Analiza kongruencji

Kongruencje – Wykład 3

Kongruencje algebraiczne

Kongruencje – jak już podkreślaliśmy – mają własności analogiczne do *równań* algebraicznych. Zajmijmy się więc problemem znajdowania *pierwiastka równania algebraicznego* $f(x) = 0$.

W języku kongruencji $f(x) \equiv 0 \pmod{m}$ – na przykład:

(1)

$$f(x) = x^3 + 5x - 4 \equiv 0 \pmod{7};\ x = 2 \pmod{7};\ f(2) = 14$$

W rachunku kongruencji *wszystkie* wartości $x \equiv 2 \pmod{7}$ traktujemy jako *jedno* rozwiązanie.

Aby znaleźć *wszystkie* rozwiązania (1) należałoby sprawdzić kompletny układ siedmiu reszt modulo 7: $0, 1, \ldots, 6$ albo $-3, \ldots, 0, \ldots, 3$.

Przykłady

- $x^2 + 5 \equiv 0 \pmod{11}$; nie ma rozwiązań.
- $x^3 - 2x + 6 \equiv 0 \pmod{5}$; $x \equiv 1,\ 2 \pmod{5}$.
- $x^3 \equiv 0 \pmod{27}$; $x \equiv 0,\ \pm 3,\ \pm 6,\ \pm 9 \pm 12 \pmod{27}$.

Kongruencje liniowe

definicja

$$(2) \qquad ax \equiv b \pmod{m}$$

Przykłady

- $7x \equiv 3 \pmod{12}$; $x \equiv 9 \pmod{12}$.
- $12x \equiv 2 \pmod{8}$; nie ma rozwiązań.
- $6x \equiv 9 \pmod{15}$; $x \equiv 4,\ 9,\ 14 \pmod{15}$.

definicja – konsekwencje

$$ax - b = my, \qquad \text{albo} \qquad \boxed{ax - my = b.}$$

twierdzenie AK1

Liniowa kongruencja (2) ma rozwiązanie wtedy i tylko wtedy, gdy b jest podzielne przez $d = (a, m)$.

Kongruencje liniowe – forma ogólna

Jeżeli warunki twierdzenia AK1 są spełnione to kongruencję (2) zapiszemy jako

definicja

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{3}$$

Nowe współczynniki x-a i y-a są teraz liczbami względnie pierwszymi; rozwiązanie ogólne (3) to rozwiązanie „szczególne” x_0, y_0 do którego dodajemy wielokrotność (dowolną) modułu

$$x = x_0 + \frac{m}{d} \cdot t, \qquad y = y_0 + \frac{m}{d} \cdot t,$$

a jeśli tak to nasze szukane rozwiązanie to

$$x \equiv x_0 \pmod{\frac{m}{d}}. \tag{4}$$

uwaga:

Nie wszystkie rozwiązania dane równaniem (4) są kongruentne modulo m! Dlatego rozwiązania

$$(5) \quad x_0,\ x_0+\frac{m}{d},\ x_0+2\frac{m}{d},\ x_0+3\frac{m}{d},\ \ldots,\ x_0+(d-1)\frac{m}{d}$$

będą *różnymi* rozwiązania kongruencji (1).

Twierdzenie AK1 możemy uściślić:

twierdzenie AK2

Liniowa kongruencja (2) ma rozwiązanie wtedy i tylko wtedy, gdy b jest podzielne przez $d=(a,m)$;
wówczas mamy d różnych rozwiązań, danych wzorami (5).
Dla względnie pierwszych a i m mamy jedno (modulo m) rozwiązanie.

Układy kongruencji liniowych

Często interesuje nas znalezienia rozwiązania dwóch (lub więcej) kongruencji, dla różnych modułów – znalezienia liczby x, która przy dzieleniu przez te moduły daje określone reszty.

