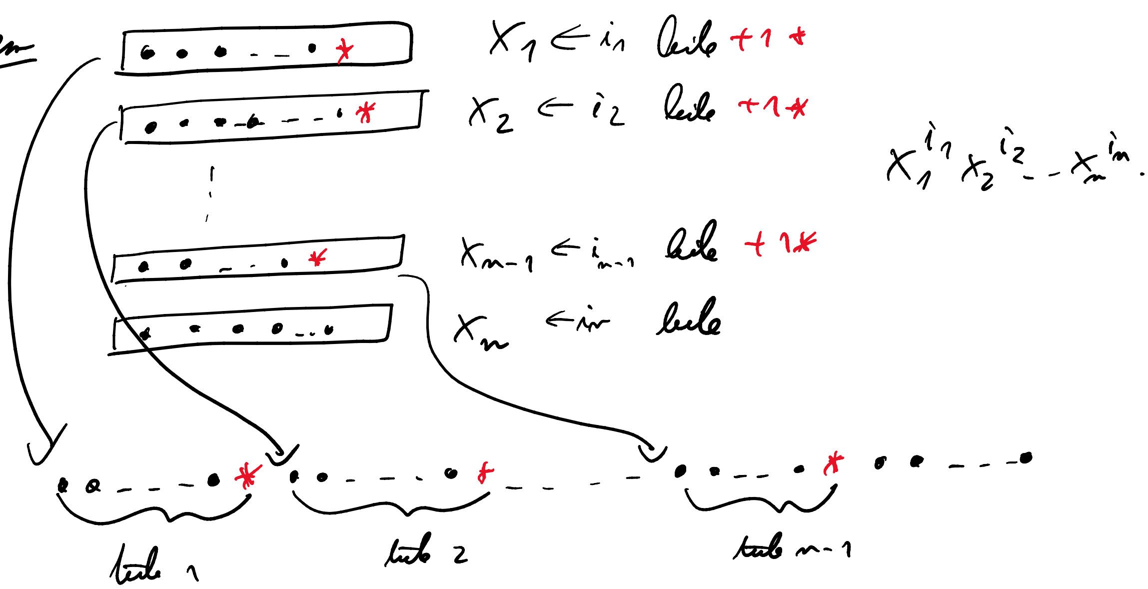
Inele de polinoame

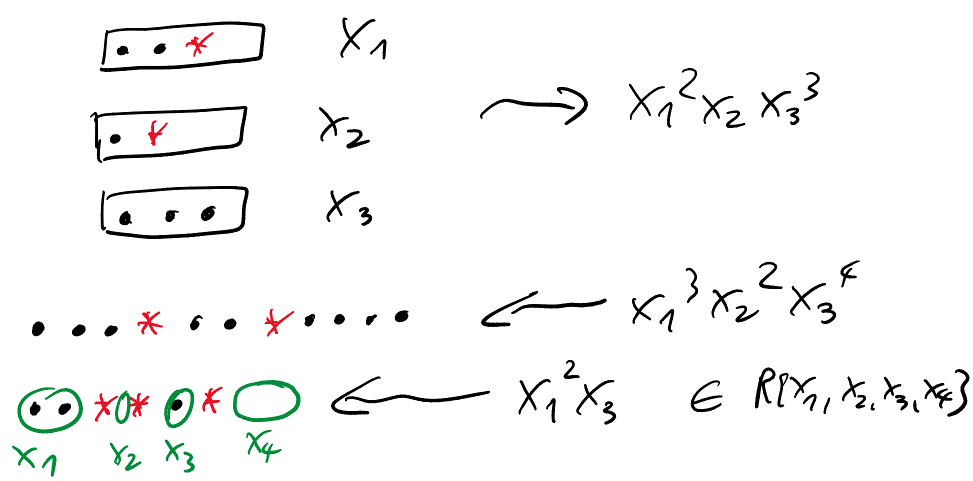
1.1. a) Câte monoame de grad d există în n variabile?

Ex: de grad 4 în 2 variabile: $\underbrace{x_1^4, x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2^4}_{5}$.

Dem



Exemplu $n=3$



Există o corespondență bijectivă între monoame și șirurile de bile negre și *!

Monoame de grad d în n variabile?

