

Criterii de ireductibilitate în inele de polinoame

Lazorec Mihai Silviu

Facultatea de Matematică

Universitatea "Alexandru Ioan Cuza", Iași

Februarie, 2019

Fie $(R, +, \cdot, 0, 1)$ un inel integru și $(K, +, \cdot, 0, 1)$ un corp comutativ. Notăm cu:

- $U(R)$ mulțimea elementelor inversabile ale lui R , i.e.

$$U(R) = \{a \in R \mid \exists b \in R \text{ astfel încât } a \cdot b = 1\};$$

- R^0 mulțimea elementelor nenule și neinvertabile ale lui R , i.e.

$$R^0 = R \setminus (U(R) \cup \{0\}).$$

Fie $(R, +, \cdot, 0, 1)$ un inel integru și $(K, +, \cdot, 0, 1)$ un corp comutativ. Notăm cu:

- $U(R)$ mulțimea elementelor inversabile ale lui R , i.e.

$$U(R) = \{a \in R \mid \exists b \in R \text{ astfel încât } a \cdot b = 1\};$$

- R^0 mulțimea elementelor nenule și neinvertabile ale lui R , i.e.

$$R^0 = R \setminus (U(R) \cup \{0\}).$$

Observăm că:

- $\mathbb{Z}^0 = \mathbb{Z} \setminus \{-1, 0, 1\}$;
- $K^0 = \emptyset$.

Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in R[X]$ un polinom de grad $n \in \mathbb{N}$.

Definiția 1. Spunem că polinomul f este ireductibil în $R[X]$ dacă nu există $d \in R^0$, astfel încât $d|f$, și nu există $g, h \in R[X]$, cu $1 \leq \text{gr}(g), \text{gr}(h) < n$, astfel încât $f = gh$.

Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in R[X]$ un polinom de grad $n \in \mathbb{N}$.

Definiția 1. Spunem că polinomul f este ireductibil în $R[X]$ dacă nu există $d \in R^0$, astfel încât $d|f$, și nu există $g, h \in R[X]$, cu $1 \leq \text{gr}(g), \text{gr}(h) < n$, astfel încât $f = gh$.

Dacă f are coeficienți în K , Definiția 1 se rescrie astfel:

Spunem că polinomul f este ireductibil în $K[X]$ dacă nu există $g, h \in K[X]$, cu $1 \leq \text{gr}(g), \text{gr}(h) < n$, astfel încât $f = gh$.

În particular:

a) dacă $f \in \mathbb{Z}[X]$ și:

- $gr(f) = 0$, atunci f ireductibil în $\mathbb{Z}[X] \iff a_0$ este ireductibil în \mathbb{Z} ;
- $gr(f) = 1$, atunci f este ireductibil în $\mathbb{Z}[X] \iff \nexists d \in \mathbb{Z} \setminus \{-1, 0, 1\}$ astfel încât $d|f$;
- $gr(f) = n > 1$, atunci f ireductibil în $\mathbb{Z}[X] \iff \nexists d \in \mathbb{Z} \setminus \{-1, 0, 1\}$, astfel încât $d|f$, și $\nexists g, h \in \mathbb{Z}[X]$, cu $1 \leq gr(g), gr(h) < n$, astfel încât $f = gh$.

În particular:

a) dacă $f \in \mathbb{Z}[X]$ și:

- $gr(f) = 0$, atunci f ireductibil în $\mathbb{Z}[X] \iff a_0$ este ireductibil în \mathbb{Z} ;
- $gr(f) = 1$, atunci f este ireductibil în $\mathbb{Z}[X] \iff \nexists d \in \mathbb{Z} \setminus \{-1, 0, 1\}$ astfel încât $d|f$;
- $gr(f) = n > 1$, atunci f ireductibil în $\mathbb{Z}[X] \iff \nexists d \in \mathbb{Z} \setminus \{-1, 0, 1\}$, astfel încât $d|f$, și $\nexists g, h \in \mathbb{Z}[X]$, cu $1 \leq gr(g), gr(h) < n$, astfel încât $f = gh$.