Na przykład szukamy x, dla którego

$$(6) \qquad x \equiv 5 \pmod{11}, \qquad x \equiv 3 \pmod{23}.$$

Z pierwszego równania wynika, że $\boxed{x = 5 + 11t}$;
podstawiamy do drugiego: $5 + 11t \equiv 3 \pmod{23}$, albo $11t \equiv -2 \pmod{23}$.
Wystarczy pomnożyć obie strony przez 2: $22t \equiv (-1)t \equiv -4 \pmod{23}$, a więc $\boxed{t \equiv 4 \pmod{23}}$, albo $t = 4 + 23u$.
Podstawiamy do wyrażenia na x:

$$x = 5 + 11(4 + 23u) = 49 + (11 \cdot 23 \cdot u) \quad \rightarrow \quad .$$

$$\boxed{\rightarrow \quad x \equiv 49 \pmod{11 \cdot 23}}.$$

Układy kongruencji liniowych, c.d

Ogólnie, prezentowany schemat możemy zapisać

(7)

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n} \quad \rightarrow \quad x = a + mt,$$
$$\rightarrow \; mt \equiv b - a \pmod{n}.$$

Rozwiązanie tej ostatniej będzie możliwe jeżeli $d = (m, n)$ dzieli $(b - a)$, albo $a \equiv b \pmod{d}$. Przy spełnieniu tego warunku ostatnią kongruencję z (7) możemy podzielić przez d

(8)
$$\frac{m}{d}t \equiv \frac{b-a}{d} \pmod{\frac{n}{d}}.$$

Rozwiązaniem tej kongruencji będzie jakieś t_0; rozwiązanie ogólne:

$$t = t_0 + u\frac{n}{d}; \qquad u \in \mathbb{N};$$

po podstawieniu za x dostajemy więc

$$x \equiv a + m\left(t_0 + u\frac{n}{d}\right) = x_0 + u\frac{mn}{d},$$

a ponieważ $\frac{mn}{d} = [m, n]$ to $\boxed{x \equiv x_0 \pmod{[m, n]}}$.

Układy kongruencji liniowych – podsumowanie

Mamy więc

Twierdzenie AK3

Dwie równoczesne kongruencje

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

będą miały rozwiązanie pod warunkiem, że

$$a \equiv b \pmod{(m,n)}; \quad \text{wówczas} \quad x \equiv x_0 \pmod{[m,n]}$$

gdzie x_0 znajdujemy według opisanej wyżej metody.

Przypadek dwóch kongruencji równoczesnych można bez trudu uogólnić na przypadek r kongruencji; wówczas sukcesywne zastosowanie opisanego algorytmu: rozwiązanie pierwszych dwóch, rozwiązanie układu: pierwsze rozwiązanie + trzecia kongruencja, rozwiązanie układu: drugie rozwiązanie + czwarta, itd. prowadzi do $x \equiv x_0 \pmod{[m_1, m_2, \ldots, m_r]}$.

Twierdzenie AK4

warunkiem koniecznym i wystarczającym na to, aby układ kongruencji

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, r$$

miał rozwiązanie jest

$a_i \equiv a_j \pmod{(m_j, m_j)}$, dla każdej pary i, j.

Rozwiązaniem jest wówczas pewna liczba x dla modułu $M_r = [m_1, m_2, \ldots, m_r]$.

przykład

W koszyku znajduje się pewna ilość jajek. Wyjmując po 2, 3, 4, 5 i 6 jajek na raz pozostawiamy w koszyku zawsze jedno jajko; wyjmując po siedem jajek opróżniamy koszyk kompletnie. Jaka jest (najmniejsza) liczba jajek w koszyku? Mamy

$x \equiv 0 \pmod{7}$, $x \equiv 1 \pmod{(2, 3, 4, 5, 6)}$

$\rightarrow \quad x \equiv 1 \pmod{[2, 3, 4, 5, 6]}$.

Drugie z równań to $x \equiv 1 \pmod{60}$;

rozwiązanie obu równań to $x \equiv 301 \pmod{420}$.

Szczególnym przypadkiem „układów kongruencji” jest tak zwane ...

