Kongruencje w akcji

Bartłomiej BZDĘGA Uniwersytet im. A. Mickiewicza w Poznaniu

Kongruencje pojawiały się już kilka razy w Kąciku, ale zawsze grały rolę co najwyżej drugoplanową. Tym razem będzie inaczej.

Niech a, b i n będą liczbami całkowitymi. Kongruencję $a \equiv b \pmod n$ (czytaj: *a przystaje do b modulo n*) możemy zdefiniować na dwa równoważne sposoby:

(1) Liczby a, b dają tę samą resztę z dzielenia przez n.
(2) Liczba n dzieli $a - b$.

Będziemy tutaj używać krótszej notacji: $a \equiv_n b$.

Z (1) natychmiast wynikają własności:

$$a \equiv_n a, \qquad a \equiv_n b \Rightarrow b \equiv_n a, \qquad a \equiv_n b \wedge b \equiv_n c \Rightarrow a \equiv_n c.$$

Kongruencje modulo n możemy dodawać, odejmować i mnożyć stronami, czyli jeśli $a \equiv_n b$ oraz $c \equiv_n d$, to

$$a \pm c \equiv_n b \pm d \qquad \text{oraz} \qquad ac \equiv_n bd.$$

Dla dowodu wystarczy zauważyć, że liczby $(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$ oraz $ac - bd = c(a - b) + b(c - d)$ są podzielne przez n na mocy (2).
Dzięki możliwości mnożenia kongruencji stronami można wykazać indukcyjnie, że jeśli $a \equiv_n b$, to $a^k \equiv_n b^k$ dla naturalnych k.
Pierwiastkowania kongruencji na ogół wykonywać nie można. Na przykład zachodzi $8 \equiv_7 1$, ale po wyciągnięciu obustronnie pierwiastka sześciennego otrzymamy nieprawdziwą kongruencję $2 \equiv_7 1$.

Najogólniejszym wnioskiem z powyższych faktów jest następujące twierdzenie: dla wielomianu P o współczynnikach całkowitych zachodzi implikacja

$$x \equiv_n y \quad \Rightarrow \quad P(x) \equiv_n P(y).$$

Dla dowodu niech $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$. Z kongruencji $x \equiv_n y$ otrzymujemy $x^k \equiv_n y^k$, a po pomnożeniu przez a_k mamy $a_k x^k \equiv_n a_k y^k$. Wystarczy teraz zsumować ostatnią kongruencję dla $k = 0, 1, 2, \ldots, d$.

Jeśli $n = x - y \neq 0$, to oczywiście $x \equiv_n y$. Wnioskiem z tego jest podzielność $x - y \mid P(x) - P(y)$ dla $x \neq y$ (jest to twierdzenie 2 z Kącika 12. w Δ_{19}^{12} – tam można znaleźć inny dowód).

Z dzieleniem jest trochę trudniej – można je wykonać tylko w szczególnych okolicznościach. Niech $a \equiv_n b$ oraz $c \equiv_n d$. Przyjmijmy, że $c \mid a$ i $d \mid b$. Jeśli dodatkowo $\mathtt{NWD}(c, n) = 1$, to wówczas $\frac{a}{c} \equiv_n \frac{b}{d}$. Aby to wykazać, zauważmy, że $a - b = c \cdot \frac{a}{c} - d \cdot \frac{b}{d} \equiv_n c \cdot \frac{a}{c} - c \cdot \frac{b}{d} = c(\frac{a}{c} - \frac{b}{d})$. Ostatnia liczba jest podzielna przez n oraz $\mathtt{NWD}(c, n) = 1$, więc $n \mid \frac{a}{c} - \frac{b}{d}$ (zobacz (1) w 29. Kąciku, w Δ_{21}^{5}).

Z powyższej własności najczęściej korzysta się w szczególnym przypadku $c = d$ oraz gdy n jest liczbą pierwszą.

