$$\left(\frac{3}{p}\right) = \begin{cases} p\equiv 1\ (4): & \left(\frac{p}{3}\right) \overset{p\equiv 1\ (3)}{=\!=\!=} \left(\frac{1}{3}\right) = +1 \\ & p\equiv 2\ (3): \quad \left(\frac{2}{3}\right) = -1 \\ p\equiv 3\ (4): & -\left(\frac{p}{3}\right) \overset{p\equiv 1\ (3)}{=\!=\!=} -\left(\frac{1}{3}\right) = -1 \\ & p\equiv 2\ (3): \quad -\left(\frac{2}{3}\right) = +1 \end{cases}$$

$3 \equiv 3 \pmod 4$

$p \equiv ? \pmod 4$

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv 1, 11 \pmod{12} \\ -1 & p \equiv 5, 7 \pmod{12} \end{cases}$$

$p = 35; \quad a = 2$

$a \cdot b^c$

$2^{34} \equiv ? \pmod{35}$

$\equiv 1 \cdot 2^{34} \equiv 1 \cdot (2^2)^{17}$

$\equiv 1 \cdot 4^{17} \equiv (1 \cdot 4) \cdot (4^2)^8$

$\equiv 4 \cdot 16^8 \equiv 4 \cdot (16^2)^4$

$\equiv 4 \cdot 11^4 \equiv 4 \cdot 16^2 \equiv 4 \cdot 11^1$

$\equiv 9 \not\equiv 1 \pmod{35} \Rightarrow$ 35 není prv.

561 je pseudoprvočíslo:

$$561 = 3 \cdot 11 \cdot 17$$

$$a^2 \equiv 1 \pmod 3$$

$$a^{10} \equiv 1 \pmod{11}$$

$$a^{16} \equiv 1 \pmod{17}$$

$$\Rightarrow a^{80} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$$

$$\Rightarrow a^{560} \equiv 1 \pmod{561}$$

test neodhalí, že 561 není prvočíslo

$$[p-1, q-1, r-1] \mid (pqr-1)$$

$p = 561$ $\quad a = 2 : 2^{280} \equiv 1 \pmod{561}$

$a = 5 : 5^{280} \not\equiv 1 \pmod{561}$

$p = 1729$ $\quad a = 11 : 11^{864} \equiv 1 \not\equiv \left(\frac{11}{1729}\right)$

$\left(\frac{11}{865}\right) = \left(\frac{865}{11}\right) = \left(\frac{7}{11}\right) = (-1) \cdot \left(\frac{11}{7}\right) = (-1)\left(\frac{2}{7}\right)\left(\frac{2}{7}\right)$

$11 \equiv 3 \quad (4)$ $\qquad 7 \equiv 3 \quad (4)$ $\qquad = -1$

$865 \equiv 1 \quad (4)$ $\qquad 11 \equiv 3 \quad (4)$

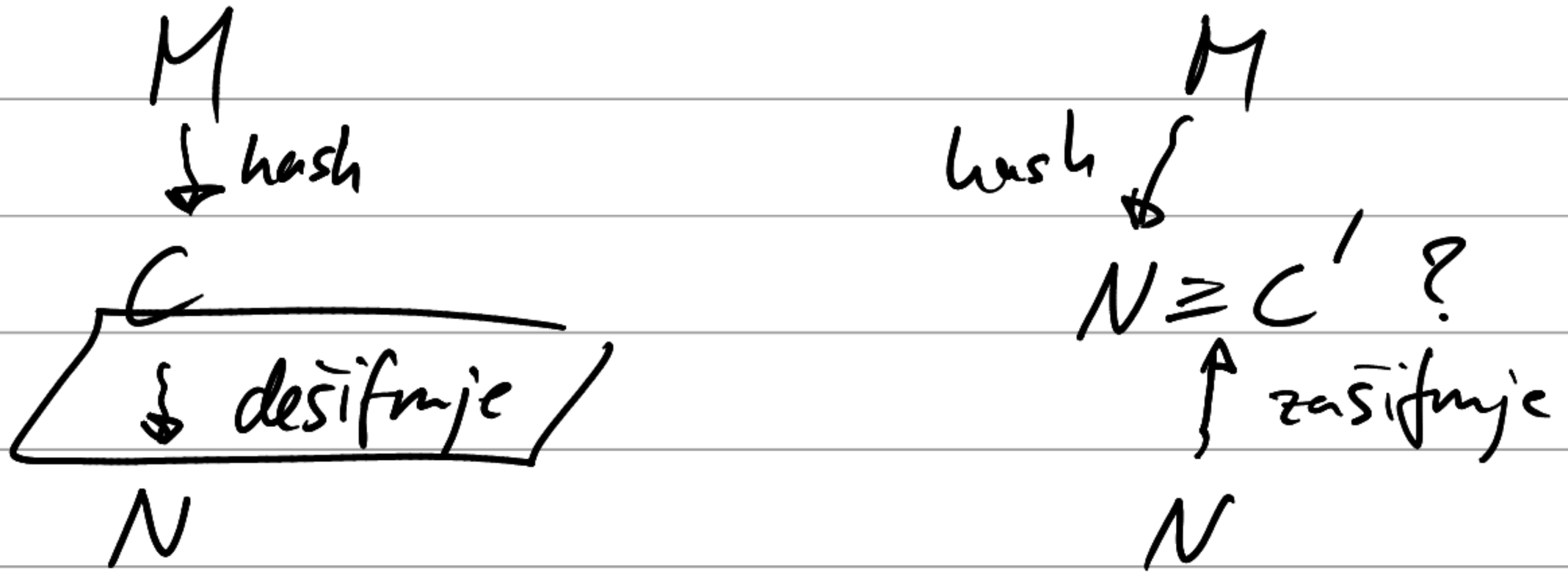
ale taky to vyjde -1 !