b) dacă $f \in \mathbb{Q}[X]$ și:

- $gr(f) = 0$, atunci $f \in \mathbb{Q}^*$, deci f nu este ireductibil fiind inversabil;
- $gr(f) = 1$, atunci f este ireductibil în $\mathbb{Q}[X]$;
- $gr(f) = n > 1$, atunci f este ireductibil în $\mathbb{Q}[X] \iff \nexists g, h \in \mathbb{Q}[X]$, cu $1 \leq gr(g), gr(h) < n$, astfel încât $f = gh$.

În particular:

a) dacă $f \in \mathbb{Z}[X]$ și:

- $gr(f) = 0$, atunci f ireductibil în $\mathbb{Z}[X] \iff a_0$ este ireductibil în \mathbb{Z} ;
- $gr(f) = 1$, atunci f este ireductibil în $\mathbb{Z}[X] \iff \nexists d \in \mathbb{Z} \setminus \{-1, 0, 1\}$ astfel încât $d|f$;
- $gr(f) = n > 1$, atunci f ireductibil în $\mathbb{Z}[X] \iff \nexists d \in \mathbb{Z} \setminus \{-1, 0, 1\}$, astfel încât $d|f$, și $\nexists g, h \in \mathbb{Z}[X]$, cu $1 \leq gr(g), gr(h) < n$, astfel încât $f = gh$.

b) dacă $f \in \mathbb{Q}[X]$ și:

- $gr(f) = 0$, atunci $f \in \mathbb{Q}^*$, deci f nu este ireductibil fiind inversabil;
- $gr(f) = 1$, atunci f este ireductibil în $\mathbb{Q}[X]$;
- $gr(f) = n > 1$, atunci f este ireductibil în $\mathbb{Q}[X] \iff \nexists g, h \in \mathbb{Q}[X]$, cu $1 \leq gr(g), gr(h) < n$, astfel încât $f = gh$.

Exemplul 1. $f = 2X + 4$ este reductibil în $\mathbb{Z}[X]$, dar este ireductibil în $\mathbb{Q}[X]$.

Definiția 2. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$. Spunem că f este un polinom primitiv în $\mathbb{Z}[X]$ dacă $(a_0, a_1, a_2, \dots, a_n) = \pm 1$.

Definiția 2. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$. Spunem că f este un polinom primitiv în $\mathbb{Z}[X]$ dacă $(a_0, a_1, a_2, \dots, a_n) = \pm 1$.

Observația 1. Elementul $(a_0, a_1, a_2, \dots, a_n) \in \mathbb{Z}$ se mai notează cu $c(f)$ și se numește conținutul lui f .

Definiția 2. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$. Spunem că f este un polinom primitiv în $\mathbb{Z}[X]$ dacă $(a_0, a_1, a_2, \dots, a_n) = \pm 1$.

Observația 1. Elementul $(a_0, a_1, a_2, \dots, a_n) \in \mathbb{Z}$ se mai notează cu $c(f)$ și se numește conținutul lui f .

Lema lui Gauss (privitoare la primitivitate). Fie $f, g \in \mathbb{Z}[X]$ două polinoame primitive în $\mathbb{Z}[X]$. Atunci și polinomul produs fg este primitiv în $\mathbb{Z}[X]$.

Lema lui Gauss (privitoare la ireductibilitate). Fie $f \in \mathbb{Z}[X]$ având $gr(f) \geq 1$. Atunci

$$f \text{ este ireductibil în } \mathbb{Z}[X] \iff \begin{cases} f \text{ este primitiv în } \mathbb{Z}[X] \\ f \text{ este ireductibil în } \mathbb{Q}[X] \end{cases}$$

Criteriul 1. Fie K un corp comutativ și fie $f \in K[X]$ cu $gr(f) \in \{2, 3\}$.
Atunci

f este ireductibil în $K[X] \iff f$ nu are rădăcini în K .

