**Definicja**

Niech $m \in \mathbb{N}_+$ oraz $a, b \in \mathbb{Z}$.
Mówimy, że $a$ przystaje do $b$ modulo $m$ (i piszemy $a \equiv b \pmod{m}$ lub $a \equiv_m b$), jeśli $m \mid a - b$.
Równoważnie, $a \equiv b \pmod{m}$ wtedy tylko wtedy, gdy $a \bmod m = b \bmod m$.

**Przykłady**

- $-1 \equiv 11 \pmod{4}$.
- $3 \not\equiv 5 \pmod{4}$.

**Własności**

- Kongruencja jest relacją równoważności.
- Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to

$$a \pm c \equiv b \pm d \pmod{m} \qquad \text{oraz} \qquad a \cdot c \equiv b \cdot d \pmod{m}.$$

**Problem**

Dla danych liczb $m \in \mathbb{N}_+$ oraz $a, b \in \mathbb{Z}$ znaleźć wszystkie liczby $x \in \mathbb{Z}$ takie, że $a \cdot x \equiv b \pmod{m}$.

**Metoda**

1. Wykorzystując rozszerzony algorytm Euklidesa, znajdujemy liczby $d \in \mathbb{N}_+$ oraz $k, l \in \mathbb{Z}$ takie, że
$$d = \mathrm{NWD}(m, a) \qquad \text{i} \qquad d = k \cdot m + l \cdot a.$$
2. Jeśli $d \nmid b$, to kończymy rozwiązanie.

   Odpowiedzią jest: $x \in \varnothing$.
3. Jeśli $d \mid b$, to „zastępujemy" (o ile $d \neq 1$) kongruencję $a \cdot x \equiv b \pmod{m}$ kongruencją $a' \cdot x \equiv b' \pmod{m'}$, gdzie
$$a' := \tfrac{a}{d}, \qquad b' := \tfrac{b}{d}, \qquad m' := \tfrac{m}{d}.$$
4. Mnożąc kongruencję $a' \cdot x \equiv b' \pmod{m'}$ stronami przez $l$, otrzymujemy kongruencję $x \equiv l \cdot b' \pmod{m'}$.
5. Jeśli $r := (l \cdot b') \bmod m'$, to odpowiedzią jest: $x \equiv r \pmod{m'}$.

# Rozwiązywanie kongruencji – przykład

**Zadanie**

Znaleźć wszystkie liczby $x \in \mathbb{Z}$ takie, że $8x \equiv 12 \pmod{22}$.

Rozwiązanie

1. Stosujemy rozszerzony algorytm Euklidesa dla 22 i 8:

| $a$ | $b$ | $r$ | $q$ | $k$ | $l$ |
|---|---|---|---|---|---|
| | | | | 1 | 0 |
| 22 | 8 | 6 | 2 | 0 | 1 |
| 8 | 6 | 2 | 1 | 1 | -2 |
| 6 | 2 | 0 | 3 | -1 | 3 |
| 2 | 0 | | | | |

3. Ponieważ $2 \mid 12$, więc musimy rozwiązać kongruencję

$$4x \equiv 6 \pmod{11}.$$

4. Mnożąc powyższą kongruencję stronami przez 3, otrzymujemy kongruencję

$$x \equiv 18 \pmod{11}.$$

5. Ponieważ $18 \bmod 11 = 7$, więc odpowiedzią jest: $x \equiv 7 \pmod{11}$.

# Rozwiązywanie układów kongruencji - Metoda I

**Problem**

Dla danych liczb $a_1, b_1, \ldots, a_k, b_k \in \mathbb{Z}$ oraz $m_1, \ldots, m_k \in \mathbb{N}_+$ takich, że $\mathrm{NWD}(m_i, m_j) = 1$ dla $i \neq j$, znaleźć wszystkie liczby $x \in \mathbb{Z}$ takie, że $a_i \cdot x \equiv b_i \pmod{m_i}$, dla każdego $i = 1, \ldots, k$.

