$\boxed{\text{Fermatov izrek}}$ $\boxed{a^{p-1} \equiv 1 \mod p}$

p - praštevilo

vsako celo število je kongruentno z

$0, 1, 2, \ldots, p-1 \mod p$

vsi večkratniki p, $p \nmid a$ (p ni delitelj a-ja

$a = 1, 2, 3, \ldots, p-1$

$a, 2a, 3a, \ldots (p-1) \cdot a$

(1) $\overline{r \cdot a \equiv \emptyset \mod p}$

$p \mid r \cdot a \Rightarrow$ nemogoče, ker $p \nmid a$ & $r < p$

(2) r, s - števili, ki nista kongruentni med sabo

$r \cdot a, \; s \cdot a$ $\qquad r \cdot a \equiv s \cdot a \pmod p$

$0 < r < p$ $\qquad r \cdot a - s \cdot a = a \cdot (r - s)$

$0 < s < p$

$p \nmid a$, ali je lahko $p \mid (r-s)$

$p \nmid (r-s)$ $\qquad a, 2a, 3a, \ldots (p-1)a$

prerazporediter

$0 < r < p$

$0 > -s > -p$

$-p < -s < 0$

$-p < r - s < p$

$r - s \neq \emptyset$

$\cancel{(p-1)!}\, a^{p-1} \equiv \cancel{(p-1)!} \mod p$

$\Rightarrow \boxed{a^{p-1} \equiv 1 \mod p}$

$a \cdot 2a \cdot 3a \cdots (p-1) a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$

$$24^{38} \bmod 7 = ?$$

$$\boxed{3^{(p-1)} \equiv 1 \bmod p}$$

Fermatov izrek

$$24^{38} \bmod 7 \equiv 3^{6\cdot 6+2} \bmod 7$$

$$\equiv (3^6)^6 \cdot 3^2 \bmod 7 \equiv$$

$$\equiv 1^6 \cdot 9 \bmod 7 \equiv$$

$$\equiv 2 \bmod 7$$

---

p - praštevilo & $p \nmid a$

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

$p = 5$

$5 \nmid 2$	$2^{5-1} \equiv 1 \pmod{p}$
$5 \nmid 3$	$3^{5-1} \equiv 1 \pmod{5}$
$5 \nmid 4$	$4^{5-1} \equiv 1 \pmod{5}$
$5 \mid 5$	$5^{5-1} \equiv \emptyset \pmod{5}$
$5 \nmid 6$	$6^{5-1} \equiv 1 \pmod{5}$
$5 \nmid 7$	$7^{5-1} \equiv 1 \pmod{5}$

...

$3^{100000} \bmod 53 \equiv ?$

$p = 53$
– praštevilo

$53 \nmid 3$ $\qquad 3^{53-1} \equiv 1 \bmod 53$

$100.000 : 52 = 1923$
ostanek 4

$\Rightarrow \left(3^{52}\right)^{1923} \equiv 1 \bmod 53$

$\equiv 3^4 \equiv 81 \equiv \underline{\underline{28}} \bmod 53$ ✓

Permutacije

$p = 7$

$0, 1, 2, \ldots, 6 \bmod 7$

$a = 12$

$12 \quad 24 \quad 36 \quad 48 \quad 60 \quad 72 \quad \bmod 7$

$\boxed{5 \quad 3 \quad 1 \quad 6 \quad 4 \quad 2 \quad \leftarrow \text{permutacije}}$

$2^{-1} \equiv 13 \mod 25$ invertz

$2 \cdot 13 \equiv 1 \mod 25$

$7^{-1} \equiv \frac{1}{7}$

$e^{-1} \equiv d \mod p$

$2^{-11} \equiv (2^{-1})^{11} \equiv 13^{11} \pmod{25}$

RSA

difficulty in factoring prime numbers

100 digit

$n = p \cdot q$ $\quad$ p & q equal length $\approx$ large

$e \nmid (p-1)\cdot(q-1)$ $\quad$ relatively prime

$e \cdot d \equiv 1 \mod ((p-1)(q-1))$

$d = e^{-1} \mod ((p-1)(q-1))$

$m \rightarrow$ message $\quad$ blocks smaller than n

< 200 digits

padding with 0ø on the left
to keep < 200 bits

$c = m^e \mod n$

$m = c^d \mod n$

$c^d \equiv (m^e)^d \equiv m^{k(p-1)(q-1)+1} \equiv$

$\equiv m \cdot m^{k(p-1)(q-1)} \equiv m \cdot 1 \equiv m$

recovers the message

Diffie-Hellman key exchange // Ralph Merkle

$\boxed{1976}$

A

mod $p = 23$

base $g = 5$

B

secret $a = 4$

secret $b = 3$

$A = g^a \bmod p$

$\equiv 5^4 \bmod 23$

$= 4$

$B = g^b \bmod p$

$\equiv 5^3 \bmod 23$

$\equiv 10$

$A = 4$ →

← $B = 10$

shared $= B^a \bmod 23$

$\equiv 10^4 \bmod 23$

$\equiv 18$

key

shared $A^b \bmod p$

$\equiv 4^3 \bmod 23$

$\equiv 18$

key