Seminarul 12

Wednesday, May 12, 2021 8:54 AM

# Polinoame ireductibile

**Exc 1.1. (Obs!)** $K$ corp și $a, b \in K$, $a \neq 0$. Fie $f(X) \in K[X]$.

Atunci $f(X)$ ireductibil $\Leftrightarrow$ $f(aX+b)$ ireductibil.

**Dem:** „$\Leftarrow$" Pp $f(X) = g(X)\, h(X)$, $1 \leq \deg g < \deg f$

$1 \leq \deg h < \deg f$

$\Rightarrow f(aX+b) = g(aX+b)\, h(aX+b)$ reductibil

$\deg g(aX+b) = \deg g \leftarrow a \neq 0$

„$\Rightarrow$" Nu e necesar, pt că $f(X) = f\left(a\left(\frac{1}{a}X - \frac{b}{a}\right) + b\right)$. ($a \neq 0$)

**Exc 1.2.** Dem, folosind criteriul lui Eisenstein, că următoarele poli sunt ired în $\mathbb{Q}[X]$:

**Criteriul lui Eisenstein**

Fie $f \in \mathbb{Z}[X]$, $f = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$.

Dacă $\exists\, p$ prim ai $p \mid a_i$, $i = \overline{0, n-1}$

$p^2 \nmid a_0$ $\quad (p \parallel a_0)$

$\Rightarrow f$ este ireductibil în $\mathbb{Q}[X]$ (Lema lui Gauss $\overset{\text{monic}}{\Rightarrow}$ ired și în $\mathbb{Z}[X]$)

$\Rightarrow f$ este ireductibil în $\mathbb{Q}[X]$ (Lema lui Gauss $\Rightarrow$ ired și în $\mathbb{Z}[X]$)

---

a) $X^4-4X^3+6$ $\quad p=2$

b) $X^n-2$ $\quad p=2$

c) $X^6+30X^5-15X^3+6X-120$ $\quad p=3$

d) $X^{p-1}+X^{p-2}+\dots+X+1$, $p$ prim

e) $X^4+4X^3+6X^2+2X+1$

f) $\dfrac{(X+2)^p-2^p}{X}$, $p$ prim, $p\neq 2$.

---

d) $f(X)=X^{p-1}+\dots+X+1=\dfrac{X^p-1}{X-1}$

Ex 1.1: $f(X)$ ired $\Leftrightarrow f(X+1)$ ired

și $f(X+1)=\dfrac{(X+1)^p-1}{X+1-1}=\dfrac{\sum_{k=\cancel{0}\,1}^{p} C_p^k X^k \cancel{-1}}{X}$

$$=\sum_{k=1}^{p} C_p^k X^{k-1} = X^{p-1}+C_p^{p-1}X^{p-2}+C_p^{p-2}X^{p-3}+\dots+C_p^2X+p$$

Acum aplicăm criteriul lui Eisenstein pt $p$

$p \mid p \; = a_0$

$p^2 \nmid p$

$p \mid C_p^k, \quad \forall\, k = \overline{1, p-1}$

$$C_p^k = \frac{p!}{k!\,(p-k)!} \quad : p$$

se mai mici cap

e) $f(x) = X^4 + 4X^3 + 6X^2 + 2X + 1$

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

$f(x)$ ired $\Leftrightarrow f(X-1)$ ired $\Leftrightarrow X^4 - 2(X-1) = X^4 - 2X + 2$

& Eisenstein pt $p=2$

f) $f(x) = \dfrac{(X+2)^p - 2^p}{X}$, $p$ prim, $p \neq 2$

$$f(X-2) = \frac{X^p - 2^p}{X-2} = \frac{\cancel{(X-2)}\left(X^{p-1} + 2X^{p-2} + 2^2X^{p-3} + \dots + 2^{p-2}X + 2^{p-1}\right)}{\cancel{X-2}}$$

