Seminarul 10

Wednesday, April 21, 2021 9:02 AM

Aritmetică în $\mathbb{Z}$ și $K[X]$

2. Fie $F_n = 2^{2^n}+1$, $n \geq 0$.

a) Dem că $F_n = F_0 F_1 \dots F_{n-1} + 2$, $\forall n \geq 1$ și că $(F_r, F_m)=1$, $\forall r \neq m$

b) Dem că $\exists$ o infinitate de numere prime.

Dem $F_0 F_1 \dots F_{n-1} = (2^{2^0}+1)(2^{2^1}+1) \dots (2^{2^{n-1}}+1)$

$$= \sum_{\ell=0}^{2^n-1} 2^\ell$$

Scrierea în baza 2: $\forall \ell \in \mathbb{N}$, $\exists k \geq 0$, $\exists!\ a_i \in \{0,1\}$, $1 \leq i \leq k$ a.î.

$$\ell = \sum_{i=0}^{k} a_i 2^i$$

$29 = 1\cdot 16 + 1\cdot 8 + 1\cdot 4 + 1\cdot 2^0$

$= 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$

$29 = (11101)_2$

$\Rightarrow F_0 F_1 \dots F_{n-1} + 1 = \sum_{\ell=0}^{2^n-1} 2^\ell + 1 \overset{!}{=} 2^{2^n}$

$= F_n - 1$

$\Rightarrow F_n = F_0 F_1 \dots F_{n-1} + 2$

Var 2 Prin inducție: pp că relația are loc până la n

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n}-1)(2^{2^n}+1)$$

$$= (2^{2^n}-1) F_n = (F_n - 2) F_n \overset{\text{ip. ind}}{=} (F_0 F_1 \dots F_{n-1}) \cdot F_n$$

$$= F_0 F_1 \dots F_n.$$

$(F_n, F_m) = 1$: $\boxed{F_n = F_0 F_1 \dots F_{n-1} + 2}$

Dacă $d \mid F_n,\ d \mid F_m \overset{n<m}{\Longrightarrow} d \mid \underbrace{F_0 F_1 \dots F_{m-1}}_{\text{apare și } F_n}$

$d \mid F_m$

$\Rightarrow d \mid 2 \Rightarrow d = \pm 1$, sau $d = \pm 2$. Dar $2 \nmid F_n$

$\Rightarrow d = \pm 1 \quad \Rightarrow \quad (F_n, F_m) = 1.$

b) Fie $p_n \mid F_n$, p_n prim.

$\Rightarrow (p_n)_n$ nu are repetiții ($\nexists\, p \mid F_n,\ p \mid F_m$)

$\Rightarrow$ e și infinit!

F_n sunt numerele Fermat. Sunt toate prime?

$F_0 = 3,\ F_1 = 5,\ F_2 = 2^{2^2} + 1 = 17,\ F_3 = 2^{2^3} + 1 = 257$

$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$ prim!

Euler: F_5 nu e prim!

Până acum, dintre F_n-uri, doar F_0, F_1, F_2, F_3, F_4 știm că sunt prime!

1.3. Calculați cmmdc și cmmmc în $\mathbb{Q}[X]$ pentru:

a) $X^3 - 2$ și $X + 1$

– Alg lui Euclid

a) X^3-2 și $X+1$

Idei generale — Alg lui Euclid
— Descompunerea în factori ireductibili

Aici: X^3-2 e ireductibil pt că $\boxed{\deg \leq 3 \text{ și nu are rădăcini}}$

$X+1$ e ireductibil pt că $\deg X+1 = 1$

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

b) $X^5+2X^3+X^2+X+1$ și $X^5+X^4+2X^3+2X^2+2X+1$

Dată trecută: Alg lui Euclid:

$$X^3+X+1 = (X+1)(X^5+2X^3+X^2+X+1) - X(X^5+X^4+2X^3+2X+1)$$

$$\Rightarrow (X^5+2X^3+X^2+X+1, X^5+X^4+2X^3+2X^2+2X+1) = X^3+X+1$$

$$[\ ,\ ] = \frac{(X^5+2X^3+X^2+X+1)(X^5+X^4+2X^3+2X^2+2X+1)}{X^3+X+1}$$

$$\boxed{a \cdot b = (a,b) \cdot [a,b]}$$

$$= (X^2+1)(X^5+X^4+2X^3+2X^2+2X+1)$$

$$\begin{array}{l|l} X^5+2X^3+X^2+X+1 & X^3+X+1 \\ \hline -X^5-X^3-X^2 & X^2+1 \\ \quad X^3+X+1 & \\ -X^3-X-1 & \\ \quad // & \end{array}$$