. . . Chińskie twierdzenie o resztach – tw. AK5

Dla *względnie pierwszych parami* modułów $m_1, m_2, \ldots, m_i, \ldots, m_r$ ($m_i \in \mathbb{N}\backslash\{1\}$) oraz liczb $a_1, a_2, \ldots, a_i, \ldots, a_r$ ($a_i \in \mathbb{Z}$) układ kongruencji

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots\ldots\ldots \\ x &\equiv a_i \pmod{m_i} \\ &\ldots\ldots\ldots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

ma dokładnie jedno rozwiązanie modulo $M = m_1 m_2 \ldots m_i \ldots m_r$.

Dowód

Rozpatrujemy przypadek szczególny:

$a_1 = a_2 \ldots = a_{i-1} = a_{i+1} = \ldots a_r = 0; \qquad a_i = 1.$

Oznaczmy $M_i = M/m_i$. Ponieważ $M_i \perp m_i$ dla *każdego* i istnieją liczby $u_i, v_i \in \mathbb{Z}$, takie że $u_i M_i + v_i m_i = 1,\ u_i, v_i \in \mathbb{Z}$.

$$u_i M_i \equiv 0 \pmod{M_i} \qquad \text{i} \qquad u_i M_i \equiv 1 \pmod{m_i}.$$

. . . Chińskie twierdzenie o resztach – dowód, c.d.

Liczba $u_i M_i$ jest podzielna bez reszty przez *prawie wszystkie* $m_1, m_2, \ldots, m_{i-1}, m_{i+1} \ldots, m_r$;
spełnia ona więc układ kongruencji – oznaczamy $u_i M_i = x_i$

$$\begin{aligned}
x_i &\equiv 0 \pmod{m_1} \\
x_i &\equiv 0 \pmod{m_2} \\
&\ldots\ldots\ldots \\
x_i &\equiv 0 \pmod{m_{i-1}} \\
x_i &\equiv 1 \pmod{m_i} \\
x_i &\equiv 0 \pmod{m_{i+1}} \\
&\ldots\ldots\ldots \\
x_i &\equiv 0 \pmod{m_r}
\end{aligned}$$

Znajdujemy, dla każdego i, takie x_i. Wyrażenie
$x = a_1 x_1 + a_2 x_2 + \ldots + a_r x_r$ będzie rozwiązaniem naszego układu.
Rzeczywiście

$$x \equiv \sum_i a_i x_i \equiv a_i \pmod{m_i} \quad \text{dla każdego} \quad 1 \leqslant i \leqslant r.$$

. . . Chińskie twierdzenie o resztach – jednoznaczność rozwiązania

Jeżeli istniałoby inne – oprócz znalezionego x – rozwiązanie układu kongruencji, np y to:

- $\rightarrow \quad x \equiv y \pmod{m_i} \quad \forall i$
- $\rightarrow \quad m_i \mid (x - y) \quad \forall i$
- $\rightarrow \quad (x - y)$ wspólna wielokrotność wszystkich m_i
- Taka wspólna wielokrotność liczb m_i musi być podzielna przez $M = [m_1, \ldots, m_r] = m_1 m_2 \ldots m_r$.
- $M \mid (x - y) \quad \rightarrow \quad x \equiv y \pmod{M}$.

. . . Chińskie twierdzenie o resztach – przykład historyczny; układ Sun Zi

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

$M = 3 \cdot 5 \cdot 7 = 105,$
$M_1 = M/m_1 = 35,\ M_2 = M/m_2 = 21,$
$M_3 = M/m_3 = 15.$

Mamy do rozwiązania trzy kongruencje

$$u_1 \cdot 35 \equiv 1 \pmod 3, \quad u_2 \cdot 21 \equiv 1 \pmod 5, \quad u_3 \cdot 15 \equiv 1 \pmod 7.$$

Wkrótce poznamy „przyspieszoną” metodę rozwiązywania takich kongruencji, ale widać, że $u_1 = 2$, $u_2 = 1$, $u_3 = 1$ i dostajemy

$$x = a_1\,(u_1 M_1) + a_2\,(u_2 M_2) + a_3\,(u_3 M_3) = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 \equiv 23$$

— oczywiście modulo $M = 105$.

przykład do samodzielnego rozwiązania – Regiomontanus

$$x \equiv 3 \pmod{11}, \qquad x \equiv 5 \pmod{19}, \qquad x \equiv 10 \pmod{29}.$$

