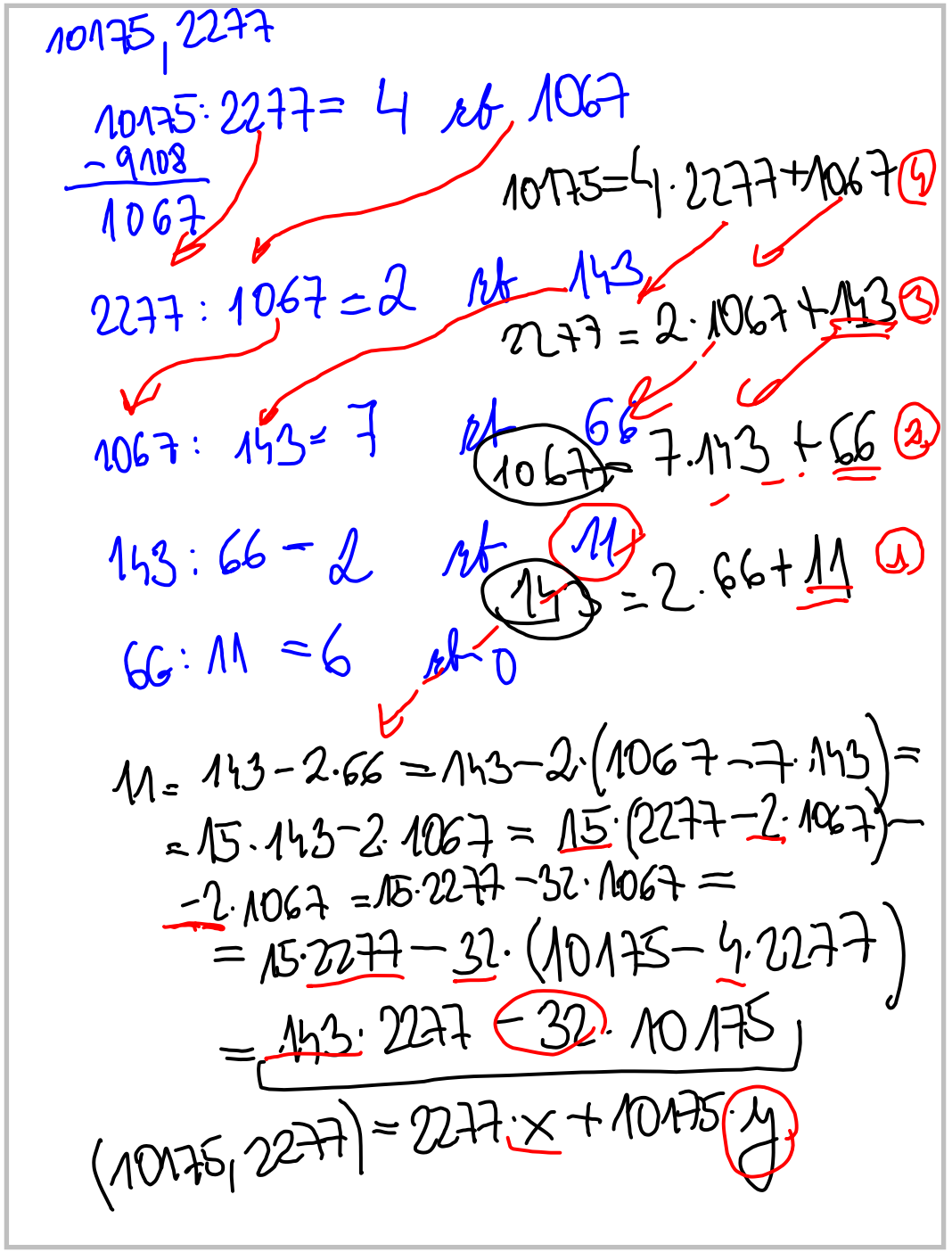

(10175, 2277)
10175 : 2277 = 4 zb 1067
−9108
1067
10175 = 4 · 2277 + 1067 (4)
2277 : 1067 = 2 zb 143
2277 = 2 · 1067 + 143 (3)
1067 : 143 = 7 zb 66
1067 = 7 · 143 + 66 (2)
143 : 66 = 2 zb 11
143 = 2 · 66 + 11 (1)
66 : 11 = 6 zb 0
11 = 143 − 2 · 66 = 143 − 2 · (1067 − 7 · 143) =
= 15 · 143 − 2 · 1067 = 15 · (2277 − 2 · 1067) −
− 2 · 1067 = 15 · 2277 − 32 · 1067 =
= 15 · 2277 − 32 · (10175 − 4 · 2277)
= 143 · 2277 − 32 · 10175
(10175, 2277) = 2277 · x + 10175 · y

$\varphi(m) = |\{a \in \mathbb{N} \mid a \leq m;\ (a,m)=1\}|$

$m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$

$\varphi(m) = (p_1-1)\cdot p_1^{\alpha_1-1} \cdot \ldots \cdot (p_k-1)\cdot p_k^{\alpha_k-1}$

$\varphi(120) = \varphi(6 \cdot 20) = \varphi(2\cdot 3 \cdot 2^2 \cdot 5) =$

$= \varphi(2^3 \cdot 3 \cdot 5) =$

$= 1 \cdot 2^2 \cdot 2 \cdot 3^0 \cdot 4 \cdot 5^0 =$

$= 32$

$\varphi(n) = 6$

$\varphi(n) = (p_1-1)p_1^{\alpha_1-1} \cdot \ldots \cdot (p_k-1)p_k^{\alpha_k-1}$

