Teoria liczb: NWD, Euklides, Euler

Tymoteusz Kucharek, Igor Staszkiewicz, Jerzy Szempliński

25 października 2022

1 Teoria

Wszystkie definicje potrzebne na kółko:

1. Liczba p jest pierwsza, wtedy, gdy nie istnieje żadna mniejsza liczba (oprócz 1), która by ją dzieliła.
2. $NWD(a, b)$ - największy wspólny dzielnik a i b. Nazwa mówi sama za siebie
3. Jeżeli a i b są względnie pierwsze $(a \perp b) \iff NWD(a, b) = 1$
4. Funkcja Eulera $\varphi(n)$ to liczba liczb x ze zbioru $1, 2, 3, ..., n-1$ takich, że $x \perp n$.
5. Dla liczb całkowitych a, b, $a \equiv b \pmod m \iff m \mid (a - b)$.

1.1 Podstawowe twierdzenie arytmetyki

Każda liczba ma jednoznaczny rozkład na liczby pierwsze. Dowód nie mieści się na marginesie

1.2 Algorytm Euklidesa

Mając dane dwie liczby a i b, mamy zadaną równość $NWD(a, b) = NWD(a - b, b)$. Możemy zatem zmniejszać większą z liczb tak długo, aż mniejsza z nich stanie się równa 0. W ten sposób jesteśmy w stanie "szybko" znaleźć NWD dwóch dowolnych liczb a i b.

Ćwiczenie na rozgrzewkę: Udowodnij, że dla każdej pary a, b gdzie $a \perp b$, istnieją takie całkowite liczby c i d, że $ac + bd = 1$.

Ćwiczenie z gwiazdką: Określ, jak szybko działa algorytm Euklidesa.

1.3 Twierdzenia Eulera

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

Dowód. Mając dany zbiór wszystkich liczb względnie pierwszych z n, przemnażamy każdy jego element przez a. Wówczas uzyskamy nadal ten sam zbiór (ćwiczenie dla czytelnika). Iloczyn wszystkich elementów z tych zbiorów jest taki sam, a iloczyn pierwotnych elementów jest względnie pierwszy z n, czyli a podniesione to potęgi $\varphi(n)$ musi byc równe 1. □

Ćwiczenie na rozgrzewkę: Znajdź dwie ostatnie cyfry liczby $2137^{13^{100}}$

2 Zadansy

1. Jeżeli p jest pierwsze, to dla $1 < k < p$ zachodzi $p \mid \binom{p}{k}$.
2. Znajdź wszystkie takie liczby pierwsze p, takie że $6p^2 + 1$ i $4p^2 + 1$ też są pierwsze.
3. Udowodnij, że dla $a \perp b$, zachodzi $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.
4. Udowodnij, że dla $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_k^{\alpha_k}$, zachodzi $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot (1 - \frac{1}{p_3}) \cdot ... \cdot (1 - \frac{1}{p_k})$.
5. Wykaż, że dla każdego naturalnego n $\sum_{d|n} \varphi(d) = n$.
6. Jeśli x, y są całkowite, to $29 \mid 10x + y \iff 29 \mid x + 3y$.

7. Mając dany odcinek na płaszczyźnie, którego jeden koniec to początek układu współrzędnych, a drugi ma współrzędne (x, y), policz ile punktów kratowych zawiera się w tym odcinku.

8. Wiedząc, że $6a \equiv 19 \pmod{107}$, oblicz jaka jest reszta z dzielenia a przez 107.

9. Pokaż, że dla każdej nieparzystej liczby n zachodzi $n \mid 2^{(n-1)!} - 1$.

10. (LXXIII OM, I etap, zadanie 9) Udowodnij, że dla dowolnej liczby pierwszej p istnieje nieskończenie wiele liczb n, takich że $p \mid 2^{3^n} - n$.

11. (LIV OM, II etap, zadanie 1) Znajdź wszystkie liczby pierwsze dla których $11 \mid 2^p + 3^p$.

12. (LXIV OM, III etap, zadanie 2) Udowodnij, że dla a, b takich że $a \neq 0$, oraz $6a \mid 3+a+b^2 \implies a < 0$.

13. (LXVI OM, III etap, zadanie 6) Wykaż, że dla każdej liczby naturalnej a istnieje taka liczba całkowita $b > a$, że liczba $1 + 2^b + 3^b$ dzieli sie przez $1 + 2^a + 3^a$.

14. (Twierdzenie Sylvestera) Dane są dwie względnie pierwsze dodatnie licby całkowite a, b. Rozważmy wszystkie liczby n, takie że n nie da się zapisać jako $n = ax + by$ dla pewnych nieujemnych x, y. Udowodnij, że takich liczb jest dokładnie $\frac{1}{2}(a-1)(b-1)$, zaś największą z nich jest $ab - a - b$.

15. Dane są dodatnie, względnie pierwsze liczby $a > b$. Udowodnij, że ciąg $c_n = a^n - b^n$ jest NWD-ciągiem, tj. $NWD(c_i, c_j) = c_{NWD(c_i,c_j)}$.

16. (LXVIII OM, 3 etap) Dane jest n liczb całkowitych, spełniających nierówność $1 < a_1 < .. < a_n < 2a_1$. Udowodnij, że $(a_1 \cdot ... \cdot a_n)^{n-1} \geq (n!)^m$, gdzie m to liczba różnych dzielników pierwszych iloczynu $a_1 \cdot ... \cdot a_n$.

17. (Rumuńskie TST 2019) Dane jest całkowite $k \geq 2$ i takie liby całkowite dodatnie $n_1, n_2, ..n_k$, że $n_i | 2^{n_{i-1}} - 1$ dla $2 \leq i \leq k$ oraz $n_1 | 2^{n_k} - 1$. Udowodnij, że $n_i = 1$ dla wszystkich $1 \leq i \leq n$.