \cdot 9$

$= 23 \cdot 2 - (120 - 23 \cdot 5) \cdot 9 = 23 \cdot 2 - 120 \cdot 9 + 23 \cdot 45 = 23 \cdot 47 - 120 \cdot 9$

$1 = 120(-9) + 47 \cdot 23$

$u_1 = -9$

$v_1 = 47$

$120 : 1 = 120 \Rightarrow v = 47 + 120k$; $\forall k \in \mathbb{Z}$

$47 : 1 = 47 \Rightarrow u = -9 - 23k$

c) $a = 1950$, $b = 45$

$1950 = 45 \cdot 43 + 15$

$45 = 15 \cdot 3 + 0$

$\gcd(1950, 45) = 15$

$15 = 1950 \cdot 1 + 45 \cdot (-43) \Rightarrow$ $u_1 = 1$, $v_1 = (-43)$

$$\begin{array}{r|l} 1950 & 15 \\ \underline{15} & \overline{130} \\ =45 & \end{array}$$

$15 = 1950 \cdot u + 45 \cdot v$

$1950 : 15 = 130 \Rightarrow v = -43 + 130k$; $\forall k \in \mathbb{Z}$

$45 : 15 = 3 \Rightarrow u = 1 + 3k$

2) Arătați că $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$

Obs: $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$

pt n = impar : $x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1})$

$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$

$x - 1 \mid x^n - 1$, $\forall n \in \mathbb{N}$

pt $x = 2^b \Rightarrow 2^b - 1 \mid (2^b)^n - 1 = 2^{bn} - 1$

Dc $b < a$:

$a : b = q$ rest r

$a = q \cdot b + r$

$\Rightarrow 2^b - 1 \mid (2^b)^q - 1 \Rightarrow 2^{bq} - 1$

$2^a - 1 = 2^{b \cdot q + r} - 1$

$2^a - 1 = 2^{b \cdot q} \cdot 2^r - 1 = 2^r(\underbrace{2^{b \cdot q} - 1}_{\vdots 2^b - 1}) + 2^r - 1$

$2^a - 1 = (2^b - 1)Q_1 + \underbrace{2^r - 1}_{R_1}$

$2^b - 1 = R_1 \cdot Q_2 + R_2$

$\vdots$

$R_{t-1} = R_t \cdot Q_{t+1} + R_{t+1} = 2^{r_{t+1}} - 1 = 2^{\gcd(a,b)} - 1$

$R_t = R_{t+1} \cdot Q_{t+2} + 0 = 2^0 - 1 = 0$

$a = b \cdot q_1 + r_1$

$b = r_1 \cdot q_2 + r_2$

$r_1 = r_2 \cdot q_3 + r_3$

$\vdots$

$r_{t-1} = r_t \cdot q_{t+1} + r_t = \gcd(a,b)$

$r_t = r_{t+1} \cdot q_{t+2} + 0$

Temă: Dem că $\gcd(x^a - 1, x^b - 1) = x^{\gcd(a,b)} - 1$

3) Arătați că desc în fact primi în $\mathbb{Z}$ este unică până la o rearanjare a termenilor și semnelor.

$n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k}$, unde $p_1, \ldots, p_k \in \mathbb{N}$ prime (in mod cresc)

$\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$

$\pm$ depinde de $n \Rightarrow$ e unic

Fie $n = \pm q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_t^{\beta_t}$, $q_1 \ldots q_t \in \mathbb{N}$ prime (in mod cresc)

$\alpha_1 \ldots \alpha_k \in \mathbb{N}^*$

Fie $\alpha = \alpha_1 + \ldots + \alpha_k$

Inducție după $\alpha \geq 1$

$P(1)$: $\alpha = 1 \Rightarrow n = \pm p_1$, p_1 - prim — Se verifică

$\Rightarrow p_1 = q_i$ și restul $q_i \not\exists$

Presupunem $P(\alpha-1)$ – adev și dem $P(\alpha)$

$n = \pm p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$, $\alpha_k \geq 1$ $\Rightarrow p_k \mid n = \pm q_1^{\beta_1} \cdot \ldots \cdot q_t^{\beta_t}$, p_k - prim, q_i - prime $\Rightarrow p_k \mid q_j$, de ex $p_k \mid q_t$, p_k - prim, q_t - prim $\Rightarrow$

$\Rightarrow p_k = q_t$

$n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = \pm q_1^{\beta_1} \cdot \ldots \cdot q_t^{\beta_t}$ $\vdots p_k$; $\vdots p_k = q_t$

$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k - 1} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_t^{\beta_t - 1}$

$P(\alpha-1)$ – Adevărat $\Rightarrow \alpha - 1 = \alpha_1 + \alpha_2 + \ldots + \alpha_k - 1 \Rightarrow p_i = q_i$ și $\alpha_i = \beta_i$ și k_t $\forall i = \overline{1,k}$

Test - 1 fct criteriu grafic
- inj
- surj
- bij

2) Rel de echivalență, S.C.R

Rel de ordine

Parțial ordonată, Total ordonată, el. min, el. max, maxim, minim, d. Hasse

3) Euclid

Ex 4:

Pe $\mathbb{R}$, $x \sim y \Leftrightarrow (x^2 - x + 1)^2 = (y^2 - y + 1)^2$

a) Det $\sim$ - echiv

b) $[0]$, $[2]$ – Temă

a) Reflexivă: $\forall x \in \mathbb{R}$, $x \sim x = (x^2 - x + 1)^2 = (x^2 - x + 1)^2$ – Adev

b) Simetrică $x, y \in \mathbb{R}$ cu $x \sim y \overset{?}{\Rightarrow} y \sim x$

$x \sim y = (x^2 - x + 1)^2 = (y^2 - y + 1)^2 \Rightarrow (y^2 - y + 1)^2 = (x^2 - x + 1)^2 \Rightarrow y \sim x$ – Adev

c) Tranzitivă: $x, y, z \in \mathbb{R}$, $x \sim y$ și $y \sim z \overset{?}{\Rightarrow} x \sim z$

$x \sim y \Rightarrow (x^2 - x + 1)^2 = (y^2 - y + 1)^2$

$y \sim z \Rightarrow (y^2 - y + 1)^2 = (z^2 - z + 1)^2$ (+)

$(x^2 - x + 1)^2 = (z^2 - z + 1)^2 \Rightarrow x \sim z$ – Adev

$\Rightarrow \sim$ - echiv

b) $[0] = \{x \in \mathbb{R} \mid x \sim 0\}$

$x \sim 0 \Rightarrow (x^2 - x + 1)^2 = 1 \Rightarrow x^2 - x + 1 = \pm 1 \Rightarrow x^2 - x + 1 = 1 \Rightarrow x^2 - x = 0 \Rightarrow x \in \{0, 1\}$

$\Rightarrow x^2 - x + 1 = -1 \Rightarrow x^2 - x + 2 = 0$, $\Delta = 1 - 8 = -7 < 0 \notin \mathbb{R}$ $\Rightarrow$

$\Rightarrow [0] = \{0, 1\}$

$\Rightarrow [0] = \{0, \}$

5) Pe $\mathbb{C}^*$: $z \sim w \Leftrightarrow z, w, 0$ - coliniare

$z = \underset{x}{a} + \underset{y}{b}i \Rightarrow (a, b)$

a) $\sim$ - echiv

b) clase de echiv

c) S.C.R =?

b) $[z] = \{w \in \mathbb{C}^* \mid z, w, 0, \text{- coliniare}\}$

= toate pct de pe dr det de O și z

Cls de echiv = toate dr care trec prin O

c) S.C.R = semicercul fără un capăt