Criteriul 1. Fie K un corp comutativ și fie $f \in K[X]$ cu $gr(f) \in \{2, 3\}$.
Atunci

f este ireductibil în $K[X] \iff f$ nu are rădăcini în K .

Criteriul 1 și Lema lui Gauss conduc la următorul rezultat:
Fie $f \in \mathbb{Z}[X]$ un polinom primitiv de grad 2 sau 3. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff f$ nu are rădăcini în \mathbb{Q} .

Criteriul 1. Fie K un corp comutativ și fie $f \in K[X]$ cu $gr(f) \in \{2, 3\}$.
Atunci

f este ireductibil în $K[X] \iff f$ nu are rădăcini în K .

Criteriul 1 și Lema lui Gauss conduc la următorul rezultat:
Fie $f \in \mathbb{Z}[X]$ un polinom primitiv de grad 2 sau 3. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff f$ nu are rădăcini în \mathbb{Q} .

Exemplul 2.

- Polinomul primitiv $f = 6X^2 + 5X + 1 \in \mathbb{Z}[X]$ nu are rădăcini în \mathbb{Z} .
Dar, ambele rădăcini sunt raționale ($x_1 = -\frac{1}{2}, x_2 = -\frac{1}{3}$). Deci, f este reductibil în $\mathbb{Z}[X]$.

Criteriul 1. Fie K un corp comutativ și fie $f \in K[X]$ cu $gr(f) \in \{2, 3\}$.
Atunci

f este ireductibil în $K[X] \iff f$ nu are rădăcini în K .

Criteriul 1 și Lema lui Gauss conduc la următorul rezultat:
Fie $f \in \mathbb{Z}[X]$ un polinom primitiv de grad 2 sau 3. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff f$ nu are rădăcini în \mathbb{Q} .

Exemplul 2.

- Polinomul primitiv $f = 6X^2 + 5X + 1 \in \mathbb{Z}[X]$ nu are rădăcini în \mathbb{Z} .
Dar, ambele rădăcini sunt raționale ($x_1 = -\frac{1}{2}, x_2 = -\frac{1}{3}$). Deci, f este reductibil în $\mathbb{Z}[X]$.
- Polinomul primitiv $f = X^4 + 4X^2 + 3 \in \mathbb{Z}[X]$ nu are rădăcini în \mathbb{Q} ,
dar f este reductibil în $\mathbb{Z}[X]$ deoarece $f = (X^2 + 1)(X^2 + 3)$.

Criteriul 2 (Eisenstein). Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$. Dacă există un număr prim $p \in \mathbb{Z}$ ce satisface proprietățile $p|a_i, \forall i \in \{0, 1, 2, \dots, n-1\}$, $p \nmid a_n$ și $p^2 \nmid a_0$, atunci f este ireductibil în $\mathbb{Q}[X]$. Dacă, în plus, f este primitiv, atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 2 (Eisenstein). Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$. Dacă există un număr prim $p \in \mathbb{Z}$ ce satisface proprietățile $p|a_i, \forall i \in \{0, 1, 2, \dots, n-1\}, p \nmid a_n$ și $p^2 \nmid a_0$, atunci f este ireductibil în $\mathbb{Q}[X]$. Dacă, în plus, f este primitiv, atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 3. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, și fie $b \in \mathbb{Z}$. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff f(\pm X + b)$ este ireductibil în $\mathbb{Z}[X]$.

Criteriul 2 (Eisenstein). Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$. Dacă există un număr prim $p \in \mathbb{Z}$ ce satisface proprietățile $p|a_i$, $\forall i \in \{0, 1, 2, \dots, n-1\}$, $p \nmid a_n$ și $p^2 \nmid a_0$, atunci f este ireductibil în $\mathbb{Q}[X]$. Dacă, în plus, f este primitiv, atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 3. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, și fie $b \in \mathbb{Z}$. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff f(\pm X + b)$ este ireductibil în $\mathbb{Z}[X]$.

