17 Folosind QS sau Fermat, factorizați numărul: 10353

$n = 10353$

$\sqrt{10353}$ | 101

1 | 10·0 = 0

= 03 | 201·1 = 201

0

= 353

201

152

101 · 101 = 10201

Deci $[\sqrt{10353}] = 101$

Pornesc cu $\boxed{t = 102}$

$t^2 - n = 102^2 - 10353 = (101+1)^2 - 10353 = 101^2 + 1 + 202 - 10353$

$= 10201 + 203 - 10353 = (-152) + 203 = 51 \neq \square$

$10353 : 10201 = 1$ (10201 | 152)

$203 - 152 = 51$

$10404 : 10353 = 1$ (10353 | 51)

$205 + 51 = 256$

$103 - 16 = 87$

$103 + 16 = 119$

$\boxed{t = 103}$

$t^2 - n = 103^2 - 10353 = (102+1)^2 = 10404 + 204 + 1$

$- 10353 = 10404 + 205 = 51 + 205 = 256 = 16^2$

$103^2 - 10353 = 16^2 \Rightarrow 10353 = 103^2 - 16^2 =$

$= (103 - 16)(103 + 16) = 87 \cdot 119$

$\Rightarrow \boxed{t = 103 \quad s = 16 \quad \text{și} \quad a = 87 \quad b = 119}$

17

$n = 991$ - impar

$n = 1 + 990$

$n = 1 + 2 \cdot 495$ $\Rightarrow t = 495,\ d = 1$

Aadar $b^{2^d \cdot t} \equiv 1 \pmod n$

$b^{2 \cdot 495} \equiv 1 \pmod{991}$

$991 - 827 = 164$

$991 - 164$

$n = 991$

$991 = n - 1 = 990 = 2 \cdot 495$

Martorul $b = 2$ pt $n = 0$

$2^{495} \pmod{991} = 2 \cdot 2^{494} = 2 \cdot (2^2)^{247} = 2 \cdot 4^{247} = 2 \cdot 4 \cdot 4^{246}$

$= 2 \cdot 4 \cdot (4^2)^{123} = 2 \cdot 4 \cdot 16 \cdot (16^2)^{61} = 128 \cdot 256^{61} = 128 \cdot 256 \cdot 256^{60}$

$= 128 \cdot 256 \cdot (256^2)^{30} = 32768 \cdot (65.536)^{30} = 65 \cdot (130)^{30} =$

$= 65 \cdot (130^2)^{15} = 65 \cdot (16900)^{15} = 65 \cdot (53)^{15} = 65 \cdot 53 \cdot 53^{14}$

$= 3.445 \cdot (53^2)^7 = 472 \cdot (2809)^7 = 472 \cdot (827)^7 =$

$= (-164)^7 \cdot 472 = (-164) \cdot 164^6 \cdot 472 = \underbrace{-77408}_{\text{mod}} \cdot (164^3)^3$

$= -110 \cdot (26.896)^3 = -110 \cdot (139)^3 = -110 \cdot 139 \cdot 139^2$

$= -15290 \cdot 139^2 = -425 \cdot 19.321 = -425 \cdot 492$

$= \underbrace{-209.100}_{\text{mod}} = -990 \pmod{991} = 1 \bmod 991$

$\Rightarrow$ e posibil ca 991 să fie prim

$b=3$

$3^{495} \pmod{991} = 3 \cdot 3^{494} = 3 (3^2)^{247} = 3 \cdot 9^{247} = 3 \cdot 9 \cdot 9^{246}$

$= 27 \cdot 9^{246} = 27 \cdot (9^2)^{123} = 27 \cdot 81^{123} = 27 \cdot 81 \cdot 81^{122}$

$= 2187 \cdot 81^{122} = 205 \cdot 81^{122} = 205 \cdot (81^2)^{61} = 205 \cdot 6561^{61}$

$= 205 \cdot 6561 \cdot 6561^{60} = 1345005 \cdot (6561^2)^{30} = 218 \cdot (615^2)^{30}$

$= 218 \cdot (654)^{30} = 218 \cdot ((-337)^2)^{15} = 218 \cdot (113569)^{15}$

$= 218 \cdot 595 \cdot 595^{14} = 218 \cdot 595 \cdot (595^2)^7 =$

$= 129710 \cdot (354025)^7 = 880 \cdot 238^7 = (-111) \cdot 238 \cdot 238^6$

$= -652 \cdot (238^2)^3 = -652 \cdot (157)^3 = (-652) \cdot 157 \cdot 157^2$

$= (-291) \cdot 865 = (-291) \cdot (-126) = 990 = (-1) \pmod{991}$

$b=4$

$4^{495} \pmod{991} = (2^2)^{495} = (2^{495})^2 = 1^2 = 1 \pmod{991}$

$\Rightarrow (991)$ pare fi prim

$2187 : 991 = 2$
1982
$= 205$

$991 -$
865
126

(Ex)

$2^n - 1$ prim $\Rightarrow$

n prim $\Rightarrow$

Pp RA n e compus $\Rightarrow \exists\, a, b \in \mathbb{N}^* \setminus \{1\}$ a.î. $n = a \cdot b$

$$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 = \underbrace{(2^a - 1)}_{t_1}\underbrace{((2^a)^{b-1} + (2^a)^{b-2} + \dots + 2^a + 1)}_{t_2}$$

$a \in \mathbb{N}^* \setminus \{1\} \Rightarrow t_2 \geq 2$

$a \geq 2 \Rightarrow t_1 \geq 3 \Rightarrow 2^n - 1$ nu e prim (contradicție)

Identități formule

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \dots + y^{n-1})$$