$\updownarrow$

șir cu $\underbrace{d \text{ bile și } (n-1)\,*}_{n+d-1 \text{ elemente în șir}}$ $\leftarrow$ $\boxed{C_{n+d-1}^{n-1} = C_{n+d-1}^{d}}$

alegerea pozițiilor pentru *

Pt $n=2$, $d=4$: $C_{2+4-1}^{1} = C_5^1 = 5$

b) Câte monoame de grad 8 în 5 variabile sunt mai mici strict ca $x_1^3 x_3 x_4$?

a) $2 \cdot 8^4$ b) 370 c) 375 d) 376

$x_1^a x_2^b x_3^c x_4^d x_5^e <_{lex} x_1^3 x_3 x_4$ și de grad 8.

$\boxed{a \le 3}$

- $x_1^3 x_3 x_5^4$ — 1
- $x_1^3 x_4^d x_5^e$, $d+e=5 \Rightarrow C_{2+5-1}^{5} = C_6^1 = 6$
- $x_1^2 x_2^b x_3^c x_4^d x_5^e \Rightarrow$ 4 variabile, grad 6, $C_{4+6-1}^{6} = C_9^6 = \frac{9!}{6!\cdot 3!} = \frac{\cancel{7}\cdot\cancel{8}\cdot\cancel{9}}{} = 84$
- $x_1^1 x_2^b x_3^c x_4^d x_5^e \Rightarrow$ 4 variabile, grad 7, $C_{4+7-1}^{7} = C_{10}^{7} = \frac{8\cdot 9\cdot 10}{6} = 120$

$$= \frac{\quad}{6} = 120$$

- $X_1^0 X_2^b X_3^c X_4^d X_5^e \Rightarrow$ 4 variabile grad 8 $\quad C_{4+8-1}^{8} = C_{11}^{8} = \frac{9 \cdot 10 \cdot 11}{6} = 165$

$$\longrightarrow 165 + 120 + 84 + 6 + 1 = 376$$

1.2. Fie K corp comutativ și $f, g \in K[X_1, \dots X_n]$.

a) Dem că, dacă K e infinit, atunci, dacă $f(x_1, \dots x_n) = g(x_1, \dots x_n)$, $\forall x_1, \dots x_n \in K \Rightarrow f = g$ (ca polinoame în $K[X_1, \dots X_n]$)

<u>Dem</u> În lista 1 de probleme: D <u>domeniu infinit</u>,

$\exists\ A_1 \times A_2 \times \dots \times A_n \subset D^n$, A_i infinite, a.î.

$$f(a_1, \dots a_n) = 0 \qquad \forall\ a_i \in A_i.$$

$$\Rightarrow f = 0 \in D[X_1, \dots X_n]$$

<u>Inducție</u> <u>$n=1$</u> Th Bézout (un polinom nenul f are cel mult $\deg f$ rădăcini)

Facem $n-1 \to n$:

Fie $f \in D[X_1, \dots X_n] \simeq \left(D[X_1, \dots X_{n-1}]\right)[X_n]$.

$$\Rightarrow f = \sum_{i=0}^{m} \underbrace{c_i(X_1, \dots X_{n-1})}_{\in D[X_1, \dots X_{n-1}]} \cdot X_n^i$$

Fie $(a_1, \dots a_{n-1}) \in A_1 \times \dots \times A_{n-1}$ fixat.

$$f(a_1, a_2, \dots a_{n-1}, X_n) = \sum_{i=0}^{n} C_i(a_1, \dots a_{n-1}) \cdot X_n^i \in D[X_n]$$

$$\begin{array}{c} f(a_1, a_2, \dots a_{n-1}, X_n) \\ \parallel \\ f_{(a_1, a_2, \dots a_{n-1})} \in D[X_n]. \end{array}$$

Obs $f_{(a_1, \dots a_{n-1})}(a_n) = 0, \ \forall a_n \in A_n \leftarrow$ infinită

$\xRightarrow{n=1} f_{(a_1 \dots a_{n-1})} = 0 \iff C_i(a_1, a_2, \dots a_{n-1}) = 0$

$C_i \in D[X_1, \dots X_{n-1}]$

$\xRightarrow[\text{inducție pt toți } c_i]{\text{pasul de}} C_i = 0 \in D[X_1, \dots X_{n-1}] \implies f = 0 \in D[X_1, \dots X_n]$.

b) Rămâne adevărată afirmația dacă K finit?