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

① $\varphi(n) = 2\cdot 3$

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

$\varphi(n) = 6$

① $\varphi(n) = 1\cdot 2\cdot 3$

$(p_1-1) = 1$

$p_1 = 2$

$n = 2\cdot m$

$\varphi(m) = 6$

$p_1 = 1$ $\quad \alpha_1 = 2$ $\quad \alpha_1 \geq 3$

$\varphi(n) = 4\cdot k$

i) $\alpha_1 = 1$

$n = 2\cdot m$; 2 tmo

$\varphi(n) = \varphi(2\cdot m) = \varphi(2)\cdot\varphi(m)$

$= \varphi(m) = 6$

$= 2\cdot 3$

$= 6$

$\varphi(m) = 2\cdot 3$

$(p_2-1) = 2$

$p_2 = 3$

$\alpha_2 = 1$ $\quad \alpha_2 = 2$ $\quad \alpha_2 \geq 3$ ×

$n = 2\cdot 3\cdot m_2$

$\varphi(n) = \varphi(2)\cdot\varphi(3)\cdot\varphi(m_2)$

$\varphi(m) = 2\cdot\varphi(m_2)$

$\varphi(m_2) = 3$ ×

$n = 2\cdot 3^2 \cdot m_3$

$\varphi(m) = 6\cdot\varphi(m_3)$

$n = 18$

$n = 2\cdot m$

$\varphi(m) = 6$

$(p_3-1) = 6$

$p_3 = 7$

$n = 2\cdot 7 = 14$

② $\varphi(n) = 2\cdot 3$

$n = 9$

③ $\varphi(n) = 6$

$n = 7$

$n \in \mathbb{N}$

$k \in \mathbb{N}$

$$\varphi(n) = \frac{n}{2}$$

$n = 2^k \cdot m$ $\quad 2 \nmid m$

