Autor: Jan Piotrowicz
Prowadzący: Jan Piotrowicz

Teoria liczb – II etap

Teoria

Reszty z dzielenia

Jeśli a jest dzielnikiem b, to piszemy $a \mid b$ (czytamy: a dzieli b). Zatem:

$$a \mid b \text{ wtedy i tylko wtedy, gdy istnieje liczba } c \text{ taka, że } \quad b = ac.$$

Jeśli a nie jest dzielnikiem b, to piszemy $a \nmid b$ (czytamy: a nie dzieli b).

Załóżmy, że dane są liczby całkowite a i b, przy czym $b > 0$. Mówimy, że liczba a daje iloraz q i resztę r przy dzieleniu przez b, jeśli

$$a = b \cdot q + r \quad \text{oraz} \quad 0 \leqslant r < b.$$

Stwierdzenie 1. Jeśli a, b są dodatnie i $a \mid b$, to $a \leqslant b$.

Stwierdzenie 2. Jedyną liczbą podzielną przez wszystkie liczby naturalne jest 0.

Uwaga 1 (Sztuczka z przedstawianiem liczb w innej formie)**.** Jak przedstawić inaczej liczbę o n takich samych cyfrach? Zauważmy, że $10^n - 1$ to liczba składająca się z n dziewiątek, więc zachodzi:

$$\underbrace{kkk\ldots k}_{n \text{ cyfr } k} = \frac{10^n - 1}{9} \cdot k.$$

Kongruencje

Załóżmy, że dana jest liczba całkowita dodatnia n. Mówimy, że dwie liczby całkowite a i b przystają modulo n wtedy i tylko wtedy, gdy liczby a i b dają takie same reszty przy dzieleniu przez n. Piszemy wówczas $a \equiv b \pmod{n}$. Inaczej mówiąc

$$a \equiv b \pmod{n} \text{ wtedy i tylko wtedy, gdy } \quad n \mid a - b.$$

Dodawanie, mnożenie i odejmowanie modulo n zachowuje się tak jak byśmy chcieli, czyli:

$$a \pmod{n} + b \pmod{n} \equiv_n (a + b) \pmod{n},$$

$$a \pmod{n} \cdot b \pmod{n} \equiv_n ab \pmod{n}.$$

Dzielenie modulo n mamy ogólnie tylko wtedy gdy n jest liczbą pierwszą. Oczywiście dalej nie mamy dzielenia przez 0, czyli nie możemy dzielić przez liczby podzielne przez n.

Odwrotność liczby a modulo n to taka liczba b, że $ab \equiv_n 1$. Ta liczba b istnieje wtedy i tylko wtedy gdy $a \perp n$ i wtedy oznaczamy ją a^{-1} lub $\frac{1}{a}$.

Autor: Jan Piotrowicz

Prowadzący: Jan Piotrowicz

Liczby pierwsze

Definicja 1. Liczbę naturalną różną od jedynki, której jedynimi dzielnikami są 1 oraz ona sama, nazywamy **liczbą pierwszą**.

Każda liczba może być przedstawiona jako iloczyn liczb pierwszych (jednoznaczność tego rozkładu można udowodnić korzystając z następnych lematów). Liczb pierwszych jest nieskończenie wiele co udowodnić można rozważając $p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$.

Lemat 1. Liczby pierwsze większe od 3 przystają do 1 lub 5 mod 6.

NWD

Definicja 2 (Największy Wspólny Dzielnik)**.** Mówimy, że $d = NWD(a, b)$ jeśli $d \mid a$ i $d \mid b$ (czyli jest wspólnym dzielnikiem) oraz dla każdego wspólnego dzielnika e liczb a i b, $e|d$ (czyli każdy wspólny dzielnik dzieli NWD).

$NWD(a, b)$ jest najmniejszą dodatnią liczbą postaci $ax + by$ dla x, y całkowitych (inaczej mówiąc jest ich najmniejszą kombinacją liniową). Można udowodnić, że ta definicja daje nam to samo NWD, co definicja szkolna.

Definicja 3. Liczby naturalne a i b są **względnie pierwsze**, gdy $NWD(a, b) = 1$, co zapisujemy: $a \perp b$.

Lemaciki (oznaczenia: p jest liczbą pierwszą a n, a, b są liczbami całkowitymi):

- Jeśli $a \perp n$ i $n \mid ab$ to $n \mid b$.
- Jeśli $p \nmid a$ to $a \perp p$.
- Jeśli $p \mid ab$ to $p \mid a$ lub $p \mid b$.

Lemat 2. Jeśli dana jest permutacja σ_i liczb od 0 do $n-1$ oraz liczba p, która jest względnie pierwsza z n ($p \perp n$), to po przemnożeniu każdego elementu permutacji przez p ($\sigma'_i = p \cdot \sigma_i$) i wzięciu reszty z dzielenia przez n, otrzymujemy nową permutację liczb od 0 do $n-1$.