$K = \mathbb{Z}_p \quad : \quad f = X^p - X \in \mathbb{Z}_p[X]$.

Din Th Fermat: $a^p \equiv a \pmod p$

$\implies f(\hat{a}) = \hat{0} \in \mathbb{Z}_p, \ \forall \hat{a} \in \mathbb{Z}_p$

Dar $f \neq 0$ în $\mathbb{Z}_p[X]$!

1.3. $A \in M_n(\mathbb{R})$. Dem că

A este nilpotentă $\iff tr(A) = tr(A^2) = \dots = tr(A^n) = 0$

__Dem__ $\operatorname{Spec}(A) = \{ \lambda \in \mathbb{C} \mid \exists\, v \in \mathbb{C}^n,\ v \neq 0 \text{ a.î. } Av = \lambda v \}$

$$\Updownarrow$$

$$P_A(\lambda) = \det(A - \lambda I_n) = 0$$

mulțimea valorilor proprii

$\lambda_1, \lambda_2, \dots, \lambda_n$ valorile proprii (cu multiplicități)

$$\operatorname{tr}(A) = \sum_{i=1}^{n} \lambda_i$$

(Viète: $P_A(\lambda) = \begin{vmatrix} a_{11}-\lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-\lambda & \dots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \dots & a_{nn}-\lambda \end{vmatrix}$

$$P_A(\lambda) = (-1)^n \lambda^n + (-1)^{n-1} \underbrace{(a_{11} + \dots + a_{nn})}_{\operatorname{tr} A} \lambda^{n-1} + \dots$$

$$\Rightarrow \lambda_1 + \dots + \lambda_n = s_1 = -\frac{(-1)^{n-1} \operatorname{tr} A}{(-1)^n} = \operatorname{tr} A. \ )$$

! Valorile proprii ale lui A^ℓ sunt $\lambda_1^\ell, \lambda_2^\ell, \dots, \lambda_n^\ell$ (cu multiplicități)

„$\Rightarrow$" A este nilpotentă

$\Rightarrow A^m = 0$ pt un $m \geq 1 \overset{\text{Obs}}{\Longrightarrow} \lambda_i^m = 0,\ \forall i = \overline{1,n} \Leftrightarrow \lambda_i = 0.$

__Obs__ Dacă A respectă o relație polinomială $\Rightarrow$ orice valoare proprie o respectă

$$A^5 - 3A^2 + A + 5I_n = 0 \quad | \ (v)$$

Fie λ valoare proprie. Fie v a.î. $Av = \lambda v$, $v \neq 0$

$$\Rightarrow A^5 v - 3A^2 v + Av + 5v = 0$$

$$(\lambda^5 - 3\lambda^2 + \lambda + 5)\underset{\neq 0}{v} = 0 \Rightarrow \lambda^5 - 3\lambda^2 + \lambda + 5 = 0$$

$(\lambda^5 - 3\lambda^2 + \lambda + 5)\underset{\underset{0}{\shortparallel}}{v} = 0 \Rightarrow \lambda^5 - 3\lambda^2 + \lambda + 5 = 0$

$\Rightarrow \operatorname{tr}(A^l) = \sum_{i=1}^{n} \lambda_i^l = 0.$

"$\Leftarrow$" Pp că $\operatorname{tr}(A^l) = 0, \ \forall l = \overline{1,n}.$

$\Leftrightarrow \lambda_1^l + \lambda_2^l + \dots + \lambda_n^l = 0, \ \forall l = \overline{1,n}$

$\xRightarrow[\text{trecut}]{\text{Ex. seminarul}} \lambda_i = 0, \quad \forall i = \overline{1,n}.$

Dar $P_A(\lambda) = (-1)^n(\lambda^n - s_1\lambda^{n-1} + s_2\lambda^{n-2} - \dots + (-1)^n s_n)$

$\xlongequal{\lambda_i = 0 \Rightarrow s_i = 0} (-1)^n \lambda^n.$

$\xRightarrow{\text{Cayley-Hamilton}} O_n = P_A(A) = (-1)^n A^n!$

Ex. în plus față de listă:

- p prim, $F(X) = X^{p-1} + \dots + X + 1$. Calculați restul împărțirii lui $F(X^p)$ la $F(X)$.
- Arătați că $P(X) = (1 + X + \dots + X^n)^2 - X^n \in \mathbb{Q}[X]$ este reductibil, $\forall n \geq 2$.