$$\varphi(2^k \cdot m) = \frac{2^k m}{2}$$

$n = 2^k$

$$\varphi(2^k) \cdot \varphi(m) = 2^{k-1} \cdot m$$

$$2^{k-1} \cdot \varphi(m) = 2^{k-1} \cdot m$$

$$\varphi(m) = m$$

$m = 1$

$13^{12} + 12^{11} + 11^{10} \equiv x \quad (9)$

$13^{12} \equiv x_1 \ (9)$

$4^{12} \equiv x_1 \ (9)$

$2^{24} \equiv x_1 \ (9)$

$2^{24} \equiv 1 \ (9)$

$2^1 \equiv 2 \ (9)$

$2^2 \equiv 4 \ (9)$

$2^3 \equiv -1 \ (9)$

$2^6 \equiv 1 \ (9)$

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 \cdot 2 \cdot 2 \cdot 2$

$1 \ (9)$

$12^{11} \equiv x_2 \ (9)$

$3^{11} \equiv x_2 \ (9)$

$3^{11} \equiv 0 \ (9)$

$3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot \ldots \cdot 3$

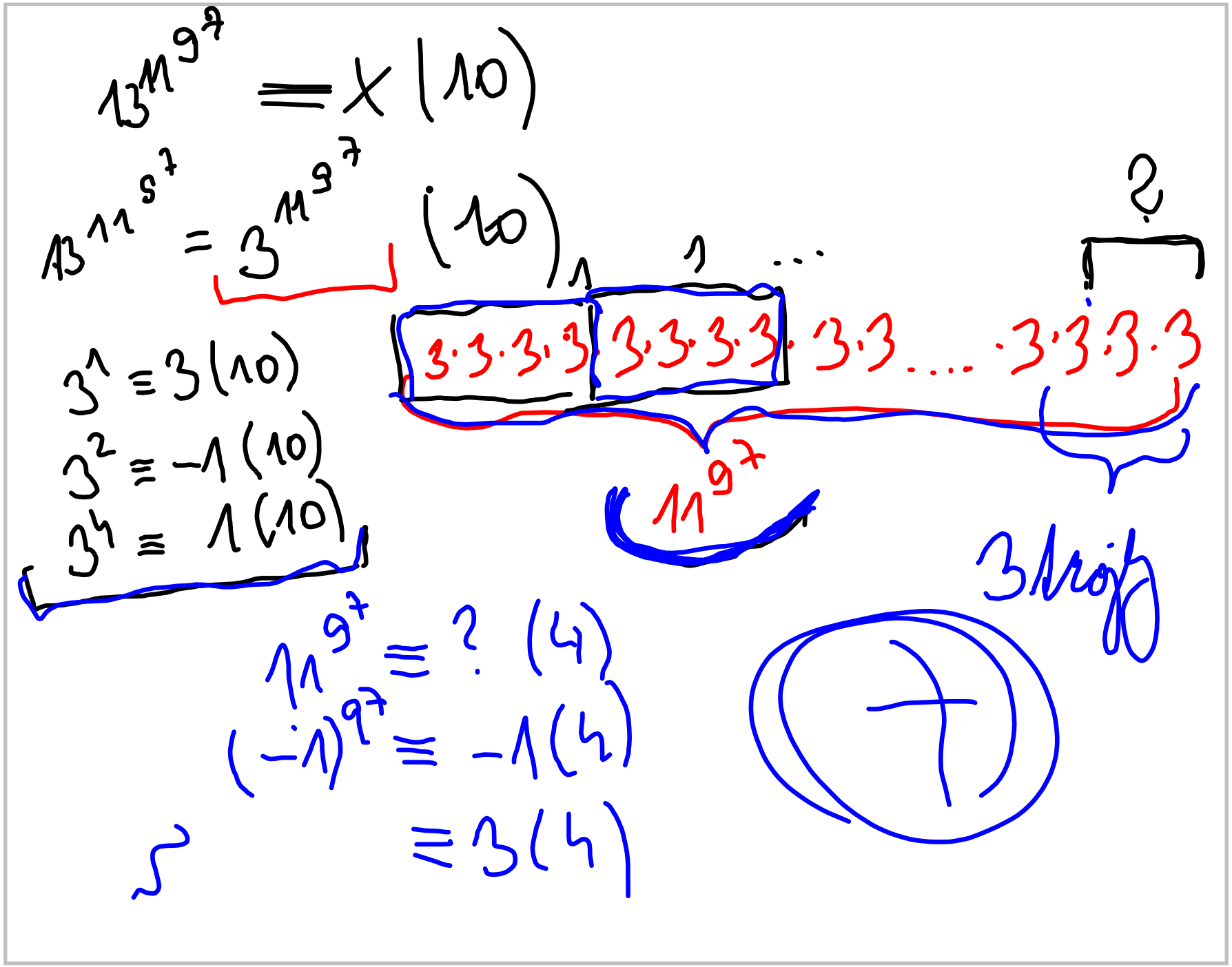
$11^{10} \equiv x_3 \ (9)$

$1^{10} \equiv x_3 \ (9)$

$2^6 \cdot 2^n \equiv 2^4 \equiv 7 \ (9)$

1

8


$13^{11^{9^7}} \equiv x \ (10)$
$13^{11^{9^7}} = 3^{11^{9^7}} \ (10)$
$3^1 \equiv 3 \ (10)$
$3^2 \equiv -1 \ (10)$
$3^4 \equiv 1 \ (10)$
1
1
...
?
3·3·3·3
3·3·3·3
3·3 .... ·3·3·3·3
11^{9^7}
3 kroky
$11^{9^7} \equiv ? \ (4)$
$(-1)^{9^7} \equiv -1 \ (4)$
$\equiv 3 \ (4)$

