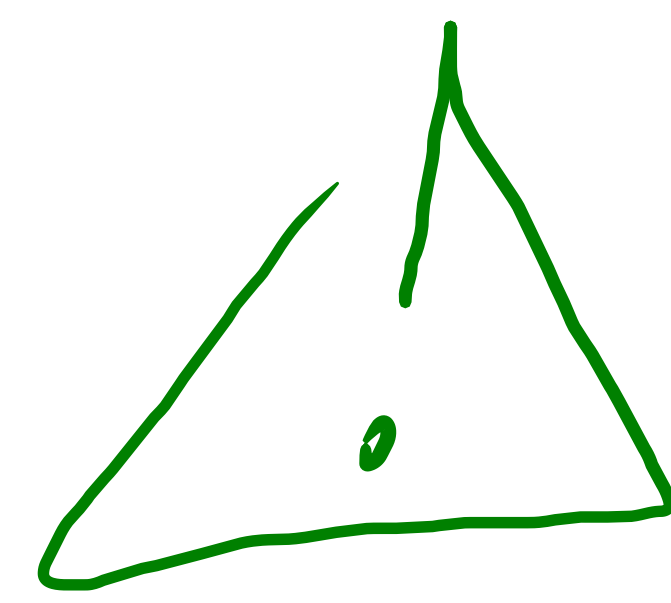


20 II

OS

23 II

TEOS

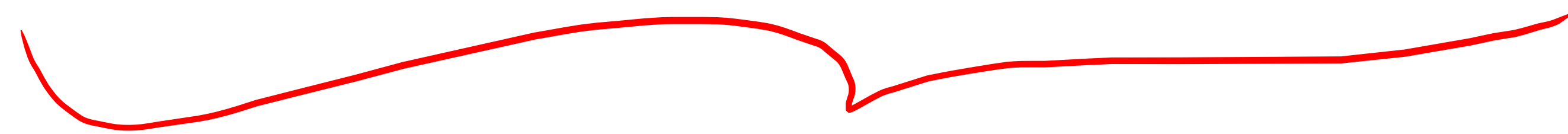


6248

27 II

—

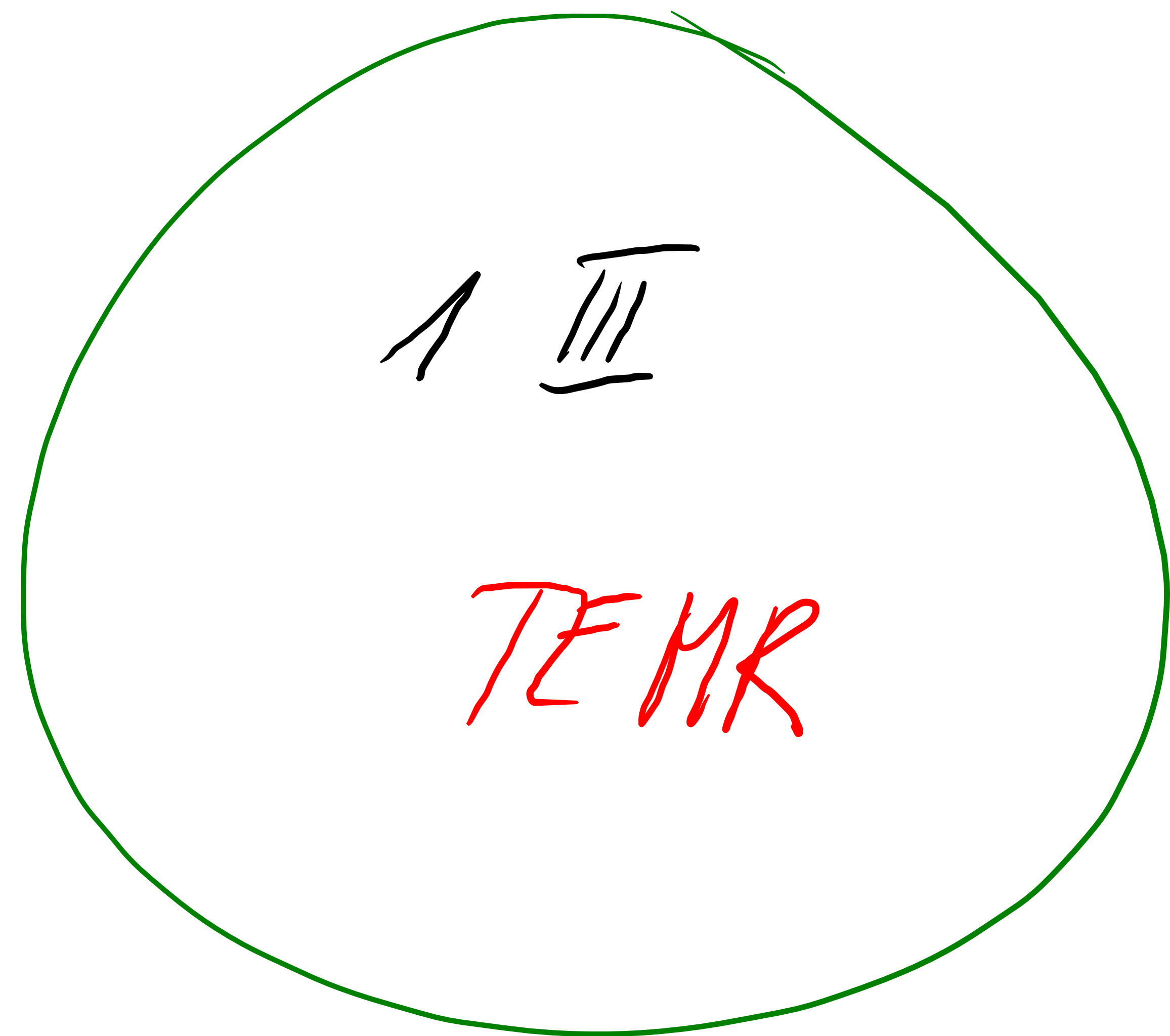
29 II



MR

1 III

TEMR



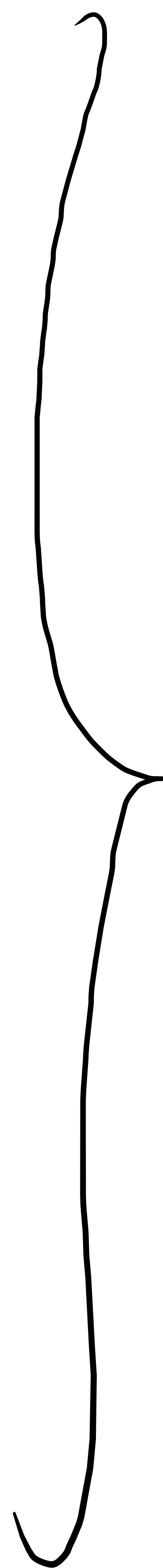
2.6.2 a' 2.6.19

2.8.1

2.8.4 a' 2.8.6

2.8.9

2.8.12



TE crypto

Thm  $a^{\varphi(m)} \equiv 1 \pmod{m}$  EULER

$$m = p^2$$

$$\varphi(m) = p(p-1) = 3 \cdot 2$$

nombre d'inversibles  $\downarrow$  l'ensemble des inversibles

$$\varphi(m) = \left| \mathbb{Z}_m^* \right| \quad m=9 = 3 \cdot 3$$

Exemple:  $\uparrow$  nombre d'éléments d'un ensemble

$$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$\uparrow \quad \uparrow \quad \quad \uparrow \quad \uparrow \quad \quad \uparrow \quad \uparrow$