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

$$f(x) = \frac{(X+2)^p - 2^p}{\phantom{X}} = \frac{\sum_{k=0}^{\cancel{p}\; p-1} C_p^k\, 2^k X^{p-k} \; \cancel{-2^p}}{\phantom{X}}$$

$$f(X) = \frac{(X+2)^p - 2^p}{X} = \frac{\sum_{k=0} C_p^k 2^k X^{p-k} - \cancel{2^p}}{X}$$

$$= \sum_{k=0}^{p-1} C_p^k 2^k X^{p-k-1} = X^{p-1} + 2C_p^1 X^{p-2} + 2^2 C_p^2 X^{p-3}$$

$$+ \ldots + 2^{p-2} C_p^{p-2} X + 2^{p-1} C_p^{p-1}$$

+ Eisenstein pt $p$ prim ($p \neq 2$!)

---

Exc 1.3.* $X^2 - YZ \in \mathbb{R}[X,Y,Z]$ ired pt $P=(Y)$ $\boxed{\text{Eisenstein}}$

$X^2 + Y^2 - 1 \in \mathbb{R}[X,Y]$ ired pt $P=(Y-1)$

---

Exc 1.7. $X^{n-1} + X^{n-2} + \ldots + X + 1$ ired în $\mathbb{Q}[X] \Leftrightarrow n$ e prim

Dem „$\Leftarrow$" făcut mai sus

„$\Rightarrow$" Pp că $n = ab$ (compus)

$$\Rightarrow X^{a-1} + X^{a-2} + \ldots + X + 1 \mid X^{n-1} + \ldots + X + 1$$

Reamintesc: $(X^{n-1} + X^{n-2} + \ldots + X + 1, X^{m-1} + \ldots + X + 1) =$

(acum 2-3 seminarii) $= (X^{(n,m)-1} + X^{(n,m)-2} + \ldots + X + 1)$

$p$ prim

[illegible]

Exc 1.4. $f(X) \in \mathbb{Z}[X]$ $\checkmark^{p \text{ prim}}$ e "Eisenstein modulo $p$"

dacă $\exists\, a \in \mathbb{Z}$ a.î. $f(X+a)$ este reductibil conform

criteriului lui Eisenstein pt $p$.

Det $p$ prim a.î. $f(X) = X^3 + 65$ este Eisenstein modulo $p$.

Pt fiecare $p$ găsit, precizați un $a \in \mathbb{Z}$ corespunzător.

Dem $X^3+65 = f(X)$ Eisen. modulo $p$

$\Leftrightarrow \exists\, a \in \mathbb{Z}$ a.î. pt. $(X+a)^3 + 65$ se aplică Eisenstein

(cu un prim $p$)

$$(X+a)^3 + 65 = X^3 + 3a\,X^2 + 3a^2 X + (a^3+65)$$

$\Leftrightarrow \exists\, a \in \mathbb{Z}$ a.î. $p \mid a^3+65$, $p \mid 3a^2$, $p \mid 3a$

$p^2 \nmid a^3+65$

$p \mid 3a$ $\nearrow$ $p \mid 3 \Leftrightarrow p = 3$. Caut $a$ a.î. $3 \mid a^3+65 \Leftrightarrow a^3 \equiv 1 \pmod 3$

$9 \nmid a^3+65$ $\quad$ $a^3 \equiv a$

Merge pt $\boxed{a = 1}$

$\searrow$ $p \mid a$

și $p \mid a^3+65$ $\Big\} \Rightarrow p \mid 65 = 5 \cdot 13$

Dacă $p = 5$, aleg $a = 0$ $\quad X^3+65$ $\quad$ Merge pt $p = 5$ sau $p = 13$

$\quad$ 13, alege $a = 0$ $\quad X^3+65$

ired pt p=5 sau p=13

$p=13$, deg $a=0$ $X^3+65$

În final, $X^3+65$ este Eisenstein modulo 3, 5 și 13

$\downarrow$ $a=1$, $\downarrow$ $a=0$, $\downarrow$ $a=0$.