Dowód. Wystarczy pokazać, że każda z liczb, po przemnożeniu, trafia na inną. Jeśli byłoby inaczej, to znaczy, że jakieś dwie liczby $\sigma_i, \sigma_j < n$ takie, że:

$$p \cdot (\sigma_i - \sigma_j) \equiv 0 \pmod{n}$$

Skoro $p \perp n$, to $\sigma_i - \sigma_j \equiv 0 \pmod{n}$, czyli $\sigma_i = \sigma_j$. ■

Twierdzenie 1 (Algorytm Euklidesa)**.** Możemy znaleźć NWD bez rozkładania liczb na czynniki pierwsze (w szczególności nawet nie trzeba wiedzieć czym jest liczba pierwsza) wielokrotnie wykorzystując zależności $NWD(a, b) = NWD(a - kb, b)$. Można też, odwracając ten algorytm, uzyskać NWD jako kombinację liniową a i b.

Ważne twierdzenia

Twierdzenie 2 (Małe twierdzenie Fermata)**.** Dla dowolnej liczby naturalnej n oraz dowolnej liczby pierwszej p zachodzi

$$p \mid n^p - n,$$

czyli w języku kongruencji

$$n^p \equiv n \pmod{p}.$$

Dowód. Dzielimy koło na p części i rozważamy możliwe kolorowania n rożnymi kolorami. Wszystkich kolorowań jest n^p, takich które są jednokolorowe (wszystkie części koła są pomalowane jednym kolorem) jest n.
Pozostałe możemy pogrupować w zbiory po p - jeśli jakieś kolorowanie można uzyskać poprzez obrót innego to te dwa należą do tej samej grupy.

Pokażemy, że każda grupa ma dokładnie p kolorowań: załóżmy nie wprost, że po obrocie jakiegoś kolorowania o k fragmentów ($0 \leqslant k < n$), dostaliśmy takie samo kolorowanie. Ponieważ p jest pierwsze, to $p \perp k$, to żeby jakiś fragment wrócił do początkowej pozycji, musimy wykonać p obrotów, czyli każdy fragment koła ma ten sam kolor, czyli dostajemy sprzeczność. ■

Twierdzenie 3 (twierdzenie Willsona)**.** p jest pierwsza wtedy i tylko wtedy, gdy

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

Dowód. Rozważamy w Z_p równanie $x^2 = 1$. Liczby spełniające to równanie to takie, które same są swoją własną odwrotnością. Ma ono tylko dwa rozwiązania: $x = 1$ i $x = -1$, przy czym $-1 \equiv p - 1$. Z tego wynika, że wszystkie liczby z przedziału [2, p-1] mają swoją odwrotność w tym przedziale. Możemy zatem każdą z nich sparować z jakąś inną liczbą z tego przedziału, więc jeśli wymnożymy je wszystkie, to iloczyn będzie przystawał do 1: $(p-2)! \equiv 1 \pmod{p}$. Po pomnożeniu przez $p-1$ otrzymujemy tezę. ■

Twierdzenie 4 (Chińskie Twierdzenie o Resztach)**.** Niech $m_1, m_2, ..., m_k$ będą parami względnie pierwsze i niech $a_1, a_2, ..., a_k$ będą liczbami całkowitymi. Wtedy układ kongruencji:

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

Jest równoważny z pewną kongruencją postaci $x \equiv A \pmod{m_1 m_2 ... m_k}$

Technika: **Nieskończone schodzenie**
Ta metoda polega na wzięciu (w wybranym przez siebie kontekście) rozwiązania najmniejszego i pokazaniu, że istnieje mniejsze.

Przykład 1. Znajdź wszystkie całkowite, dodatnie rozwiązania równania

$$x^3 + 2y^3 = 4z^3$$

Rozwiązanie 1. Weźmy jedno z rozwiązań, dla którego suma $x + y + z$ jest najmniejsza. Skoro:

$$2y^3 \equiv 0 \pmod 2,$$
$$4z^3 \equiv 0 \pmod 2,$$

to x również musi dzielić się przez 2.
Podstawmy do równania $x' = x/2$ i dzielimy przez 2, mamy:

$$4x'^3 + y^3 = 2z^3$$

Operację możemy powtórzyć jeszcze dwa razy, otrymując równanie tej samej postaci, co na początku.
Dostajemy sprzeczność, bo liczby x, y, z miały być najmniejsze, spełniające równaznie. Zatem nie ma ono rozwiązań.