1	0	a
0	1	b
k	l	d

$$2^{560} \equiv 1 \cdot 2^{560} \equiv 1 \cdot (2^2)^{280}$$
$$\equiv 1 \cdot 4^{280} \equiv 1 \cdot (4^2)^{140}$$
$$\equiv 1 \cdot 16^{140} \equiv 1 \cdot (16^2)^{70}$$
$$\equiv 1 \cdot 256^{70} \equiv 1 \cdot (256^2)^{35}$$
$$\equiv 1 \cdot 460^{35} \equiv (1 \cdot 460) \cdot (460^2)^{17}$$
$$\equiv 460 \cdot 103^{17} \equiv (460 \cdot 103) \cdot (103^2)^{8}$$
$$\equiv 256 \cdot 511^{8} \equiv 256 \cdot (511^2)^{4}$$
$$\equiv 256 \cdot 256^{4} \equiv 256 \cdot (256^2)^{2}$$
$$\equiv 256 \cdot 460^{2} \equiv 256 \cdot (460^2)^{1}$$
$$\equiv 256 \cdot 103^{1} \equiv 1$$

$$a^{24} \equiv (((a^2)^2)^2)^3$$

podepisování:



S_A : „ p, q “ ⟶ „ $\varphi(n) = (p-1)(q-1)$ “

V_A : $p \cdot q = n$, e ⟶ $\underline{\underline{d}}$

$d \cdot e \equiv 1 \pmod{\varphi(n)}$

(A) (B)

$M \pmod n \longrightarrow C \equiv M^e \pmod n$

$M \equiv C^{1/e}$ ⟵ C

$\equiv C^d$

$(M^e)^d \equiv M^{e \cdot d} \equiv M^1 \equiv M \pmod n$

$p = 23$, $q = 29$; $n = 23 \cdot 29 = 667$

$\varphi(n) = 22 \cdot 28 = 616$

$m \equiv 25 \quad (667)$

$e = 487 \quad (616)$

$C \equiv 25^{487} \equiv ? \quad (667)$

$25^{487} \equiv 2^3 \equiv 8 \qquad (23)$

$25 \equiv 2 \quad (23)$

$487 \equiv 3 \quad (22)$

$25^{487} \equiv (-4)^{11} \equiv -2^{11} \cdot 2^{11} \qquad (29)$

$\equiv -2048 \cdot 2048 \equiv -5$

$$a^k \equiv b^l \pmod{\overset{23}{\overset{\shortparallel}{m}}} \Leftarrow \underset{(a,m)=1}{} \quad a \equiv b \pmod{m}$$

$$k \equiv l \pmod{\varphi(m)}$$

$c \equiv 25^{487} \equiv 8 \quad (23)$

$c \equiv 25^{487} \equiv -5 \quad (29)$

$c = 23t + 8$

$23t + 8 \equiv -5 \quad (29)$

$29t \equiv 0$

$23t \equiv -13 \quad (29)$

$6t \equiv 13$

$5t \equiv -52 \equiv 6$

$t \equiv 7 \quad (29)$

$c = 23(29s + 7) + 8$

$= 667s + 169$

$c \equiv 169 \pmod{667}$

desifrovat ?

$e \equiv 487 \pmod{616}$

$d \cdot e \equiv 1 \pmod{616}$

$d \equiv ?$

$616\,d \equiv 0 \pmod{616}$

$487\,d \equiv 1 \pmod{616}$

$129\,d \equiv -1$

$100\,d \equiv 4$

$29\,d \equiv -5$

$13\,d \equiv 19$

$3\,d \equiv -43$

$d \equiv 191$

$c \equiv 169 \pmod{667}$ $d \equiv 191 \pmod{616}$

$m \equiv 169^{191} \pmod{667}$

$m \equiv 169^{191} \equiv 8^{15} \equiv 8^{-7} \equiv (8^{-1})^7 \pmod{23}$

$\equiv 3^7 \equiv 2$

$$m \equiv 169^{191} \equiv (-5)^{-5} \equiv ((-5)^{-1})^5 \quad (29)$$
$$\equiv (-6)^5 \equiv 25$$

$$\rightsquigarrow \begin{matrix} m \equiv 2 \quad (23) \\ m \equiv 25 \quad (29) \end{matrix} \Big\} \quad m \equiv 25 \quad (667)$$