---

<u>Ex 1.5.</u> K corp (com) și $f\in K[X]$, $f(0)\neq 0$

Atunci $f(X)=a_0+a_1X+\dots+a_nX^n$ e ireductibil

$$\Updownarrow$$

$(R(f))(X)=a_n+a_{n-1}X+\dots+a_0X^n$ e ireductibil

De ex $X^5+3X^4+X^2-X-2$ ired $\Leftrightarrow -2X^5-X^4+X^3+3X+1$ ireductibil

<u>Dem</u> <u>Obs</u> 1) $\deg f=n \Rightarrow (R(f))(X)=X^n f\left(\frac{1}{X}\right)$

$$=X^n\left(a_0+a_1\frac{1}{X}+a_2\frac{1}{X^2}+\dots+a_n\frac{1}{X^n}\right)$$

$$=a_0X^n+a_1X^{n-1}+\dots+a_n$$

2) $R(R(f))(X)=f(X) \Leftrightarrow \boxed{f(0)\neq 0}$ (are loc mereu deloc)

Altfel: $R(R(X))=R(1)=1$.

"⇑" Pp că $R(f)$ este reductibil. Pp că $f(x) = g(x)\cdot h(x)$.

$$\overset{\text{aplic } R}{\Longrightarrow} \quad R(f)(X) = R(gh)(X) = X^{\deg(gh)}\, g\left(\tfrac{1}{X}\right) h\left(\tfrac{1}{X}\right)$$

$$= X^{\deg g}\, g\left(\tfrac{1}{X}\right) \cdot X^{\deg h}\, h\left(\tfrac{1}{X}\right) = R(g)(X)\cdot R(h)(X)$$

Dacă $R(f)$ reductibil $\Rightarrow$ ~~de exemplu, $R(h) = c\cdot R(f)$~~

$$\overset{\text{aplic } R}{\Longrightarrow} \quad \cancel{R(R(h)) = c\cdot R(R(f))}$$

$\Rightarrow$ de exemplu, $R(g) = c \neq 0 \iff g = cX^{\deg g}$

$\Rightarrow X^{\deg g} \mid f$.

Dacă $\deg g \geq 1 \Rightarrow \underset{a_0}{\underset{\parallel}{f(0)}} = 0$ Ab ipoteza.

**Exc 1.6.** a) $6X^4 - 4X + 1 \overset{R}{\longleftrightarrow} X^4 - 4X^3 + 6$ Eisenstein $p=2$

b) $120X^6 + 6X^5 - 15X^3 + 30X + 1 \overset{R}{\longleftrightarrow}$ 1.2. c)

c) $X^4 + 2X^3 + 6X^2 + 4X + 1 \overset{R}{\longleftrightarrow}$ 1.2 e)

**Exc 1.8** Scrieți factorizarea lui $X^n - 1$ pt $1 \leq n \leq 8$ în:

a) $\mathbb{Q}$

b) $\mathbb{Z}_2$

c) $\mathbb{Z}_3$

<u>Dem</u> a) $X-1=X-1$

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

$X^3-1=(X-1)(X^2+X+1)$ pt că (deg $\leq 3$) nu are rădăcini sau Exc 1.7.

$X^4-1=(X-1)(X+1)(X^2+1)$ ired pt că deg $\leq 3$ și nu are rădăcini

$X^5-1=(X-1)(X^4+X^3+X^2+X+1)$ Exc 1.7.

deg $\leq 3$, nu are răd

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

$X^7-1=(X-1)(X^6+X^5+\dots+X+1)$ Exc. 1.7.

$X^8-1=(X^4-1)(X^4+1) = (X-1)(X+1)(X^2+1)(X^4+1)$ ireductibil?

<u>Exc</u> Decideți dacă $X^4+1$ e ireductibil în $\mathbb{Q}[X]$.

$X\longmapsto X+1$: $(X+1)^4+1 = X^4+4X^3+6X^2+4X+2$

+ Eisenstein pt $p=2$!

b) $\mathbb{Z}_2$ și c) $\mathbb{Z}_3$ Temă!

