$a \mid n$

$b \mid n$

$a \mid n_1 \wedge b \mid n_1 \Rightarrow n \mid n_1$

$13 : 2 \cdot 5 + 3$

$a = b \cdot q_1 + r_1$

$b = r_1 \cdot q_2 + r_2$

$r_1 = r_2 \cdot q_3 + r_3$

$\vdots$

$r_{n-2} = q_n \cdot r_{n-1} + r_n$

$r_{n-1} = q_{n+1} \cdot r_n + 0$

$p \mid a$

$p \mid p$

$10145 : 2274 = 4$ zb. $1064 \Rightarrow 10145 = 4 \cdot 2274 + 1064$

$2274 : 1064 = 2$ zb. $143 \Rightarrow 2274 = 2 \cdot 1064 + 143$

$1064 : 143 = 7$ zb. $66 \Rightarrow 1064 = 7 \cdot 143 + 66$

$143 : 66 = 2$ zb. $11 \Rightarrow 143 = 66 \cdot 2 + 11$

$66 : 11 = 6$ zb. $0 \Rightarrow 66 = 6 \cdot 11 + 0$

$11 = 143 - 2 \cdot 66 = 143 - 2(1064 - 7 \cdot 143) = -2 \cdot 1064 + 15 \cdot 143 = -2 \cdot 1064 + 15 \cdot (2274 - 2 \cdot 1064) =$

$-32 \cdot 1064 + 15 \cdot 2274 = -32(10145 - 4 \cdot 2274) + 15 \cdot 2274 = -32 \cdot 10145 + 143 \cdot 2274$

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

$$\varphi(n) = (p_1 - 1) p_1^{e_1 - 1} \cdot (p_2 - 1) p_2^{e_2 - 1} \ldots (p_r - 1) p_r^{e_r - 1}$$

$\varphi(n) = 6 = 2 \cdot 3$

i) $p_1 - 1 = 2$

$p_1 = 3$

$n = 3^2 = 9$

$n = 3^{e_1}$

$\Rightarrow p_1^{e_1 - 1} = 3$

$3^{e_1 - 1} = 3^1$

$e_1 - 1 = 1$

$e_1 = 2$

ii) $1 \cdot 2 \cdot 3 = 6$

$b = 18$

$(p_2 - 1) = 1$

$3 = p_2 - 1$

$p_2 = 4$ ✗

$p_1 - 1 = 6$

$p_1 = 7$

$n = 7$

$\varphi(n) = 1 \cdot 6$

$n = 2 \cdot 7 = 14$

$m = 5$

$1 \not\equiv 4 \ (5)$

$8 \equiv 23 \ (5)$ ✓

$$\left.\begin{array}{l} a \equiv b \ (m) \\ c \equiv d \ (m) \end{array}\right\} \Rightarrow a + c \equiv b + d \ (m)$$