Aritmetică în $\mathbb{Z}$ și $K[X]$

2.1. Folosiți alg lui Euclid pt a afla $(a,b) = d$ și o combinație liniară $ax + by = d$.

a) $a = 20, \ b = 13:$

a) $a = 20, \quad b = 13$:

$$20 = 1\cdot 13 + \underset{}{7}^{\,x_1} \implies 7 = 20 - 1\cdot 13$$

$$13 = 1\cdot 7 + 6^{\,x_2} \implies 6 = 13 - 1\cdot 7 = 13 - 1\cdot(20 - 1\cdot 13) = 2\cdot 13 - 1\cdot 20$$

$$7 = 1\cdot 6 + \boxed{1^{\,x_3}} = d = (20, 13)$$

$$6 = 6\cdot 1 + 0$$

$$\implies 1 = 7 - 1\cdot 6 = (20 - 1\cdot 13) - 1\cdot(2\cdot 13 - 1\cdot 20) = \underset{x}{\boxed{2}}\cdot 20 \underset{y}{\boxed{-3}}\cdot 13.$$

c) $a = 11391, \quad b = 5673$

$$11391 = 2\cdot 5673 + 45 \implies 45 = 11391 - 2\cdot 5673$$

$$5673 = 126\cdot 45 + \boxed{3} \implies 3 = 5673 - 126\cdot 45 = 5673 - 126\cdot(11391 - 2\cdot 5673) = \boxed{253}\cdot 5673 - \boxed{126}\cdot 11391.$$

$$45 = 15\cdot 3 + 0$$

Exc 2.3. Decideți dacă $\hat{69}$ este inversabil în $\mathbb{Z}_{89}$.
Dacă da, calculați $\hat{69}^{-1}$.

Idee: $\hat{a}^{-1} = ?$ în $\mathbb{Z}_n$

$$(a, n) = d \implies \exists\, x, y \in \mathbb{Z} \text{ a.î. } xa + yn = d.$$

Dacă $d = 1 \implies xa + yn = 1 \xRightarrow{\bmod n} \hat{x}\cdot\hat{a} = \hat{1}$.

Alg lui Euclid pt 69 și 89:

$$89 = 1\cdot 69 + 20 \implies 20 = 89 - 1\cdot 69$$

$$69 = 3\cdot 20 + 9 \implies 9 = 69 - 3\cdot 20 = 69 - 3(89 - 1\cdot 69)$$

$$69 = 3\cdot 20 + 9 \Rightarrow 9 = 69 - 3\cdot 20 = 69 - 3(89 - 1\cdot 69) = 4\cdot 69 - 3\cdot 89$$

$$20 = 2\cdot 9 + 2 \Rightarrow 2 = 20 - 2\cdot 9 = (89 - 1\cdot 69) - 2\cdot(4\cdot 69 - 3\cdot 89) = 7\cdot 89 - 9\cdot 69$$

$$9 = 4\cdot 2 + \boxed{1}$$

$$2 = 2\cdot 1 + 0$$

$$1 = 9 - 4\cdot 2 = (4\cdot 69 - 3\cdot 89) - 4\cdot(7\cdot 89 - 9\cdot 69) = \underline{40}\cdot 69 - 31\cdot 89$$

$\Rightarrow \hat{69}$ e inversabil în $\mathbb{Z}_{89}$ și $\hat{69}^{-1} = \hat{40}$.