De exemplu, $X^8-1 \overset{\text{în } \mathbb{Z}_2[X]}{=\!=\!=} (X-1)(X+1)(X^2+1)(X^4+1)$

$= (X+1)^8$, $8=p^n$, $p=2$, $n=3$

În $\mathbb{Z}_3[X]$, $X^8-1=(X-1)(X+1)(X^2+1)(X^4+1)$

ired. pt că nu are răd. — ired? Verificați!

Exe 9 $f = X^9+X^8+X^6+X+\hat{1}$, $g = X^9+X^8+X^3+X+\hat{1}$ $\in \mathbb{Z}_2[X]$.

$(f,g)=?$ și $f, g$ ca produs de factori ireductibili.

Dem Alg lui Euclid:

$$f = 1\cdot g + X^3(X^3-1)$$

$$(f,g) = (f-g, g) = (X^3(X^3-\hat{1}), g) = (X^3-\hat{1}, g) =$$

Dar $(X^3, g)=\hat{1}$ pt că $X \nmid g$

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

$x^3 - \hat{1} = (x+\hat{1})(x^2+x+\hat{1})$

$x+\hat{1} \nmid g$

$x^2+x+\hat{1} \mid g \longrightarrow$

$$\begin{array}{l|l} x^9+x^8+x^3+x+\hat{1} & x^2+x+\hat{1} \\ \underline{x^9+x^8+x^7} & x^7+x^5+x^4+x^2+\hat{1} \\ x^7+x^3+x+\hat{1} & \\ \underline{x^7+x^6+x^5} & \\ x^6+x^5+x^3+x+1 & \\ \underline{x^6+x^5+x^4} & \\ // \quad x^4+x^3+x+1 & \\ \underline{x^4+x^3+x^2} & \\ // \quad x^2+x+1 & \end{array}$$

Deci $(f,g) = x^2+x+\hat{1}$.

**Obs** $R(f) = g \Rightarrow$ e suficient $g$!

$g = (x^2+x+\hat{1})(x^7+x^5+x^4+x^2+\hat{1})$

$\Rightarrow f = (x^2+x+\hat{1})(x^7+x^5+x^3+x^2+\hat{1})$

$7 = 3+4$
$= 2+5$

**Obs** Deci $x^7+x^5+x^4+x^2+\hat{1} = h_1 \cdot h_2$ cu $\deg h_1 = 2$

$\Rightarrow h_1 = x^2+x+\hat{1}$ (singurul din $\mathbb{Z}_2[X]$ ireductibil)

$\Rightarrow R(h_1) \mid f$ și $(f,g) = x^2+x+\hat{1}$

$\Rightarrow R(h_1) \mid f$ și $(f, g) = x^2+x+\hat{1}$

$R(h_1) = (x^2+x+\hat{1})^2$

Rămâne $x^7+x^5+x^4+x^2+\hat{1} = h_1 \cdot h_2$, $\deg h_1 = 3$, $\deg h_2 = 4$.

+ calcule: $x^7+x^5+x^4+x^2+1 = (x^3+x^2+\hat{1})(x^4+x^3+\hat{1})$

**Exc 10** Sunt următoarele polinoame ireductibile în $\mathbb{Q}[X]$?

a) $X^3+X+2$ ✗ are răd $-1$

b) $X^3+X+1$ ✓ nu are rădăcini (rad posibile sunt $\pm 1$)

c) $X^3+2X+2$ ✓ Eisenstein pt $p=2$ (sau verificăm că nu are răd $\pm 1, \pm 2$)

d) $2X^4-3X^3+4X^2-4X-3$ ✗ Are răd posibile: $\pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2}$ Este rădăcină

e) $X^4+3X^3+6X^2+5X+3$

f) $X^4+2X^3+5X^2+6X+1$

g) $X^4+7X^3-2X^2+6X-1$

h) $X^4-2X^3+6X^2+4X-2$ ← Eisen pt $p=2$

i) $X^4+6X^3+15X^2+9X+3$ ← Eisen pt $p=3$

j) $X^4+3X^3+3X^2-5$ ← Temă!