c) X^4-1 și X^6-1

1 Alg lui Euclid: $(X^6-1, X^4-1) = X^{(6,4)}-1 = X^2-1$

1. Alg lui Euclid: $(X^6-1,\ X^4-1) = X^{(6,4)}-1 = X^2-1$

2. Descompunerea în factori ireductibili:

ired pt că deg=2 și nu are răd în $\mathbb{Q}$

$$X^4-1 = (X^2-1)(X^2+1) = \underline{(X-1)(X+1)}(X^2+1)$$

$$X^6-1 = (X^3-1)(X^3+1) = (X-1)(X^2+X+1)(X^3+1)$$

$$= \underline{(X-1)}(X^2+X+1)\underline{(X+1)}(X^2-X+1)$$

$$\Rightarrow (X^6-1,\ X^4-1) = (X-1)(X+1) = X^2-1$$

d) $P=(X-1)(X^2-1)(X^3-1)(X^4-1)$ și $Q=(X+1)(X^2+1)(X^3+1)(X^4+1)$

$$P = \underbrace{(X-1)}\,\underbrace{(X-1)(X+1)}\,\underbrace{(X-1)(X^2+X+1)}\,\underbrace{(X-1)(X+1)(X^2+1)}$$

$$= (X-1)^4(X+1)^2(X^2+X+1)(X^2+1)$$

$$Q = (X+1)(X^2+1)(X+1)(X^2-X+1)(X^4+1)$$ e ireductibil ?

Obs X^4+1 nu are rădăcini, DAR, fiind de grad 4, nu știm că este ireductibil încă!

Var 1 Neavând rădăcini, dacă nu este ireductibil, atunci $X^4+1 = (X^2+aX+b)(X^2+cX+d)$, $a,b,c,d\in\mathbb{Q}$

le putem pp monice

$$\begin{cases} bd=1 \\ bc+ad=0 \\ b+d+ac=0 \end{cases} \Rightarrow a(b-d)=0$$

$\nearrow$ $a=0 \Rightarrow c=0 \Rightarrow b+d=0$, $d=-b$ și $b^2=-1$ ab $b\in\mathbb{Q}$

$\searrow$ $b=d \Rightarrow b^2=1 \Rightarrow b=\pm 1$

$$\begin{cases} b+d+ac=0 \\ c+a=0 \Rightarrow c=-a \end{cases}$$

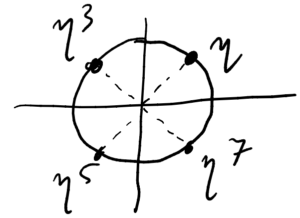
$\checkmark$ $b=d \Rightarrow b^2=1 \Rightarrow b=\pm 1$ ($=d$)

$\Rightarrow \pm 2 - a^2 = 0 \Rightarrow a^2 = \pm 2$ contradicție ($a \in \mathbb{Q}$)

$\times$ $b^2=-1$ contradicție ($b\in\mathbb{Q}$)

$\Rightarrow X^4+1$ este ireductibil în $\mathbb{Q}[X]$.

Var 2 Dacă X^4+1 reductibil, se scrie ca $f\cdot g$ cu $\deg f = \deg g = 2$.



$$X^4+1 \overset{\text{în } \mathbb{C}[X]}{=\!=\!=} (X-\eta)(X-\eta^3)(X-\eta^5)(X-\eta^7)$$

$\eta = \cos\frac{\pi}{4} + i \sin\frac{\pi}{4}$

și pp că $X^4+1 \overset{\text{în } \mathbb{Q}[X]}{=\!=\!=} f\cdot g$

$\Rightarrow f, g$ sunt produse de câte 2 din . Dar produsul a oricare 2 nu este în $\mathbb{Q}[X]$ (Ex!)

1.4. $I=(X^3+1)$, $J=(X^5+1) \trianglelefteq \mathbb{Q}[X]$.

Calculați $I+J$ și $I\cap J$.