2.2. Folosiți alg lui Euclid pt a afla $(P, Q) = D$ și o combinație liniară $fP + gQ = D$, unde $P, Q \in \mathbb{Q}[X]$.

corp

a) $P = X^3 - 2$, $Q = X + 1$

Dem

$$X^3 - 2 = (X^2 - X + 1)(X + 1) \boxed{-3} \quad R_1$$

$$X + 1 = -\tfrac{1}{3}(X+1)(-3) + \boxed{0}$$

$$\begin{array}{r|l} X^3 - 2 & X + 1 \\ \hline -X^3 - X^2 & X^2 - X + 1 \\ \hline -X^2 - 2 & \\ X^2 + X & \\ \hline X - 2 & \\ -X - 1 & \\ \hline -3 & \end{array}$$

$\Rightarrow (X^3 - 2, X + 1) = -3$

i.e. $(X^3 - 2, X + 1) = 1$

Def În $R = \mathbb{Z}$ sau $K[X]$, un cel mai mare divizor comun al $a, b \in R$ un element $d \in R$ a.î. dacă $c | a$, $c | b \Rightarrow c | d$.

Clasa a 6-a: $(24, 54) = \pm 6$?

Convenție: se alege cel pozitiv

Obs: d este un cel mai mare divizor comun al lui a și b $\Rightarrow$ $u \cdot d$ este și el un cel mai mare div. comun al lui a și b, $\forall u \in U(R)$

În $\mathbb{Z}$: d un cmmdc al a și b $\Rightarrow$ $\pm d$ este un cmmdc al a și b

În $K[X]$: T un cmmdc al P și Q $\Rightarrow$ aT ——— P și Q, $\forall a \in K, a \neq 0$

Convenție:
În $\mathbb{Z}$: se alege cel pozitiv
În $K[X]$: se alege cel monic
} vrem să alegem cel mai mare divizor comun

$\Rightarrow (X^3-2, X+1) = 1$.

Altfel: $X+1 \nmid X^3-2 \Rightarrow (X^3-2, X+1) = 1$.
($X+1$ de grad 1)

b) $P = X^5+2X^3+X^2+X+1$, $Q = X^5+X^4+2X^3+2X^2+2X+1$.

$X^5+X^4+2X^3+2X^2+2X+1 = 1 \cdot (X^5+2X^3+X^2+X+1) + \underbrace{(X^4+X^2+X)}_{R_1} \Rightarrow R_1 = Q-P$

$$X^5+2X^3+X^2+X+1 = X(X^4+X^2+X)+X^3+X+1 \Rightarrow R_2 = P - XR_1 =$$

R_2

$$= P - X(Q-P)$$

$$= (X+1)P - XQ$$

$$\begin{array}{r|l} X^5+2X^3+X^2+X+1 & X^4+X^2+X \\ -X^5-X^3-X^2 & \overline{X} \\ \hline R = X^3 \quad +X+1 & \end{array}$$

$$X^4+X^2+X = X(X^3+X+1) + 0$$

$(Q, P) = X^3+X+1$ și $\boxed{X^3+X+1 = (X+1)P - XQ}$

Obs. Are loc și în $\mathbb{Z}[X]$!

c) Temă (NU merge și în $\mathbb{Z}[X]$!)

Q $ax+by=d$

Cum rezolvăm în $x,y \in \mathbb{Z}$ ecuația ?

$\underbrace{\text{rezolvăm în } x,y \in \mathbb{Z}}_{\text{ecuație diofantică}}$

De ex, $17x+29y=31$.

Exe 2.4. Fie $R = \mathbb{Z}$ sau $K[X]$, K corp.

a)

$\Uparrow$ $a, b, c \in R$. De $a \mid bc \Rightarrow \frac{a}{(a,b)} \mid c$.

a) $\Uparrow$ b) $a, b, c \in R$. Dc $a \mid bc \Rightarrow \frac{a}{(a,b)} \mid c$.

Dem $bc = ax$. Fie $d = (a,b)$

$\Rightarrow \frac{b}{d} \cdot c = \frac{a}{d} \cdot x$, $\frac{b}{d}, \frac{a}{d} \in R$ pt că $d \mid a, d \mid b$.