Exemplul 3. Folosind Criteriile 2 și 3 se poate arăta că, pentru orice număr prim p , al p -ulea polinom ciclotomic $\Phi_p = 1 + X + X^2 + \dots + X^{p-1} \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Q}[X]$ (și în $\mathbb{Z}[X]$ fiind primitiv).

Criteriul 4. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, și $a_0 \neq 0$. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff r(f)$ este ireductibil în $\mathbb{Z}[X]$,

unde $r(f) = a_n + a_{n-1}X + a_{n-2}X^2 + \dots + a_0X^n \in \mathbb{Z}[X]$.

Criteriul 4. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, și $a_0 \neq 0$. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff r(f)$ este ireductibil în $\mathbb{Z}[X]$,

unde $r(f) = a_n + a_{n-1}X + a_{n-2}X^2 + \dots + a_0X^n \in \mathbb{Z}[X]$.

Observația 2. $r(f)$ se numește reciprocul polinomului f .

Criteriul 4. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, și $a_0 \neq 0$. Atunci

f este ireductibil în $\mathbb{Z}[X] \iff r(f)$ este ireductibil în $\mathbb{Z}[X]$,

unde $r(f) = a_n + a_{n-1}X + a_{n-2}X^2 + \dots + a_0X^n \in \mathbb{Z}[X]$.

Observația 2. $r(f)$ se numește reciprocul polinomului f .

Exemplul 4. Utilizând Criteriile 2 și 4 se poate arăta că polinomul $f = 6X^{11} + 27X^5 + 3X + 8 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Criteriul 5 (Perron). Fie $f = a_0 + a_1X + a_2X^2 + \dots + X^n \in \mathbb{Z}[X]$, unde $n \geq 2$, și $a_0 \neq 0$. Dacă

$$|a_{n-1}| > 1 + |a_0| + |a_1| + \dots + |a_{n-2}|,$$

atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 5 (Perron). Fie $f = a_0 + a_1X + a_2X^2 + \dots + X^n \in \mathbb{Z}[X]$, unde $n \geq 2$, și $a_0 \neq 0$. Dacă

$$|a_{n-1}| > 1 + |a_0| + |a_1| + \dots + |a_{n-2}|,$$

atunci f este ireductibil în $\mathbb{Z}[X]$.

Exemplul 5.

- Polinomul $f = X^{10} + 2002X^9 + 1999X^4 + 1 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.
- Polinomul $f = X^n + 6X^{n-1} + 4 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$, $\forall n \geq 2$.

Criteriul 6. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$.

Dacă există un număr natural $m \geq 2$ astfel încât

- i) $f(m-1) \neq 0$,
 - ii) $f(m) = \text{prim}$,
 - iii) $\text{Re}(z) < m - \frac{1}{2}$, pentru toate rădăcinile $z \in \mathbb{C}$ ale lui f ,
- atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 6. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$.
Dacă există un număr natural $m \geq 2$ astfel încât

- i) $f(m-1) \neq 0$,
 - ii) $f(m) = \text{prim}$,
 - iii) $\text{Re}(z) < m - \frac{1}{2}$, pentru toate rădăcinile $z \in \mathbb{C}$ ale lui f ,
- atunci f este ireductibil în $\mathbb{Z}[X]$.

Exemplul 6. Aplicând Criteriul 6, pentru $m = 2$, obținem că polinomul $f = X^4 - X^2 + 1 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$. Rădăcinile sunt:
 $z_1 = \frac{\sqrt{3}}{2} + \frac{1}{2}i, z_2 = \frac{\sqrt{3}}{2} - \frac{1}{2}i, z_3 = -\frac{\sqrt{3}}{2} + \frac{1}{2}i, z_4 = -\frac{\sqrt{3}}{2} - \frac{1}{2}i$.