$$\Rightarrow a \cdot c \equiv b \cdot d \ (m)$$

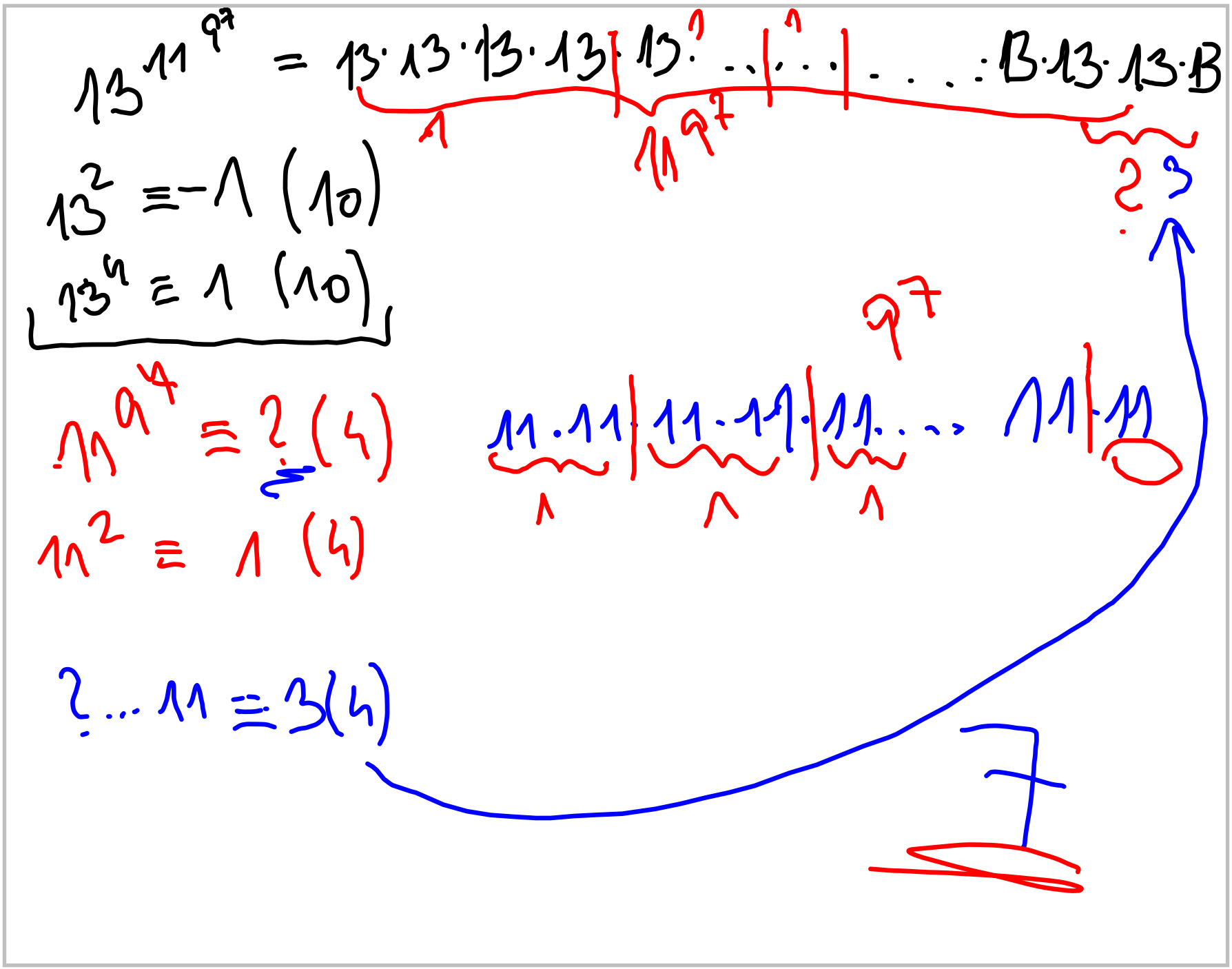
$$13^{12}+12^{11}+11^{10} \equiv 4^{12}+3^{11}+2^{10} \pmod 9$$
$$\equiv 2^{24}+3^{11}+2^{10} \pmod 9$$
$$\equiv (2^3)^8+(3^2)^5\cdot 3+(2^3)^3\cdot 2 \pmod 9$$
$$\equiv (-1)^8+0+(-1)^3\cdot 2 \pmod 9$$
$$\equiv 1+0-2 \pmod 9$$
$$\equiv -1 \pmod 9$$
$$\equiv 8 \pmod 9$$

