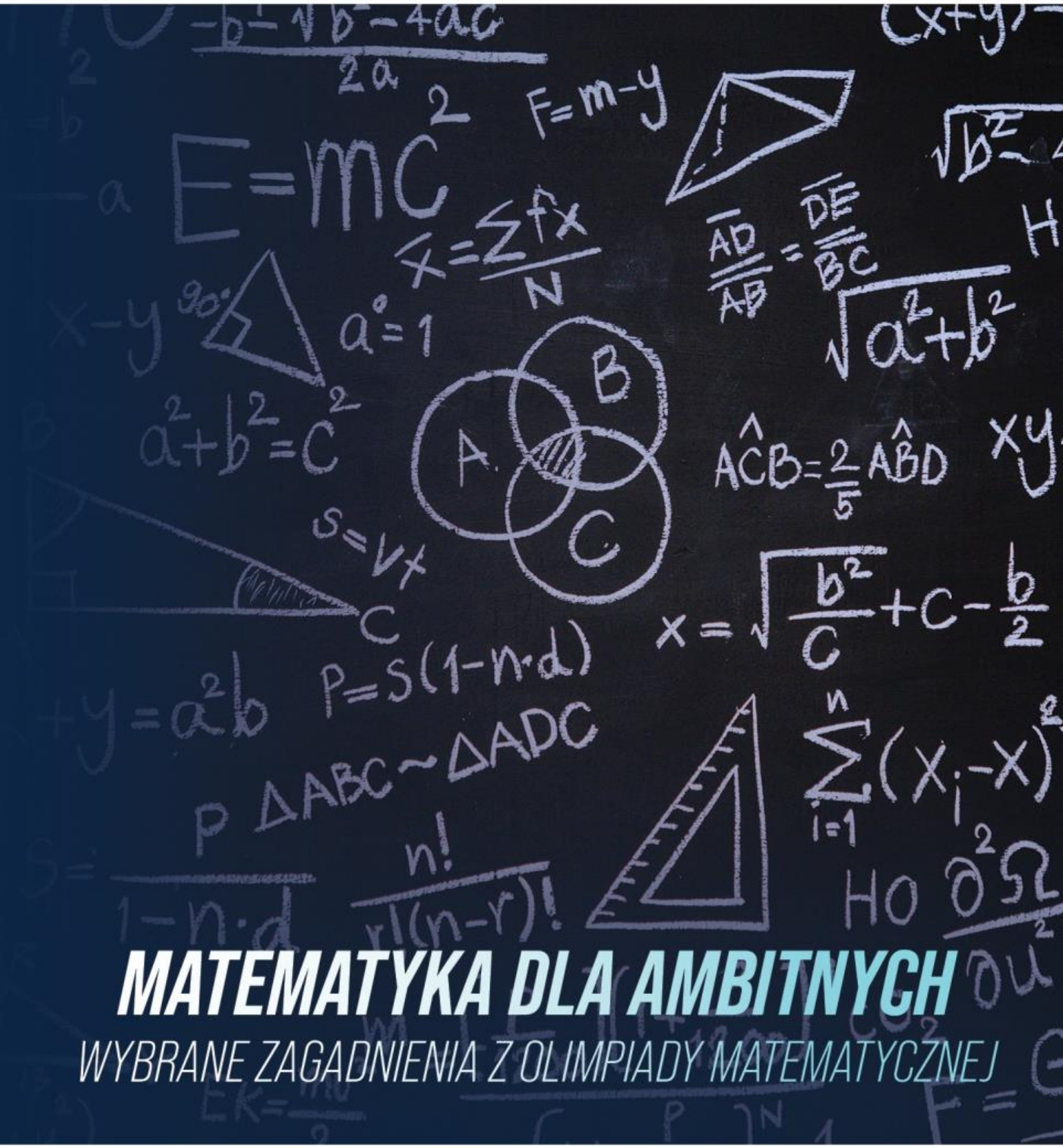
INDEKS W KIESZENI



MATEMATYKA DLA AMBITNYCH

WYBRANE ZAGADNIENIA Z OLIMPIADY MATEMATYCZNEJ

PIOTR WOJTALA

INDEKS W KIESZENI

PIOTR WOJTALA

Matematyka dla ambitnych

Wybrane zagadnienia
z Olimpiady Matematycznej

WARSZAWA 2024

Wydanie I

Autor: Piotr Wojtala

Projekt graficzny okładki: Justyna Książek

ISBN: 978-83-68290-06-6

Wydawnictwo Indeks w Kieszeni

IWK MAT sp. z o.o.

www.indekswkieszeni.pl

1

Teoria liczb

Omówimy tutaj podstawy teorii liczb, czyli działu dotyczącego liczb całkowitych.

