1. Utilizând algoritmul lui Fermat, verificați dacă 11317 este prim sau compus.

$n = 11317$

$2^{11317-1} = 2^{11316} = (2^2)^{5658} = (4^2)^{2829} = 16 \cdot 16^{2828} = \cancel{16}$

$= 16 \cdot (16^2)^{1414} = 16 \cdot (256^2)^{707} = 16 \cdot 8951 \cdot (8951)^{706} =$

$= 7412 \cdot (8951^2)^{353} = 7412 \cdot 7358 \cdot (7358)^{352} = 873 \cdot (7358)^{35}$

$= 873 \cdot (7358^2)^{176} = 873 \cdot (10953^2)^{88} = 873 \cdot (8009^2)^{44} =$

$= 873 \cdot (10642^2)^{22} = 873 (2945^2)^{11} = 873 \cdot 4203 \cdot (4203)^{10}$

$= 2511 \cdot (4203^2)^5 = 2511 \cdot 10689 \cdot (10689^2)^2 = 7472 \cdot (9606)^2$

$= 7472 \cdot 7735 = 1 \bmod 11317 \Rightarrow$ nr este prim

Scanat cu CamScanner

2. Folosind algoritmul Miller-Rabin, determinați dacă nr. 21803 este prim sau compus

$n = 21803$

$2^s t = n-1 \Rightarrow 21802 = 2^s \cdot t \Rightarrow 21802 = 2^1 \cdot 10901$

~~Calculăm $b^{2^r t}$ mod n pt r ∈ {0, ...}~~

$b^{2^s t} \equiv 1 \pmod n \Rightarrow b = 2$

$2^{2\cdot 10901} = 4^{10901} = 4 \cdot 4^{10900} = 4 \cdot (4^2)^{5450} = 4 \cdot (16^2)^{2725} =$

$= 4 \cdot 256 \cdot (256)^{2724} = 1024 \cdot (256^2)^{1362} = 1024 \cdot (127^2)^{681} =$

$= 1024 \cdot 16129 \cdot (16129^2)^{340} = 11225 \cdot (13048^2)^{170} = 11225 \cdot (12480^2)^{85}$

$= 11225 \cdot (11571) \cdot (11571^2)^{42} = 4064 \cdot (17621^2)^{21} = 4004 \cdot 3118 \cdot (3118^2)^{10}$

$= 13156 \cdot (19589^2)^5 = 13156 \cdot 17924 \cdot (17924^2)^2 = 8699 \cdot 2571^2$

$= 8699 \cdot 3732 = 1 \pmod{21803}$

Testul ne spune că dacă nu găsim −1 înainte de 1, n compus

În cazul nostru am găsit prima dată 1 $\Rightarrow$ ~~n este~~ 21803 este compus

3. Verificați folosind algoritmul Solovay-Strassen dacă numărul 49937 este prim sau compus

$b^{\frac{49937-1}{2}} \equiv \left(\frac{b}{49937}\right) \bmod (49937) \Rightarrow b^{24968} \equiv \left(\frac{b}{49937}\right) \bmod (49937)$

• $b = 2$. $\frac{2}{49937} = (-1)^{\frac{49937^2-1}{8}} = (-1)^{311712996} = 1$

$2^{24968} = (2^2)^{12484} = (4^2)^{6242} = (16^2)^{3121} = 256 \cdot 256^{3120} = ~~256 \cdot 256~~$

$= 256 \cdot (256^2)^{1560} = 256 \cdot (15599^2)^{780} = 256 \cdot (35737^2)^{390} =$

$= 256 \cdot (44331^2)^{195} = 256 \cdot 16863 \cdot (16863^2)^{97} = 22346 \cdot 19491 \cdot (19491^2)^{96}$

$= 45309 \cdot (19491^2)^{48} = 45309 \cdot (28322^2)^{24} = 45309 \cdot (47590^2)^{12} = 45309 \cdot$

$\cdot (15339^2)^6 = 45309 \cdot (31714^2)^3 = 45309 \cdot 46616 \cdot 46616$

$= 38929 \cdot 42901 = 1 \pmod{49937}$

- $b = 4$: $\left(\frac{4}{49937}\right) = \left(\frac{2}{49937}\right)\left(\frac{2}{49937}\right) = 1 \cdot 1 = 1$

$4^{24968} = \left(2^{24968}\right)^2 \equiv 1^2 = 1 \pmod{49937}$