Zadanie 1

Zadanie

Udowodnić, że jeśli n jest liczbą całkowitą taką, że $3 \nmid n$, to $3 \mid n^4 + n^2 + 1$.

Rozwiązanie

Pokażemy najpierw, że jeśli $3 \nmid n$, to $n^2 \equiv 1 \pmod 3$.

Istotnie, jeśli $3 \nmid n$, to $n \equiv 1 \pmod 3$ lub $n \equiv 2 \pmod 3$.

Jeśli $n \equiv 1 \pmod 3$, to $n^2 \equiv 1^2 = 1 \pmod 3$.

Podobnie, gdy $n \equiv 2 \pmod 3$, to $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Ponieważ $n^2 \equiv 1 \pmod 3$, więc $n^4 = (n^2)^2 \equiv 1^2 = 1 \pmod 3$.

Ostatecznie,

$$n^4 + n^2 + 1 \equiv 1 + 1 + 1 = 3 \equiv 0 \pmod 3,$$

tzn. $3 \mid n^4 + n^2 + 1$.

Zadanie

Rozwiązać kongruencję $3x \equiv 4 \pmod 7$.

Rozwiązanie

1. Stosujemy algorytm Euklidesa dla 7 i 3:

a	b	r	q	k	l
				1	0
7	3	1	2	0	1
3	1	0	3	1	-2
1	0				

3. Ponieważ $1 \mid 4$, więc musimy rozwiązać kongruencję

$$3x \equiv 4 \pmod 7.$$

4. Mnożąc powyższą kongruencję stronami przez -2, otrzymujemy kongruencję

$$x \equiv -8 \pmod 7.$$

5. Ponieważ $-8 \bmod 7 = 6$, więc odpowiedzią jest: $x \equiv 6 \pmod 7$.

Zadanie 7 (2)

Zadanie

Rozwiązać kongruencję $27x \equiv 25 \pmod{256}$.

Rozwiązanie

1. Stosujemy algorytm Euklidesa dla 256 i 27:

a	b	r	q	k	l
				1	0
256	27	13	9	0	1
27	13	1	2	1	-9
13	1	0	13	-2	19
1	0				

3. Ponieważ $1 \mid 25$, więc musimy rozwiązać kongruencję

$$27x \equiv 25 \pmod{256}.$$

4. Mnożąc powyższą kongruencję stronami przez 19, otrzymujemy kongruencję

$$x \equiv 475 \pmod{256}.$$

5. Ponieważ $475 \bmod 256 = 219$, więc odpowiedzią jest: $x \equiv 219 \pmod{256}$.

Zadanie

Rozwiązać kongruencję $2x \equiv 37 \pmod{21}$.

Rozwiązanie

1. Stosujemy algorytm Euklidesa dla 21 i 2:

a	b	r	q	k	l
				1	0
21	2	1	10	0	1
2	1	0	2	1	-10
1	0				

3. Ponieważ $1 \mid 37$, więc musimy rozwiązać kongruencję
$$2x \equiv 37 \pmod{21}.$$
4. Mnożąc powyższą kongruencję stronami przez -10, otrzymujemy kongruencję
$$x \equiv -370 \pmod{21}.$$
5. Ponieważ $-370 \bmod 21 = 8$, więc odpowiedzią jest: $x \equiv 8 \pmod{21}$.

Zadanie

Rozwiązać kongruencję $10x \equiv 15 \pmod{35}$.

Rozwiązanie

1. Stosujemy algorytm Euklidesa dla 35 i 10:

a	b	r	q	k	l
				1	0
35	10	5	3	0	1
10	5	0	2	1	-3
5	0				

3. Ponieważ $5 \mid 15$, więc musimy rozwiązać kongruencję

$$2x \equiv 3 \pmod{7}.$$

4. Mnożąc powyższą kongruencję stronami przez -3, otrzymujemy kongruencję

$$x \equiv -9 \pmod{7}.$$

5. Ponieważ $-9 \bmod 7 = 5$, więc odpowiedzią jest: $x \equiv 5 \pmod{7}$.

Zadanie 7 (5)

Zadanie

Rozwiązać kongruencję $3x \equiv 7 \pmod{18}$.

Rozwiązanie

1. Stosujemy algorytm Euklidesa dla 18 i 3:

a	b	r	q	k	l
				1	0
18	3	0	6	$\boxed{0}$	$\boxed{1}$
$\boxed{3}$	0				

2. Ponieważ $3 \nmid 7$, więc odpowiedzią jest: $x \in \varnothing$.

Zadanie

Rozwiązać układ kongruencji: $x \equiv 3 \pmod 4$, $x \equiv 2 \pmod 7$, $x \equiv 1 \pmod 9$.

