Markowe
Wykłady
z **M**atematyki

Markowe Wykłady z Matematyki

teoria liczb

Marek Zakrzewski

Projekt okładki
Andrzej Krupa

Skład komputerowy książki w systemie LaTeX wykonał autor.
Rysunki wykonał Marian Gewert.

ISBN 978–83–62780–49–5

Wydanie I, Wrocław 2017
Oficyna Wydawnicza GiS, s.c., www.gis.wroc.pl
Druk i oprawa: I-BiS Usługi Komputerowe - Wydawnictwo s.c.

Pan [Joseph] Fourier uważał, że głównym celem nauki jest społeczna użyteczność i objaśnianie zjawisk przyrody; ale taki filozof jak on powinien był wiedzieć, że jedynym celem nauki jest honor ludzkiego umysłu, dlatego kwestie dotyczące liczb są równie ważne, co kwestie dotyczące systemu świata.

Carl Gustav Jacobi, z listu do A.M. Legendre'a, 2 VII 1830

Wielu ludzi wciąż ma fałszywe przekonanie, że wszystko, co w matematyce ważne zostało już odkryte, a matematyka jest interesująca jedynie ze względu na jej zastosowania w nauce i technice.

Avner Ash, Robert Gross, z przedmowy do
Fearless symmetry, Princeton University Press 2006

Spis treści

Wstęp

Matematyka jest królową nauk, a teoria liczb królową matematyki.

Carl Friedrich Gauss

[Teoria liczb] naprawdę zaczyna się od 1, 2, 3, 4, 5, ... i nie możesz być ani zbyt młody, ani zbyt stary, by cieszyć się tą cudowną historią.

John J. Watkins, *Number Theory*
Princeton University Press 2014

Książka może służyć jako podstawowy podręcznik dla semestralnego kursu teorii liczb. Znaczna część materiału jest też dostępna dla ambitniejszego ucznia starszych klas szkoły średniej.

Czym się zajmuje teoria liczb ...

Elementarna teoria liczb zajmuje się liczbami naturalnymi. Na poziomie bardziej zaawansowanym zajmuje się też innymi rodzajami liczb: wymiernymi, algebraicznymi itd.

Przyglądając się liczbom naturalnym można odkryć mnóstwo ciekawych prawidłowości i postawić wiele niebanalnych pytań. Proste obserwacje na poziomie starszych klas szkoły podstawowej mogą doprowadzić do odkrycia, że każda liczba parzysta większa od 2 jest prawdopodobnie sumą dwu liczb pierwszych (hipoteza Goldbacha, 1742), czy przypuszczenia, że istnieje nieskończenie wiele par liczb pierwszych różniących się o 2 (hipoteza liczb bliźniaczych, V-IV w. p.n.e.). Do dziś (IX 2017) żaden z tych dwu problemów nie został rozwiązany, choć w ostatnich latach osiągnięty tu został znaczny postęp.

. . . i po co się jej uczymy?

Pisząc tę książkę długo zastanawiałem się, po co uczymy się teorii liczb. Oczywiście, część osób uczy się jej ze względu na zastosowania w kryptografii. Ale rzadko kiedy jest to jedyna motywacja.

Na wykładach analizy matematycznej student poznaje *metody* analizy, czasem także ciekawe wyniki uzyskane za pomocą tych metod. Na wykładach algebry — *metody* algebry, z rzadka jakieś zastosowania. Teoria liczb jest zupełnie inna. Składa się z prostych, intrygujących pytań o otaczający nas świat liczb i zdumiewająco wyrafinowanych odpowiedzi na nie, z użyciem metod analizy, algebry abstrakcyjnej i liniowej, czasem metod kombinatorycznych i geometrycznych. Teoria liczb w idealny sposób **łączy prostotę pytań z bogactwem metod**. Na tym polega jej urok.

Wykłady z teorii liczb mogą być dla studenta matematyki czy informatyki pierwszą okazją, aby zobaczyć, jak bardzo kręta bywa droga od prostego pytania do zadowalającej odpowiedzi. Przy okazji zdobywa pierwsze motywacje, aby studiować zagadnienia bardziej abstrakcyjne.

Początki teorii liczb sięgają Babilończyków (ok. 1500 lat p.n.e.), znaczące wyniki uzyskano w Grecji i świecie hellenistycznym (V w. p.n.e. - III w. n.e.). Nowożytna jej historia zaczyna się od Fermata (XVII w.). Począwszy od XVIII w. teoria liczb staje się stopniowo siłą napędową m.in. dla analizy, algebry abstrakcyjnej i geometrii algebraicznej. Dwa spośród siedmiu problemów milenijnych[1] dotyczą teorii liczb.

Ogólna konstrukcja

Książka składa się z pięciu części. Część pierwsza jest rodzajem elementarza teorii liczb. Korzystamy z niej niemal we wszystkich wykładach. Dalsze części są w zasadzie niezależne.

Trudniejsze części wykładów, nie mające wpływu na dalszą lekturę, zaznaczono gwiazdką.