Reamintire $K[X]$ (K corp) este inel principal ($\Leftrightarrow$ $\forall$ ideal este principal)

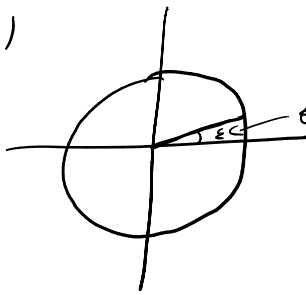
$$(f)+(g) = \underset{\text{idealul generat de } f \text{ și } g}{(f,g)} = \underset{\text{idealul generat de } \gcd(f,g)}{((f,g))}$$

$$\boxed{(X^3+1)+(X^5+1) = (X+1)}$$

$X^5+1 = (X+1)(X^4-X^3+X^2-X+1)$ ← nu știm dacă este descompunere

$X^3+1 = (X+1)(X^2-X+1)$

↗ descompunere în factori ireductibili



Fie $\varepsilon = \cos\frac{2\pi}{10} + i\sin\frac{2\pi}{10}$, $\theta = \frac{\pi}{5} = 36^\circ$

$\Rightarrow X^5+1$ are, în $\mathbb{C}$, rădăcinile ε^{2k+1}, $k=\overline{0,4}$

$\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7, \varepsilon^9$

$\varepsilon^5 = -1$

răd ale lui $X^4-X^3+X^2-X+1$

Dar $(X^4-X^3+X^2-X+1,\ X^2-X+1) = 1$

$\Rightarrow (X^5+1, X^3+1) = X+1$

$$(X^5+1)\cap(X^3+1) = (\mathrm{lcm}(X^5+1, X^3+1)) = \left(\frac{(X^5+1)(X^3+1)}{X+1}\right)$$

$$= \left((X^5+1)(X^2-X+1)\right)$$

1.5. Care dintre următoarele polinoame este ireductibil în $\mathbb{Q}[X]$?

	Rădăcini posibile	Ired în $\mathbb{Q}[X]$?	
$3X^2-7X+1$	$\pm 1, \pm \frac{1}{3}$	---	
$6X^3-3X-18$	$\pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{2}, \pm\frac{3}{2}$	--	
X^3-7X+1	± 1	✓	
X^3-9X-9	$\pm 1, \pm 3, \pm 9$	---	

Prop. Fie $f \in K[X]$, $\deg f \geq 2$.

i) Dacă f are rădăcini $\overset{\text{Bézout}}{\Longrightarrow}$ f este reductibil

ii) $\boxed{\text{Dacă } \deg f \leq 3}$, f ireductibil $\Leftrightarrow$ f nu are rădăcini

ii) $\boxed{\text{Dacă } \deg f \leq 3}$, f ireductibil $\Leftrightarrow$ f nu are rădăcini

dem: $3 = 1+2$

$2 = 1+1$

$6X^3 - 3X - 18 = 3\boxed{(2X^3 - X - 6)}$ $\frac{a}{b}$ rădăcină în $\mathbb{Q} \Rightarrow a|6$, $b|2$

verificăm rădăcinile

Def Fie R inel. $a \in R$ s.n. <u>ireductibil</u> dacă $a \neq 0$, $a \notin U(R)$ și $a = bc \Rightarrow b \in U(R)$ sau $c \in U(R)$

De exemplu: $f = 2X - 2 \in \mathbb{Z}[X]$.

În $\mathbb{Q}[X]$, f este ireductibil ($\deg f = 1$)

În $\mathbb{Z}[X]$: $2X - 2 = 2(X-1)$

nu sunt ireductibile.

<u>Lema Gauss</u> Fie $f \in \mathbb{Z}[X]$ a.î. cmmdc al coeficienților lui f este 1.

Atunci f ired în $\mathbb{Z}[X] \Leftrightarrow$ f ired în $\mathbb{Q}[X]$.

<u>Ex 1.6.</u> Dem că $X^3 + nX + 2$ este ired în $\mathbb{Q}[X] \Leftrightarrow$ $n \neq 1, -3, -5$. $n \in \mathbb{Z}$

<u>Dem</u> $f(X) = X^3 + nX + 2$ e ired $\Leftrightarrow$ $f(\pm 1) \neq 0$, $f(\pm 2) \neq 0$.

