Zestaw 3

7 Rozwiązywanie kongruencji

Teoria

Jeśli $n > 0$ oraz a i b są liczbami całkowitymi, to zapis $a \equiv b \pmod{n}$ oznacza, że $n \mid a - b$, lub, równoważnie, że liczby a i b dają tę samą resztę z dzielenia przez n.

Naszym celem jest przedstawienie metody, która dla danych liczb całkowitych a i b oraz $n > 0$ znajduje wszystkie liczby całkowite x takie, że

$$ax \equiv b \pmod{n}. \tag{7.1}$$

1. Korzystając z rozszerzonego algorytmu Euklidesa, znajdujemy liczby całkowite k i l takie, że
$$d = ka + ln,$$
gdzie $d := \gcd(a, n)$.

2. Jeśli $d \nmid b$, to kongruencja (7.1) nie ma rozwiązania, a więc odpowiedź ma postać $x \in \varnothing$.

3. Jeśli $d \mid b$, to zastępujemy kongruencję (7.1) kongruencją
$$a'x \equiv b \pmod{n'}, \tag{7.2}$$
gdzie
$$a' := \frac{a}{d}, \qquad b' := \frac{b}{d} \qquad \text{i} \qquad n' := \frac{n}{d}$$
(a więc, mówiąc obrazowo, „dzielimy” współczynniki kongruencji (7.1) przez d). Następnie mnożymy kongruencję (7.2) stronami przez k i otrzymujemy kongruencję
$$x \equiv kb' \pmod{n'}.$$
Jeśli r jest resztą z dzielenia kb' przez n', to rozwiązanie kongruencji (7.1) ma postać
$$x \equiv r \pmod{n'}.$$

Przykład

Rozważmy kongruencję

$$8x \equiv 12 \pmod{22}. \tag{7.3}$$

Z rozszerzonego algorytmu Euklidesa otrzymujemy, że

$$\gcd(8, 22) = 2 = 3 \cdot 8 + (-1) \cdot 22. \tag{7.4}$$

Ponieważ $2 \mid 12$, więc zastępujemy kongruencję (7.3) kongruencją

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

Mnożąc powyższą kongruencję przez 3 (3 jest współczynnikiem przy 8 w równości (7.4)), otrzymujemy kongruencję

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

Ponieważ resztą z dzielenia 18 przez 11 jest 7, więc rozwiązanie kongruencji (7.3) ma postać

$$x \equiv 7 \pmod{11}.$$

Odpowiedzi do Zadania 7

(1) $x \equiv 6 \pmod{7}$.

(2) $x \equiv 219 \pmod{256}$.

(3) $x \equiv 8 \pmod{21}$.

(4) $x \equiv 5 \pmod{7}$.

(5) $x \in \varnothing$.

8 Rozwiązywanie układów kongruencji

Teoria

Celem tej części jest przedstawienie metody rozwiązywania układów kongruencji, tj. znajdowania dla danych liczb całkowitych $a_1, \ldots, a_k, b_1, \ldots, b_k$, $n_1 > 0, \ldots, n_k > 0$ takich, że liczby $n_1, \ldots, n_k$ są parami względnie pierwsze (tj. $\gcd(n_i, n_j) = 1$ dla $1 \leq i < j \leq k$), wszystkich liczb całkowitych x takich, że

$$a_1 x \equiv b_1 \pmod{n_1}, \ \ldots, \ a_k x \equiv b_k \pmod{n_k} \tag{8.5}$$

(domyślnie pomiędzy kolejnymi kongruencjami znajduje się spójnik „i").

Metoda I Pierwsza metoda jest najprostsza do przedstawienia, ale wymaga wykonywania operacji arytmetycznych na większych liczbach.

Niech n będzie iloczynem wszystkich liczb $n_1, \ldots, n_k$, tj.

$$n := n_1 \cdots n_k.$$

Dla $i = 1, \ldots, k$, niech

$$m_i := \frac{n}{n_i},$$

tj. m_i jest iloczynem wszystkich liczb $n_1, \ldots, n_k$ z wyjątkiem liczby n_i. Oczywiście $n_i m_i = n$.

Dla każdego $i = 1, \ldots, k$ mnożymy współczynniki kongruencji $a_i x \equiv b_i \pmod{n_i}$ przez m_i i w efekcie zastępujemy układ (8.5) układem

$$m_1 a_1 x \equiv m_1 b_1 \pmod{n}, \ \ldots, \ m_k a_k x \equiv m_k b_k \pmod{n}.$$

Dodając stronami powyższe kongruencje, otrzymujemy kongruencję

$$ax \equiv b \pmod{n},$$

gdzie

$$a := m_1 a_1 + \cdots + m_k a_k \qquad \text{i} \qquad b := m_1 b_1 + \cdots + m_k b_k,$$

którą rozwiązujemy metodami opisanymi w poprzedniej części.

Metoda II Druga metoda pozwala na wykonywanie rachunków na mniejszych liczbach, kosztem większej liczby wykonywań algorytmu Euklidesa.

W pierwszym kroku rozwiązujemy każdą z kongruencji $a_i x \equiv b_i \pmod{n_i}$, $i = 1, \ldots, k$, tj. zastępujemy układ (8.5) układem

$$x \equiv b_1' \pmod{n_1'}, \ \ldots, \ x \equiv b_k' \pmod{n_k'}. \tag{8.6}$$

Oczywiście, jeśli któraś z wyjściowych kongruencji jest sprzeczna, to sprzeczny jest również wyjściowy układ.

