30.04.24 (1)

Elementul 10

Def 1 Fie $n \in \mathbb{N}^* \setminus \{1\}$, și fie $b \in \mathbb{Z}$ cu $(b,n)=1$. Spunem că n e PSEUDOPRIM ÎN RAPORT CU BAZA b dacă $b^{n-1} \equiv 1 \pmod{n}$

Obs 2 Orice număr prim e pseudoprim în raport cu orice bază (prima cu el)

Fie n și b ca în def. 1 astfel ca n să nu fie pseudoprim în raport cu baza b. Să notăm cu $b_1, b_2, \ldots, b_r$ bazele (diferite două câte două $\pmod{n}$) în care n e pseudoprim.

Atunci $(bb_j)^{n-1} \equiv b^{n-1} b_j^{n-1} \equiv b^{n-1} \not\equiv 1 \pmod{n}$, ca urmare n NU e pseudoprim în raport cu bazele (și ele diferite două câte două $\pmod{n}$) $bb_1, bb_2, \ldots, bb_r$.

În concluzie, are loc

Prop 3 Dacă există baze în raport cu care n nu e pseudoprim, atunci n e pseudoprim în raport cu cel ~~mult~~ mult 50% dintre bazele posibile

Corolar 4 Dacă găsim că n e pseudoprim într-o bază b aleasă arbitrar, atunci probabilitatea ca n să fie compus e $\leq \frac{1}{2}$.

Abordarea problemei probabilității al primalității de maniera prezentată mai înainte s-ar baza pe premisa că ~~oricare~~ pentru orice număr (impar) compus n există baze b în raport cu care n să nu fie pseudoprim.

Această premisă nu e, însă, corectă, după cum arată următorul exemplu!

Fie $b \in \mathbb{Z}$ cu $(b, 561) = 1$

Atunci $b^{560} \equiv 1 \pmod{3}$

$b^{560} \equiv (b^{10})^{56} \equiv 1 \pmod{11}$

și $b^{560} \equiv (b^{16})^{35} \equiv 1 \pmod{17}$

$\Rightarrow b^{560} - 1 \vdots [3, 11, 17] = 561$, deci $b^{560} \equiv 1 \pmod{561}$

Ca urmare, 561 e pseudoprim în baza b.

Aceste considerații ne conduc la:

Def 5 Un număr natural $n \in 2\mathbb{N}+1$ s.n. NUMĂR CARMICHAEL dacă el e pseudoprim în raport cu orice bază primă cu el.

Obs 6 De mai sus, 561 e număr Carmichael.

$\boxed{\text{Prop 7}}$ Fie $n \in 2\mathbb{N}+1$ un număr Carmichael. Atunci n e liber de pătrate.

Idee: Fie p un număr prim pentru care $p^2 | n$.

Fie b o rădăcină primitivă $\pmod{p^2}$ și fie $a \in \mathbb{Z}$ cu (a, n) așa încât $a \equiv b \pmod{p^2}$ și $a \equiv 1$

pentru orice alt factor prim q de-al lui n.

Presupunem că $b^{n-1} \equiv 1 \pmod n$.

Atunci $b^{n-1} \equiv 1 \pmod{p^2}$, deci $p(p-1) = \gamma_{p^2}(b) \mid n-1 \Rightarrow \exists \lambda \in \mathbb{Z}$ $\lambda p(p-1) = \overset{p^2 t}{\overset{\|}{n}} - 1$

De aici, $\exists \lambda \in \mathbb{Z}$ $\lambda p \equiv -1 \pmod{p^2}$, deci p e inversabil $\pmod{p^2}$, deci $(p, p^2) = 1$, Abs. □

$\boxed{\text{Prop 8}}$ Fie $n \in \mathbb{N}$ impar și liber de pătrate. Sunt echivalente afirmațiile:

(i) n e număr Carmichael

(ii) Pentru orice divizor prim p al lui n avem $p-1 \mid n-1$.

<u>Dem</u>: „$\Rightarrow$": Fie p un divizor prim al lui n, și fie $b \in \mathbb{Z}$ cu $(b, n) = 1$.

Atunci $b^{n-1} \equiv 1 \pmod n \Rightarrow b^{n-1} \equiv 1 \pmod p \Rightarrow$ $p-1 = \gamma_p(b) \mid n-1$.

„$\Leftarrow$": Fie $b \in \mathbb{Z}$ cu $(b, n) = 1$.

