Kongruencje - podstawy

Teoria

Oznaczenia. $\mathbb{Z}_+$ oznacza zbiór liczb całkowitych dodatnich.

Definicja 1. Niech $m > 1$ będzie ustaloną liczbą całkowitą dodatnią. Mówimy, że liczba calkowita a przystaje do liczby całkowitej b *modulo* m, gdy $m \mid a - b$. Będziemy zapisywać to tak:

$$a \equiv b \pmod m \text{ lub } a \equiv_m b.$$

Twierdzenie 1. *Dla dowolnych $a, b, c, d, m \in \mathbb{Z}$ oraz $m > 1$, zachodzą poniższe własności:*

1. $a \equiv a \pmod m$,
2. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$,
3. *jeżeli* $a \equiv b \pmod m$ *oraz* $b \equiv c \pmod m$, *to* $a \equiv c \pmod m$,
4. *jeżeli* $a \equiv b \pmod m$ *i* $c \equiv d \pmod m$, *to* $a \pm c \equiv b \pm d \pmod m$ *oraz* $ac \equiv bd \pmod m$.
5. *jeżeli* $a \equiv b \pmod m$, *to* $a^n \equiv b^n \pmod m$ *dla każdej liczb całkowitej dodatniej* n.
6. *jeżeli* $k \in \mathbb{Z}_+$ *oraz* $a \equiv b \pmod m$, *to* $ak \equiv bk \pmod{mk}$,
7. *jeżeli* $k \in \mathbb{Z}_+$ *jest* ***względnie pierwsze*** *z* m, *to jeżeli* $ka \equiv kb \pmod m$, *to* $a \equiv b \pmod m$.

Twierdzenie 2. *Niech p będzie liczbą pierwszą oraz a liczbą całkowitą niepodzielną przez p. Wówczas liczby*

$$a,\ 2a,\ \dots\ ,\ (p-1)a,\ pa \pmod p$$

tworzą cały zbiór reszt modulo p, tzn. utworzony zbiór jest równy zbiorowi $\{0, 1, 2, \dots, p-1\}$.

Wniosek 1 (Istnieje odwrotności)**.** Dane są względnie pierwsze liczby całkowite a i $m > 1$. Wówczas istnieje liczba całkowita x, która spełnia $ax \equiv 1 \pmod m$. Nazywamy wtedy x - odwrotnością a modulo m.

Wniosek 2 (Jednoznaczność)**.** Dla liczby pierwszej p i $a, b \in \mathbb{Z}$, $p \nmid a$, kongruencja $ax \equiv b \pmod p$ ma dokładnie jedno rozwiązanie ze zbioru $\{0, 1, \dots, p-1\}$.

Twierdzenie 3 (Małe twierdzenie Fermata)**.** *Dla dowolnej liczb całkowitej a oraz liczby pierwszej p, zachodzi*

$$p \mid a^p - a.$$

Twierdzenie 4 (Twierdzenie Wilsona)**.** *Niech $n > 1$ będzie liczbą całkowitą. Wówczas n jest liczbą pierwszą wtedy i tylko wtedy, gdy*

$$1 \cdot 2 \cdot \ldots \cdot (n-1) = (n-1)! \equiv -1 \pmod n.$$

Twierdzenie 5 (Chińskie twierdzenie o resztach)**.** *Niech $m_1, m_2, \dots, m_k > 1$ będą liczbami całkowitymi, parami względnie pierwszymi, a liczby $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Wówczas istnieje dokładnie jedno rozwiązanie ze zbioru $\{0, 1, \dots, M-1\}$, gdzie $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, spełniające układ kongruencji:*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv a_k \pmod{m_k}. \end{cases}$$

Przykłady

1. Udowodnij, że liczba $93^{93} - 33^{33}$ jest podzielna przez 10.
2. Dane są $m, n \in \mathbb{Z}_+$. Udowodnij, że $83 \mid 25m + 3n \iff 83 \mid 3m + 7n$
3. Rozwiąż układ kongruencji:
$$\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 6 \pmod 7, \\ x \equiv 6 \pmod 8, \\ x \equiv 6 \pmod 9. \end{cases}$$
4. Udowodnij, że dla liczb $a_1, a_2 \ldots, a_k \in \mathbb{Z}$ oraz liczby pierwszej p zachodzi
$$p \mid a_1^p + a_2^p + \ldots + a_k^p \iff p \mid a_1 + a_2 + \ldots + a_k.$$
5. Niech p jest liczbą pierwszą. Znajdź resztę z dzielenia liczby $(p-1)!$ przez $p(p-1)$.

Zadania

1. Znaleźć wszystkie liczby pierwsze p takie, że $4p^2 + 1$ oraz $6p^2 + 1$ też są pierwsze.
2. Niech $m, n, d \in \mathbb{Z}_+$, takie że $d|m^2n + 1$ oraz $d|mn^2 + 1$. Dowieść, że $d|m^3 + 1$ i $d|n^3 + 1$.
3. Dana jest liczba pierwsza p. Udowodnić, że istnieje taka liczba całkowita dodatnia n, że $2^n \equiv n \pmod p$.
4. Dane są liczby całkowite dodatnie a, b, c, d spełniające równanie $a^2 + 3ab + b^2 = c^2 + 3cd + d^2$. Udowodnij, że $a + b + c + d$ nie jest liczbą pierwszą.
5. Niech a i b będą dodatnimi liczbami całkowitymi oraz p, q różne liczby pierwsze takie, że $aq \equiv 1 \pmod p$ oraz $bp \equiv 1 \pmod q$. Udowodnij, że
$$\frac{a}{p} + \frac{b}{q} > 1.$$
6. Rozstrzygnij, czy istnieje pięć kolejnych liczb całkowitych dodatnich, których suma kwadratów jest kwadratem liczby całkowitej.
7. Dane są ciągi $a_1, a_2, \ldots, a_{p-1}$ i $b_1, b_2, \ldots, b_{p-1}$, które są permutacjami ciągu $1, 2, \ldots, p-1$, gdzie p jest liczbą pierwszą. Czy ciąg $a_1b_1, a_2, b_2, \ldots, a_{p-1}b_{p-1}$ też może być taką permutacją.
8. Dowieść, że istnieje 2022 kolejnych liczb całkowitych dodatnich, z których żadna nie jest pierwsza.
9. Wykazać, że istnieje 2022 kolejnych liczb całkowitych dodatnich, z których żadna nie jest potęgą liczby całkowitej o wykładniku co najmniej 2.
10. Niech $n \geqslant 3$ będzie liczbą całkowitą taką, że $4n+1$ jest liczbą pierwszą. Udowodnij, że $4n+1$ dzieli $n^{2n}-1$.
11. Udowodnij, że istnieje nieskończenie wiele liczb całkowitych $n > 1$ takich, że równanie
$$(x+1)^{n+1} - (x-1)^{n+1} = y^n$$
nie ma rozwiązań w liczbach całkowitych.
12. Udowodnij, że dla każdej liczby pierwszej p istnieje $n \in \mathbb{Z}_+$ taka, że
$$2^n + 3^n + 6^n \equiv 1 \pmod p.$$
13. Dana jest liczba pierwsza p w postaci $3k + 2$ ($k \in \mathbb{Z}_+$). Niech $a_k = k^2 + k + 1$, dla $k = 1, 2, \ldots, p-1$. Udowodnij, że
$$a_1 \cdot a_2 \cdot \ldots \cdot a_{p-1} \equiv 3 \pmod p.$$