Wykonując rozszerzony algorytm Euklidesa dla n_1' i n_2', znajdujemy liczby całkowite k_1 i k_2 takie, że

$$1 = k_1 n_1' + k_2 n_2'$$

(przypomnijmy, że założenia implikują, iż $\gcd(n_1', n_2') = 1$). Wtedy układ kongruencji

$$x \equiv b_1' \pmod{n_1'}, \qquad x \equiv b_2' \pmod{n_2'}$$

jest równoważny kongruencji

$$x \equiv b'_1(k_2 n'_2) + b'_2(k_1 n'_1) \pmod{n'_1 n'_2}.$$

Iterujące powyższe postępowanie – w drugim kroku zastępujemy układ

$$x \equiv b'_1(k_2 n'_2) + b'_2(k_1 n'_1) \pmod{n'_1 n'_2}, \qquad x \equiv b'_3 \pmod{n'_3},$$

jedną kongruencją (o ile oczywiście jest to konieczne, tj. $k > 2$) – zastępujemy układ (8.6) kongruencją

$$x \equiv b' \pmod{n'_1 \cdots n'_k},$$

(dla pewnej liczby całkowitej b'), która stanowi rozwiązanie układu (8.5).

Metoda II' Modyfikacja drugiej metody pozwala zastąpić układ (8.6) pojedynczą kongruencją w jednym kroku. Podobnie jak w pierwszej metodzie, niech

$$n' := n'_1 \cdots n'_k \tag{8.7}$$

oraz

$$m'_i := \frac{n'}{n'_i}, \tag{8.8}$$

dla $i = 1, \ldots, k$.

Korzystając k razy z rozszerzonego algorytmu Euklidesa, znajdujemy dla każdego $i = 1, \ldots, k$ liczby całkowite k_i i l_i takie, że

$$1 = k_i n'_i + l_i m'_i.$$

Wtedy rozwiązanie układu (8.5) jest postaci

$$x \equiv b'_1(l_1 m'_1) + \cdots + b'_k(l_k m'_k) \pmod{n'}. \tag{8.9}$$

8.1 Przykład

Zilustrujemy teraz powyższe trzy metody na przykładzie układu

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

Metoda I Mamy

$$n := 5 \cdot 6 \cdot 7 = 210$$

oraz

$$m_1 := 6 \cdot 7 = 42, \qquad m_2 := 5 \cdot 7 = 35, \qquad m_3 := 5 \cdot 6 = 30.$$

Mnożąc współczynniki wyjściowych kongruencji przez 42, 35 i 30, odpowiednio, otrzymujemy układ

$$42x \equiv 126 \pmod{210}, \quad 70x \equiv 140 \pmod{210}, \quad 90x \equiv 30 \pmod{210}.$$

Po dodaniu powyższych kongruencji stronami dostajemy kongruencję

$$202x \equiv 296 \pmod{210},$$

której rozwiązanie ma postać

$$x \equiv 68 \pmod{105}.$$

Metoda II Rozwiązując wyjściowe kongruencje, otrzymujemy układ

$$x \equiv 3 \pmod{5}, \qquad x \equiv 2 \pmod{3}, \qquad x \equiv 5 \pmod{7}. \qquad (8.10)$$

Stosując rozszerzony algorytm Euklidesa dla 5 i 3, otrzymujemy

$$1 = \gcd(5, 3) = (-1) \cdot 5 + 2 \cdot 3,$$

zatem układ (8.11) jest równoważny układowi

$$x \equiv 3 \cdot 2 \cdot 3 + 2 \cdot (-1) \cdot 5 = 8 \pmod{15}, \qquad x \equiv 5 \pmod{7}.$$

Stosując ponownie rozszerzony algorytm Euklidesa, tym razem dla 15 i 7, otrzymujemy, że

$$1 = \gcd(15, 7) = 1 \cdot 15 + (-2) \cdot 7,$$

więc rozwiązaniem naszego układu ma postać

$$x \equiv 8 \cdot (-2) \cdot 7 + 5 \cdot 1 \cdot 15 = -37 \equiv 68 \pmod{105}.$$

Metoda II' Podobnie jak w przypadku drugiej metody zastępujemy wyjściowy układ układem

$$x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 3, \qquad x \equiv 5 \pmod 7. \tag{8.11}$$

Zgodnie ze wzorami (8.7) i (8.8) wyliczamy

$$n' := 5 \cdot 3 \cdot 7 = 105$$

oraz

$$m_1' := 3 \cdot 7 = 21, \qquad m_2' := 5 \cdot 7 = 35, \qquad m_3' := 5 \cdot 3 = 15.$$

zatem zgodnie ze wzorem (8.9) rozwiązanie naszego układu ma postać

$$x \equiv 3 \cdot 1 \cdot 21 + 2 \cdot (-1) \cdot 35 + 5 \cdot 1 \cdot 15 = 68 \pmod{105}.$$

Odpowiedzi do Zadania 8

(1) $x \equiv 163 \pmod{252}$.

(2) $x \equiv 713 \pmod{1320}$.

(3) $x \equiv 409 \pmod{693}$.

(4) $x \equiv 47 \pmod{84}$.