Zadania

1. Liczby $a_1, a_2, \ldots, a_n$ są całkowite. Niech d będzie wspólnym dzielnikiem liczb $a_1 - 1, a_2 - 1, \ldots, a_n - 1$. Udowodnić, że $d \mid a_1 a_2 \ldots a_n - 1$.
2. Dane są takie liczby całkowite dodatnie d, m, n, że $d \mid mn^4 - 1$ i $d \mid m^4 n - 1$. Wykazać, że $d \mid n^{15} - 1$.
3. Liczby naturalne n i k są nieparzyste. Dowieść, że liczba $1^k + 2^k + \ldots + n^k$ dzieli się przez n.
4. Liczby a, b, c są całkowite. Liczba nieparzysta n jest dzielnikiem liczb $a + b + c$ i $a^2 + b^2 + c^2$. Wykazać, że liczby a^3, b^3, c^3 dają takie same reszty z dzielenia przez n.
5. Niech P będzie wielomianem o współczynnikach całkowitych. Liczby całkowite x, y, z spełniają równości: $P(x) = y$, $P(y) = z$, $P(z) = x$. Wykazać, że $x = y = z$.
6. Niech p będzie liczbą pierwszą. Liczby całkowite $x_1, x_2, \ldots, x_p$ spełniają podzielności $p \mid x_1 x_2 \ldots x_k - k$ dla $k = 1, 2, \ldots, p$. Udowodnić, że liczby $x_1, x_2, \ldots, x_p$ są różne.
7. Liczby a i b są całkowite, a $p > 2$ jest liczbą pierwszą, która nie dzieli ab. Liczby $a^2 + b^2$ i $a^3 + b^3$ dają resztę 1 z dzielenia przez p. Dowieść, że $p \mid a + b + 2$.

Wskazówki do zadań

1. Pomnożyć stronami kongruencje $a_i \equiv_d 1$ dla $i = 1, 2, \ldots, n$.
2. Kongruencję $mn^4 \equiv_d 1$ podnieść obustronnie do potęgi 4. Sprawdzić, że tak otrzymane równanie można podzielić przez $m^4 n \equiv_d 1$.
3. Udowodnić, że $i^k + (n - i)^k \equiv_n 0$ i zsumować dla $k = 0, 1, 2, \ldots, \lfloor n/2 \rfloor$.
4. Kongruencję $-a \equiv_n b + c$ podnieść do kwadratu i odjąć od niej $-a^2 \equiv_n b^2 + c^2$. Można stąd otrzymać $a^3 \equiv_n abc$, analogicznie dla b i c.
5. Jeśli pewne dwie z liczb x, y, z są równe, to $x = y = z$. Przypuśćmy, że są to trzy różne liczby. Wtedy $x - y \mid P(x) - P(y) = y - z$, zachodzą też dwie analogiczne podzielności.
Wnioskujemy, że $|x - y| = |y - z| = |z - x|$, co daje $x = y = z$.
6. Zauważmy, że $x_1 \equiv_p 1$. Dla $k > 1$ mamy $k \equiv_p x_1 x_2 \ldots x_k \equiv_p (k - 1)x_k$, co dowodzi, że $x_k \not\equiv_p 1$. Jeśli $x_k \equiv_p x_l \equiv_p x$ dla pewnych dwóch różnych $k, l \in \{2, 3, \ldots, p\}$, to z kongruencji $(k - 1)x \equiv_p k$ i $(l - 1)x \equiv_p l$ można otrzymać $x \equiv_p 1$ – sprzeczność. A zatem liczby $x_1, x_2, \ldots, x_p$ dają różne reszty z dzielenia przez p, więc są różne.
7. Dobrym punktem wyjścia jest kongruencja $(a^2 + b^2)^3 \equiv_p 1^3 = 1^2 \equiv_p (a^3 + b^3)^2$.
Po otrzymaniu $2ab \equiv_p 3$ zająć się $1 \equiv_p a^3 + b^3 = (a + b)(a^2 - ab + b^2)$ – pomnożyć obustronnie przez 2, żeby mieć $2ab$.