1.1 Oznaczenia i własności kongruencji

Oznaczenia:

- $a|b$ — liczba a jest dzielnikiem liczby b;
- $NWD(a, b)$ — największy wspólny dzielnik liczb a, b;
- $NWW(a, b)$ — najmniejsza wspólna wielokrotność liczb a, b;
- $a \perp b$ — liczby a i b są względnie pierwsze, czyli ich NWD jest równe 1;
- $a \equiv b \pmod{n}$ — liczby a oraz b dają tę samą resztę z dzielenia przez n. Inaczej mówiąc, jest to równoważne temu, że $n|a - b$.

Własności kongruencji:

- $a \equiv a \pmod{n}$;
- jeśli $a \equiv b \pmod{n}$, to $b \equiv a \pmod{n}$;
- $a \equiv a + n \pmod{n}$;
- $a \equiv a - n \pmod{n}$;
- jeśli $a \equiv b \pmod{n}$ oraz $b \equiv c \pmod{n}$, to $a \equiv c \pmod{n}$;
- jeśli $a \equiv b \pmod{n}$ oraz $m|n$, to $a \equiv b \pmod{m}$;
- $a \equiv b \pmod{n}$ wtedy i tylko wtedy, gdy $ac \equiv bc \pmod{mc}$;
- jeśli $m \perp n$, $a \equiv b \pmod{m}$ oraz $a \equiv b \pmod{n}$, to $a \equiv b \pmod{mn}$;

- jeśli $a \equiv c \pmod{n}$ oraz $b \equiv d \pmod{n}$, to:
  $a + b \equiv c + d \pmod{n}$;
  $a - b \equiv c - d \pmod{n}$;
  $ab \equiv cd \pmod{n}$;
- jeśli $a \equiv b \pmod{n}$, to $a^k \equiv b^k \pmod{n}$;
- jeśli $ak \equiv bk \pmod{n}$ oraz $k \perp n$, to $a \equiv b \pmod{n}$.

1.2 Podstawowe fakty

- jeśli $c|ab$ oraz $c \perp a$, to $c|b$;
- $NWD(a,b) \cdot NWW(a,b) = a \cdot b$;
- $NWD(a,b) = NWD(a, b-a)$;
- jeśli p jest liczbą pierwszą, zaś $a, b \in \mathbb{Z}$, to $p|ab \Rightarrow (p|a \vee p|b)$;
- liczb pierwszych jest nieskończenie wiele;
- rozkład na czynniki pierwsze liczby całkowitej dodatniej jest jednoznaczny.

1.3 Funkcja Eulera

- $\phi(n)$ - liczba liczb całkowitych dodatnich mniejszych od n oraz względnie pierwszych z n. Funkcję tę nazywamy funkcją Eulera;
- jeśli p jest pierwsze, to $\phi(p) = p - 1$;
- jeśli p jest pierwsze, k całkowite, to $\phi(p^k) = (p-1)p^{k-1}$;
- jeśli $a \perp b$, to $\phi(ab) = \phi(a) \cdot \phi(b)$;
- dla liczby całkowitej dodatniej n dany jest jej rozkład na czynniki pierwsze: $n = p_1^{q_1} \cdot p_2^{q_2} \cdot ... \cdot p_k^{q_k}$. Wtedy $\phi(n) = (p_1 - 1)p_1^{q_1 - 1} \cdot (p_2 - 1)^{q_2 - 1} \cdot ... \cdot (p_k - 1)^{q_k - 1}$.

1.4 Twierdzenia

Rozszerzony algorytm Euklidesa

Poniżej opisany jest wniosek z rzeczonego algorytmu.

Dla liczb całkowitych nieujemnych a, b istnieją takie liczby całkowite x, y, że $NWD(a, b) = ax + by$.

Dowód:

Skorzystamy z algorytmu Euklidesa, który wyznacza $NWD(a, b)$ i przebiega następująco[1]:

- porządkujemy liczby a, b tak, by $a \leq b$;
- jeśli $a = 0$, to b jest szukaną liczbą;
- szukamy $NWD(a, b - a)$ za pomocą algorytmu Euklidesa.

Oczywiście powyższy algorytm musi zakończyć się po skończonej liczbie rekurencyjnych wykonań, bowiem wraz z każdym z nich suma argumentów się zmniejsza, chyba że jeden z tych argumentów jest zerem, bo wtedy następuje ostatni krok algorytmu. Co więcej, ponieważ $NWD(a, b) = NWD(a, b - a)$, to w każdym rekurencyjnym wykonaniu algorytmu NWD argumentów jest takie samo. Zatem gdy na końcu otrzymujemy parę $(d, 0)$, liczba d jest szukanym NWD.