$$\text{pgcd}(2, 9) = 1$$

$$8 \cdot x \equiv 1 \pmod{9}$$

$$9 \mid (8x-1) \Leftrightarrow 8x-1 = k \cdot 9$$

$$\Leftrightarrow 8 \cdot x + k \cdot 9 = 1$$

$$9 = 1 \cdot 9 + 0 \cdot 8$$

$$8 = 0 \cdot 9 + 1 \cdot 8$$

$$1 = 1 \cdot 9 - 1 \cdot 8$$

$$1 = k \cdot 9 + x \cdot 8$$

$$k=1 \quad x=-1$$

$$\Rightarrow (-1) \cdot 8 \equiv 1 \pmod{9}$$

$$\Leftrightarrow 8 \cdot 8 \equiv 1 \pmod{9}$$

$$64 = 1 + 7 \cdot 9$$

$$1^6 \pmod{9} = 1$$

$$2^6 \pmod{9} / 64 \pmod{9} = 1$$

$$4^6 \pmod{9} = 1$$

$$5^6 \pmod{9} = 1$$

$$7^6 \pmod{9} = 1$$

$$8^6 \pmod{9} / (8 \cdot 8)^3 \pmod{9} = (1)^3 \pmod{9} = 1$$

$$\mathbb{Z}_{15} = \{0; \dots; 14\}$$

$$\mathbb{Z}_{3 \cdot 5}$$

$$15 = 3 \cdot 5$$

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

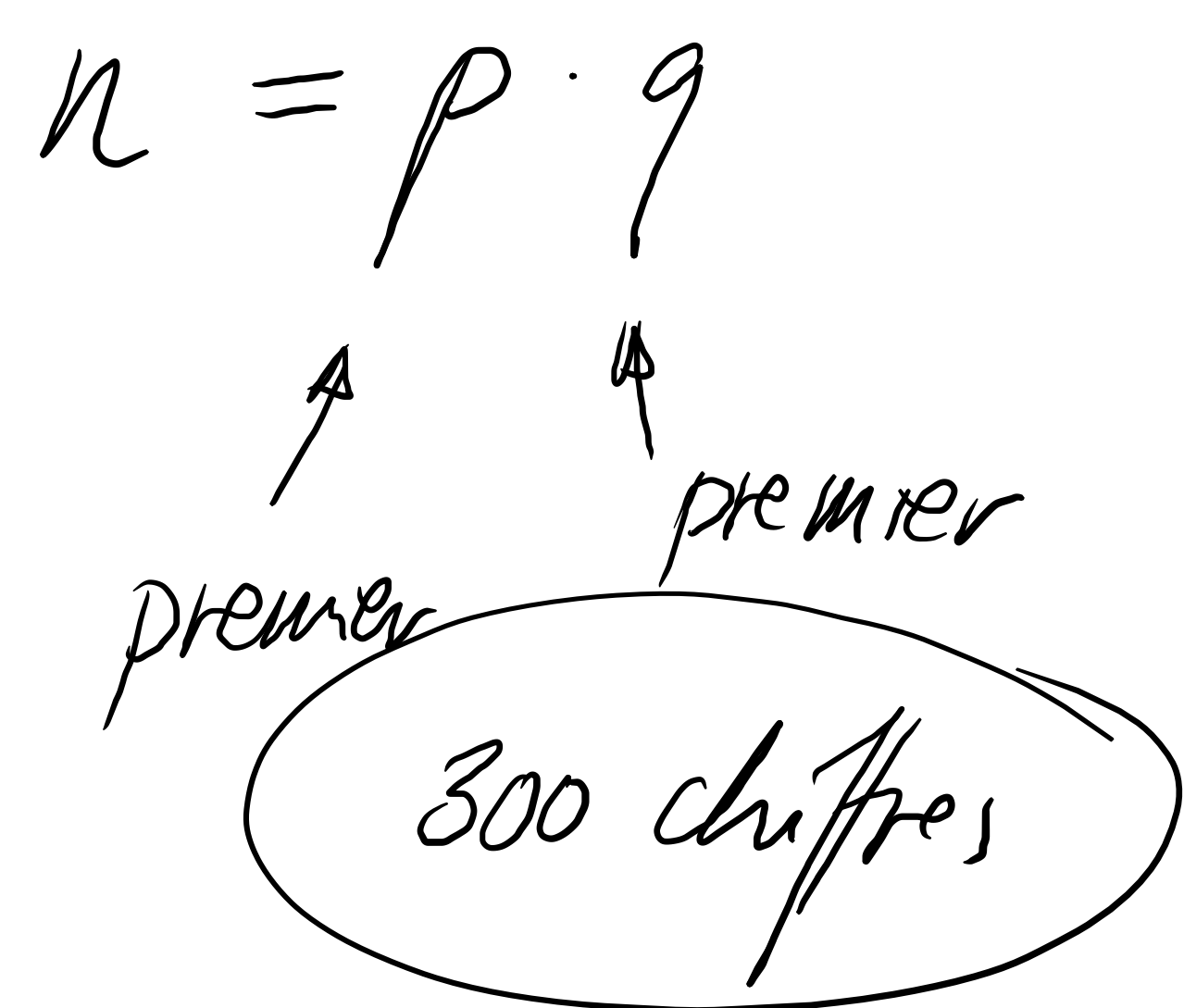
8 inversibles

$$11^8 \pmod{15} = 1$$

↑

$$(3-1)(5-1)$$

Clef RSA:  $(n; e)$



$m \in \mathbb{Z}_n$

Chiffrer:  $C = m^e \pmod n$

Pour déchiffrer

$$d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$$