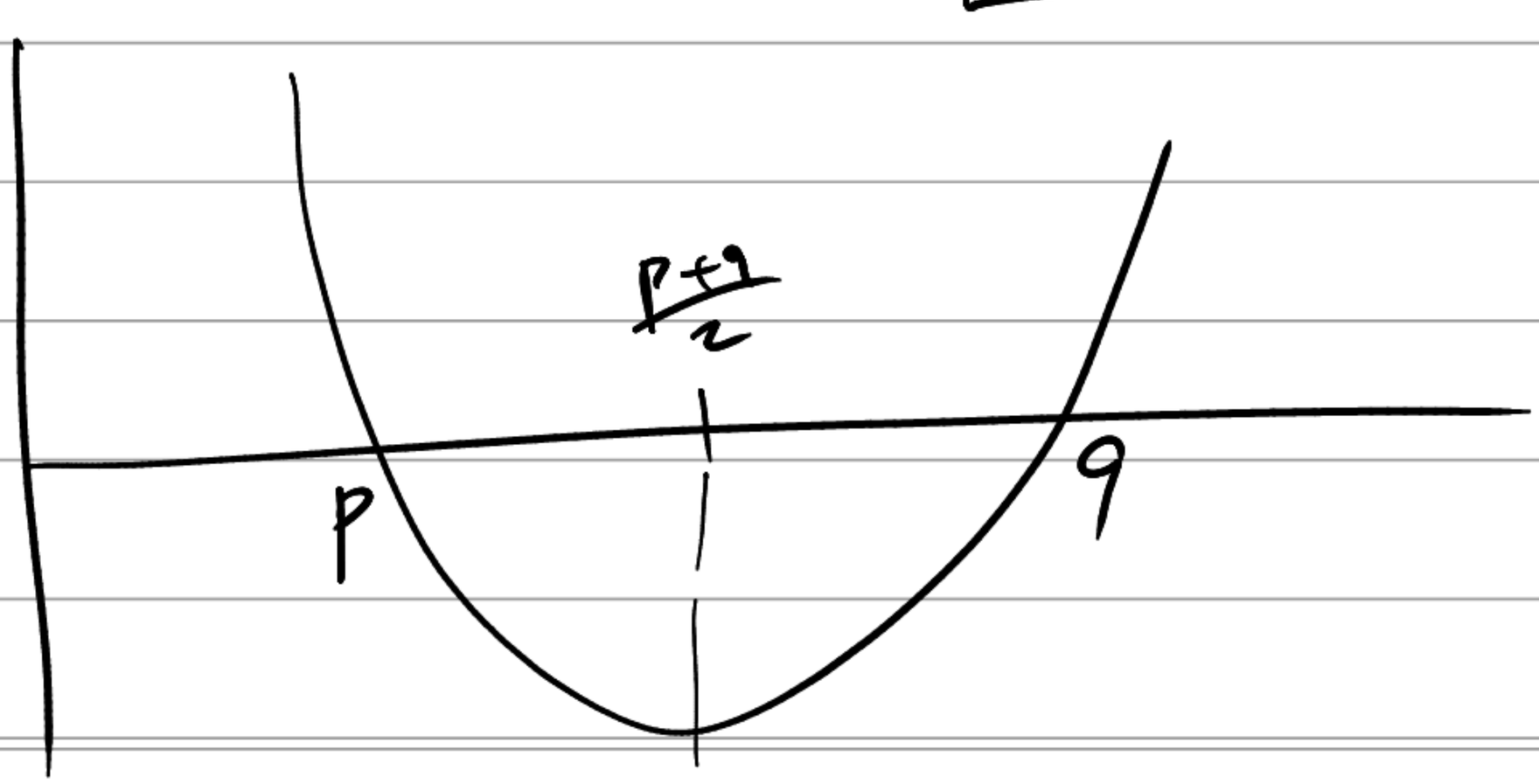
$n \qquad \varphi(n) \longrightarrow p, q$

$n = p \cdot q$

$\varphi(n) = (p-1)(q-1) = p \cdot q - p - q + 1$

$n - \varphi(n) + 1 = p + q$

$$(x-p)(x-q) = \underline{x^2 - (p+q)x + p \cdot q}$$



(A) (B)

$m \pmod n \longrightarrow c \equiv m^2 \pmod n$

$m \equiv c^{1/2} \longleftarrow c$

(p | g) verejné

(A) (B)

$S : a \longrightarrow g^a$

$g^b \longleftarrow b : S$

$(g^b)^a \equiv g^{ab} \equiv (g^a)^b$