Kolejną warta odnotowania obserwacja mówi nam, że w każdym kroku algorytmu Euklidesa argumenty są kombinacjami liniowymi początkowych liczb a, b nad liczbami całkowitymi[2]: ponieważ oczywiście para (a, b) jest kombinacją liniową a, b, zatem na samym początku ta własność jest spełniona. Niech po którymś kroku algorytmu aktualne argumenty będą kombinacjami liniowymi a, b przyjmującymi wartości odpowiednio $x_1a + y_1b$, $x_2a + y_2b$. Wtedy $(x_1a + y_1b) - (x_2a + y_2b) = (x_1 - x_2)a + (y_1 - y_2)b$, co jest kombinacją liniową liczb a, b.

Zatem wynik algorytmu jest kombinacją liniową liczb a, b, toteż istnieją liczby całkowite t.ż. $NWD(a, b) = ax + by$.

Właściwy algorytm Euklidesa pozwala wyznaczyć parę x, y. Powyżej opisano wyłącznie dowód wniosku o istnieniu tych liczb. W zadaniach olimpijskich zazwyczaj nie jest konieczne wskazanie explicite x, y, wystarczające bywa tylko powołanie się na ich istnienie.

---

[1] ponieważ $NWD(0, 0)$ jest niezdefiniowane, przyjmujemy, że przynajmniej jedna z liczb a, b nie jest zerem

[2] mówimy, że c jest kombinacją liniową nad liczbami całkowitymi liczb naturalnych a, b, gdy istnieją liczby całkowite x, y takie, że $c = ax + by$

Lemat o generowaniu reszt

Dane są liczby całkowite dodatnie a, b, n, przy czym $a \perp n$. Wśród liczb $a+b, 2a+b, 3a+b, \ldots, na+b$ mamy wszystkie możliwe reszty modulo n.

Dowód:

Przypuśćmy nie wprost, że wśród liczb $a+b, 2a+b, 3a+b, \ldots, na+b$ są dwie dające tę samą resztę z dzielenia przez n, czyli istnieją liczby k, l t. ż. $0 < k-l < n$ oraz $ka+b \equiv la+b \mod n$. Zatem $n|a(k-l)$. Ponieważ $a \perp n$, to $n|k-l$. Ale $0 < k-l < n$, co daje sprzeczność.

Odwrotność modulo p

Dla liczby pierwszej p oraz każdej liczby całkowitej k, takiej że $0 < k < p$, istnieje dokładnie jedna liczba całkowita l, $0 < l < p$, taka że $kl \equiv 1$ modulo p . Liczbę l nazywamy wtedy odwrotnością k mod p, możemy napisać $l \equiv \frac{1}{k} \mod p$ lub $l \equiv k^{-1}$ modulo p; definiuje nam to operację dzielenia w ciele $\mathbb{Z}_p$. Dodatkowo wyłącznie 1 oraz $p-1$ są same dla siebie odwrotnościami.

Wersja ogólniejsza: jeśli $k \perp n$ (n nie musi być pierwsze), to k ma dokładnie jedną odwrotność mod n.

Dowód:

Niech $kl_1 \equiv kl_2 \equiv n \mod n$. Wtedy $n|k(l_1 - l_2)$. Zatem skoro $n \perp k$, mamy $n|l_1 - l_1$, toteż $l_1 \equiv l_2 \mod n$.

Twierdzenie Wilsona

Liczba p jest pierwsza wtedy i tylko wtedy, gdy $p|(p-1)!+1$.

Wykazanie tego faktu jest ciekawym zadaniem, zatem warto spróbować zrobić to samodzielnie, zanim zdecydujesz się na lekturę poniższego dowodu.

Dowód:

Niech p będzie liczbą pierwszą. Wtedy każda wśród liczb $1, 2, ..., p-1$ posiada swoją odwrotność mod p. Co więcej, tylko 1 oraz $p-1$ są same dla siebie odwrotnościami. Zatem liczby $2, 3, ..., p-2$ można dobrać w pary tak, że iloczyn liczb w każdej parze daje resztę 1 mod p. Zatem $(p-1)! \equiv 1 \cdot (-1) \equiv -1 \mod p$. Zatem $p|(p-1)!+1$.

W drugą stronę, niech $p|(p-1)!+1$. Przypuśćmy, że p nie jest pierwsza. Wtedy posiada jakiś dzielnik pierwszy $d < p$. Toteż $d|(p-1)!$. A skoro $d|p$ i $p|(p-1)!+1$, to $d|(p-1)!+1$. Przeto $d|(p-1)!+1-(p-1)! = 1$, co daje sprzeczność.