Układy kongruencji – różne stopnie

Przykład 1:

Aby rozwiązać układ kongruencji:

$$(9) \qquad x^3 - 2x + 3 \equiv 0 \pmod 7 \qquad 2x^2 \equiv 3 \pmod{15}$$

rozwiązujemy (próby i błędy)
pierwszą $x \equiv 2 \pmod 7$ i drugą $x \equiv \pm 3 \pmod{15}$, a następnie – dyskutowaną metodą (chińskie twierdzenie o resztach)
– rozwiązujemy dwa układy:

$$x \equiv 2 \pmod 7, \quad x \equiv 3 \pmod{15} \quad \rightarrow \quad x \equiv 93 \pmod{105}$$
$$x \equiv 2 \pmod 7, \quad x \equiv -3 \pmod{15} \quad \rightarrow \quad x \equiv 72 \pmod{105}$$

Przykład 2:

Aby rozwiązać układ kongruencji:

$$(10) \qquad 12x \equiv 3 \pmod{15} \qquad 10x \equiv 14 \pmod{8}$$

rozwiązujemy (próby i błędy)
pierwszą $x \equiv 4,\ 9,\ 14 \pmod{15}$ i drugą $x \equiv 3,\ 7 \pmod{8}$.
Mamy więc 3×2 możliwych kombinacji –
układów kongruencji typu $x \equiv a_i \pmod{m_i}$, $i = 1, 2$.
Ich rozwiązania dla modułu $120 = [8, 15]$ to:

$$\left.\begin{array}{ll} x \equiv 19, & x \equiv 79 \\ x \equiv 39, & x \equiv 99 \\ x \equiv 59, & x \equiv 119 \end{array}\right\} \pmod{120}$$

Analiza tych „równoczesnych kongruencji” pozwala na ...

Stwierdzenie: Kongruencja $f(x) \equiv 0 \pmod{m}$ dla modułu złożonego

$$m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}$$

będzie spełniona tylko dla x, dla których zachodzi

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \qquad i = 1, 2, \dots, r.$$

Przykład 3:

Aby rozwiązać kongruencję:

$$(11) \qquad x^3 - 7x^2 + 4 \equiv 0 \pmod{88}$$

rozbijamy moduł $88 = 8 \cdot 11$ i rozwiązujemy

$x^3 - 7x^2 + 4 \equiv 0 \pmod{8} \quad \rightarrow \quad x \equiv 2,\ 3,\ 6 \pmod{8}$

oraz $x^3 - 7x^2 + 4 \equiv 0 \pmod{11} \quad \rightarrow \quad x \equiv 4 \pmod{11}$.

Złożenie tych rozwiązań daje trzy rozwiązania kongruencji (11)

$x \equiv 26,\ 59,\ 70 \pmod{88}$

Zadanie – rozwiąż kongruencję: $5x^2 + 1 \equiv 0$

Kongruencję $f(x) \equiv 0 \pmod{m}$ dla modułu typu p^α ...

rozwiązujemy w oparciu o rozwiązanie tej samej kongruencji dla modułu p.

Przykład

Kongruencja $f(x) = x^3 - 8x^2 + 21x - 11 \equiv 0 \pmod{7}$ ma dwa rozwiązania $x \equiv 2 \pmod{7}$ i $x \equiv 3 \pmod{7}$. Aby rozwiązać kongruencję

$$(12) \qquad f(x) = x^3 - 8x^2 + 21x - 11 \equiv 0 \pmod{7^2}$$

szukamy liczby x pomiędzy rozwiązaniami kongruencji „wyjściowej” kładąc odpowiednio $x = 2 + 7t$ lub $x = 3 + 7t$.
Pierwsze podstawienie przekształca (12) w $7 + 7t \equiv 0 \pmod{49}$, tak więc $x = 2 + 7t \equiv -5 \pmod{49}$.
Drugie podstawienie prowadzi do sprzecznej (! –tak) kongruencji $7 \equiv 0 \pmod{49}$.
zadanie: rozwiąż kongruencję (12) modulo $7^3 = 343$

Twierdzenie:

Jeżeli kongruencja algebraiczna stopnia n
$f(x) \equiv 0 \pmod{m}$ ma rozwiązanie $x \equiv a_1 \pmod{m}$ to mamy

$$f(x) \equiv (x - a_1) f_1(x) \pmod{m},$$

gdzie $f_1(x)$ jest wielomianem stopnia $n - 1$.