↑  
existe

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

Déchiffrer:  $C^d \pmod n =$

$$(m^e)^d \pmod n =$$

$$m^{e \cdot d} \pmod n =$$

Construction

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

$$\Leftrightarrow e \cdot d + k \cdot \varphi(n) = 1$$

$$m^{1 - k \cdot \varphi(n)} \pmod n =$$

$$\Leftrightarrow e \cdot d = 1 - k \cdot \varphi(n)$$

$$m \cdot (m^{\varphi(n)})^{-k} \pmod n =$$

$$m \cdot 1^{-k} \pmod n = m \pmod n$$

$$2^{b-c} = 2^b \cdot 2^{-c}$$

$$2^{-x \cdot y} = (2^y)^{-x}$$

$$(n_{\text{beo}}, e_{\text{beo}})$$

$$n_{\text{beo}} = p_{\text{beo}} \cdot q_{\text{beo}}$$

$$(p_{\text{beo}}, q_{\text{beo}}, d_{\text{beo}})$$

$$m \in \mathbb{Z}_{n_{\text{beo}}}$$

$$\varphi(n_{\text{beo}}) = (p_{\text{beo}} - 1)(q_{\text{beo}} - 1)$$

$$C = m^e \pmod{n_{\text{beo}}}$$

Chiffre



$$C^{d_{\text{beo}}} \pmod{n_{\text{beo}}} = m$$

$p = 23$   
 $q = 31$   
 $e = 17$   
 $n = p \cdot q$

c) Clef publique:  $(713; 17)$