Chińskie twierdzenie o resztach

Liczby całkowite $p_1, p_2, \ldots p_n$ są parami względnie pierwsze, $a_1, a_2, \ldots a_n$ są całkowite. Wówczas istnieje dokładnie jedno rozwiązanie modulo $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ układu kongruencji

$$x \equiv a_i \bmod p_i$$

dla $i \in \{1, 2, \ldots n\}$.

Małe twierdzenie Fermata

Dla dowolnego $a \in \mathbb{Z}$ oraz dla dowolnego $p \in \mathbb{P}$ zachodzi $p|a^p - a$. Jeżeli ponadto $p \perp a$, to $p|a^{p-1} - 1$.

Uogólnienie — twierdzenie Eulera: jeśli $a \perp n$, to $a^{\phi(n)} \equiv 1 \pmod{n}$

1.5 Zadania

1. Czy istnieją takie liczby całkowite a i b, że liczby $a^2 + b$ oraz $a + b^2$ są kolejnymi liczbami całkowitymi?

2. Dowieść, że istnieje $2024^{2024^{2024}}$ kolejnych liczb naturalnych, z których każda jest podzielna przez co najmniej $2024^{2024^{2024}}$ liczb pierwszych.

3. Niech $n \in \mathbb{N}$. Udowodnij, że $3^{2^n} + 1$ jest podzielne przez 2, ale nie przez 4.

4. Znaleźć resztę z dzielenia $3^{105} + 4^{105}$ przez 11.

5. Pokaż, że dla każdego $n \in \mathbb{N}$ kongruencja $6x^2 + 5x + 1 \equiv 0 \pmod{n}$ ma rozwiązanie.

6. Dane są liczby naturalne a, b takie, że liczba $\frac{a+1}{b} + \frac{b+1}{a}$ jest całkowita. Udowodnij, że
$$NWD(a, b) \leq \sqrt{a + b}.$$

7. Niech $n, m \in \mathbb{Z}_+$ będą takie, że $NWW(m, n) + NWD(m, n) = m + n$. Udowodnij, że jedna z tych liczb dzieli drugą.

8. Znajdź wszystkie liczby całkowite dodatnie x, y takie, że $7^x - 3^y = 4$.

9. Udowodnij, że jeśli n jest dodatnią liczbą całkowitą, to liczba $2(n^2 + 1) - n$ nie jest kwadratem liczby całkowitej.

10. Udowodnij, że jeśli liczba pierwsza p jest postaci $4k+3$, to co najmniej jedna z liczb $(2k + 1)! + 1$, $(2k + 1)! - 1$ jest podzielna przez p.

11. Dana jest liczba pierwsza $p > 2$. Niech S będzie zbiorem $p + 1$ liczb całkowitych. Wykazać, że istnieją parami różne liczby $a_1, a_2, \ldots, a_{p-1}$, należące do zbioru S, dla których liczba $a_1+2a_2+3a_3+...+(p-1)a_{p-1}$ jest podzielna przez p.

12. Rozstrzygnąć, czy można wpisać w pola nieskończonej szachownicy liczby całkowite dodatnie tak, aby suma liczb wpisanych w każdy prostokąt $m \times n$, gdzie $m, n > 2024$, była podzielna przez $m + n$.

13. Na tablicy napisana jest permutacja ciągu $(1, 2, \ldots, k+n)$, gdzie $k \perp n$. W jednym ruchu możemy zamienić liczby różniące się o k lub o n. Pokazać, ze można otrzymać ciąg $(1, 2, \ldots, k + n)$.

14. Udowodnić, że dla dowolnej dodatniej liczby całkowitej n zachodzi

$$n!|(2^n - 2^0)(2^n - 2^1)(2^n - 2^2)...(2^n - 2^{n-1}).$$

W niniejszej książce omówionych zostało kilka podstawowych zagadnień przydatnych na **Olimpiadzie Matematycznej**. Znaleźć można w niej **wachlarz rozmaitych technik oraz twierdzeń** z zakresu geometrii, teorii liczb, kombinatoryki i algebry, których opanowanie jest dobrym wprowadzeniem do skutecznych zmagań z zadaniami olimpijskimi.

Każdy temat został opatrzony **zestawem pouczających ćwiczeń o różnym poziomie trudności wraz z przykładowymi rozwiązaniami**. Zachęcamy do lektury publikacji zarówno uczestników rozpoczynających przygotowania do Olimpiady, a więc dopiero budujących bazę narzędzi matematycznych, jak i bardziej zaawansowanych, pragnących podszlifować swoje umiejętności.

Wydawnictwo INDEKS W KIESZENI

Warszawa 2024
ISBN: 978-83-68290-06-6