Din prop. 7, n e liber de pătrate; fie $n = p_1 p_2 \dots p_r$ cu $p_i \neq p_j$ pt $i \neq j$ și $p_1, \dots, p_r$ prime.

~~Atunci~~ $\left(\forall j \ b^{p_j - 1} \overset{\text{Fermat}}{\equiv} 1 \pmod{p_j}\right) \Rightarrow$ $\left(\forall j \ b^{n-1} \equiv 1 \pmod{p_j}\right) \xrightarrow{\text{LCR}} b^{n-1} \equiv 1 \pmod n$

Def 9) Fie $n \in \mathbb{N}^* \setminus \{1\}$ impar și fie $a \in \mathbb{Z}$ cu $(a,n)=1$. Fie $p_1 p_2 \dots p_r$ descompunerea lui n în factori primi (nu neapărat distincți!). Prin SIMBOLUL JACOBI al lui a în raport cu n înțelegem numărul

$$\left(\frac{a}{n}\right)_J \overset{not}{=} \left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) \in \{-1,1\}$$

Obs 10) i) Dacă $\left(\frac{a}{n}\right)_J = -1$, atunci a nu e rest pătratic $(\mathrm{mod}\ n)$,

dar

ii) Dacă $\left(\frac{a}{n}\right)_J = 1$, nu e sigur nici că a e rest pătratic mod n, nici că nu!

$$\left(\frac{1}{15}\right)_J = 1 \text{ și } \left(\frac{-1}{21}\right)_J = \left(\frac{-1}{3}\right)\cdot\left(\frac{-1}{7}\right) = (-1)\cdot(-1) = 1,$$

dar:

$$\begin{array}{lll} 1^2 \equiv 1 \not\equiv -1 & 5^2 \equiv 4 \not\equiv -1 & 9^2 \equiv -3 \not\equiv -1 \\ 2^2 \equiv 4 \not\equiv -1 & 6^2 \equiv -6 \not\equiv -1 & 10^2 \equiv -5 \not\equiv -1; \\ 3^2 \equiv 9 \not\equiv -1 & 7^2 \equiv 1 \not\equiv -1 & \\ 4^2 \equiv 16 \not\equiv -1 & 8^2 \equiv 1 \not\equiv -1 & \end{array}$$

pt orice $\lambda \in \{11, 12, \dots, 20\}$ $\lambda^2 \equiv (21-\lambda)^2$, care e în lista de mai sus, deci $\lambda^2 \not\equiv -1$.

Ca urmare, -1 nu-i rest pătratic ([illegible]) $(\mathrm{mod}\ 21)$.

$$\left.\begin{array}{l}\left(\frac{2}{15}\right)_J = \left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1 \\ 2^{\frac{15-1}{2}} = 2^7 \equiv 8 \ (\mathrm{mod}\ 15)\end{array}\right\} \Rightarrow \left(\frac{2}{15}\right)_J \not\equiv 2^{\frac{15-1}{2}} \ (\mathrm{mod}\ 15)$$

Ca urmare, relația lui Euler din con- (5)
textul simbolului Legendre nu e verificată
neapărat în contextul simbolului Jacobi.
Pe de altă parte:

$$a \equiv b \ (\mathrm{mod}\ n = p_1 p_2 \dots p_r) \Rightarrow (a \equiv b \ (\mathrm{mod}\ p_j)\ \forall j).$$

Deci $$\left(\frac{a}{n}\right)_J = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right) = \prod_{j=1}^{r}\left(\frac{b}{p_j}\right) = \left(\frac{b}{n}\right)_J$$

$$\left(\frac{ab}{n}\right)_J = \prod_{j=1}^{r}\left(\frac{ab}{p_j}\right) = \prod_{j=1}^{r}\left(\left(\frac{a}{p_j}\right)\left(\frac{b}{p_j}\right)\right) = \left(\frac{a}{n}\right)_J\left(\frac{b}{n}\right)_J$$

$$\left(\frac{-1}{n}\right)_J = \prod_{j=1}^{r}\left(\frac{-1}{p_j}\right) = \prod_{j=1}^{r}(-1)^{\frac{p_j-1}{2}} = (-1)^{\sum_{j=1}^{r}\frac{p_j-1}{2}} = (1)$$

Acum: Aș vrea să obțin $(-1)^{\frac{p_1 \dots p_r - 1}{2}}$

Punând $q_j = \frac{p_j - 1}{2}$, deci $p_j = 2q_j + 1$,

deci $$\frac{n-1}{2} = \frac{\prod_{j=1}^{r}(2q_j+1) - 1}{2} \equiv q_1 + q_2 + \dots + q_r = \sum_{j=1}^{r}\frac{p_j - 1}{2}.$$