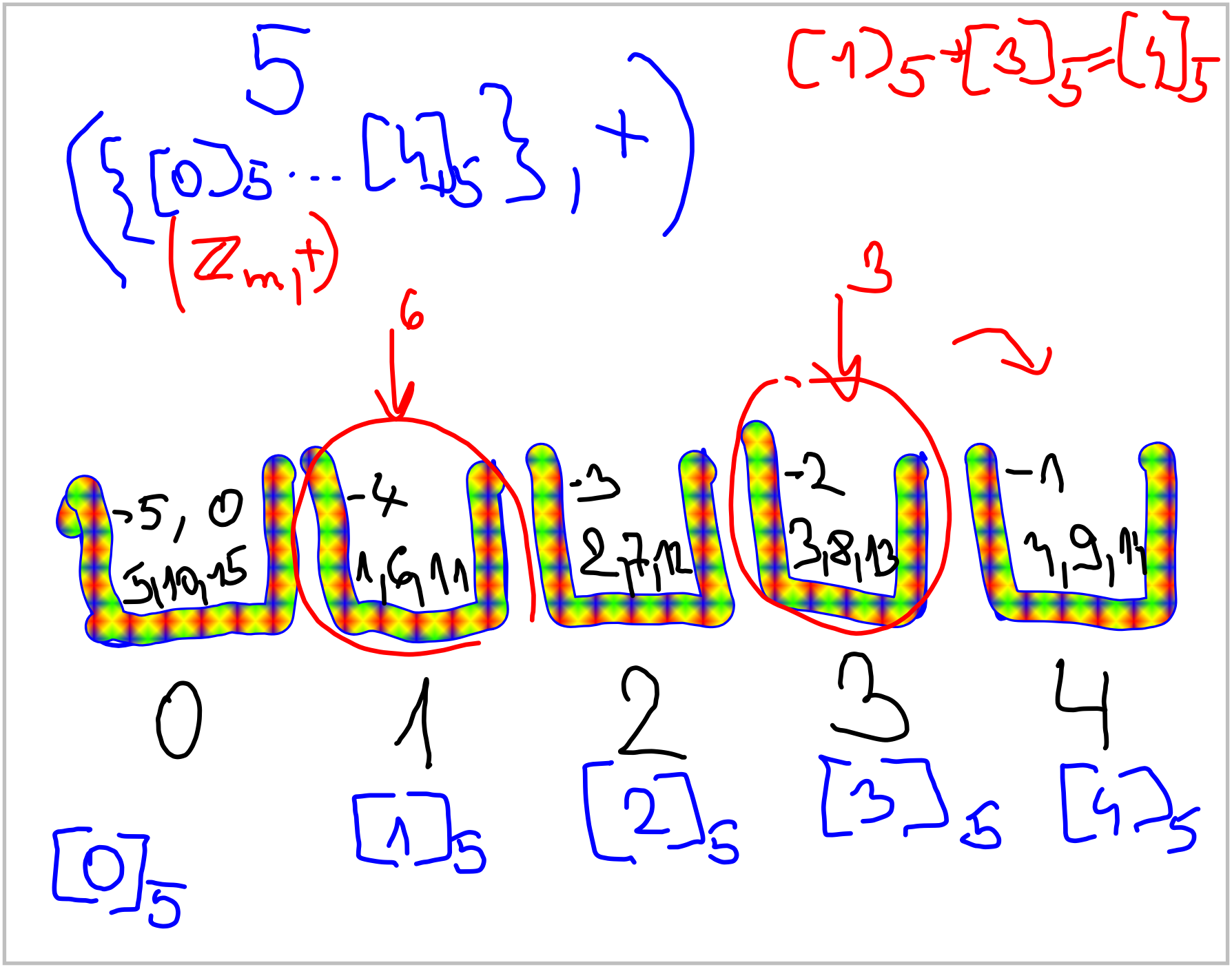
$$16^{15} + 29^{14} + 42^{13} \equiv 3^{15} + 3^{14} + 3^{13} \pmod{13}$$

$$\equiv 3^{13}(9 + 3 + 1) \pmod{13}$$

$$\equiv 3^{13} \cdot (13) \pmod{13}$$

$$\equiv 0 \pmod{13}$$


$13^{11^{9^7}} = 13 \cdot 13 \cdot 13 \cdot 13 \cdot 13^? \ldots \ldots \ldots B \cdot 13 \cdot 13 \cdot B$
11^{9^7}
2^3
$13^2 \equiv -1 \ (10)$
$13^4 \equiv 1 \ (10)$
9^7
$11^{9^4} \equiv ? \ (4)$
$11 \cdot 11 \mid 11 \cdot 11 \mid 11 \ldots 11 \mid 11$
$11^2 \equiv 1 \ (4)$
$? \ldots 11 \equiv 3 \ (4)$