Dowód: Dzieląc $f(x)$ przez $x - a_1$ mamy $f(x) = (x - a_1) f_1(x) + r$, gdzie reszta z dzielenia r jest pewną liczbą, a stopień wielomianu $f(x)$ został obniżony o 1. Kładąc $x = a_1$ mamy

$$f(a_1) = r \equiv 0 \pmod{m}$$

□

Przykład:

Kongruencja (11) $x^3 - 7x^2 + 4 \equiv 0 \pmod{88}$
ma pierwiastki $x \equiv 26,\ 59,\ 70 \pmod{88}$.
Dzieląc przez $x - 26$

$$x^3 - 7x^2 + 4 = (x - 26)(x^2 + 19x + 494) + 12\,848.$$

$88 \mid 12\,848$, a więc

$$x^3 - 7x^2 + 4 \equiv (x - 26)(x^2 + 19x + 494) \pmod{88}.$$

Zadanie – rozłóż kongruencję i znajdź jej drugi pierwiastek.

$f(x) = 3x^2 + 7x - 2 \equiv 0 \pmod{23}$; wsk. – pierwiastek $x \equiv 3 \pmod{23}$

Kongruencje algebraiczne dla modułu będącego liczbą pierwszą p

Uogólnieniem ostatniego twierdzenia, *ale dla modułu będącego liczbą pierwszą* jest ...

... twierdzenie:

Jeżeli kongruencja n-tego stopnia

$$f(x) \equiv 0 \pmod{p}$$

ma r różnych (modulo p) pierwiastków a_i

$$x \equiv a_1 \pmod{p},\ x \equiv a_2 \pmod{p},\ \ldots,\ x \equiv a_r \pmod{p}$$

to zachodzi

$$f(x) \equiv (x - a_1)(x - a_2)\ldots(x - a_r)f_1(x) \pmod{p},$$

gdzie $f_1(x)$ jest wielomianem stopnia $n - r$.

przykład

Kongruencja $x^4 - 5x^3 - 5x - 1 \equiv 0 \pmod{7}$ ma dwa pierwiastki $x = 2,\ 3 \pmod{7}$; dlatego zachodzi

$$x^4 - 5x^3 - 5x - 1 \equiv (x - 2)(x - 3)(x^2 + 1) \pmod{7}.$$

Kongruencje algebraiczne dla modułu p, c.d.

. . . twierdzenie (Lagrange, 1768 – bez pojęcia kongruencji):

Kongruencja n-tego stopnia dla modułu będącego liczba pierwszą

$$f(x) \equiv 0 \pmod{p}$$

nie może mieć więcej różnych pierwiastków niż n, za wyjątkiem przypadku trywialnego, kiedy $p \mid$(wszystkie współczynniki $f(x)$).

. . . dowód:

na mocy poprzedniego twierdzenia możemy zapisać

$$f(x) \equiv (x - a_1)(x - a_2) \dots (x - a_n)F \pmod{p},$$

gdzie F, będąc wielomianem stopnia $n - n = 0$ jest pewną stałą.
gdyby istniało jeszcze jedno rozwiązanie $x \equiv a_{n+1} \pmod{p}$
mielibyśmy

$$f(a_{n+1}) \equiv (a_{n+1} - a_1)(a_{n+1} - a_2) \dots (a_{n+1} - a_n)F \equiv 0 \pmod{p}.$$

W powyższym wyrażeniu żadna z różnic $a_{n+1} - a_k$ nie może być podzielna przez p (bo nasze pierwiastki są różne modulo p).
W takim razie $p \mid F \quad \rightarrow \quad p \mid f(x)$ co jest możliwe kiedy
$p \mid$(wszystkie współczynniki $f(x)$) $\square$.