$d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$   
 $\uparrow$   
 $17$

$(p-1)(q-1) = 22 \cdot 30 = 660$

$s \cdot 660 + t \cdot 17 = 1$

2)  $660 = 1 \cdot 660 + 0 \cdot 17$   
 $17 = 0 \cdot 660 + 1 \cdot 17$

$$\begin{array}{r|l} 660 & 17 \\ \hline & 38 \\ \hline & 14 \end{array}$$

$14 = 1 \cdot 660 - 38 \cdot 17$       $L_3 = L_1 - 38 \cdot L_2$

$3 = -1 \cdot 660 + 39 \cdot 17$

$L_5 = L_3 - 4 \cdot L_4$

$2 = 5 \cdot 660 - 194 \cdot 17$

$1 = -6 \cdot 660 + 233 \cdot 17$

b) Clef privée  $(23; 31; 233)$

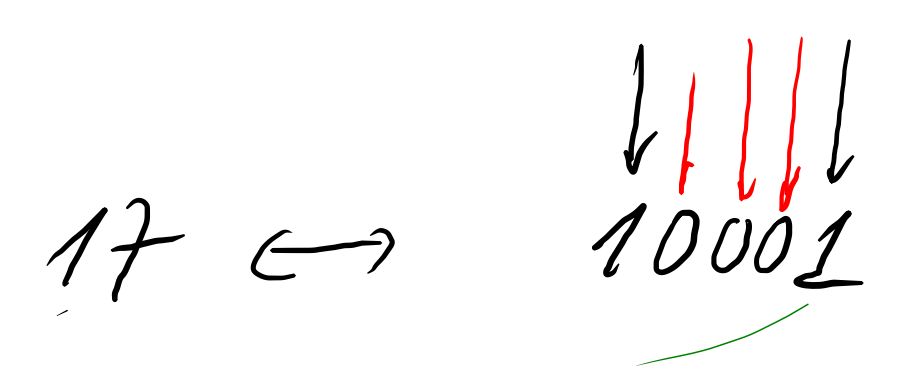
$233 \cdot 17 \equiv 1 \pmod{660}$

d)  $333^{17} \pmod{713}$

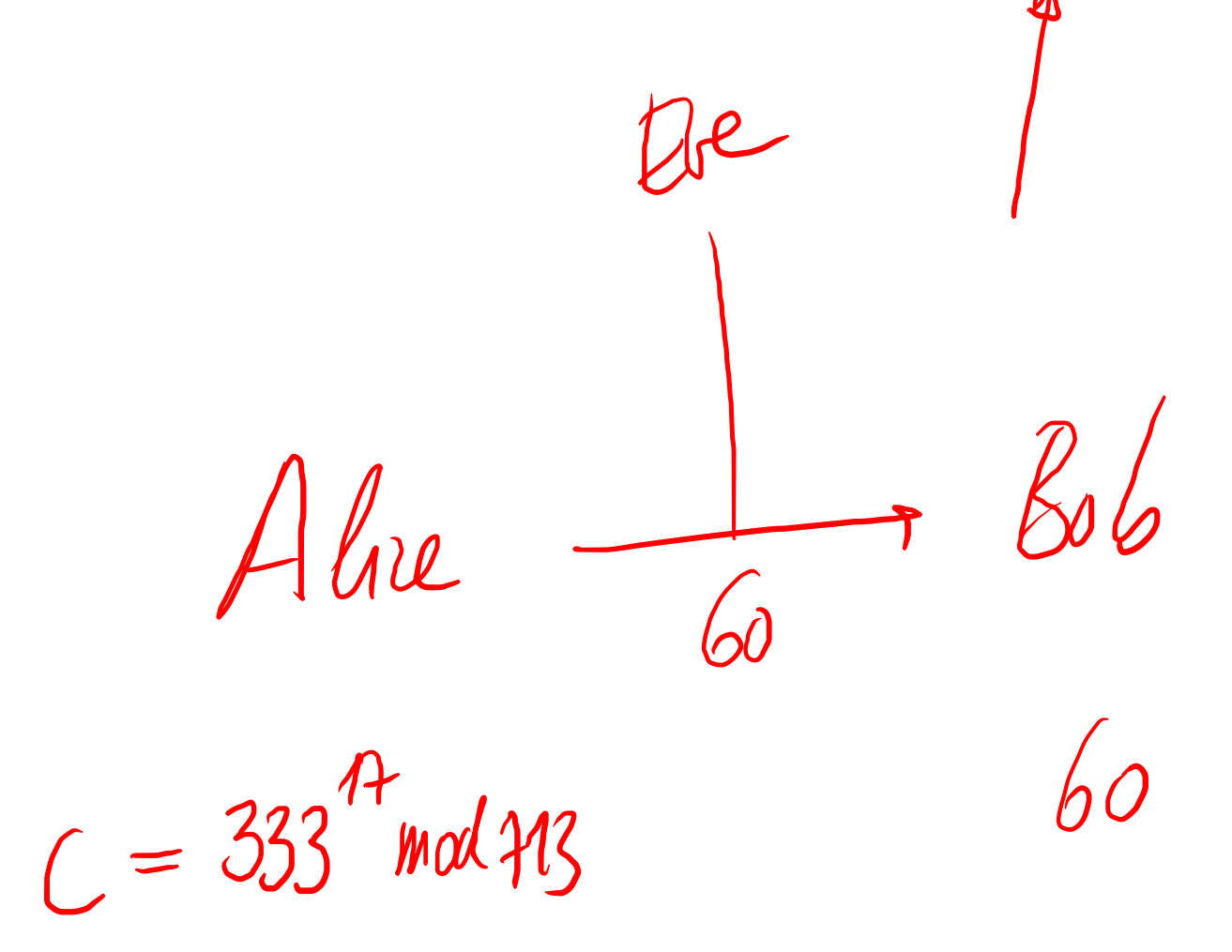
EXPONMOD

333	1	1
<del>377</del>	2	0
<del>128</del>	4	0
<del>638</del>	8	0
225	16	1

$333^2 = 110889$



$r = 333 \cdot 225 \equiv 60 \pmod{713}$





$$\varphi(p^k) = (p-1)p^{k-1}$$

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

RSA

$$\varphi(p^k \cdot q^l) = (p-1)p^{k-1} (q-1)q^{l-1}$$