e) $f(x) = X^4 + 3x^3 + 6X^2 + 5X + 3$

- nu are rădăcini $\pm 1, \pm 3$ $\Rightarrow$ nu are rădăcini în $\mathbb{Q}$
- nu funcționează Eisenstein
- 13653 nu e prim!
- $f(x-1) = (X-1)^4 + 3(X-1)^3 + 6(x-1)^2 + 5(X-1) + 3$

$= X^4 + 7X^3 + \_ \_ \_ + 2$

sau -1

Dacă ar fi reductibil, $X^4 + 3X^3 + 6X^2 + 5X + 3 = (X^2 + aX + b)(X^2 + cX + d)$

$a, b, c, d \in \mathbb{Q}$ ireductibile

Lema Gauss (sau reducție)

$a, b, c, d \in \mathbb{Z}$

$$\begin{cases} bd = 3 \Rightarrow b = \pm 3,\ d = \pm 1 \\ ad + bc = 5 \\ ac + b + d = 6 \Rightarrow ac \nearrow ac = 2 \\ \qquad\qquad\qquad\qquad\ \ \searrow ac = 10 \\ a + c = 3 \end{cases}$$

$a, c$ sunt răd lui $\nearrow T^2 - 3T + 10$ $\not\!\!\!$

$\searrow T^2 - 3T + 2 \Leftrightarrow$ a și c sunt 1 și 2

$b = 3, d = 1$

$ad + bc = 5 \Leftrightarrow a + 3c = 5 \Rightarrow a = 2, c = 1$

$\Rightarrow X^4 + 3X^3 + 6X^2 + 5X + 3 = (X^2 + 2X + 3)(X^2 + X + 1)$

f) $X^4+2X^3+5X^2+6X+1$

- Rădăcini posibile: $\pm 1$ nu are!
- Eisenstein nu merge!
- $12561$ prim? $\vdots 3$ nu!

$\longrightarrow$ Lăsăm temă (veți dem. că este ireductibil)

g) $P(X)=X^4+7X^3-2X^2+6X-1$

- Răd posibile: $\pm 1$ nu are!
- Eisenstein nu merge!
- Nu se poate încerca criteriul lui Cohn!
- Redus modulo 2: $X^4+X^3+\hat{1}$ e ireductibil în $\mathbb{Z}_2[X]$

$\Rightarrow$ $P(X)$ este ireductibil

<u>Ex 11.</u> Fie $p$ prim, $n \in \mathbb{N}$. $f(X)=X^{p^n}+(p-1)$ ireductibil în $\mathbb{Q}[X]$.

<u>Rez</u> Reducem modulo $p$ $\longmapsto$ $X^{p^n}-\hat{1} = (X-\hat{1})^{p^n}$

Facem sch. de variabile $X \mapsto X+1$:

$$f(X+1) = (X+1)^{p^n} + p - 1 = \sum_{k=1}^{p^n} C_{p^n}^{k} X^k + p$$

Ca să aplicăm Eisenstein, dem. că $p \mid C_{p^n}^{k}$ $\forall 1 \le k < p^n$.

$$C_{p^n}^{k} = \frac{(p^n)!}{k!\,(p^n-k)!}$$

Care este $m$ maxim a.î. $p^m \mid (p^n)!$ ?

Nr. care se divid cu $p$: $p^{n-1}$ $(1\cdot p, 2\cdot p, 3\cdot p, \ldots p^{n-1}\cdot p)$

$\le p^n$

———————— $p^2$: $p^{n-2}$

———————— $p^l$: $p^{n-l}$

Exemplu: $8! = (2^3)! = 1\cdot \underline{2}\cdot 3\cdot \underline{\underline{4}}\cdot 5\cdot \underline{6}\cdot 7\cdot \underline{\underline{\underline{8}}}$ $\quad 2^2 + 2^1 + 2^0$

$\Rightarrow p^m \mid (p^n)!$ unde $m = p^{n-1} + p^{n-2} + \ldots + p + 1$

$\Rightarrow p \mid (p^n)!$ unde $m = p + p + \dots + p + 1$

$= \frac{p^n - 1}{p - 1}$

Care este $m_1$ maximal a.î. $p^{m} \mid k!$ ?