$16^{15}+29^{14}+42^{13} \equiv x \ (13)$

$a^{p-1} \equiv 1 \ (p)$

$16^{15} \equiv 3^{15} \equiv 3^{12} \cdot 3^3 \equiv 27 \equiv 1 \ (13)$

$29^{14} \equiv 3^{14} \equiv 3^{12} \cdot 3^2 \equiv 9 \ (13)$

$42^{13} \equiv 3^{13} \equiv 3^{12} \cdot 3 \equiv 3 \ (13)$

$x \equiv 1+9+3 \equiv 13 \equiv 0 \ (13)$

$a \equiv b \ (13) \Rightarrow 13 \mid (a-b)$

$17 \cdot n \equiv 1 \ (181)$

$[17]^{-1}_{181}$

$\mathbb{Z}^{\times}_{181}$

$n \equiv 17^{-1} \ (181)$

$[17]^{-1}_{181}$

$An \equiv 1 \ (181)$

$17n = 1 - 181x$

$17n + 181x = 1$

$(17, 181)$

$181 : 17 = 10 \ z \ 11 \qquad 181 = 10 \cdot 17 + 11$

$17 : 11 = 1 \ z \ 6 \qquad 17 = 1 \cdot 11 + 6$

$11 : 6 = 1 \ z \ 5 \qquad 11 = 1 \cdot 6 + 5$

$6 : 5 = 1 \ z \ 1 \qquad 6 = 1 \cdot 5 + 1$

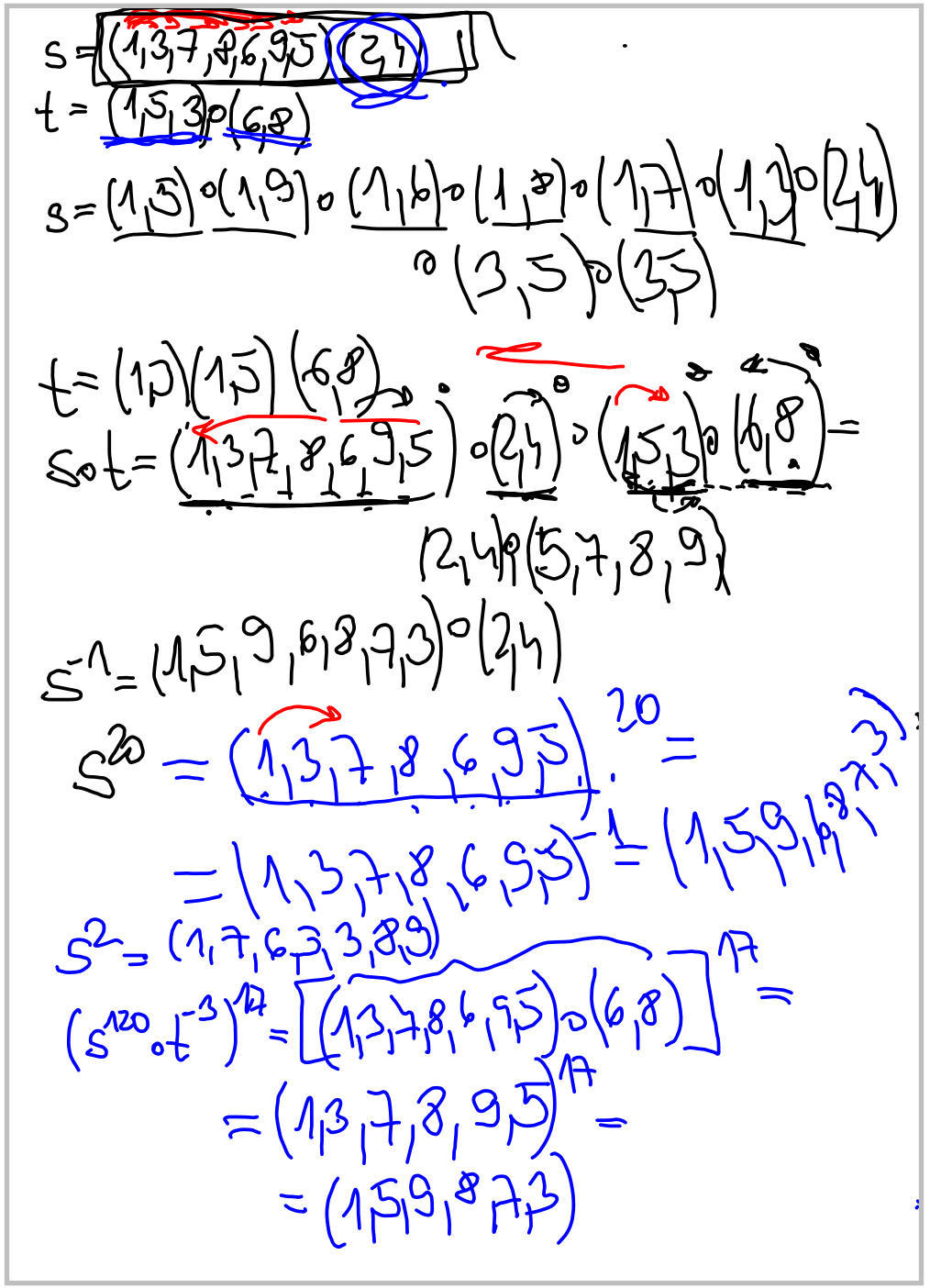
$5 : 1 = 5 \ z \ 0$

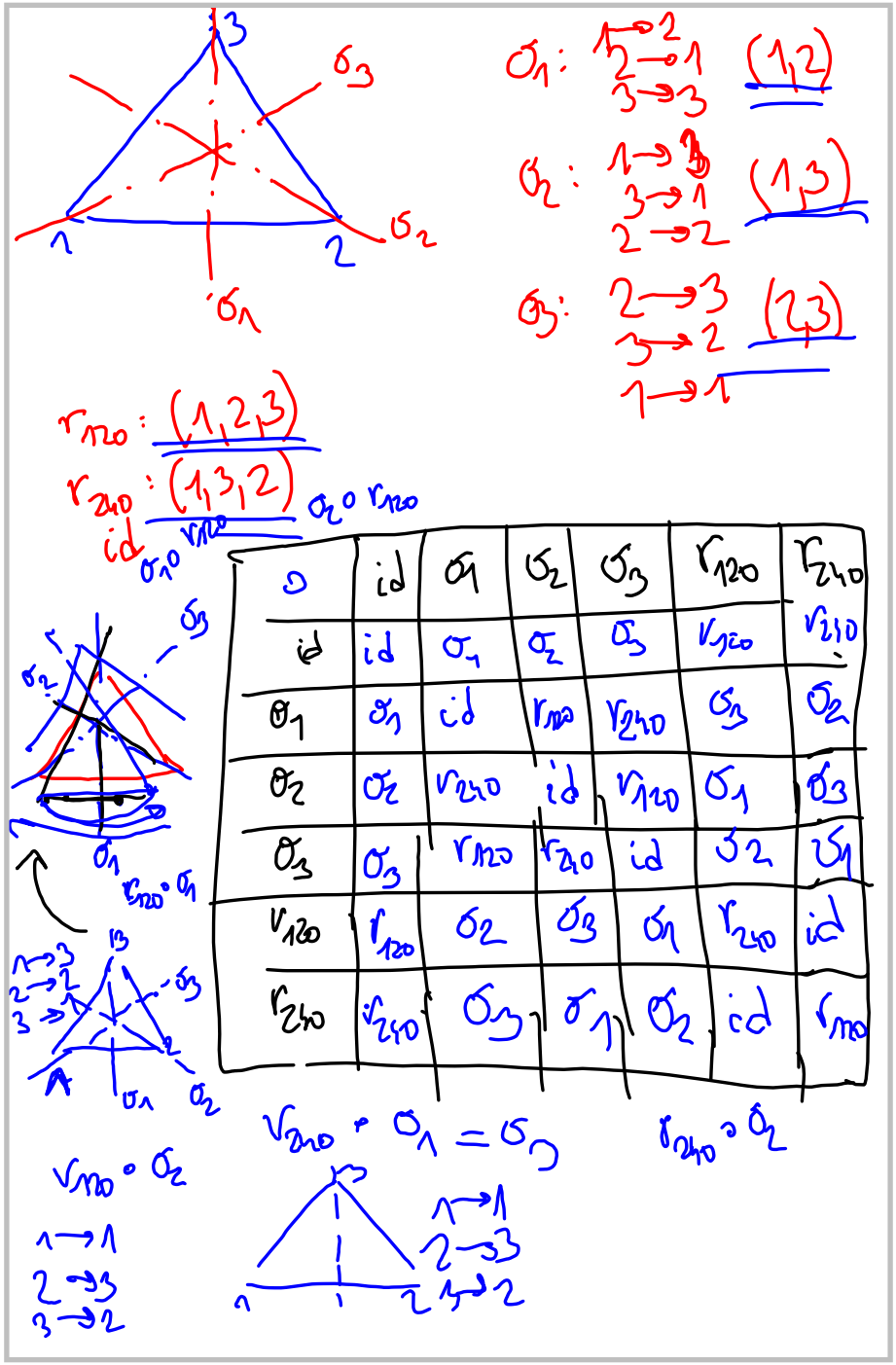
$1 = 6 - 1 \cdot 5 = 6 - (11 - 1 \cdot 6) = 2 \cdot 6 - 11 =$