Przykład 2. Znajdź wszystkie takie liczby całkowite nieujemne a, b, że $ab \mid a^n + b$, gdzie $n \in \mathbb{N}_{>1}$ jest stałe

Rozwiązanie 2. Zauważamy, że a i b mają ten sam zbiór dzielników, oraz że $a = 1$ wtw. gdy $b = 1$. Przyjmijmy więc, że $a, b > 1$ i rozpatrzmy dwójkę o najmniejszej sumie. Niech $p \in \mathbb{P}$ będzie pewną liczbą pierwszą dzielącą a oraz b. Wtedy $p^2 \mid a^n + b$, z czego wprost wynika, że $p^2 \mid b$. Powtarzamy ten trik do momentu, gdy $p^n \mid b$. Niech $a = pa_1$ oraz $b = p^n b_1$. Wtedy

$$a_1 b_1 p^n \mid ab_1 p^n \mid p^n(a_1^n + b_1) \implies a_1 b_1 \mid a_1^n + b_1$$

Wobec minimalności a, b widzimy, że $a_1 = b_1 = 1$, z czego wprost wynika, że $a = p$ oraz $b = p^n$. Podstawiając to do oryginalnej podzielności widzimy, że $p^{n+1} \mid 2p^n \implies p = 2$.

Wykładniki p-adyczne

- Rozkład na czynniki pierwsze to silny sposób żeby patrzeć na liczby. Pomagać nam w tym będą wykładniki p-adyczne. Jak p jest liczbą pierwszą to wykładnik p-adyczny z liczby n to po prostu liczba razy ile p pojawia się w rozkładzie n na czynniki pierwsze. Oznaczamy go $v_p(n)$.
- $p^{v_p(n)} \mid n$ ale już $p^{v_p(n)+1} \nmid n$.
- $a \mid b$ jest równoważne temu, że dla każdej liczby pierwszej p, $v_p(a) \leqslant v_p(b)$
- $a = b$ jest równoważne temu, że dla każdej liczby pierwszej p, zachodzi $v_p(a) = v_p(b)$
- $v_p(ab) = v_p(a) + v_p(b)$
- $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$. W ten sposób możemy też z łatwością rozszerzyć definicję wykładników p-adycznych na liczby wymierne.
- Gdy $v_p(a) \neq v_p(b)$, to $v_p(a + b) = \min(v_p(a), v_p(b))$.

Autor: Jan Piotrowicz

Prowadzący: Jan Piotrowicz

Na rozgrzewkę

1. Wykaż poniższe własności kongruencji.
   - Jeśli $a \equiv b \pmod{m}$, to $b \equiv a \pmod{m}$.
   - Jeśli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $b \equiv a \pmod{m}$.
   - $a \equiv b \pmod{m}$ wtedy i tylko wtedy, gdy $ac \equiv bc \pmod{mc}$.
   - Jeśli $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$, to $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, $ac \equiv bd \pmod{m}$.
2. Pokaż, że jeśli $p \nmid n$, to $n^{p-1} \equiv 1 \pmod{p}$.
3. Przedstaw $\underbrace{222\ldots2}_{2024}\underbrace{444\ldots4}_{2024}$ jako sumę dwóch wyrażeń (jak w sztuczce).

Zadania

1. Dla jakich naturalnych n ułamek $\frac{21n+4}{14n+3}$ jest nieskracalny?
2. Znaleźć ostatnią cyfrę liczby $2023^{2024^{2025}}$.
3. Udowodnij, że $F_n \perp F_{n+1}$ dla każdego naturalnego n, gdzie F_n to n-ta liczba Fibonacciego. To jest $F_0 = 0$, $F_1 = 1$ oraz dla $n > 1$ rekurencyjnie definiujemy $F_n = F_{n-1} + F_{n-2}$.
4. Czy istnieje 1000 kolejnych liczb naturalnych takich, że dokładnie 5 z nich jest liczbą pierwszą?
5. Czy liczba $4^6 + 4 \cdot 6^5 + 9^5$ jest złożona?
6. Znajdź zasady podzielności przez 11 oraz 101. Znajdź zasadę podzielności przez 7, wiedząc, że $7 \mid 1001$.
7. Wybrano $n + 1$ liczb że zbioru $\{1,\ 2,\ 3,\ \ldots 2n\}$. Udowodnij, że pewne dwie z nich są względnie pierwsze.
8. Udowodnij, że istnieje nieskończenie wiele liczb pierwszych dających resztę 3 modulo 4. Czy ten sam dowód zadziała jeśli będziemy rozważali liczby pierwsze postaci $4k + 1$ dla naturalnych k?
9. Udowodnij, że dla n naturalnego i k nieparzystego
$$1 + 2 + 3 + \cdots + n \mid 1^k + 2^k + 3^k + \cdots + n^k$$
10. *VII OM* Dowieść, że równanie $2x^2 - 215y^2 = 1$ nie ma rozwiązań w liczbach całkowitych.
11. Udowodnij, że każda liczba całkowita n spełnia podzielność: $120 \mid n^5 - 5n^3 + 4n$
12. Znajdź wszystkie takie liczby całkowite k, że dla każdej liczby naturalnej n, zachodzi $n \mid (n-1)^k + 1$
13. Udowodnij, że istnieje nieskończenie wiele liczb pierwszych, które są postaci $\sqrt{24n+1}$ dla pewnej liczby naturalnej n.