$\mathbb{Z}_5$
$(\mathbb{Z}_m, +)$
$\{[0]_5 \dots [4]_5\}$
$[1]_5 + [3]_5 = [4]_5$
6
3
-5, 0
5, 10, 15
-4
1, 6, 11
-3
2, 7, 12
-2
3, 8, 13
-1
4, 9, 14
0
1
2
3
4
$[0]_5$
$[1]_5$
$[2]_5$
$[3]_5$
$[4]_5$

$(\mathbb{Z}_m, +)$ ... kom. grupa

$(\mathbb{Z}_m^*, \cdot)$ ... -"- $\Leftrightarrow$ m je prvočíslo

$$14 \cdot n \equiv 1 \pmod{181}$$

n = inverz k 14 $\sim \left(\mathbb{Z}_{181}^{*}, \cdot\right)$

$$14 \cdot n = 1 + 181 \cdot r$$

$$14n - 181r = 1$$

$181 : 14 = 10$ zb 11

$14 : 11 = 1$ zb 6

$11 : 6 = 1$ 5

$6 : 5 = 1$ 1

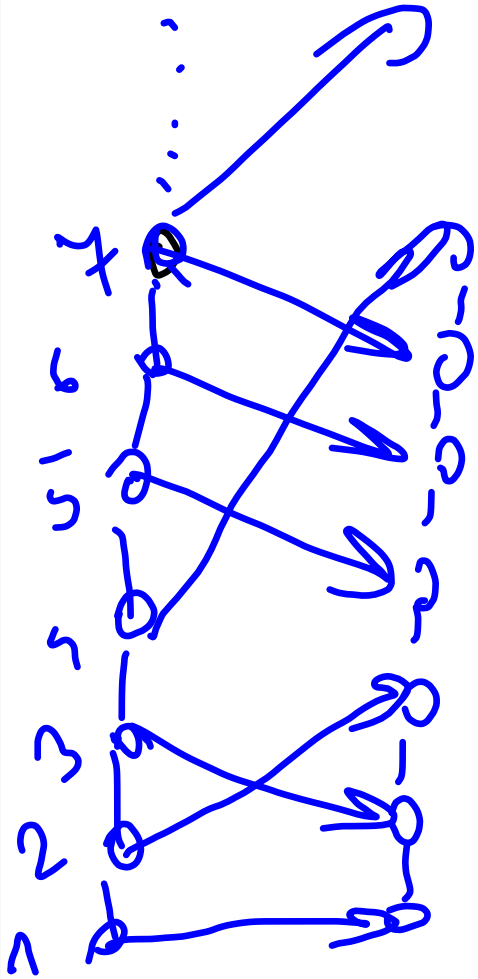
$5 : 1 = 5$ 0

$1 = 6 - 5 \cdot 1 = 6 -$

$1 \cdot (11 - 1 \cdot 6) = \ldots$

$\ldots$

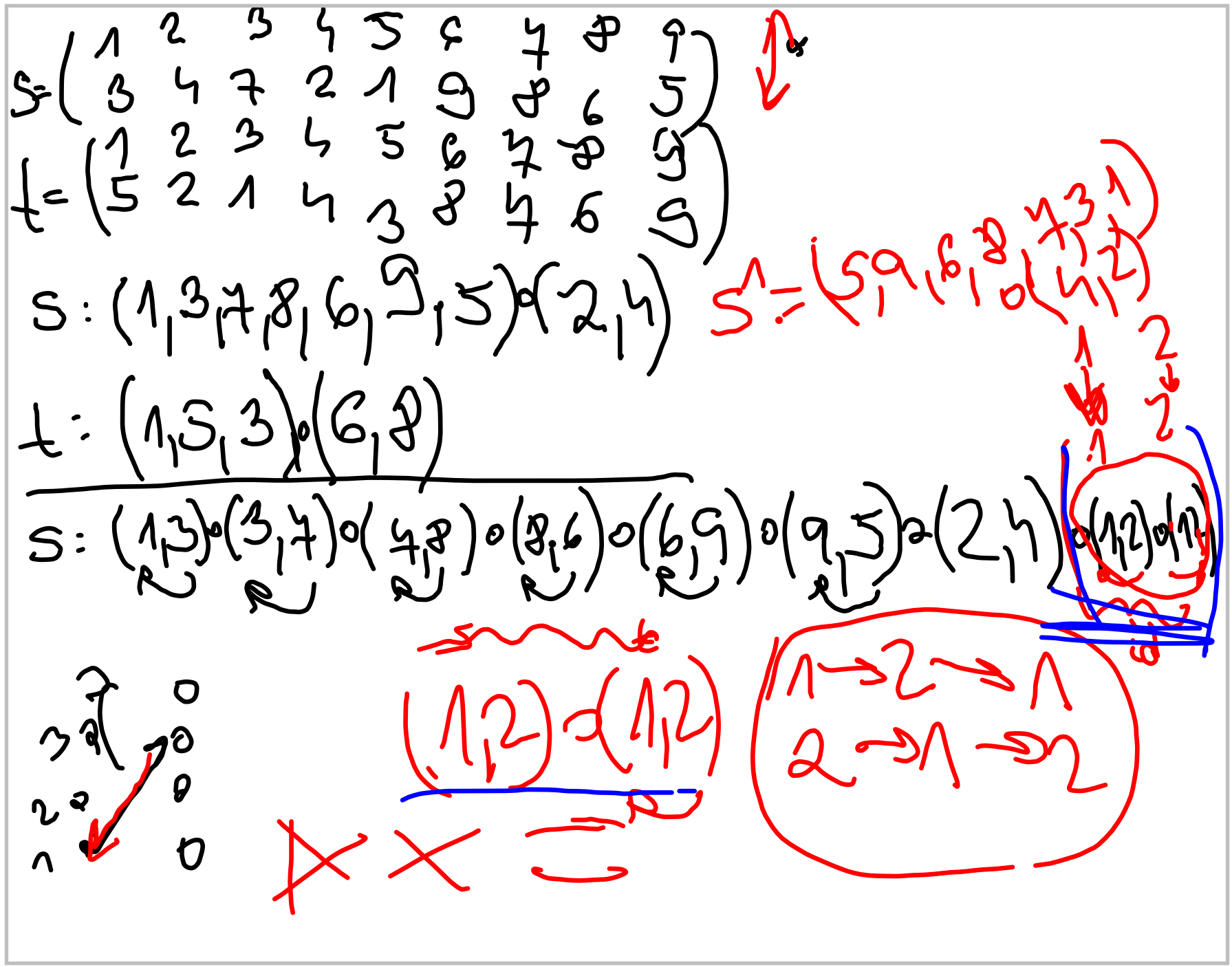
$1 = 32 \cdot 14 - 3 \cdot 181$



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$(1,2,3) \circ (4,5)$

$(1,2)(2,3)(4,5)$


s: (1,3,7,8,6,9,5)(2,4)
t: (1,5,3)(6,8)
s: (1,3)(3,7)(4,8)(8,6)(6,9)(9,5)(2,4)
(1,2)(1,2)
1→2→1
2→1→2