$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$: $\boxed{\text{Pp că } \exists\, l \in R \text{ ai } l \mid \frac{a}{d},\ l \mid \frac{b}{d}.}$

$\Rightarrow ld \mid a,\ ld \mid b \Rightarrow ld \mid d \Rightarrow l \in U(R)$

$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

$\frac{b}{d} \cdot c = \frac{a}{d} \cdot x \Rightarrow \exists\, y, z \in R$ ai $y \cdot \frac{b}{d} + z \cdot \frac{a}{d} = 1 \mid \cdot c$

$\Rightarrow y \cdot \underbrace{\boxed{\frac{b}{d} \cdot c}}_{= \frac{a}{d} x} + z \cdot \frac{a}{d} \cdot c = c \Rightarrow \frac{a}{d}(yx + zc) = c$

$\Rightarrow \frac{a}{d} \mid c$!

c) Fie $a, b \in R$, $n \in R$. At $\exists\, x, y \in R$ ai $ax + by = n$

$\Leftrightarrow (a,b) \mid n$.

„$\Rightarrow$" $\forall\, d \mid a, d \mid b \Rightarrow d \mid (ax + by) \Rightarrow d \mid n$.

„$\Leftarrow$" Alg lui Euclid: $\exists\, x', y' \in R$ ai $ax' + by' = d$

Dar $d \mid n$ din ipoteză.

Dar $d \cdot c = n$ prin ipoteză.

$$\Rightarrow a\underbrace{\boxed{x'c}}_{x} + b\underbrace{\boxed{y'c}}_{y} = dc = n$$

Deci $2x+4y=15$ nu are soluții

și $17x+29y=31$ <u>are</u> soluții

d) Fie $a, b \in R$, $n \in R$. Arătați că, dacă (x_0, y_0) este o soluție particulară, atunci <u>toate</u> soluțiile sunt de forma $x_0 + m\frac{b}{(a,b)}$, $y_0 - m\frac{a}{(a,b)}$, $m \in R$

$$a\left(x_0 + m\frac{b}{(a,b)}\right) + b\left(y_0 - m\frac{a}{(a,b)}\right) = n,$$

$$\boxed{m \in R}$$

<u>Dem</u> Știm $ax_0 + by_0 = n$. Fie (x, y) altă soluție:

$$ax + by = n.$$

$$\Rightarrow a(x-x_0) + b(y-y_0) = 0 \Leftrightarrow a(x-x_0) = -b(y-y_0)$$

~~împart la (a,b)~~ $\cancel{\Rightarrow \frac{a}{d}(x-x_0) = -\frac{b}{d}(y-y_0)}$;

$$\Rightarrow a \mid -b(y-y_0) \overset{b)}{\Rightarrow} \frac{a}{(a,b)} \mid (y-y_0)$$

$\Rightarrow \exists\, m \in \mathbb{R}$ a.î. $m \cdot \frac{a}{(a,b)} = y - y_0 \Rightarrow \boxed{y = y_0 + m \frac{a}{(a,b)}}$

$\Rightarrow \cancel{a}(x - x_0) = -b \cdot m \cdot \frac{\cancel{a}}{(a,b)}$

$\Rightarrow \boxed{x = x_0 - m \cdot \frac{b}{(a,b)}}$. $\quad (m \leftrightarrow -m)$

2.5. b) $17x + 29y = 31$.

Alg. lui Euclid pt 17 și 29:

$29 = 1 \cdot 17 + 12 \Rightarrow 12 = 29 - 1 \cdot 17$

$17 = 1 \cdot 12 + 5 \Rightarrow 5 = 17 - 1 \cdot 12 = 17 - (29 - 1 \cdot 17)$

$= 2 \cdot 17 - 29$

$12 = 2 \cdot 5 + 2 \Rightarrow 2 = 12 - 2 \cdot 5 = (29 - 1 \cdot 17) - 2(2 \cdot \cancel{17} - 29)$

$5 = 2 \cdot 2 + \boxed{1}$

$= 3 \cdot 29 - 5 \cdot 17$

$2 = 2 \cdot 1 + 0$

$\Rightarrow 1 = 5 - 2 \cdot 2 = (2 \cdot 17 - 29) - 2(3 \cdot 29 - 5 \cdot 17)$

$= 12 \cdot 17 - 7 \cdot 29$

$\Rightarrow 12 \cdot 17 + (-7) \cdot 29 = 1 \quad | \cdot 31$

$\underbrace{(12 \cdot 31)}_{x_0} \cdot 17 + \underbrace{(-7 \cdot 31)}_{y_0} \cdot 29 = 31$ soluție particulară

d) Soluția generală este: $(x, y) = \left(x_0 + m\frac{b}{(a,b)}, y_0 - m\frac{a}{(a,b)}\right)$, $m \in \mathbb{Z}$

$$\Rightarrow \boxed{(x,y) = (12\cdot 31 + m\cdot 29, -7\cdot 31 - m\cdot 97), \; m\in\mathbb{Z}}$$

c) Temă!

