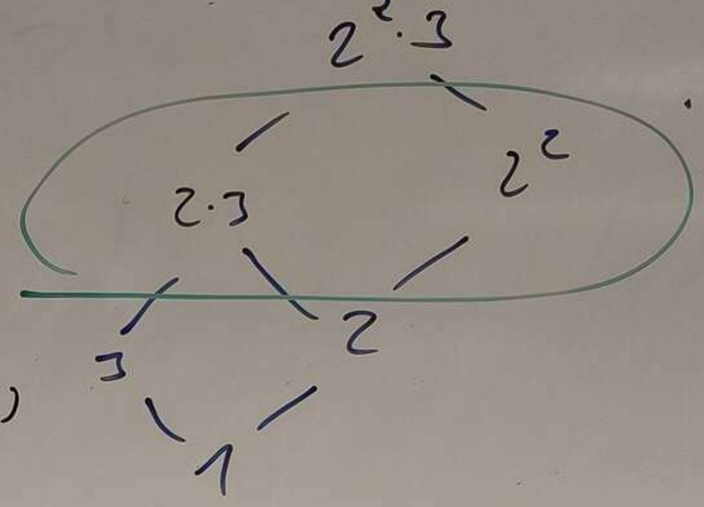
$a^{\varphi(m)} \equiv 1 \mod m \quad (a,m)=1$

$a^k \equiv 1 \mod m \xrightarrow{k \text{ nejmenší}} k \mid \varphi(m)$

$(a,m)=1$

a je prim. k. pokud k nejmenší $= \varphi(m)$



Najděte prim. kořeny modulo 26.

Hledáme a t.ž. $a^k \not\equiv 1 \mod 26 \quad \forall k < \varphi(26) = \varphi(2 \cdot 13) = 12$

12	
2	6
3	4

$12 = 2^2 \cdot 3$ odebereme jedno prvoč.

$2 \cdot 3 = 6$

$2^2 = 4$

$\Rightarrow$ stačí nalézt a t.ž.

$a^6 \not\equiv 1 \mod 26$

$a^4 \not\equiv 1 \mod 26$

všechna $k \mid 12$, tak zároveň $k \mid 6$ nebo $k \mid 4$

možné č.: $\overset{\times}{3}, \overset{\times}{5}, \overset{\checkmark}{7}, \overset{\times}{9}, 11, 15, 17, 19, 21, 23, 25$

$3^6 \equiv a^3 \equiv 9 \cdot 8 \cdot 1 \equiv 9 \cdot 3 \equiv 27 \equiv 1 \mod 26$

$5^6 \equiv 25^3 \equiv (-1)^3 \equiv -1 \mod 26$

$5^4 \equiv 25^2 \equiv (-1)^2 \equiv 1 \mod 26$

$7^6 \equiv 4a^3 \equiv (-3)^3 \equiv -27 \equiv -1 \mod 26$

$7^4 \equiv 4a^2 = (-3)^2 \equiv 9 \mod 26$

$(a,26)=1$

7^k je pr. k. $\Leftrightarrow (k,m)=1$

$\varphi(\varphi(m)) = \varphi(12) = 4$

$7^1, 7^5, 7^7, 7^{11}$

Verejný kľúč: $n = 95$ $e = 55$ zašifrovaná zp. $Z = 42$

$M^{k\varphi(n)+1}$ $= M^e$

$M \to M^e \bmod n \longrightarrow (M^e)^f = M^{e \cdot f} \equiv M \leftarrow e \cdot f \equiv 1 \bmod \varphi(n)$ $(e, \varphi(n)) = 1$

$n = 95 = 5 \cdot 19$ $\varphi(95) = 4 \cdot 18 = 72$ $M = 23$

chceme inv. prvek $\in 55$ modulo 72 $(55, 72) = 1$

$55 = 1 \bmod 72$

$a \cdot 55 + b \cdot 72 = 1$ $a \cdot 55 \equiv 1 \bmod 72$

a	b	$a \cdot 55 + b \cdot 72$
0	1	72
1	0	55
-1	1	17
4	-3	4
-17	13	1

$-17 \cdot 55 \equiv 55 \cdot 55 \bmod 72$

$55 - 3 \cdot 17 = 4$

$17 - 4 \cdot 4 = 1$

Inv. prvek 55 je 55.

$Z^b = 42^{55} \bmod 95 = 5 \cdot 19$

$42^{55} \equiv 2^{55} \equiv 2 \cdot 2^{54} \equiv 2 \cdot 4^{27} \equiv 2 \cdot (-1)^{27} \equiv -2 \bmod 5$

$42^{55} \equiv 4^{55} \equiv 4^{18k+1} \equiv 4 \bmod 19$

$42^{55} \equiv 4^{55} \equiv 4 \bmod 18$

$55 \equiv 1 \bmod 18$

4, 23, 42, 61, 80

X ✓ X X X