$$Sot = [(1,3,7,8,6,9,5)(2,4)] \circ [(1,5,3)(6,8)] = (2,4) \circ (5,7,8,9)$$

$$S^{20} = \underbrace{S \circ S \circ S \circ \dots \circ S}_{20}$$

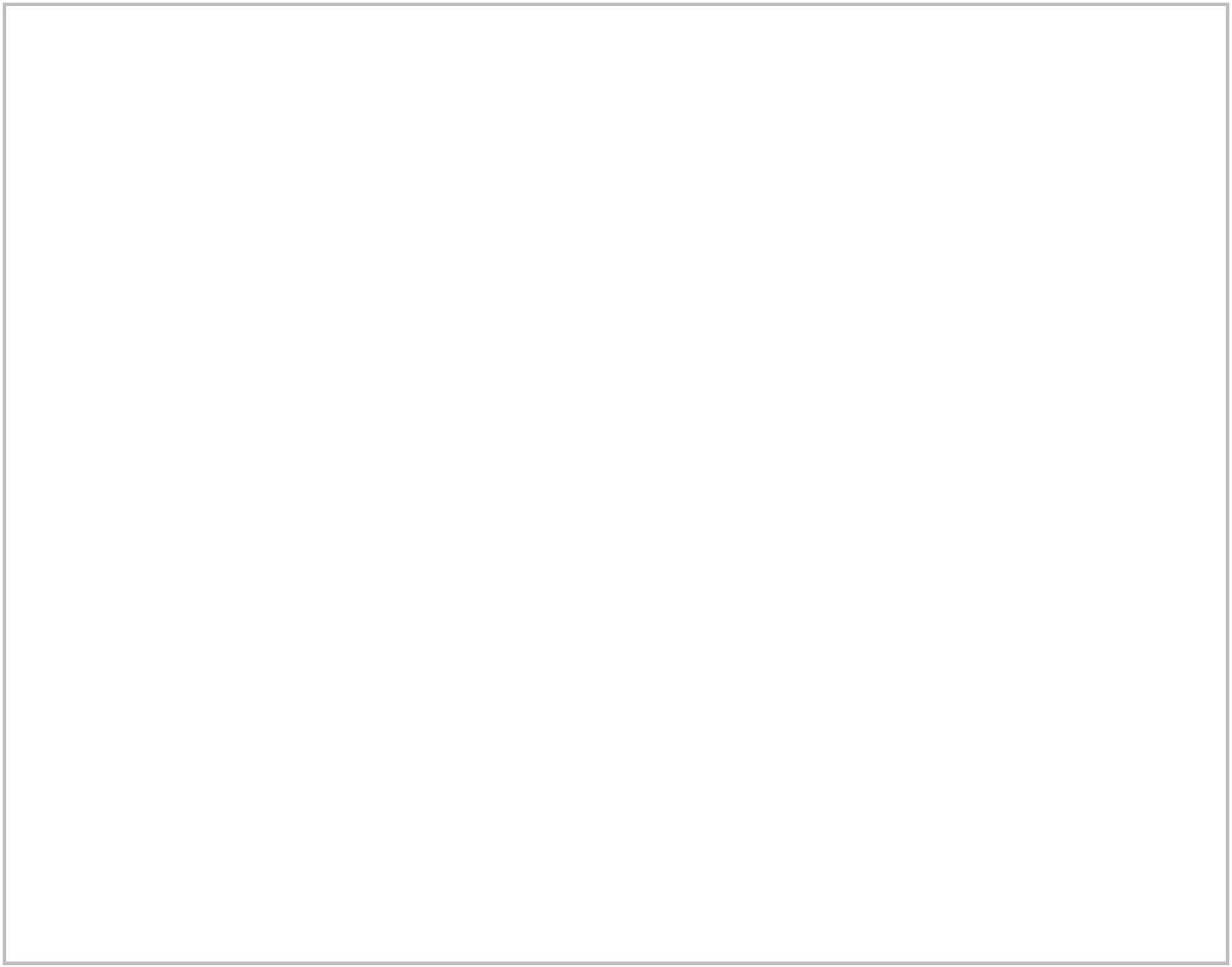
$$S = \underbrace{(1,3,7,8,6,9,5) \circ (2,4)}_{i^{14}\ id}$$