Deci $(1) = (-1)^{\frac{n-1}{2}}$

$$\left(\frac{2}{n}\right)_J = \prod_{j=1}^{r}\left(\frac{2}{p_j}\right) = \prod_{j=1}^{r}(-1)^{\frac{p_j^2-1}{8}} = (-1)^{\sum_{j=1}^{r}\frac{p_j^2-1}{8}} = (2)$$

Acum: Aș vrea $(-1)^{\frac{p_1^2 p_2^2 \dots p_r^2 - 1}{8}}$.

Pun $A_j = \frac{p_j^2 - 1}{8}$; atunci $p_j^2 = 8A_j + 1$,

(6)

deci $\frac{p_1^2 p_2^2 \cdots p_r^2 - 1}{8} = \frac{\prod_{j=1}^{r}(8a_j+1) - 1}{8} \overset{8}{\equiv}$

$\overset{8}{\equiv} a_1 + a_2 + \dots + a_r = \sum_{j=1}^{r} \frac{p_j^2-1}{8}$.

(cf cerinței)

$(-1) = (-1)^{\frac{n^2-1}{8}}$

Dacă m și n sunt naturale, >1, $(m,n)=1$, atunci, punând $m = q_1 q_2 \cdots q_s$, $n = p_1 p_2 \cdots p_r$:

$$\left(\frac{m}{n}\right)_J \cdot \left(\frac{n}{m}\right) = \prod_{j=1}^{r}\left(\frac{m}{p_j}\right)\prod_{i=1}^{s}\left(\frac{n}{q_i}\right) =$$

$$= \prod_{j=1}^{r}\left(\frac{q_1 q_2 \cdots q_s}{p_j}\right) \cdot \prod_{i=1}^{s}\left(\frac{p_1 p_2 \cdots p_r}{q_i}\right) =$$

$$= \prod_{\substack{1\le j\le r\\ 1\le i\le s}}\left(\frac{q_i}{p_j}\right) \prod_{\substack{1\le i\le s\\ 1\le j\le r}}\left(\frac{p_j}{q_i}\right) = \prod_{\substack{1\le i\le s\\ 1\le j\le r}}\left(\frac{p_j}{q_i}\right)\cdot\left(\frac{q_i}{p_j}\right) =$$

$$= \prod_{\substack{1\le i\le s\\ 1\le j\le r}} (-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}} = (-1)^{\sum_{\substack{1\le i\le s\\ 1\le j\le r}} \frac{p_j-1}{2}\cdot\frac{q_i-1}{2}} = (3)$$

Cerința: Am vrea $(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} =$

$= (-1)^{\frac{q_1 q_2 \cdots q_s - 1}{2}\cdot\frac{p_1 p_2 \cdots p_r - 1}{2}} = (4)$

Punând $\frac{p_j-1}{2} = a_j$ și $\frac{q_i-1}{2} = b_i$, (4) devine

$(-1)^{\frac{\prod_{i=1}^{s}(2b_i+1)-1}{2}\cdot\frac{\prod_{j=1}^{r}(2a_j+1)-1}{2}}$ (5)

Dar ~~exponentul lui~~ $(5) = (-1)^{(t_1+\dots+t_s)(r_1+\dots+r_k)} = (3)$

cf cursului
$$(3) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$
Am probat, deci!

Prop 11 Simbolul Jacobi se bucură de toate proprietățile de calculabilitate ale simbolului Legendre, cu excepția celei date de teorema lui Euler.

Def 12 Fie $n \in 2\mathbb{N}+1$ și fie $b \in \mathbb{Z}$ cu $(b,n)=1$. Spunem că n e PSEUDOPRIM EULER ÎN RAPORT CU BAZA b dacă
$$\left(\frac{b}{n}\right)_J \equiv b^{\frac{n-1}{2}} \pmod{n}$$

Prop 13 Dacă n e pseudoprim Euler în raport cu baza b, atunci n e pseudoprim în raport cu baza b.

Dem: $$b^{n-1} = \left(b^{\frac{n-1}{2}}\right)^2 \equiv \left(\frac{b}{n}\right)_J^2 = 1 \pmod{n}$$

Există algoritmi deterministici de studiul primalității care să funcționeze în timp polinomial:
AGRAWAL – KAYAL – SAXENA.