$f(1) = m+3 \neq 0 \Rightarrow m \neq -3$

$f(-1) = -1-m+2 = -m+1 \Rightarrow m \neq 1$ ✓

$f(2) = 2m+10 \Rightarrow m \neq -5$

$f(-2) = -8-2m+2 \Rightarrow m \neq -3.$

<u>Ex 1.7.</u> Determinați toate polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

$\#\{\text{Polinoame de grad } \leq 5\} = 2^6$

$$\boxed{f = a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0},$$

$a_i \in \{\hat{0}, \hat{1}\}$

<u>Rem</u> Pentru cele de grad ≤ 3:

<u>deg 1</u>: $X, X+\hat{1}$

<u>Obs</u> $f(\hat{0}) \neq \hat{0} \Leftrightarrow f$ are termen liber (i.e. $\hat{1}$)

$f(\hat{1}) \neq \hat{0} \Leftrightarrow f$ are un număr impar de termeni (nenuli)

<u>deg 2</u>: X^2+X+1 singurul!

<u>deg 3</u>: X^3+X^2+1, X^3+X+1

} nu au rădăcini și au grad ≤ 3 $\Rightarrow$ sunt ireductibile

---

deg ≥ 4: Încep prin a le scrie doar pe cele care nu au rădăcini (celelalte sunt sigur reductibile) deg 4: $X^4+X^3+\hat{1}$, $\cancel{X^4+X^2+\hat{1}}$, $X^4+X+\hat{1}$

$X^4+X^3+X^2+X+1$

Idee: Dacă P ar fi reductibil, $\deg P=4$ și P nu are rădăcini, atunci $P=f\cdot g$, f, g ireductibile de grad 2

$$\Rightarrow f=g=X^2+X+\hat{1}$$

$(X^2+X+\hat{1})^2 = X^4+X^2+\hat{1}$ singurul reductibil de mai sus!

deg 5: $\cancel{X^5+X^4+\hat{1}}$, $X^5+X^3+\hat{1}$, $X^5+X^2+\hat{1}$, $\cancel{X^5+X+\hat{1}}$

$X^5+X^4+X^3+X^2+\hat{1}$, $X^5+X^4+X^3+X+\hat{1}$, $X^5+X^4+X^2+X+\hat{1}$, $X^5+X^3+X^2+X+\hat{1}$.

La fel, $\underset{\deg 5}{P}=\underset{\deg 3}{f}\cdot\underset{\deg 2}{g}$ $\Rightarrow g = X^2+X+\hat{1}$

$f=X^3+X^2+\hat{1}$ sau $f=X^3+X+\hat{1}$.

$$(X^3+X^2+\hat{1})(X^2+X+\hat{1}) = X^5+X+\hat{1}$$
$$(X^3+X+\hat{1})(X^2+X+\hat{1}) = X^5+X^4+\hat{1}$$

Exc 1.8. Descompuneți în factori ireductibili polinoamele următoare din $\mathbb{Z}_2[X]$:

a) $X^5+X^3+\hat{1}$ - ired, vedeți mai sus

b) $X^6+X^4+X+\hat{1}$ — Temă

c) $X^{15}+\hat{1} = X^{15}-\hat{1} = (X^5-\hat{1})\left((X^5)^2+X^5+\hat{1}\right)$

c) $X^{15}+\hat{1} = X^{15}-1 = (X^5-\hat{1})((X^5)^2+X^5+1)$

$= (X^5-\hat{1})(X^{10}+X^5+\hat{1}) = (X+\hat{1})(X^4+X^3+X^2+X+\hat{1})\cdot$

$\cdot(X^{10}+X^5+\hat{1}) = (X+\hat{1})(X^4+X^3+X^2+X+\hat{1})(X^2+X+\hat{1})(X^8+X^7+X^5+X^4+X^3+X+\hat{1})$

Tema e ired?