Rozwiązanie (Metoda III)

1. Musimy rozwiązać układ kongruencji

$$x \equiv 3 \pmod 4, \qquad x \equiv 2 \pmod 7, \qquad x \equiv 1 \pmod 9.$$

2. Mamy $n = 4 \cdot 7 \cdot 9 = 252$ oraz

$$n_1 := 7 \cdot 9 = 63, \qquad n_2 := 4 \cdot 9 := 36, \qquad n_3 := 4 \cdot 7 = 28.$$

3. Stosujemy rozszerzony algorytm Euklidesa dla par $(63, 4)$, $(36, 7)$ i $(28, 9)$:

a	b	r	q	k	l
				1	0
63	4	3	15	0	1
4	3	1	1	1	-15
3	1	0	6	-1	16
1	0				

a	b	r	q	k	l
				1	0
36	7	1	5	0	1
7	1	0	7	1	-5
1	0				

Rozwiązanie (c.d.)

1. Musimy rozwiązać układ kongruencji

$$x \equiv 3 \pmod 4, \qquad x \equiv 2 \pmod 7, \qquad x \equiv 1 \pmod 9.$$

2. Mamy $n = 4 \cdot 7 \cdot 9 = 252$ oraz

$$n_1 := 7 \cdot 9 = 63, \qquad n_2 := 4 \cdot 9 := 36, \qquad n_3 := 4 \cdot 7 = 28.$$

3. Stosujemy rozszerzony algorytm Euklidesa dla par $(63, 4)$, $(36, 7)$ i $(28, 9)$:

$$1 = (-1) \cdot 63 + 16 \cdot 4 \qquad \text{i} \qquad 1 = 1 \cdot 36 + (-5) \cdot 7.$$

a	b	r	q	k	l
				1	0
28	9	1	3	0	1
9	1	0	9	1	-3
1	0				

4. Ponieważ

$$(3 \cdot (-1) \cdot 63 + 2 \cdot 1 \cdot 36 + 1 \cdot 1 \cdot 28) \bmod 252 = 163,$$

więc odpowiedzią jest: $x \equiv 163 \pmod{252}$.

Zadanie

Rozwiązać układ kongruencji: $x \equiv 20 \pmod{33}$, $x \equiv 33 \pmod{40}$.

Rozwiązanie (Metoda II)

1. Musimy rozwiązać układ kongruencji

$$x \equiv 20 \pmod{33}, \qquad x \equiv 33 \pmod{40}.$$

2. Stosujemy rozszerzony algorytm Euklidesa dla pary $(33, 40)$:

a	b	r	q	k	l
				1	0
33	40	33	0	0	1
40	33	7	1	1	0
33	7	5	4	-1	1
7	5	2	1	5	-4
5	2	1	2	-6	5
2	1	0	2	17	-14
1	0				

3. Ponieważ $33 \cdot 44 = 1320$ i

$$(20 \cdot (-14) \cdot 40 + 33 \cdot 17 \cdot 33) \bmod 1320 = 713,$$

więc odpowiedzią jest: $x \equiv 713 \pmod{1320}$.

Zadanie

Rozwiązać układ kongruencji: $x \equiv 4 \pmod 9$, $62x \equiv 102 \pmod{154}$.

Rozwiązanie (Metoda II)

1. Posługując się metodą z Zadania 7, otrzymujemy, że rozwiązanie kongruencji $62x \equiv 102 \pmod{154}$, jest postaci $x \equiv 24 \pmod{77}$.

   Zatem musimy rozwiązać układ kongruencji

   $$x \equiv 4 \pmod 9, \qquad x \equiv 24 \pmod{77}.$$

2. Stosujemy rozszerzony algorytm Euklidesa dla pary $(9, 77)$:

a	b	r	q	k	l
				1	0
9	77	9	0	0	1
77	9	5	8	1	0
9	5	4	1	-8	1
5	4	1	1	9	-1
4	1	0	4	-17	2
1	0				

3. Ponieważ $9 \cdot 77 = 693$ i

   $$(4 \cdot 2 \cdot 77 + 24 \cdot (-17) \cdot 9) \bmod 1320 = 409,$$

   więc odpowiedzią jest: $x \equiv 409 \pmod{693}$.

Zadanie

Rozwiązać układ kongruencji: $2x \equiv 1 \pmod 3$, $3x \equiv 1 \pmod 4$, $5x \equiv 4 \pmod 7$.

Rozwiązanie (Metoda I)

1. Mamy $n = 3 \cdot 4 \cdot 7 = 84$ oraz
$$n_1 := 4 \cdot 7 = 28, \qquad n_2 := 3 \cdot 7 := 21, \qquad n_3 := 3 \cdot 4 = 12.$$
2. Mnożąc współczynniki wyjściowych kongruencji przez 28, 21 i 12, odpowiednio, otrzymujemy
$$56x \equiv 28 \pmod{84}, \quad 63x \equiv 21 \pmod{84}, \quad 60x \equiv 48 \pmod{84}.$$
Dodając powyższe kongruencje stronami, dostajemy kongruencję
$$179x \equiv 97 \pmod{84}.$$
Ponieważ
$$179 \bmod 84 = 9 \qquad \text{i} \qquad 97 \bmod 84 = 13,$$
więc powyższą kongruencję możemy zastąpić kongruencją
$$11x \equiv 13 \pmod{84}.$$
3. Rozwiązując powyższą kongruencję metodą z Zadania 7, otrzymujemy odpowiedź:
$$x \equiv 47 \pmod{84}.$$