**Metoda I**

1. Niech $n := m_1 \cdots m_k$ oraz
$$n_1 := m_2 \cdots m_k, \qquad n_2 := m_1 \cdot m_3 \cdots m_k, \qquad \ldots, \qquad n_k := m_1 \cdots m_{k-1}.$$
2. Zastępujemy kongruencje
$$a_1 \cdot x \equiv b_1 \pmod{m_1}, \qquad a_2 \cdot x \equiv b_2 \pmod{m_2}, \qquad \ldots, \qquad a_k \cdot x \equiv b_k \pmod{m_k},$$
kongurencjami
$$n_1 a_1 \cdot x \equiv n_1 b_1 \pmod{n}, \quad n_2 a_2 \cdot x \equiv n_2 b_2 \pmod{n}, \quad \ldots, \quad n_k a_k \cdot x \equiv n_k b_k \pmod{n}.$$
Dodając stronami powyższe kongruencje, otrzymujemy kongruencję
$$(n_1 a_1 + n_2 a_2 + \cdots + n_k a_k) \cdot x \equiv n_1 b_1 + n_2 b_2 + \cdots + n_k b_k \pmod{n}.$$
3. Rozwiązując powyższą kongruencję, znajdujemy odpowiedź.

# Rozwiązywanie układów kongruencji - Metoda I, przykład

**Zadanie**

Znaleźć wszystkie liczby $x \in \mathbb{Z}$ takie, że

$$x \equiv 3 \pmod 5, \qquad 2x \equiv 4 \pmod 6, \qquad 3x \equiv 1 \pmod 7.$$

Rozwiązanie

1. Mamy $n = 5 \cdot 6 \cdot 7 = 210$ oraz
$$n_1 := 6 \cdot 7 = 42, \qquad n_2 := 5 \cdot 7 := 35, \qquad n_3 := 5 \cdot 6 = 30.$$
2. Mnożąc współczynniki wyjściowych kongruencji przez 42, 35 i 30, odpowiednio, otrzymujemy
$$42x \equiv 126 \pmod{210}, \quad 70x \equiv 140 \pmod{210}, \quad 90x \equiv 30 \pmod{210}.$$
Dodając powyższe kongruencje stronami, dostajemy kongruencję
$$202x \equiv 296 \pmod{210}.$$
3. Rozwiązanie kongruencji
$$202x \equiv 296 \pmod{210},$$
ma postać
$$x \equiv 68 \pmod{105}.$$

# Rozwiązywanie układów kongruencji - Metoda II

## Założenie

Zakładamy, że $k = 2$, tj. chcemy rozwiązać układ

$$a_1 \cdot x \equiv b_1 \pmod{m_1}, \qquad a_2 \cdot x \equiv b_1 \pmod{m_2}.$$

W przypadku, gdy $k > 2$, możemy iterować stosowanie powyższej metody.

## Metoda II

1. Rozwiązujemy kongruencje $a_1 \cdot x \equiv b_1 \pmod{m_1}$, $a_2 \cdot x \equiv b_1 \pmod{m_2}$, a więc zastępujemy je kongruencjami
$$x \equiv b_1' \pmod{m_1'}, \qquad x \equiv b_2' \pmod{m_2'}.$$
2. Stosując rozszerzony algorytm Euklidesa dla pary $(m_1', m_2')$, znajdujemy liczby $l_1$ i $l_2$ takie, że
$$1 = l_1 \cdot m_1' + l_2 \cdot m_2'.$$
3. Jeśli $r := (l_2 m_2' b_1' + l_1 m_1 b_2') \bmod (m_1' m_2')$, to rozwiązanie ma postać
$$x \equiv r \pmod{m_1' m_2'}.$$

# Rozwiązywanie układów kongruencji - Metoda II, przykład

**Zadanie**

Znaleźć wszystkie liczby $x \in \mathbb{Z}$ takie, że

$$x \equiv 3 \pmod 5, \qquad 2x \equiv 4 \pmod 6, \qquad 3x \equiv 1 \pmod 7.$$

## Rozwiązanie

### Krok I

1. Rozwiązując kongruencje $x \equiv 3 \pmod 5$, $2x \equiv 4 \pmod 6$ otrzymujemy kongruencje
$$x \equiv 3 \pmod 5 \quad \text{i} \quad x \equiv 2 \pmod 3.$$
2. Stosując rozszerzony algorytm Euklidesa dla liczb 5 i 3, otrzymujemy
$$1 = (-1) \cdot 5 + 2 \cdot 3.$$
3. Ponieważ $(3 \cdot 2 \cdot 3 + 2 \cdot (-1) \cdot 5) \bmod (5 \cdot 3) = 8$, więc w Kroku I otrzymujemy rozwiązanie
$$x \equiv 8 \pmod{15}.$$

