Analiza - klasa 2a Zestaw 11. 28.11.2024

Teoria liczb VI

Definicja. Niech $a, n \in \mathbb{N}$ i $\text{NWD}(a, n) = 1$. *Rzędem liczby a modulo n* nazywamy liczbę

$$\text{ord}_n(a) = \min\{k \in \mathbb{N} : a^k \equiv 1 \pmod{n}\}.$$

Z małego tw. Fermata wynika, że jeśli n jest liczbą pierwszą, to $\text{ord}_n(a)$ jest dobrze zdefiniowaną liczbą.

Funkcja Eulera: $\varphi(n)$ oznacza liczbę dzielników naturalnych nie większych od n i względnie pierwszych z n.

Lemat 1. Niech $m, n \in \mathbb{N}$, $\text{NWD}(m, n) = 1$, $c \in \mathbb{Z}$ i $A_n = \{0, 1, 2, \ldots, n-1\}$. Dla $k \in A_n$ niech r_k oznacza resztę z dzielenia liczby $km + c$ przez n. Wówczas $\{r_0, r_1, \ldots, r_{n-1}\} = A_n$.

Uwaga. Każdy układ liczb całkowitych $(x_1, x_2, \ldots, x_n)$ takich, że $x_i \not\equiv x_j \pmod{n}$ dla $i \neq j$ jest nazywany *pełnym układem reszt* modulo n

Tw. 1. Jeżeli $m, n \in \mathbb{N}$ i $\text{NWD}(m, n) = 1$, to $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Tw. 2. Niech $n \in \mathbb{N}$, $n > 1$ i $p_1, p_2, \ldots, p_k$ to wszystkie dzielniki pierwsze liczby n. Wówczas

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

Lemat 2. Niech $a, n \in \mathbb{N}$, $\text{NWD}(a, n) = 1$ i

$$R_n = \{r \in \mathbb{N} : r \leqslant n \text{ i } \text{NWD}(r, n) = 1\} = \{r_1, r_2, \ldots, r_{\varphi(n)}\},$$

gdzie $1 = r_1 < r_x < \ldots < r_{\varphi(n)} < n$. Dla każdej z liczb r_k niech s_k oznacza resztę z dzielenia liczby $a \cdot r_k$ przez n. Wówczas $\{s_1, s_2, \ldots, s_{\varphi(n)}\} = R_n$.

Uwaga. Każdy układ liczb całkowitych $(x_1, x_2, \ldots, x_{\varphi(n)})$, gdzie $x_i \not\equiv x_j \pmod{n}$ dla $i \neq j$ oraz $x_i \equiv r \pmod{n}$ dla pewnego $r \in R_n$ dla każdego i, nazywany jest *zredukowanym układem reszt* modulo n.

Tw. Eulera. Jeżeli $a, n \in \mathbb{N}$ i $\text{NWD}(a, n) = 1$, to

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

Tw. Wilsona. Jeżeli p jest liczbą pierwszą, to

$$(p-1)! \equiv -1 \pmod{p}.$$

Definicja. Niech $p \in \mathbb{P}$, $n \in \mathbb{N}$ i $\nu_p(n)$ oznacza największy wykładnik k taki, że $p^k \mid n$. Liczbę $\nu_p(n)$ nazywamy *wykładnikiem p-adycznym* liczby n.

Tw. (Wzór Legendre'a) Jeżeli p jest liczbą pierwszą i $n \in \mathbb{N}$, to

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots.$$

1. Liczba p jest pierwsza, $a, m \in \mathbb{N}$, $\text{NWD}(a, p) = 1$ i $a^m \equiv 1 \pmod{p}$. Udowodnij, że $\text{ord}_n(a) \mid m$.

2. Liczba p jest pierwsza, $a, m, n \in \mathbb{N}$, $\text{NWD}(a, p) = 1$ i $a^m \equiv a^n \equiv 1 \pmod{p}$. Udowodnij, że $a^{\text{NWD}(m,n)} \equiv 1 \pmod{p}$.

3. Niech $a, n \in \mathbb{N}$, $n \geqslant 2$ i $p > 2$ jest liczbą pierwszą taką, że $a^p \equiv 1 \pmod{p^n}$. Udowodnij, że $a \equiv 1 \pmod{p^{n-1}}$.

4. Dla jakich $n \in \mathbb{N}$ liczba $\varphi(n)$ jest nieparzysta?

5. Znajdź wszystkie liczby naturalne n takie, że (a) $\varphi(n) = 10$, (b) $\varphi(n) = 14$.

6. Dla jakich liczb naturalnych n spełniona jest równość $\varphi(n) = \varphi(2n)$?

7. Wyznacz wszystkie liczby naturalne n takie, że $\varphi(2n) = n$.

8. Niech $d, n \in \mathbb{N}$ i $d \mid n$. Wykaż, że $\varphi(d) \mid \varphi(n)$.

9. Niech $n \in \mathbb{N}$. Udowodnij, że $n = \sum_{d \mid n} \varphi(d)$.

10. Wyznacz resztę z dzielenia liczby 2024^{2024} przez 57.

11. Niech $n \in \mathbb{N}$. Wyznacz resztę z dzielenia liczby 3^{2^n} przez 2^n.

12. Liczby $a, b \in \mathbb{N}$ są względnie pierwsze. Pokaż, że istnieją $m, n \in \mathbb{N}$ takie, że

$$a^m + b^n \equiv 1 \pmod{ab}.$$

13. Niech $n \in \mathbb{N}$ i $2 \mid n$. Udowodnij, że $n^2 - 1 \mid 2^{n!} - 1$.

14. Udowodnij, że $n \nmid 2^n - 1$ dla każdej liczby naturalnej $n > 1$.

15. Niech $n \in \mathbb{N}$ i $n > 1$. Udowodnij, że $n \mid 1^n + 2^n + \ldots + (n-1)^n$ wtedy i tylko wtedy, gdy n jest liczbą nieparzystą.

16. Liczba $p > 2$ jest pierwsza. Wyznacz resztę z dzielenia liczby $(p-1)!$ przez $p(p-1)$.

17. Niech $a, n \in \mathbb{N}$, $n \geqslant 2$ i $\text{NWD}(a, n) = 1$. Udowodnij, że

$$a^{n-1} + (n-1)! \equiv 0 \pmod{n}$$

wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

18. Liczba $p > 2$ jest pierwsza i $n < p$ jest liczbą naturalną. Udowodnij, że $(n-1)! \cdot (p-n)! \equiv (-1)^n \pmod{p}$.

19. Niech $n \in \mathbb{N}$. Udowodnij, że 2^n nie dzieli $n!$, ale 2^n dzieli $(2n)!/n!$.

20. Wyznacz wszystkie liczby naturalne n takie, że $2^{n-1} \mid n!$.

21. Dla jakich liczb naturalnych n liczba $\binom{2n}{n}$ jest podzielna przez 4?

22. Udowodnij, że dla dowolnych $n, m \in \mathbb{N}$ liczby

$$\frac{(2n)! \cdot (2m)!}{n! \cdot m! \cdot (n+m)!} \quad \text{i} \quad \frac{(mn)!}{m! \cdot (n!)^m}$$

są całkowite.