Exam TNA_312

1. Precizați dacă numărul 127363 este sau nu prim, așa încât răspunsul dvs. să fie adevărat cu o probabilitate de cel puțin 80%.

Dacă n nu e pseudoprim Euler în baza b, notând cu $b_1, b_2, \ldots, b_r$ bazele în raport cu care e,

$$(bb_j)^{\frac{n-1}{2}} = b^{\frac{n-1}{2}} b_j^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \cdot \left(\frac{b_j}{n}\right)_J \not\equiv \left(\frac{b}{n}\right)_J \left(\frac{b_j}{n}\right)_J = \left(\frac{bb_j}{n}\right)_J,$$

deci nicio bază bb_j nu are calitatea ca n să fie pseudoprim Euler în raport cu ea.

- Cu calcule similare celor discutate la cazul de azi rezultă că dacă noi, alegând o bază arbitrară b, constatăm că n e pseudoprim Euler în raport cu ea, atunci avem o probabilitate $\leq \frac{1}{2}$ ca n să fie compus.

Dacă repetăm testul, aplicându-l pt k baze aleator alese, ~~at~~ și dacă de fiecare dată obținem că n e pseudoprim Euler pt respectiva bază b, atunci probabilitatea ca n să fie compus va fi de cel mult $\frac{1}{2^k}$ (desigur, dacă la vreunul din teste obținem că n nu e pseudoprim Euler în raport cu baza b, atunci n e cu certitudine compus).

Acesta este, în esență, ALGORITMUL PROBABILIST ~~PT~~ STUDIUL PRIMALITĂȚII SOLOVAY - STRASSEN

În exemplul nostru:

- În raport cu baza 2:

$$\left(\frac{2}{127363}\right)_J = (-1)^{\frac{127362 \cdot 127364}{8}} = -1$$

$$2^{\frac{127363-1}{2}} = 2^{63681} = 2$$

63681 = 32768 + 16384 + 8192 + 4096 + 2048 + 128 + +64 + 1

$2^2 = 4$

$2^4 = 16$

$2^8 = 256$

$2^{16} \equiv 65536$

$2^{32} \equiv 32210$

$2^{64} \equiv 112465$

$2^{128} \equiv 84058$

$2^{256} \equiv 30213$

$2^{512} \equiv 14748$

$2^{1024} \equiv 94863$ $\quad 2^{2048} \equiv 28641$ ~~41847~~ $\quad 2^{4096} \equiv 89161$

$2^{8192} \equiv 67550 \quad 2^{16384} \equiv 95662 \quad 2^{32768} \equiv 59331.$

Deci, $2^{63681} \equiv \boxed{59331 \cdot 95662} \cdot \boxed{67550 \cdot 89161} \cdot \boxed{28641 \cdot 84058} \cdot \boxed{112465 \cdot 2} \equiv$

$\equiv \boxed{44753 \cdot 84006} \cdot \boxed{89752 \cdot 97567}$

$\equiv 19484 \cdot 117682 \equiv 127362 \equiv -1$

Ca urmare, 127363 e pseudoprim Euler în raport cu baza 2. (31)

- În raport cu baza 3:

$$\left(\frac{3}{127363}\right)_J = \left(\frac{127363}{3}\right) \cdot (-1)^{\frac{3-1}{2} \cdot \frac{127363-1}{2}} = -1 \quad (9)$$

$3^{\frac{127363-1}{2}} =$

$= 3^{63681} = 3^{32768} \cdot 3^{16384} \cdot 3^{8192} \cdot 3^{4096} \cdot 3^{2048} \cdot 3^{128} \cdot 3^{64} \cdot 3 = (10)$

$3^2 = 9 \quad 3^4 = 81 \quad 3^8 = 6561 \quad 3^{16} \equiv 125390$

$3^{32} \equiv 71839 \quad 3^{64} \equiv 93161 \quad 3^{128} \equiv 75012 \quad 3^{256} \equiv 30167$

$3^{512} \equiv 39254 \quad 3^{1024} \equiv 38942 \quad 3^{2048} \equiv 95486 \quad 3^{4096} \equiv 41115$

$3^{8192} \equiv 81489 \quad 3^{16384} \equiv 5027 \quad 3^{32768} \equiv 52855.$

Deci

$(10) \equiv 52855 \cdot 5027 \cdot 81489 \cdot 41115 \cdot 95486 \cdot 75012 \cdot 93161 \cdot 3 \equiv$

$\equiv 22867 \cdot 9157 \cdot 82801 \cdot 24757 \equiv$

$\equiv 8347 \cdot 124235 \equiv 127362 \equiv -1$ (11)

Din (9) și (11) ~~obț~~ obținem că 127363 e pseudoprim Euler în raport cu baza 3. (32)

- În raport cu baza 5:

$$\left(\frac{5}{127363}\right)_J = \left(\frac{127363}{5}\right)\cdot(-1)^{\frac{5-1}{2}\cdot\frac{127363-1}{2}} = \left(\frac{3}{5}\right) = -1. \quad (19)$$

$5^{\frac{127363-1}{2}} = 5^{63681} \equiv$

$\equiv 5^{32768}\cdot 5^{16384\;8192}\cdot 5^{4096}\cdot 5^{2048}\cdot 5^{128}\cdot 5^{64}\cdot 5 \equiv (20)$

$5^2 = 25$ $\quad 5^4 = 625$ $\quad 5^8 \equiv 8536$ $\quad 5^{16} \equiv 11660$

$5^{32} \equiv 59279$ $\quad 5^{64} \equiv 54671$ $\quad 5^{128} \equiv 90720$ $\quad 5^{256} \equiv$ ~~108226~~ 48703

$5^{512} \equiv$ ~~56144~~ 101060 $\quad 5^{1024} \equiv 11993$ $\quad 5^{2048} \equiv 39222$ $\quad 5^{4096} \equiv 74970$

$5^{8192} \equiv 99073$ $\quad 5^{16384} \equiv 102371$ $\quad 5^{32768} \equiv 11912.$

Deci

$(20) \equiv 11912 \cdot 102371 \cdot 99073 \cdot 74970 \cdot 39222 \cdot 90720 \cdot 54671 \cdot 5 \equiv$

$\equiv 69990 \cdot 74739 \cdot 79709 \cdot 18629 \equiv$

$\equiv 56837 \cdot 101707 \equiv 127362 \equiv -1.$ (21)

Din (19) și (21) obținem că 127363 e pseudoprim Euler și în ~~baza 5~~ raport cu baza 5 (33)

Din (31), (32) și (33) obținem, conform algoritmului Solovay-Strassen, că 127363 e prim cu probabilitate de cel puțin $1-\frac{1}{2^3}=\frac{7}{8}=87{,}5\% > 80\%$.