$$
\begin{array}{l|l}
X^{10}+X^5+\hat{1} & X^2+X+\hat{1} \\ \hline
-X^{10}-X^9-X^8 & X^8-X^7+X^5-X^4+X^3-X+\hat{1} \\ \hline
\quad -X^9-X^8+X^5+\hat{1} & \\
\quad X^9+X^8+X^7 & \\ \hline
\quad\quad X^7+X^5+\hat{1} & \\
\quad\quad -X^7-X^6-X^5 & \\ \hline
\quad\quad\quad -X^6+\hat{1} & \\
\quad\quad\quad X^6+X^5+X^4 & \\ \hline
\quad\quad\quad\quad X^5+X^4+\hat{1} & \\
\quad\quad\quad\quad -X^5-X^4-X^3 & \\ \hline
\quad\quad\quad\quad\quad -X^3+\hat{1} & \\
\quad\quad\quad\quad\quad X^3+X^2+X & \\ \hline
\quad\quad\quad\quad\quad\quad X^2+X+1 & \\
\quad\quad\quad\quad\quad\quad -X^2-X-\hat{1} & \\ \hline
\quad\quad\quad\quad\quad\quad\quad 0 &
\end{array}
$$

$f: M \to N \ni c$ val reg

$\forall x \in f^{-1}(c)$,

$d_x f$ e surjectivă

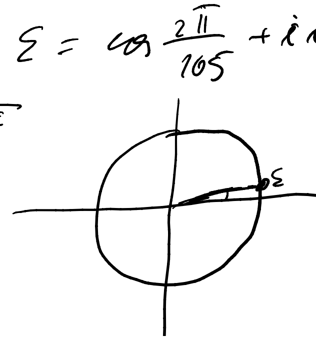
$\Rightarrow f^{-1}(c)$ e subvarietate

și $T_x f^{-1}(c) = \operatorname{Ker} d_x f$

Exc 1.11 $P(X) = X^{105}-9$ este ireductibil în $\mathbb{Q}[X]$.

$P(X)$ are, în $\mathbb{C}$, rădăcinile $\sqrt[105]{9}\cdot\varepsilon^l$, $\varepsilon = \cos\frac{2\pi}{105} + i\sin\frac{2\pi}{105}$

$l = \overline{0,104}$



$P(X) = (X - \sqrt[105]{9})(X - \sqrt[105]{9}\cdot\varepsilon)(X - \sqrt[105]{9}\,\varepsilon^2)$

$$P(x) = (X - \sqrt[105]{9})(X - \sqrt[105]{9}\cdot\varepsilon)(X - \sqrt[105]{9}\cdot \varepsilon^{2}) \ldots$$

$$\ldots (X - \sqrt[105]{9}\cdot\varepsilon^{104})$$

Dacă $P(X) = f(X)\cdot g(X)$, $\deg f, \deg g \geq 1$
$f, g \in \mathbb{Q}[X]$

$$\Rightarrow f(X) = (X - \sqrt[105]{9}\cdot\varepsilon^{i_1})(X - \sqrt[105]{9}\cdot\varepsilon^{i_2}) \ldots (X - \sqrt[105]{9}\,\varepsilon^{i_r})$$

$1 \leq r \leq 104$

$$\Rightarrow \underset{\text{termenul liber}}{f(0)} = \pm\sqrt[105]{9^r}\cdot\varepsilon^{i_1+i_2+\ldots+i_r} \in \mathbb{Q}$$

$$\Rightarrow |f(0)| \in \mathbb{Q}$$

$$|f(0)| = \sqrt[105]{9^r}, \quad 1 \leq r \leq 104$$

$$\sqrt[105]{9^r} = 3^{\frac{2r}{105}} \in \mathbb{Q} \Leftrightarrow \frac{2r}{105} \in \mathbb{N} \xRightarrow{(2,105)=1} \left.\begin{array}{l} 105 \mid r \\ 1 \leq r \leq 104 \end{array}\right\} \text{ab}$$

<u>Var 2</u> Op că $P(X) = X^{105} - 9 = f(X)g(X)$ ireductibile (vedem data viitoare)

$$\Rightarrow P(X^2) = X^{2\cdot 105} - 9 = (X^{105} - 3)(X^{105} + 3)$$

$$= f(x^2)\cdot g(x^2)$$

$\Rightarrow f(x^2) = x^{105} \pm 3$ abs, $f(x^2)$ are doar puteri pare ale lui x!

<u>Exc 1.12</u> p prim, $F(X) = X^{p-1} + X^{p-2} + \dots + X + 1$.

Calculați restul împărțirii lui $F(X^p)$ la $F(X)$.

$$F(X^p) = X^{p(p-1)} + X^{p(p-2)} + \dots + X^p + 1$$

$$\left((X-1)F(X) = X^p - 1 \right)$$

<u>Exc</u> Faceți împărțirea direct!

