Kongruencje

Tomasz Kossakowski

26 września 2025

Definicje i własności

Kongruencje stanowią bardzo wygodne narzędzie służące do badania i zapisywania rozmaitych faktów związanych z podzielnością liczb całkowitych.

Definicja 1 (dzielenie z resztą)

Dane jest $a \in \mathbb{Z}$ i $m \in \mathbb{Z}_+$. Wówczas powiemy, że a daje resztę r przy dzieleniu przez m jeśli istnieje taka liczba całkowita k, że

$$a = k \cdot m + r$$

oraz $0 \leqslant r < m$.

Na dzielenie z resztą możemy popatrzeć w inny sposób.

Definicja 2 (kongruencja)

Niech $a, b \in \mathbb{Z}$ oraz niech $m \in \mathbb{Z}_+$. Mówimy, że a przystaje do b modulo m, jeśli liczba $a - b$ dzieli się przez m. Stosujemy oznaczenie

$$a \equiv b \pmod{m}$$

i nazywamy je kongruencją.

Przykłady:

- $5 \equiv 1 \pmod{4}$, ponieważ 4 dzieli $5 - 1 = 4$
- $2025 \equiv 1 \pmod{8}$, ponieważ 8 dzieli $2025 - 1 = 2024$
- $3a \equiv a \pmod{2}$, ponieważ 2 dzieli $3a - a = 2a$.

Na kongruencje można patrzeć jak na reszty z dzielenia, np. zapis $5 \equiv 1 \pmod{4}$ informuje nas, że 5 daje taką samą resztę z dzielenia przez 4 jak 1.

Kongruencje mają wiele ciekawych własności, z których będziemy często korzystać.

Twierdzenie 1 (własności kongruencji)

Dla $a, b, c, d \in \mathbb{Z}$ oraz $m, n \in \mathbb{Z}_+$ zachodzą poniższe zależności.

1. $a \equiv a \pmod{m}$.
2. Jeśli $a \equiv b \pmod{m}$, to $b \equiv a \pmod{m}$.
3. Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$.
4. Jeśli $a \equiv b \pmod{m}$, to $a \pm c \equiv b \pm c \pmod{m}$.
5. Jeśli $a \equiv b \pmod{m}$, to $ac \equiv bc \pmod{m}$.
6. Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $a \pm c \equiv b \pm d \pmod{m}$.
7. Jeśli $a \equiv b \pmod{m}$oraz $c \equiv d \pmod{m}$, to $ac \equiv bd \pmod{m}$.
8. Jeśli $a \equiv b \pmod{m}$, to $a^n \equiv b^n \pmod{m}$.

Warto tu zwrócić uwagę, iż kongruencji na ogół *nie można dzielić stronami*. Przykładowo, zachodzą kongruencje

$$18 \equiv 3 \pmod{3} \qquad \text{oraz} \qquad 3 \equiv 3 \pmod{3},$$

ale $6 \not\equiv 1 \pmod{3}$.
Gdy rozpatrujemy podzielności, często możemy dostać po pewnych przekształceniach, że $a \equiv 0 \pmod{n}$. Oznacza to wtedy, że a jest podzielne przez n (lub inaczej zapisując $n \mid a$).
Warto również wspomnieć o tzw. *resztach kwadratowych*.

Definicja 3 (reszty i niereszty kwadratowe)

Reszta kwadratowa modulo p (gdzie p jest liczbą pierwszą) to taka liczba całkowita a, że istnieje rozwiązanie kongruencji:

$$x^2 \equiv a \pmod{p}.$$

Jeśli powyższa kongruencja nie ma rozwiązania dla pewnej liczby całkowitej a, to taką liczbę nazywamy niereszą kwadratową modulo p.

Przykładowo rozpatrując modulo 3, resztami kwadratowymi są $\{0, 1\}$, a niereszą kwadratową jest 2, dlatego, że gdy sprawdzimy wszystkie reszty podniesione do kwadratu:

$$n \equiv 0 \implies n^2 \equiv 0^2 \equiv 0 \pmod{3}$$
$$n \equiv 1 \implies n^2 \equiv 1^2 \equiv 1 \pmod{3}$$
$$n \equiv 2 \implies n^2 \equiv 2^2 \equiv 1 \pmod{3}$$

znajdujemy 0 i 1, ale nie ma tutaj 2.

Przykłady

Ćwiczenie 1 (Matura podstawowa, czerwiec 2025)**.** Wykaż, że dla każdej nieparzystej liczby naturalnej n liczba $3n^2 + 2n + 7$ jest podzielna przez 4.

Rozwiązanie 1. Oczywiście moglibyśmy to zadanie zrobić metodą „szkolną”, jednak rozwiążemy je używając kongruencji.

Dowolna liczba całkowita nieparzysta podzielona przez 4 daje resztę 1 lub 3, zatem rozpatrzmy 2 przypadki:

1. Gdy $n \equiv 1 \pmod 4$, wtedy $3n^2 + 2n + 7 \equiv 3 \cdot 1^2 + 2 \cdot 1 + 7 = 12 \equiv 0 \pmod 4$, zatem $4 \mid 3n^2 + 2n + 7$.
2. Gdy $n \equiv 3 \pmod 4$, wtedy $3n^2 + 2n + 7 \equiv 3 \cdot 3^2 + 2 \cdot 3 + 7 = 40 \equiv 0 \pmod 4$, zatem $4 \mid 3n^2 + 2n + 7$.

W obu przypadkach wyszło, że $4 \mid 3n^2 + 2n + 7$, co należało udowodnić.

Ćwiczenie 2. Znajdź wszystkie takie liczby pierwsze p, dla których liczba p^2+2 także jest pierwsza.

