N

Eulerjeva ff. $\varphi(n)$.

$$\varphi(n) = \left|\{k \in \mathbb{N};\ k \le n \wedge k \perp n\}\right|$$

„odlična ideja!"

- $a \perp b \Rightarrow \varphi(ab) = \varphi(a)\,\varphi(b)$
- $p \in \mathbb{P} \Rightarrow \varphi(p^k) = p^k - p^{k-1}$

splošen n: $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$

$$\varphi(n) = \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}) \cdots \varphi(p_m^{k_m}) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right) \cdots \left(p_m^{k_m} - p_m^{k_m-1}\right) =$$

$$= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_m^{k_m}\left(1 - \frac{1}{p_m}\right) =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

n	φ
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

MALI FERMATOV IZREK:

$$a^{p-1} \equiv 1 \pmod p;\ p \in \mathbb{P},\ a < p$$

EULERJEV IZREK: $\Rightarrow a^m = a^{k\varphi(n)+r} = a^r \cdot \underbrace{\left(a^{\varphi(n)}\right)^k}_{\to 1} \equiv a^r$

$$a^{\varphi(n)} \equiv 1 \pmod n;\ a \perp n$$

N

izračunaj naslednje ostanke upoštevajoč 5

a.) $38^{2024} \,/\!/\, 43$

b.) $2^{108} \,/\!/\, (37 \cdot 73)$

c.) $c \,/\!/\, 13 \quad ; c = 10^{10^{10^n}}$

(lahki $n=1$, $n=2$, $n>2$.)

$(a^b)^c = a^{(bc)}$

a.) $2024 = \varphi(43) \cdot k + r =$

$= 42 \cdot 48 + 8$

$$38^{2024} = 38^8 \cdot \left(38^{\varphi(43)}\right)^{48} \equiv 38^8 \pmod{43}$$

$$38^8 \equiv (-5)^8 \equiv 25^4 = 625^2 \equiv 23^2 \equiv 529 \equiv 1$$

b) $2^{108} \% (37 \cdot 73)$

$\varphi(37 \cdot 73) = \varphi(37)\varphi(73) = 36 \cdot 72$ → je več od 108 CRE EULER

DRUGI POSTOP:

$2^{108} \% 37$

$(108 = 3 \cdot 36)$

$2^{108} = (2^{36})^3 = 1^3 = 1$

↳ euler

$2^{108} + 73y = 1$

$2^{108} \% 73$

$108 = \varphi(73) \cdot t + r =$

$= 72 \cdot t + r =$

$= 72 \cdot 1 + 36$

$2^{108} = 2^{36} \cdot (2^{\varphi(73)})^1 \equiv 2^{36} \pmod{73}$

$2^{36} = 2^{6 \cdot 6} = 2^{6^6} = 64^6 \equiv (-9)^6 \pmod{73}$

$(-9)^6 = 9^{2 \cdot 3} = 81^3 \equiv 8^3 \pmod{73}$

$8^3 = 8 \cdot 8^2 = 8 \cdot 64 = 8 \cdot (-9) \pmod{73}$

$-72 \equiv 1 \pmod{73}$

$2^{108} + 37w = 1$

$2^{108} + 37w = 1$
$2^{108} + 73y = 1$

$37w = 73y$

$37w - 73y = 0$

$w = 0$ $y = 0$
$w = 73t$ $y = 37u$
$t \in \mathbb{Z}$ $u \in \mathbb{Z}$

$2^{108} \equiv 37(73t) + 1 \pmod{37 \cdot 73}$

$2^{108} \equiv 1 \pmod{37 \cdot 73}$

tako nalogo rešimo tako, da sta faktorja modula tuja:

$2^{108} \bmod (8 \cdot 6)$

bi nerešali tok

$2^{108} \bmod (16 \cdot 3)$

c) $n=1$: $10 \equiv 10 \pmod{13}$

$n=2$: $10^{10} \equiv (-3)^{10} = 9^5 \equiv (-4)^4 \cdot (-4) \equiv 16^2 \cdot (-4) \equiv 3^2 \cdot -4 \equiv 9 \cdot -4 \equiv$
$\equiv -4 \cdot -4 \equiv 16 \equiv 3$
$\equiv 3 \pmod{13}$

$n > 2$: $10^b = 10^{t\varphi(13) + r} = 10^{t \cdot 12 + r}$

iščemo torej $b \% 12$.

opazi, da je $12 = 3 \cdot 4$, $b \% 3 \cdot 4$

$b \% 4 = 0$ $b \% 3 = 1$

$b = 3x + 1$
$b = 4y + 0$

⇓ ...

$b \% 12 = 4$

$3x + 1 = 4y$

$4y - 3x = 1$

rešimo:

$y = 1 + k3$ $k \in \mathbb{Z}$

$x = 1 + k4$

$b = 4(1 + 3k) =$
$= b = 4 + 12k$

sedaj: $10^b = 10^{k12+r} \equiv 1 \cdot 10^r \pmod{13}$

r je ostanek pri deljenju b z 4

$10^4 \equiv (-3)^4 \equiv 9^2 \equiv (4^2) \equiv 3 \pmod{13}$

$10^{10^{10^{10}}} \equiv 3 \pmod{13}$.

N

HITRO POTENCIRANJE - square and multiply
exponentiation by squaring

$3^{230} \bmod 5$

$3^1 \,\%\, 5 = 3$

$3^2 \,\%\, 5 = 4$

$3^4 \,\%\, 5 = 1$

$3^8 \,\%\, 5 = 1$

$3^{16} \,\%\, 5 = 1$

$\ldots = 1$

$230_{(10)} = 11100110_{(2)}$

$3^{230} = 3^{128} \cdot 3^{102} =$

$= 3^{128} \cdot 3^{64} \cdot 3^{38} =$

$= 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^4 \cdot 3^2 \equiv 4 \pmod 5$

(1, 1, 4)