$= 2 \cdot (17 - 1 \cdot 11) - 11 = -3 \cdot 11 + 2 \cdot 17 =$

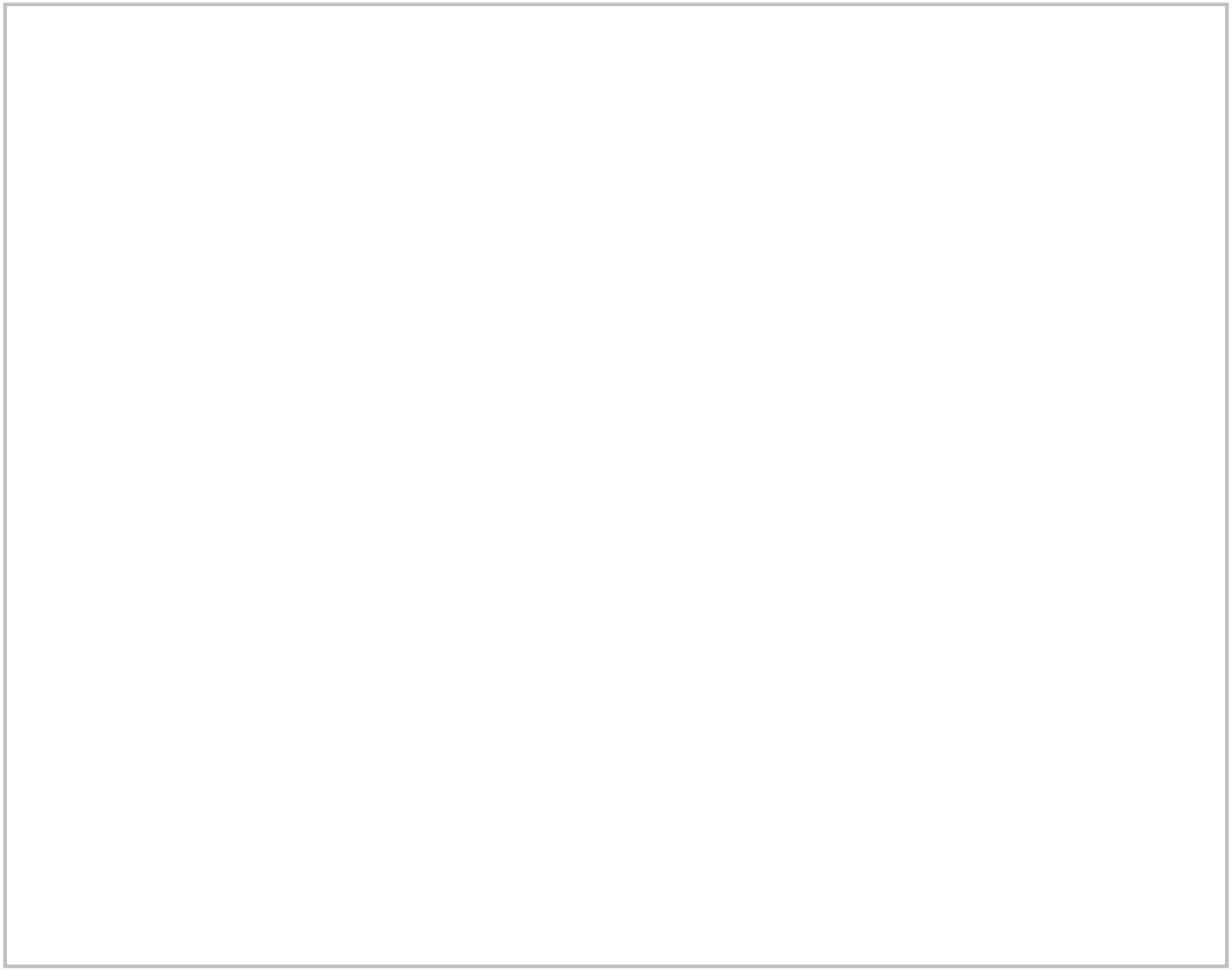
$= -3(181 - 10 \cdot 17) + 2 \cdot 17 = 32 \cdot 17 - 3 \cdot 181$

$n = 32 \ (181) \qquad 32_{181} = [17]^{-1}_{181}$


s = (1,3,7,8,6,9,5)(2,4)
t = (1,5,3)o(6,8)
s = (1,5)o(1,9)o(1,6)o(1,8)o(1,7)o(1,3)o(2,4)
o(3,5)o(3,5)
t = (1,3)(1,5)(6,8)
s∘t = (1,3,7,8,6,9,5)o(2,4)o(1,5,3)o(6,8) =
(2,4)o(5,7,8,9)
s^-1 = (1,5,9,6,8,7,3)o(2,4)
s^20 = (1,3,7,8,6,9,5)^20 =
= (1,3,7,8,6,9,5)^-1 = (1,5,9,6,8,7,3)
s^2 = (1,7,6,3,3,8,9)
(s^120 ∘ t^-3)^17 = [(1,3,7,8,6,9,5)o(6,8)]^17 =
= (1,3,7,8,9,5)^17 =
= (1,5,9,8,7,3)



∘	id	σ_1	σ_2	σ_3	r_{120}	r_{240}
id	id	σ_1	σ_2	σ_3	r_{120}	r_{240}
σ_1	σ_1	id	r_{120}	r_{240}	σ_3	σ_2
σ_2	σ_2	r_{240}	id	r_{120}	σ_1	σ_3
σ_3	σ_3	r_{120}	r_{240}	id	σ_2	σ_1
r_{120}	r_{120}	σ_2	σ_3	σ_1	r_{240}	id
r_{240}	r_{240}	σ_3	σ_1	σ_2	id	r_{120}



Název: III 3-13:21 (10 z 10)