Rozwiązanie 2. Zauważmy, że jeżeli liczba p nie dzieli się przez 3, to $p \equiv 1 \pmod 3$ lub $p \equiv 2 \pmod 3$. Stąd w obu przypadkach dostajemy $p^2 \equiv 1 \pmod 3$. A zatem

$$p^2 + 2 \equiv 0 \pmod 3$$

co oznacza, że liczba $p^2 + 2$ jest podzielna przez 3. Ponadto liczba $p^2 + 2$ jest większa od 3, gdyż p – jako liczba pierwsza – jest nie mniejsza od 2. Wobec tego liczba $p^2 + 2$ musi być złożona. Jeśli z kolei liczba p dzieli się przez 3, to musi być równa 3, gdyż jest to liczba pierwsza. Wtedy $3^2 + 2 = 11$ również jest liczbą pierwszą. Wobec tego jedyną liczbą p spełniającą warunki zadania jest $p = 3$.

Zadania

Zadanie 1. Wyznacz reszty z dzielenia (podaj najmniejsze naturalne a, b, c, d, e, f spełniające poniższe kongruencje):

1. $5 \equiv a \pmod 2$
2. $17 \equiv b \pmod 5$
3. $-4 \equiv c \pmod 6$
4. $123 \equiv d \pmod{20}$
5. $8 \cdot 421 \equiv e \pmod 4$
6. $7^9 \equiv f \pmod 8$.

Zadanie 2. Wyznacz resztę z dzielenia liczby 2^{50} przez 3.

Zadanie 3. Udowodnić, że dla dowolnej liczby całkowitej nieujemnej n liczba

$$3^{4^n} + 23$$

dzieli się przez 13.

Zadanie 4. Udowodnić, że liczba $93^{93} - 33^{33}$ dzieli się przez 10.

Zadanie 5 (VI OM-I-10)**.** Wykazać, że liczba $53^{53} - 33^{33}$ jest podzielna przez 10.

Zadanie 6. Liczby całkowite a, b, c mają tę własność, że liczby $ab - 1, bc - 1$ i $ca - 1$ są podzielne przez pewną liczbę pierwszą p. Wykaż, że liczba

$$a^2 + b^2 + c^2 - 3$$

również jest podzielna przez p.

Zadanie 7. W pewnej klasie jest mniej niż 40 osób. Gdy uczniowie chcieli podzielić się na grupy 5-osobowe, 4 osoby zostały bez grupy. Gdy natomiast chcieli podzielić się na grupy 6-osobowe, 5 osób zostało bez grupy. Ilu uczniów jest w tej klasie?

Zadanie 8. Wyznacz reszty kwadratowe modulo 3, 4, 5 i 8.

Zadanie 9. Znajdź wszystkie liczby całkowite x, y spełniające równanie

$$x^2 - 3y^2 = 1001.$$

Zadanie 10. Rozstrzygnąć, czy istnieją takie liczby całkowite: $a_1, a_2, \ldots, a_{10}$, które spełniają równość

$$a_1^4 + a_2^4 + \cdots + a_9^4 + a_{10}^4 = 201200002013.$$

Wskazówka: rozważ modulo 16.

Zadanie 11. Udowodnić, że dla nieskończenie wielu liczb całkowitych dodatnich n liczba $7 \cdot 2^n + 1$ jest złożona.

Zadanie 12. Udowodnić, że równanie $x^3+y^3+z^3 = 2005^2$ nie ma rozwiązań w liczbach całkowitych.

Zadania dodatkowe

Zadanie 13. Wyznaczyć wszystkie liczby pierwsze p, dla których liczba $3^p + 4^p$ jest podzielna przez 181.

Zadanie 14. Wykazać, że dla nieskończenie wielu liczb całkowitych dodatnich n, liczba $1+2^{4^n}+2^{5^n}$ jest złożona.

Zadanie 15. Dane są liczby całkowite dodatnie a, b, c, d, e, f takie, że

$$a + b = c + d = e + f = 101.$$

Udowodnić, że liczby $\frac{ace}{bdf}$ nie można zapisać w postaci ułamka $\frac{m}{n}$, gdzie m, n są liczbami całkowitymi dodatnimi o sumie mniejszej niż 101.

Zadanie 16. Udowodnić, że dla dowolnej liczby całkowitej dodatniej n liczba $73^{6^n} - 37^{6^n}$ dzieli się przez 35.

Zadanie 17. Wykazać, że dla dowolnej liczby naturalnej n liczba

$$\frac{n^{44} + n^{33} + n^{22} + n^{11} + 1}{n^4 + n^3 + n^2 + n + 1}$$

jest liczbą naturalną.

Zadanie 18. Udowodnić *małe twierdzenie Fermata:*
Jeśli p jest liczbą pierwszą, zaś a liczbą całkowitą dodatnią niepodzielną przez p, to a^{p-1} daje resztę 1 z dzielenia przez p.

Zadanie 19. Znajdź wszystkie takie pary dodatnich liczb całkowitych (n, m), dla których zachodzi równość

$$1! + 2! + 3! + \ldots + n! = m^2.$$

Zadanie 20. Udowodnić *chińskie twierdzenie o resztach:*
Dla dodatnich liczb całkowitych względnie pierwszych a_1 i a_2 oraz liczb całkowitych $0 \leqslant r_1 < a_1$, $0 \leqslant r_2 < a_2$ istnieje dokładnie jedna liczba $0 \leqslant n < a_1 \cdot a_2$ taka, że n daje resztę r_1 z dzielenia przez a_1 i resztę r_2 z dzielenia przez a_2.