### Krok II

1. Rozwiązując kongruencje $x \equiv 8 \pmod{15}$, $3x \equiv 1 \pmod 7$ otrzymujemy kongruencje
$$x \equiv 8 \pmod{15} \quad \text{i} \quad x \equiv 5 \pmod 7.$$
2. Stosując rozszerzony algorytm Euklidesa dla liczb 15 i 7, otrzymujemy
$$1 = 1 \cdot 15 + (-2) \cdot 7.$$
3. Ponieważ $(8 \cdot (-2) \cdot 7 + 5 \cdot 1 \cdot 15) \bmod (15 \cdot 7) = 68$, więc otrzymujemy rozwiązanie
$$x \equiv 68 \pmod{105}.$$

# Rozwiązywanie układów kongruencji - Metoda III

**Uwaga**

Poniższa metoda jest modyfikacją Metody II i może być stosowana w jej zastępstwie, gdy $k > 2$.

**Metoda III**

1. Rozwiązujemy kongruencje

   $$a_1 \cdot x \equiv b_1 \pmod{m_1}, \qquad a_2 \cdot x \equiv b_2 \pmod{m_2}, \qquad \ldots \qquad a_k \cdot x \equiv b_k \pmod{m_k},$$

   a więc zastępujemy je kongruencjami

   $$x_1 \equiv b_1' \pmod{m_1'}, \qquad x_2 \equiv b_2' \pmod{m_2'}, \qquad \ldots \qquad x_k \equiv b_k' \pmod{m_k'}.$$

2. Niech $n := m_1' \cdots m_k'$ oraz

   $$n_1 := m_2' \cdots m_k', \qquad n_2 := m_1' \cdot m_3' \cdots m_k', \qquad \ldots \qquad n_k := m_1' \cdots m_{k-1}'.$$

3. Dla każdego $i = 1, \ldots, k$, stosujemy rozszerzony algorytm Euklidesa dla pary $(n_i, m_i')$ i znajdujemy liczby $p_i$ i $q_i$ takie, że

   $$1 = p_i \cdot n_i + q_i \cdot m_i'.$$

4. Jeśli $r := (p_1 n_1 b_1' + p_2 n_2 b_2' + \cdots + p_k n_k b_k') \bmod n$, to rozwiązanie ma postać

   $$x \equiv r \pmod{n}.$$

# Rozwiązywanie układów kongruencji - Metoda III, przykład

**Zadanie**

Znaleźć wszystkie liczby $x \in \mathbb{Z}$ takie, że

$$x \equiv 3 \pmod 5, \qquad 2x \equiv 4 \pmod 6, \qquad 3x \equiv 1 \pmod 7.$$

Rozwiązanie

1. Rozwiązując kongruencje $x \equiv 3 \pmod 5$, $2x \equiv 4 \pmod 6$, $3x \equiv 1 \pmod 7$, otrzymujemy kongruencje
$$x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 3, \qquad x \equiv 5 \pmod 7.$$
2. Mamy $n = 5 \cdot 3 \cdot 7 = 105$ oraz
$$n_1 := 3 \cdot 7 = 21, \qquad n_2 := 5 \cdot 7 := 35, \qquad n_3 := 5 \cdot 3 = 15.$$
3. Stosując rozszerzony algorytm Euklidesa dla par $(21, 5)$, $(35, 6)$ i $(15, 7)$, otrzymujemy
$$1 = 1 \cdot 21 + (-4) \cdot 5, \qquad 1 = (-1) \cdot 35 + 12 \cdot 3, \qquad 1 = 1 \cdot 15 + (-2) \cdot 7.$$
odpowiednio.
4. Ponieważ
$$(3 \cdot 1 \cdot 21 + 2 \cdot (-1) \cdot 35 + 5 \cdot 1 \cdot 15) \bmod 105 = 68,$$
więc odpowiedzią jest: $x \equiv 68 \pmod{105}$.