$(a,b) = 1$, $a,b > 0$

$ax + by = n$

2.8. $n, m \geq 1$. Arătați că $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$ în $\mathbb{Q}[X]$.

Dem • $m \mid n \Rightarrow X^m - 1 \mid X^n - 1$.

$$n = qm \Rightarrow X^n - 1 = X^{qm} - 1 = (\underbrace{X^m}_{Y})^q - 1 =$$

$$= \left((X^m)^{q-1} + (X^m)^{q-2} + \dots + 1\right)\left(X^m - 1\right)$$

• $n = qm + r \leftarrow$ Th de împărțire cu rest

$$\Rightarrow X^n - 1 = \boxed{Q(X^m - 1) + (X^r - 1)}, \quad r < m.$$

Deci, dacă restul împărțirii lui n la m este r în $\mathbb{Z}$

$\Rightarrow$ $X^n - 1$ — $X^m - 1$ — X^{r-1}

Deci, dacă restul împărțirii ...

$\Rightarrow$ ______ X^n-1 — X^m-1 — $X^{r}-1$ în $\mathbb{Q}[X]$

$$X^n-1 = X^{qm+r}-1 = X^{qm+r}-X^r+\left(X^r-1\right) =$$

$$= X^r\left(X^{qm}-1\right)+X^r-1 = \overbrace{X^r\left(\left(X^m\right)^{q-1}+\dots+\left(X^m\right)+1\right)}^{Q}\left(X^m-1\right)$$

$$+\left(X^r-1\right)$$

Rezolvă problema, $n \geq m$, cu algoritmul lui Euclid: $\deg(X^n-1) \geq \deg(X^m-1)$

$n = q_1 m + r_1 \quad \Longleftrightarrow \quad X^n-1 = Q_1(X^m-1)+(X^{r_1}-1)$

$m = q_2 r_1 + r_2 \quad \Longleftrightarrow \quad X^m-1 = Q_2(X^{r_1}-1)+(X^{r_2}-1)$

$\vdots \qquad\qquad \vdots$

$r_q = q_{q+1} r_{q-1} + \boxed{r_{q+1}}$, $r_{q+1} = (n,m) \quad \Longleftrightarrow \quad X^{r_q}-1 = Q_{q+1}(X^{r_{q-1}}-1)+\boxed{(X^{r_{q+1}}-1)}$, $(X^m-1, X^n-1) = X^{r_{q+1}}-1$

$r_{q+1} = q_{q+2} r_q + 0 \qquad X^{r_{q+1}} = Q_{q+2}(X^{r_q}-1)+\boxed{0}$, $0 = X^0-1$

$\square$

2.11. $\left(X^{23}+X^{22}+\dots+X+1,\ X^{53}+X^{52}+\dots+X+1\right) = ?$

Știm că $(X-1)(X^{23}+\dots+X+1) = X^{24}-1$

$(X-1)(X^{53}+\dots+X+1) = X^{54}-1$

și $(X^{54}-1, X^{24}-1) = X^{6}-1$

$= (X-1)(X^{5}+\dots+1)$.

<u>Obs</u> $(ab, ac) = a(b,c)$, $\forall a,b,c \in \mathbb{Z}$ sau $K[X]$

$\Rightarrow \big((X-1)(X^{23}+\dots+X+1), (X-1)(X^{53}+\dots+X+1)\big) = \cancel{(X-1)}f$

$\qquad \|$

$\cancel{(X-1)}(X^5+X^4+\dots+X+1)$

$\Rightarrow f = (X^{23}+\dots+X+1, X^{53}+\dots+X+1) = X^5+\dots+X+1$

și, în general,

$(X^{a}+\dots+X+1, X^{b}+\dots+X+1) = X^{(a+1,b+1)-1}+\dots+X+1$.

<u>Ex 2.9.</u> $\forall n, m \geq 1$, $(2^n-1, 2^m-1) = 2^{(n,m)}-1$.