$$= i^{20} \circ (2,4)^{20} =$$

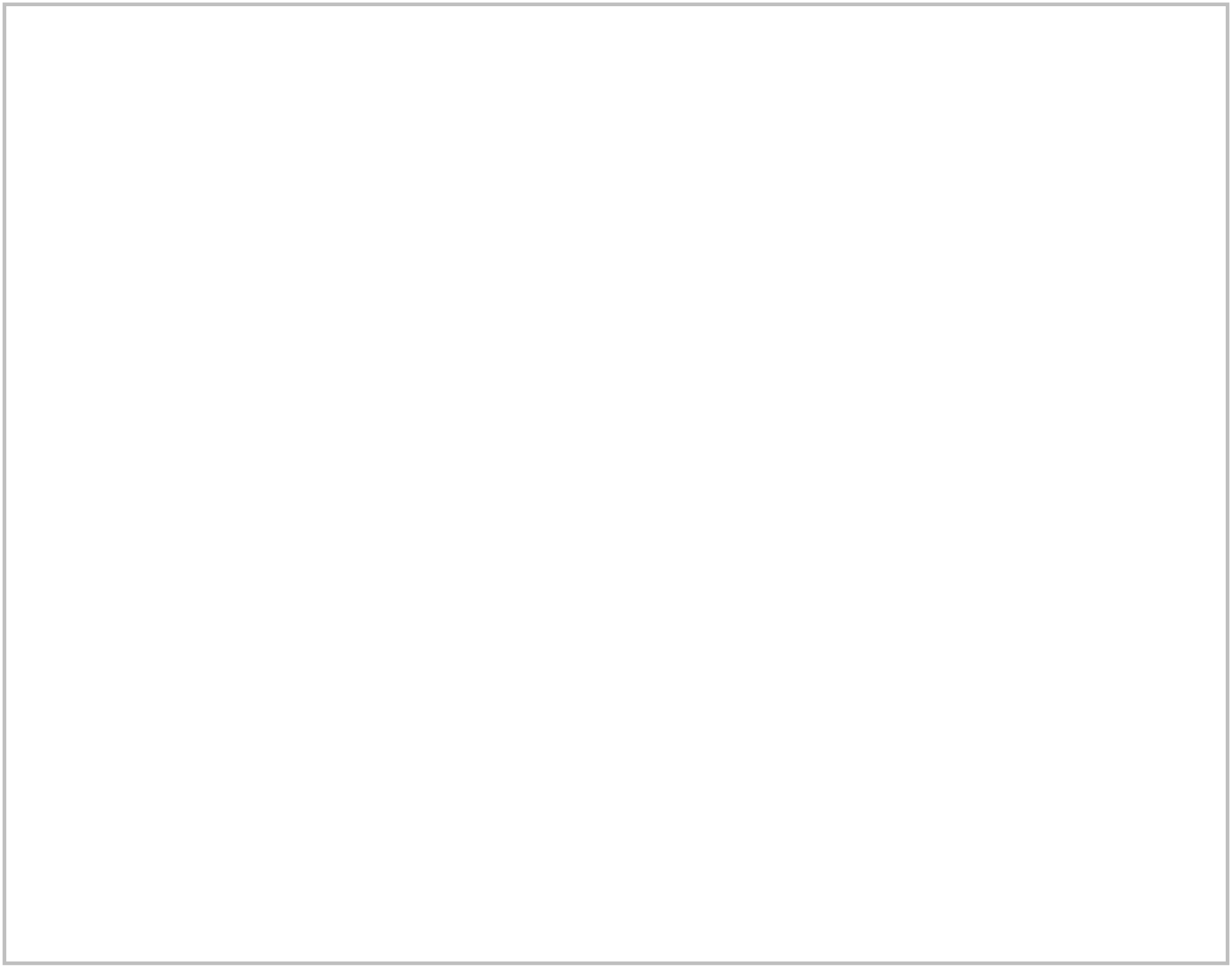
$$i^{-1} \circ [(2,4)^2]^{10}$$

$$= i^{-1} =$$

$$(5,9,6,8,7,3,1)$$



Název: II 20-9:34 (15 z 16)



Název: II 20-9:33 (16 z 16)