Nr care se divid cu $p$ : $1 \cdot p, 2 \cdot p, \dots \left\lfloor \frac{k}{p} \right\rfloor \cdot p \to \left\lfloor \frac{k}{p} \right\rfloor$
$\leq k$

———————— $p^2$ : – – – – – $\left\lfloor \frac{k}{p^2} \right\rfloor$

– – – – –

$\Rightarrow m_1 = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \dots + \left\lfloor \frac{k}{p^n} \right\rfloor$

La fel, $p^{m_2} \mid (p^n - k)!$ unde $m_2 = \left\lfloor \frac{p^n - k}{p} \right\rfloor + \left\lfloor \frac{p^n - k}{p^2} \right\rfloor + \dots$

$+ \left\lfloor \frac{p^n - k}{p^n} \right\rfloor$

$m_1 + m_2 < m$ ?

$$\sum_{l=1}^{n} \left\lfloor \frac{k}{p^l} \right\rfloor + \sum_{l=1}^{n} \left\lfloor \frac{p^n - k}{p^l} \right\rfloor < \frac{p^n - 1}{p - 1} = p^{n-1} + p^{n-2} + \dots + p + 1$$

$$\sum_{l=1} \left\lfloor \frac{\cdot}{p^l} \right\rfloor \quad \sum_{l=1} \left\lfloor \frac{\cdot}{p^l} \right\rfloor \qquad p^{n-1},$$

$$\forall\ 1 \le k < p^n\ ?$$

$$\| $$

$$\sum_{l=1}^{n} \Bigg( \underbrace{\left\lfloor \frac{k}{p^l} \right\rfloor + \left\lfloor \frac{p^n-k}{p^l} \right\rfloor}_{\le \frac{k}{p^l} + \frac{p^n-k}{p^l} = \frac{p^n}{p^l} = p^{n-l}} \Bigg)$$

În plus, $\left\lfloor \frac{k}{p^n} \right\rfloor + \left\lfloor \frac{p^n-k}{p^n} \right\rfloor < \frac{k}{p^n} + \frac{p^n-k}{p^n} = p^n-1$.

$$C_8^4 = \frac{5\cdot 6\cdot 7\cdot 8}{1\cdot 2\cdot 3\cdot 4} \quad \vdots\, 2$$

$$\not\vdots\, 4$$

<u>Var 2</u> În $\mathbb{Z}_p[X]$, $(X+\hat{1})^{p^n} \underset{\text{Frobenius}}{\overset{\text{de nou}}{=}} X^{p^n} + \hat{1}$

$$\| $$

$$\sum_{k=0}^{p^n} C_{p^n}^{k} X^k$$

$$\Rightarrow p \mid C_{p^n}^{k}, \quad \forall\ 1 \le k \le p^n - 1.$$

---

<u>Exc de acum 2-3 întâlniri</u> $a_1, \ldots, a_n \in \mathbb{Z}$ distincte

Exc de aum 2-3 întâlniri $a_1, \ldots, a_n \in \mathbb{Z}$ distincte

Dem că $f(X) = (X-a_1)\ldots(X-a_n) - 1$ este ireductibil în $\mathbb{Q}[X]$

**Soluție** Lema Gauss $f = gh \Rightarrow g(a_i)\cdot h(a_i) = -1 \Rightarrow g(a_i) + h(a_i) = 0$

$g, h \in \mathbb{Z}[X]$

Polinomul $P = g+h$ are $n$ rădăcini, $\deg P < n$ $\Big\} \Rightarrow P = 0 \Leftrightarrow g = -h$

și $f(X) = -g^2(X)$

Dar $f$ ia și valori pozitive

---

Exc 12 $f(X) = (X-1)(X-2)\ldots(X-n)+1$ este reductibil în $\mathbb{Q}[X]$, $\forall n \neq 4$.