Criteriul 7. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ un număr prim și $\hat{f} = \hat{a}_0 + \hat{a}_1X + \hat{a}_2X^2 + \dots + \hat{a}_nX^n \in \mathbb{Z}_p[X]$.

Dacă

i) $gr(\hat{f}) = gr(f)$,

ii) \hat{f} este ireductibil în $\mathbb{Z}_p[X]$,

atunci f este ireductibil în $\mathbb{Q}[X]$. Dacă, în plus, f este primitiv, atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 7. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ un număr prim și $\hat{f} = \hat{a}_0 + \hat{a}_1X + \hat{a}_2X^2 + \dots + \hat{a}_nX^n \in \mathbb{Z}_p[X]$.

Dacă

i) $gr(\hat{f}) = gr(f)$,

ii) \hat{f} este ireductibil în $\mathbb{Z}_p[X]$,

atunci f este ireductibil în $\mathbb{Q}[X]$. Dacă, în plus, f este primitiv, atunci f este ireductibil în $\mathbb{Z}[X]$.

Observația 3. Polinomul \hat{f} se numește redusul modulo p al lui f .

Criteriul 7. Fie $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ un număr prim și $\hat{f} = \hat{a}_0 + \hat{a}_1X + \hat{a}_2X^2 + \dots + \hat{a}_nX^n \in \mathbb{Z}_p[X]$.

Dacă

i) $gr(\hat{f}) = gr(f)$,

ii) \hat{f} este ireductibil în $\mathbb{Z}_p[X]$,

atunci f este ireductibil în $\mathbb{Q}[X]$. Dacă, în plus, f este primitiv, atunci f este ireductibil în $\mathbb{Z}[X]$.

Observația 3. Polinomul \hat{f} se numește redusul modulo p al lui f .

Exemplul 7. Polinomul $f = 11X^5 + 8X^4 + 12X^3 + 3X^2 + 7 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Q}[X]$, dar și în $\mathbb{Z}[X]$, întrucât este primitiv.

Criteriul 8 (Schönemann). Fie $f = a_0 + a_1X + a_2X^2 + \dots + X^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$. Presupunem că există $m \in \mathbb{N}^*$, un număr prim $p \in \mathbb{N}$ și polinoamele $g, h \in \mathbb{Z}[X]$ satisfăcând condițiile:

- i) $f = g^m + ph$,
- ii) \hat{g} este ireductibil în $\mathbb{Z}_p[X]$,
- iii) $\hat{g} \nmid \hat{h}$.

Atunci f este ireductibil în $\mathbb{Z}[X]$.

Criteriul 8 (Schönemann). Fie $f = a_0 + a_1X + a_2X^2 + \dots + X^n \in \mathbb{Z}[X]$, unde $n \in \mathbb{N}^*$. Presupunem că există $m \in \mathbb{N}^*$, un număr prim $p \in \mathbb{N}$ și polinoamele $g, h \in \mathbb{Z}[X]$ satisfăcând condițiile:

- i) $f = g^m + ph$,
- ii) \hat{g} este ireductibil în $\mathbb{Z}_p[X]$,
- iii) $\hat{g} \nmid \hat{h}$.

Atunci f este ireductibil în $\mathbb{Z}[X]$.

Exemplul 8. Polinomul $f = (X^2 + 2)^3 + 5(X^5 + 10X^3 + 5) \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Teorema 1 (Cohn). Fie $p \in \mathbb{N}$ un număr prim și $\sum_{i=0}^n a_i 10^i$ scrierea sa în baza 10. Atunci polinomul $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Teorema 1 (Cohn). Fie $p \in \mathbb{N}$ un număr prim și $\sum_{i=0}^n a_i 10^i$ scrierea sa în baza 10. Atunci polinomul $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Exemplul 9.