Th împărțirea cu rest:

$$F(X^p) = Q(X)\,F(X) + R(X), \quad \deg R \le p-2.$$

$F(X)$ are rădăcinile $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$, unde $\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} = e^{\frac{2\pi}{p}i}$

Evaluăm în ε^k:

$$F((\varepsilon^k)^p) = F(1) = p = R(\varepsilon^k),$$

sistem cu $p-1$ ecuații

$$\boxed{e^{i\pi} + 1 = 0}$$

sistem cu $p-1$ ecuații
și $p-1$ necunoscute $\Rightarrow$ coeficienții lui R

Exc! Faceți așa!

Var 3

$$F(X^p) = X^{p(p-1)} + X^{p(p-2)} + \dots + X^p + 1$$

$$= \underbrace{(X^{p(p-1)} - 1)}_{\vdots X^p - 1 \vdots F} + \underbrace{(X^{p(p-2)} - 1)}_{X^p - 1 \vdots F} + \dots + \underbrace{(X^p - 1)}_{X^p - 1 \vdots F} + p$$

$$= Q(X) F(X) + p.$$

Exc 1.13. Arătați că $P(X) = (1 + X + \dots + X^n)^2 - X^n \in \mathbb{Q}[X]$ este reductibil, $\forall n \geq 2$.

Dem $P(X) = \left(\dfrac{X^{n+1} - 1}{X - 1}\right)^2 - X^n$

$$(X-1)^2 P(X) = (X^{n+1} - 1)^2 - (X-1)^2 X^n = X^{2(n+1)} - 2X^{n+1} + 1$$

$$- (X^2 - 2X + 1) X^n = X^{2(n+1)} \cancel{- 2X^{n+1}} + 1 - X^{n+2} \cancel{+ 2X^{n+1}} - X^n$$

$$= X^{2n+2} - X^{n+2} - X^n + 1 = X^{n+2}(X^n - 1) - (X^n - 1)$$

$$= (X^{n+2} - 1)(X^n - 1)$$

$$= \left(X^{n+2} - 1\right)\left(X^{n} - 1\right)$$

$$\Rightarrow \quad P(X) = \left(X^{n+1} + X^{n} + \dots + 1\right)\left(X^{n-1} + X^{n-2} + \dots + 1\right) \qquad n \geq 2$$

$\Rightarrow$ ambele polinoame au grad ≥ 2 $\Rightarrow$ P reductibil

<u>Exc 1.14</u> Fie $a_1, \dots, a_n \in \mathbb{Z}$ distincte.

$$f(X) = (X - a_1)(X - a_2)\dots(X - a_n) - 1$$

este ireductibil în $\mathbb{Q}[X]$ $\xLeftrightarrow{\text{Lema Gauss}}$ este ired în $\mathbb{Z}[X]$.

<u>Dem</u> Pp că $f(X) = P(X) \cdot Q(X)$, $P, Q \in \mathbb{Z}[X]$, $\deg P, \deg Q < \deg f$

$$\Rightarrow P(a_i) \cdot Q(a_i) = -1 \Longrightarrow P(a_i) = \pm 1, \ Q(a_i) = \mp 1$$

(i.e. una este 1, una este -1)

Fie $g = P + Q \in \mathbb{Z}[X]$, $\deg g \leq \max\{\deg Q, \deg P\} < \deg f = n$

$$g(a_i) = 0, \ \forall i = \overline{1,n} \Rightarrow g = 0$$

$$\Rightarrow P = -Q \Rightarrow f(X) = -P^2(X).$$

Dar $f(a) > 0$, $\forall a >$ toate a_i

Dar $p^2(a) > 0, \forall a \in \mathbb{Z}$,

Pe când $-p^2(a) < 0, \forall a \in \mathbb{Z}$!

$X^4 + \hat{1} \in \mathbb{Z}_5[X]$ ireductibil? În $\mathbb{Z}[X]$ este ireductibil!

$$X^4 + \hat{1} = X^4 - \hat{4} = (X^2 - \hat{2})(X^2 + \hat{2}) \text{ în } \mathbb{Z}_5[X]!$$

Temă $X^4 + 1$ e ireductibil în $\mathbb{Z}[X]$ DAR este reductibil în orice $\mathbb{Z}_p[X]$!