În particular, $2^n-1 \mid 2^m-1 \Leftrightarrow n \mid m$.

<u>Obs</u> $P, Q \in \mathbb{Z}[X]$, $(P,Q) = h$

$\not\Rightarrow (P(2), Q(2)) = h(2)$

<u>Dem</u> Alg Euclid: $\exists f, g \in \mathbb{Q}[X]$ a.î. $fP+gQ = h \mid (2)$

Dem Alg Euclid: $\exists\ f, g \in \mathbb{Q}[X]$ a.î. $fP + gQ = R$ (2)

$$f(2)P(2) + g(2)Q(2) = R(2)$$ relație în $\mathbb{Q}$

$$\cancel{\begin{matrix} R(2) \mid P(2) \\ R(2) \mid Q(2) \end{matrix} \Longrightarrow (P(2), Q(2)) = R(2)}$$

Dar $P = X$, $Q = X - 2 \Rightarrow (P, Q) = 1$ dar

$$(P(6), Q(6)) = (6, 4) = 2!$$

Deci $(X^n - 1, X^m - 1) = X^{(n,m)} - 1$, nu pot "evalua în 2"

$$\overset{?}{\not\Rightarrow} \quad (2^n - 1, 2^m - 1) = 2^{(n,m)} - 1.$$

Dar → Var 1 Rescriem dem de la 2.8 cu 2 în loc de X

→ Var 2 Observ că, pt $X^n - 1, X^m - 1$, $f, g \in \mathbb{Q}[X]$

a.î. $f(X^n - 1) + g(X^m - 1) = X^{(n,m)} - 1$

sunt de fapt în $\mathbb{Z}[X]$!

2.10. Det toate numerele $n < 10^{100}$ a.î. $n \mid 2^n$

2.10. Det toate numerele $n < 10^{100}$ a.i. $n \mid 2^n$

$n-1 \mid 2^n - 1$

$n-2 \mid 2^n - 2$.

Dem $n \mid 2^n \Rightarrow \boxed{n = 2^k}$, $k \le n$.

$\Rightarrow 2^k \mid 2^{2^k}$.

$\Rightarrow 2^k - 1 \mid 2^{2^k} - 1 \Longrightarrow k \mid 2^k \Rightarrow k = 2^q$, $q \le k$.

$\Rightarrow n = 2^k = 2^{2^q}$.

$2^{2^q} - 2 \mid 2^{2^{2^q}} - 2$

$\cancel{2}\left(2^{2^q - 1} - 1\right) \mid \cancel{2}\left(2^{2^{2^q} - 1} - 1\right)$

$\Rightarrow 2^{2^q - 1} - 1 \mid 2^{2^{2^q} - 1} - 1 \Longrightarrow 2^q - 1 \mid 2^{2^q} - 1$

$\Rightarrow q \mid 2^q \Rightarrow q = 2^t$, $t \in \mathbb{N}$.

$\Rightarrow \boxed{n = 2^{2^{2^t}}}$, $t \in \mathbb{N}$. Vrem $n < 10^{100}$.

$$\boxed{\begin{array}{lll} t=0 & \Rightarrow & n=4 \\ t=1 & \Rightarrow & n=2^4=16 \\ t=2 & \Rightarrow & n=2^{16} \\ t=3 & \Rightarrow & n=2^{256} \end{array}} = 8^{\frac{256}{3}} < 10^{100}. \qquad 2^{16}-5 \text{ cifre}$$

$$t=4 \Rightarrow n = 2^{2^{16}} = 16^{2^{14}} > 10^{100}$$

<u>Exc 2.7</u> $n \in \mathbb{N}^*$. Arătați că

$$(n!+1, (n+1)!+1) = 1.$$

<u>Dem</u> Fie $d \mid n!+1 \Rightarrow d \mid (n!+1)\cdot(n+1) = (n+1)!+(n+1)$

$d \mid (n+1)!+1$.

$$\frac{d \mid (n+1)!+1}{}$$

$$\Rightarrow d \mid n \mid n!$$

$$\frac{d \mid n!+1}{d \mid 1} \Rightarrow d = \pm 1, \ \forall d \text{ divizor comun}$$

$$\Rightarrow (n!+1, (n+1)!+1) = 1.$$