- În 1732, Euler găsește numărul prim 6,700,417. Deci, polinomul $6X^6 + 7X^5 + 4X^2 + X + 7 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Teorema 1 (Cohn). Fie $p \in \mathbb{N}$ un număr prim și $\sum_{i=0}^n a_i 10^i$ scrierea sa în baza 10. Atunci polinomul $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Exemplul 9.

- În 1732, Euler găsește numărul prim 6,700,417. Deci, polinomul $6X^6 + 7X^5 + 4X^2 + X + 7 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.
- În 1772, Euler indică numărul prim 2,147,483,647. Deci, polinomul $2X^9 + X^8 + 4X^7 + 7X^6 + 4X^5 + 8X^4 + 3X^3 + 6X^2 + 4X + 7 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Teorema 2. Dacă un număr prim $p \in \mathbb{N}$ este exprimat într-o bază de numerație $b \geq 2$ ca $p = \sum_{i=0}^n a_i b^i$, unde $0 \leq a_1 \leq b - 1$, atunci polinomul $f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Teorema 2. Dacă un număr prim $p \in \mathbb{N}$ este exprimat într-o bază de numerație $b \geq 2$ ca $p = \sum_{i=0}^n a_i b^i$, unde $0 \leq a_i \leq b - 1$, atunci polinomul $f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Exemplul 10. Thomas Clausen găsește numărul prim 67, 280, 421, 310, 721 în 1855.

Teorema 2. Dacă un număr prim $p \in \mathbb{N}$ este exprimat într-o bază de numerație $b \geq 2$ ca $p = \sum_{i=0}^n a_i b^i$, unde $0 \leq a_i \leq b - 1$, atunci polinomul $f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Exemplul 10. Thomas Clausen găsește numărul prim 67, 280, 421, 310, 721 în 1855.

$$\overline{67280421310721}_2 = 1111010011000011110001100111001101000100000001.$$

Teorema 2. Dacă un număr prim $p \in \mathbb{N}$ este exprimat într-o bază de numerație $b \geq 2$ ca $p = \sum_{i=0}^n a_i b^i$, unde $0 \leq a_i \leq b - 1$, atunci polinomul $f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

Exemplul 10. Thomas Clausen găsește numărul prim 67, 280, 421, 310, 721 în 1855.

$$\overline{67280421310721}_2 = 1111010011000011110001100111001101000100000001.$$

Atunci, polinomul $X^{45} + X^{44} + X^{43} + X^{42} + X^{40} + X^{37} + X^{36} + X^{31} + X^{30} + X^{29} + X^{28} + X^{24} + X^{23} + X^{20} + X^{19} + X^{18} + X^{15} + X^{14} + X^{12} + X^8 + 1 \in \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$.

O legătură între numerele prime și ireductibilitatea în $\mathbb{Z}[X]$

7 Decembrie, 2018: se găsește numărul prim $2^{82,589,933} - 1$ care are 24,862,048 cifre.

O legătură între numerele prime și ireductibilitatea în $\mathbb{Z}[X]$

7 Decembrie, 2018: se găsește numărul prim $2^{82,589,933} - 1$ care are 24,862,048 cifre.

Deci, cu ceva mai multă răbdare..., urmând ideile de mai sus, putem scrie un polinom ireductibil, cu coeficienți întregi, de grad 24,862,047.

7 Decembrie, 2018: se găsește numărul prim $2^{82,589,933} - 1$ care are 24, 862, 048 cifre.

Deci, cu ceva mai multă răbdare..., urmând ideile de mai sus, putem scrie un polinom ireductibil, cu coeficienți întregi, de grad 24, 862, 047.

De asemenea, dacă exprimăm numărul de mai sus într-o bază de numerație b , am putea scrie un polinom ireductibil, cu coeficienți întregi, de grad $\lceil \log_b(2^{82,589,933} - 1) \rceil$.