**Dem** Pp că $f$ este reductibil în $\mathbb{Q}[X]$

monic $\Updownarrow$ Gauss

$f$ este reductibil în $\mathbb{Z}[X]$

$\Rightarrow \exists\, g, h \in \mathbb{Z}[X]$, $\deg g < \deg f$, $\deg h < \deg f$ a.î.

$$f(X) = g(X)\,h(X) \Longrightarrow \underset{\mathbb{Z}}{\underset{\cap}{g(k)}} \cdot \underset{\mathbb{Z}}{\underset{\cap}{h(k)}} = 1$$

$\Rightarrow g(k) = h(k) = \pm 1$. Consider $P = g - h \in \mathbb{Z}[X]$.

$$\left.\begin{array}{l} \deg P < n \\ P(k) = 0,\ \forall k = \overline{1,n} \end{array}\right\} \Rightarrow P = 0 \Leftrightarrow g = h$$

$\Rightarrow (X-1)(X-2)\ldots(X-n) + 1 = g^2(X)$ (*) Deci $n$ par!

$$f\left(n-\tfrac{1}{2}\right) = 1 + \underbrace{\left(-\tfrac{1}{2}\right)\cdot\left(\tfrac{1}{2}\right)\left(\tfrac{3}{2}\right)\left(\tfrac{5}{2}\right)\ldots\left(\tfrac{2n-3}{2}\right)}_{<0\ ?} = g^2\left(n-\tfrac{1}{2}\right) \geq 0$$

$\Leftrightarrow 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-3) > 2^n$

$\left(-\frac{1}{2}\right)\cdot\frac{1}{2} < -1$

$\left(-\frac{1}{2}\right)\cdot\frac{1}{2}\cdot\frac{3}{2} = -\frac{3}{8} < -1$

$\left(-\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\right) = -\frac{15}{16} < -1$

$-\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdot\frac{7}{2}\cdot\ldots\cdot\frac{2n-3}{2} < -1$ dacă $n \geq 6$ ($n$ par)

$n=4$ exclus din ipoteză!

$n=2$ : $f(X)=(X-1)(X-2)+1= X^2-3X+3$ + Eventual sau pe-ale rădăcini

Încercare : (*) în $n+1$: $n!+1 = g^2(n+1)$ pătrat perfect?

$n=4$ da, 25 ← exclus din ipoteză

$n=5$ da 121 ← nu e grad

$n=7$ da

S-a verificat că $n!+1$ este p.p. doar pt $n=4,5$ și $7$.

Nu se cunoaște alt $n$.

Ex 13 $a_1, \ldots a_n \in \mathbb{Z}$ distincte

$$f(X) = (X-a_1)^2 \ldots (X-a_n)^2 + 1 \quad \text{ired în } \mathbb{Q}[X]$$
$$\Updownarrow$$
$$\text{ired în } \mathbb{Z}[X]$$

Dem Pp, la fel, că $f(X) = g(X)h(X)$, $\deg g < 2n$

$\deg g + \deg h = 2n$

$g(a_i)h(a_i) = 1 \Rightarrow g(a_i) = h(a_i) = \pm 1$.

Dar $f(x) > 0$, $\forall x \in \mathbb{R} \Rightarrow g, h$ nu au rădăcini reale

Obs $f(x) > 0, \quad \forall x \in \mathbb{R} \Rightarrow g, h$ nu au rădăcini reale

$\Rightarrow$ putem pp că $g(x) > 0, \quad \forall x \in \mathbb{R}$

$h(x) > 0$

g monic, h monic

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

$\overset{\shortparallel}{h(a_i)}$

Dacă $\deg g < n$ $\Rightarrow g = 1 \in \mathbb{Z}[X]$ 

Rămâne ca $\deg g = \deg h = n$.

$\Rightarrow g(x) = (x-a_1) \ldots (x-a_n) + 1$

$h(x)$ //

$\Rightarrow f(x) = (x-a_1)^2 \ldots (x-a_n)^2 + 1 = g^2(x)$

$= \left((x-a_1) \ldots (x-a_n) + 1\right)^2$

 calcule