Fermat, Euler i Rzędy

Antoni Łuczak

Obóz OMJ, 11.06.2024

1 Kongruencje

Definicja 1

Mówimy, że $a \equiv b \pmod{n}$ (*a przystaje do b modulo n*), jeśli liczby a oraz b dają taką samą resztę z dzielenia przez n.

Kongruencje można dodawać, odejmować, mnożyć, podnosić obustronnie do potęgi.

Ćwiczenie 1. Znajdź ostatnią cyfrę liczby 2024^{2024}.

Definicja 2

Mówimy, że b *jest odwrotnością a modulo n*, jeśli liczba $ab \equiv 1 \pmod{n}$. Liczba a posiada swoją odwrotność wtedy i tylko wtedy, gdy a i n są względnie pierwsze. Dodatkowo każda liczba ma co najwyżej jedną odwrotność w zbiorze $\{0, 1, \ldots, n-1\}$.

Ćwiczenie 2. Znajdź odwrotność liczby 25 modulo 2024.

Wniosek. Jeżeli $am \equiv bm \pmod{n}$ oraz liczby m i n są względnie pierwsze, to $a \equiv b \pmod{n}$.

2 Twierdzenie Eulera

Definicja 3

Niech $\varphi(n)$ oznacza liczbę dodatnich liczb całkowitych nie większych niż n, względnie pierwszych z n. Wtedy dla liczb względnie pierwszych a, b zachodzi $\varphi(ab) = \varphi(a)\varphi(b)$.

Ćwiczenie 3. Oblicz $\varphi(2024)$.

Ćwiczenie 4. Oblicz $\varphi(p^n)$, gdzie p jest liczba pierwszą, a n dodatnią liczbą całkowitą.

Wniosek. Jeżeli $p_1, p_2, \ldots, p_k$ to wszystkie liczby pierwsze w rozkładzie n, to

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Twierdzenie 1 (Twierdzenie Eulera)

Dane są względnie pierwsze dodatnie liczby całkowite a, n. Wtedy

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Wniosek (Małe Twierdzenie Fermata)**.** Dana jest liczba pierwsza p oraz liczba całkowita a. Wtedy

$$a^p \equiv a \pmod{p}$$

3 Zadania

Zadanie 1. Udowodnij, że liczba 2024^{2024} jest podzielna przez 15.

Zadanie 2. Niech a będzie liczbą względnie pierwszą z 10. Udowodnij, że liczby a^{2001}, a mają te same trzy ostatnie cyfry w zapisie dziesiętnym.

Zadanie 3. Liczba naturalna n nie jest podzielna przez kwadrat żadnej liczby całkowitej. Dodatkowo zachodzi następujący warunek: Jeżeli liczba pierwsza p dzieli n, to $p-1$ dzieli $n-1$. Udowodnij, że n dzieli $a^n - a$ dla dowolnej liczby całkowitej a.

Zadanie 4. Udowodnić, że liczba $2^{n!} - 1$ jest podzielna przez $n^2 - 1$ dla dowolnej liczby całkowitej $n > 1$.

Zadanie 5. Dana jest liczba pierwsza p i dodatnia liczba całkowita względnie pierwsza z $p!$. Udowodnij, że

$$p! \mid a^{(p-1)!} - 1.$$

Zadanie 6. Dana jest liczba pierwsza $p > 2$. Udowodnij, że istnieje nieskończenie wiele takich dodatnich liczb całkowitych n, że liczba $2^n - n$ jest podzielna przez p.

Zadanie 7. Udowodnij, że istnieje nieskończenie wiele dodatnich liczb całkowitych n, że n dzieli $a^{n-1} - a$ dla dowolnej liczby całkowitej a.

Zadanie 8. Dana jest nieparzysta liczba pierwsza p. Udowodnij, że istnieje taka nieujemna liczba całkowita n, że liczba

$$2^n + 3^n + 6^n - 1$$

jest podzielna przez p.

Zadanie 9. Dana jest nieparzysta liczba pierwsza p oraz liczba całkowita a. Udowodnij, że jeśli liczba $a^2 + 1$ jest podzielna przez p, to liczba $p - 1$ jest podzielna przez 4.

Zadanie 10. Rozwiąż w liczbach całkowitych (x, y) równanie

$$2^x + 17 = y^4$$

4 Rzędy

Definicja 4

Rzędem liczby a modulo n nazywamy taką najmniejszą dodatnią liczbę całkowitą m, że $a^m \equiv 1 \pmod{n}$. Stosujemy wtedy oznaczenie $m = \mathrm{ord}_n(a)$.

Wnioski:

1. Jeżeli $a^k \equiv 1 \pmod{n}$, to $\mathrm{ord}_n(a) \mid k$.
2. $\mathrm{ord}_n(a) \mid \varphi(n)$.
3. Jeżeli $a^k \equiv a^l \equiv 1 \pmod{n}$, to $a^{\mathrm{NWD}(k,l)} \equiv 1 \pmod{n}$.

5 Zadania z rzędów

Zadanie 11. Znajdź wszystkie takie liczby dodatnie liczby całkowite n, że

$$n \mid 2^n - 1$$

Zadanie 12. Znajdź wszystkie takie dodatnie liczby całkowite n, że

$$n^2 \mid 3^n + 1.$$

Zadanie 13. Dana jest liczba pierwsza p. Udowodnij, że wszystkie dzielniki pierwsze liczby $2^p - 1$ są większe niż p.

Zadanie 14. Znajdź wszystkie trójki liczb całkowitych dodatnich, dla których zachodzą następujące podzielności:

$$a \mid 2^b - 1,\ b \mid 2^c - 1,\ c \mid 2^a - 1.$$