Zadanie 1(a)

a	b	r	q	k	l
				1	0
21	55	21	0	0	1
55	21	13	2	1	0
21	13	8	1	-2	1
13	8	5	1	3	-1
8	5	3	1	-5	2
5	3	2	1	8	-3
3	2	1	1	-13	5
2	1	0	2	$\boxed{21}$	$\boxed{-8}$
1	0				

$$\mathrm{NWD}(21, 55) = 1 = 21 \cdot 21 + (-8) \cdot 55.$$

Zadanie 1(b)

a	b	r	q	k	l
				1	0
15	303	15	0	0	1
303	15	3	20	1	0
15	3	0	5	$\boxed{-20}$	$\boxed{1}$
3	0				

$$\mathrm{NWD}(15, 303) = 3 = (-20) \cdot 15 + 1 \cdot 303.$$

Zadanie 1(c)

a	b	r	q	k	l
				1	0
303	159	144	1	0	1
159	144	15	1	1	-1
144	15	9	9	-1	2
15	9	6	1	10	-19
9	6	3	1	-11	21
6	3	0	2	$\boxed{21}$	$\boxed{-40}$
3	0				

$$\mathrm{NWD}(303, 159) = 3 = 21 \cdot 303 + (-40) \cdot 159.$$

Zadanie 1(d)

a	b	r	q	k	l
				1	0
77	371	77	0	0	1
371	77	63	4	1	0
77	63	14	1	-4	1
63	14	7	4	5	-1
14	7	0	2	$\boxed{-24}$	$\boxed{5}$
7	0				

$$\mathrm{NWD}(77, 371) = 7 = (-24) \cdot 77 + 5 \cdot 371.$$

Zadanie 1(e)

a	b	r	q	k	l
				1	0
183	305	183	0	0	1
305	183	122	1	1	0
183	122	61	1	-1	1
122	61	0	2	$\boxed{2}$	$\boxed{-1}$
61	0				

$$\mathrm{NWD}(183, 305) = 61 = 2 \cdot 183 + (-1) \cdot 305.$$

Zadanie 2

Zadanie

Udowodnić, że jeśli a, b i c są liczbami całkowitymi takimi, że $b \mid a - c$, to $\gcd(a, b) = \gcd(b, c)$.

Rozwiązanie

Wystarczy pokazać, że $d \mid a, b$ wtedy i tylko wtedy, gdy $d \mid b, c$.

Przez symetrię wystarczy pokazać, że jeśli $d \mid a, b$, to $d \mid c$.

Ponieważ $d \mid b$, więc z przechodniości relacji podzielności $d \mid a - c$.

Stąd $d \mid a - (a - c) = c$ (na mocy faktów 1.7 i 1.8 z wykładu). $\square$

Zadanie 3

Zadanie

Udowodnić, że $\gcd(m \cdot a, m \cdot b) = m \cdot \gcd(a, b)$ dla dowolnej liczby naturalnej m oraz dowolnych liczb całkowitych a i b.

Rozwiązanie

Jeśli $m = 0$, to teza jest oczywista, więc zakładamy, że $m > 0$.

Niech $d := \gcd(a, b)$ i $d' := \gcd(m \cdot a, m \cdot b)$.

Ponieważ $m \cdot d, d' \geq 0$, więc wystarczy pokazać, że $m \cdot d \mid d'$ i $d' \mid m \cdot d$.

Ponieważ $d \mid a, b$, więc $m \cdot d \mid m \cdot a, m \cdot b$, zatem $m \cdot d \mid \gcd(m \cdot a, m \cdot b) = d'$ z definicji największego wspólnego dzielnika.

Z drugiej strony, $m \mid m \cdot a, m \cdot b$, więc podobnie jak wcześniej $m \mid d'$, a więc $d' = m \cdot d''$.

Wtedy $m \cdot d'' \mid m \cdot a, m \cdot b$, więc $d'' \mid a, b$ (gdyż $m \neq 0$).

Stąd $d'' \mid \gcd(a, b) = d$, więc $d' = m \cdot d'' \mid m \cdot d$. $\square$