14. Czy istnieje nieskończony (niestały) ciąg arytmetyczny złożony wyłącznie z liczb pierwszych?

15. Trójkąt prostokątny ma przyprostokątne długości a, b i przeciwprostokątną długości c. Udowodnij, że jeśli a, b, c są liczbami całkowitymi, to co najmniej jedna z liczb a, b musi być parzysta.

16. Znajdź liczbę dzielników liczby $16 \cdot 27 \cdot 49 \cdot 19$. Znajdź sumę dzielników tej liczby.

17. Udowodnij, że jeśli dla liczb naturalnych a, b, c, d, e zachodzi $9 \mid a^3 + b^3 + c^3 + d^3 + e^3$, to $3 \mid abcde$

18. Udowodnij, że dla dowolnych liczb naturalnych $a_1, a_2, ..., a_n$, które spełniają $NWD(a_1, a_2, ..., a_n) = 1$, istnieją takie liczby całkowite $k_1, k_2, ..., k_n$, że

$$k_1a_1 + k_2a_2 + ... + k_na_n = 1$$

19. Niech a będzie dowolną liczbą naturalną. Udowodnij, że wśród liczb $a, a+1, a+2, ..., a+9$, istnieje jedna, która jest względnie pierwsza że wszystkimi pozostałymi.

20. Znając $v_p(a), v_p(b)$, oblicz $v_p(NWD(a, b))$ oraz $v_p(NWW(a, b))$.

21. Udowodnij:

$$\frac{NWW(a,b)NWW(b,c)NWW(c,a)}{NWW(a,b,c)^2} = \frac{NWD(a,b)NWD(b,c)NWD(c,a)}{NWD(a,b,c)^2}$$

22. Mamy takie liczby całkowite a, b, że liczba $\frac{a^2}{b} + \frac{b^2}{a}$ jest całkowita. Udowodnij że liczby $\frac{a^2}{b}$ i $\frac{b^2}{a}$ są całkowite.

23. Udowodnij, że dla naturalnych m i n

$$NWD(a^m - 1,\ a^n - 1) = a^{NWD(m,\,n)} - 1$$

24. Udowodnij, że dla każdej liczby naturalnej n liczba $2^{2^n} - 1$ ma co najmniej n różnych dzielników pierwszych

25. *II OM* Dowieść, że jeśli n jest liczbą naturalną parzystą, to liczba $13^n + 6$ jest podzielna przez 7.

26. *IV OM* Dowieść, że liczba $2^{55} + 1$ jest podzielna przez 11.

27. Wyznacz resztę z dzielenia liczby $3^{81} + 7^{72}$ przez 11.

28. Udowodnij, że ostatnią cyfrą liczby 7^{256} jest 1.

29. Udowodnij, że $7 \mid 2222^{5555} + 5555^{2222}$.

30. Znajdź dwie ostatnie cyfry liczby 2^{999}.

31. Udowodnij, że $29 \mid 2^{5n+1} + 3^{n+3}$ dla dowolnej liczby naturalnej n.

32. *VI OM* Znajdź ostatnią cyfrę liczby $53^{53} - 33^{33}$.

33. Pokaż, że liczba $1\underbrace{000\ldots0}_{2013}1$ jest złożona.

34. Udowodnij, że $F_n \mid F_{nk}$ dla każdych naturalnych n oraz k.

35. Udowodnij, że różne liczby Fermata, czyli liczby postaci $G_n = 2^{2^n} + 1$, są względnie pierwsze.

36. Znajdź wzór na $v_p(n!)$

37. Liczby naturalne a, b spełniają warunek: Dla każdej liczby naturalnej n, zachodzi $a^n \mid b^{n+1}$. Udowodnij, że $a \mid b$.

38. Udowodnij, że dla każdej liczby naturalnej n, zachodzi podzielność $(n!)^{(n-1)!} \mid (n!)!$

39. (OM 75, etap 2) Niech p będzie liczbą pierwszą. Udowodnić, że liczba $p(p^2 \cdot \frac{p^{p-1}-1}{p-1})!$ jest podzielna przez $p! \cdot (p^2)! \cdot (p^3)! \cdot \ldots \cdot (p^p)!$.