Fie $n \in \mathbb{N}^*$. Polinomul $X^n - 1 \in \mathbb{C}[X]$ are rădăcinile

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, k \in \{1, 2, \dots, n\}.$$

Fie $n \in \mathbb{N}^*$. Polinomul $X^n - 1 \in \mathbb{C}[X]$ are rădăcinile

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, k \in \{1, 2, \dots, n\}.$$

Polinomul $\Phi_n = \prod_{\substack{k=1, n \\ (k, n)=1}} (X - z_k)$ se numește al n -ulea polinom ciclotomic.

Fie $n \in \mathbb{N}^*$. Polinomul $X^n - 1 \in \mathbb{C}[X]$ are rădăcinile

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, k \in \{1, 2, \dots, n\}.$$

Polinomul $\Phi_n = \prod_{\substack{k=1, n \\ (k, n)=1}} (X - z_k)$ se numește al n -ulea polinom ciclotomic.

Proprietăți:

- $gr(\Phi_n) = \phi(n), \forall n \in \mathbb{N}^*$;
- $X^n - 1 = \prod_{d|n} \Phi_d, \forall n \in \mathbb{N}^*$;

Fie $n \in \mathbb{N}^*$. Polinomul $X^n - 1 \in \mathbb{C}[X]$ are rădăcinile

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, k \in \{1, 2, \dots, n\}.$$

Polinomul $\Phi_n = \prod_{\substack{k=1, \dots, n \\ (k, n)=1}} (X - z_k)$ se numește al n -ulea polinom ciclotomic.








Proprietăți:

- $gr(\Phi_n) = \phi(n), \forall n \in \mathbb{N}^*$;
- $X^n - 1 = \prod_{d|n} \Phi_d, \forall n \in \mathbb{N}^*$;
- $\Phi_n \in \mathbb{Z}[X], \forall n \in \mathbb{N}^*$;
- Φ_n este ireductibil în $\mathbb{Z}[X], \forall n \in \mathbb{N}^*$;

- $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$, pentru orice număr prim $p \in \mathbb{N}$;
- $\Phi_{2n}(X) = \Phi_n(-X)$, pentru orice număr natural impar $n \geq 3$;
- Φ_{105} este primul polinom ciclotomic care are cel puțin un coeficient în mulțimea $\mathbb{Z} \setminus \{-1, 0, 1\}$ (coeficienții lui X^7 și X^{41} sunt -2).

- $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$, pentru orice număr prim $p \in \mathbb{N}$;
- $\Phi_{2n}(X) = \Phi_n(-X)$, pentru orice număr natural impar $n \geq 3$;
- Φ_{105} este primul polinom ciclotomic care are cel puțin un coeficient în mulțimea $\mathbb{Z} \setminus \{-1, 0, 1\}$ (coeficienții lui X^7 și X^{41} sunt -2).

Observația 4. Și prin intermediul polinoamelor ciclotomice putem indica polinoame ireductibile, cu coeficienți întregi, de grad foarte mare:
 $gr(\Phi_{2^{82,589,933}-1}) = 2^{82,589,933} - 2.$

-  Brillhart, J., Filaseta, M., Odlyzko, A., *On an irreducibility theorem of A. Cohn*, *Canad. J. Math.* **33** (1981), 1055-1059.
-  Dorwart, H.L., *Irreducibility of polynomials*, *Amer. Math. Monthly* **42** (1935), no. 6, 369-381.
-  Ion, I.D., Radu, N., *Algebră*, Editura Didactică și Pedagogică, București, 1991.
-  Murty, M.R., *Prime numbers and irreducible polynomials*, *Amer. Math. Monthly* **109** (2002), no. 5, 452–458.
-  Tofan, I., Volf, A.C., *Algebră: Inele. Module. Teorie Galois*, Editura Matrix Rom, București, 2001.
-  Tărnăuceanu, M., *Probleme de algebră*, vol. II., Editura Universității “Al. I. Cuza”, Iași, 2004.
-  The List of Largest Known Primes Home Page,
<https://primes.utm.edu/primes/>