[1]Problemy milenijne to zestaw siedmiu problemów matematyki, w tym hipotezy Riemanna (wiąże się z rozmieszczeniem liczb pierwszych) oraz Bircha i Swinnertona-Dyera (dotyczy krzywych eliptycznych). Od roku 2000 Instytut Matematyczny Claya za rozwiązanie każdego z tych problemów oferuje nagrodę w wysokości miliona dolarów. Dotychczas rozwiązano tylko jeden z tych siedmiu problemów — hipotezę Poincarego. Udowodnił ją w roku 2002 Grigorij Perelman, ale nagrody nie przyjął.

Poziom trudności i rola zadań

Początkowe zadania po każdym podrozdziale — do miejsca oznaczonego symbolem trzech kar — mają w zasadzie charakter rachunkowy. Czytelnik powinien rozwiązywać większość z nich, aby mieć pewność, że rozumie materiał. Dalsze zadania mają charakter bardziej twórczy, czasem podejmują zagadnienia tylko luźno związane z głównym tekstem.

Zachęcamy Czytelnika, aby rozwiązywał przynajmniej część spośród tych dalszych zadań. Nawet sama próba rozwiązania bywa kształcąca. Odpowiedzi bądź wskazówki do znacznej części zadań znaleźć można na końcu książki.

Nauka czysta czy stosowana?

W ostatnim półwieczu teoria liczb znalazła zastosowania, przede wszystkim w kryptografii, zyskując w ten sposób status *matematyki stosowanej*. Dla przeciętnego użytkownika algorytmów teorii liczb ważne jest, że algorytm działa — nie musi pytać dlaczego.

Ale najnowsze zastosowania teorii liczb nie mogą przysłonić faktu, że jest ona przede wszystkim *matematyką czystą*. Za pomocą komputera sprawdzono, że wspomniana wyżej hipoteza Goldbacha jest prawdziwa dla liczb naturalnych poniżej $4{\cdot}10^{17}$, a z czasem ta granica będzie się przesuwać. Matematycy zapewne wierzą, że jest tak też dla większych liczb, ale w gruncie rzeczy interesuje ich wyłącznie, jak zdobyć w tej materii *absolutną pewność*, a także *zrozumieć dlaczego* ta hipoteza jest prawdziwa. Stąd wybitna rola wszelkich rozumowań.

Dowody, czyli wyjaśnienia

W przypadku mocno nieoczywistych twierdzeń, pytanie *skąd to wiadomo* jest naturalną na nie reakcją. Odpowiedzią jest dowód, albo przynajmniej szkic dowodu. Szkic dowodu nie daje co prawda gwarancji, że twierdzenie jest prawdziwe, ale zazwyczaj wyjaśnia, skąd to wiemy.

Wielu studentów ma skłonność do pomijania dowodów, a przynajmniej do ich lekceważenia. Powtórzę to, co napisałem we wstępie do *Matematyki dyskretnej*. Matematyka bez dowodów jest jak opera bez muzyki: można oczywiście ograniczyć się do śledzenia samej akcji, ale nikt w ten sposób opery nie polubił.

Biogramy i komentarze historyczne

Trudno sobie wyobrazić poważnego muzyka, który zupełnie nie ma pojęcia, kiedy żył Bach czy Mozart. Albo malarza, który nie słyszał o Rembrandcie.

Matematykę tworzą matematycy. Liczne biogramy i komentarze historyczne rozsiane po książce przypominają ten ludzki aspekt matematyki. Siłą rzeczy biogramy matematyków najbardziej wszechstronnych pojawiają się w różnych tomach serii. Staram się, aby w takich sytuacjach przynajmniej niektóre szczegóły wnosiły do portretu omawianego matematyka jakiś nowy rys.

Kilka uwag dla ambitniejszego licealisty

Uczeń starszych klas szkoły średniej, przy pewnym wyrobieniu matematycznym, może przebrnąć z pożytkiem przez większą część materiału. Przy pierwszej lekturze lepiej pominąć część rozumowań z wykładu 12, wykład 18 i krzywe eliptyczne, tzn. wykłady 22-24. Niewielkie braki z matematyki wyższej łatwo uzupełnić sięgając do *początkowej części* odpowiedniego hasła w Wikipedii czy Wolfram MathWorld.

Bardzo możliwe, że młodszy Czytelnik postąpi rozsądnie zaczynając od krótszego kursu (ok. 40-50 stron), jaki można znaleźć w mojej *Matematyce dyskretnej*.

Uwagi dla wykładowcy

Książka podzielona jest na 25 wykładów, ale niektóre (zwłaszcza 10. i 13.) są bardzo krótkie. Można przyjąć, że materiał odpowiada z grubsza ok. 20-22 wykładom. Oznacza to, że przy umiarkowanym tempie kilka wykładów trzeba pominąć. Kurs nastawiony na zastosowania można oprzeć na wykładach 1-9, 11-12, 14-16 plus wykład 22. Przy nastawieniu na matematykę czystą lepiej wybrać wykłady 1-6, 8-12, 14-15 i 19-22.

♢ ♢ ♢

Dziękuję moim Kolegom i Wydawcom: doc. dr. Zbyszkowi Skoczylasowi za szczegółowe przejrzenie tekstu i liczne sugestie oraz dr. Marianowi Gewertowi za przygotowanie rysunków i szereg uwag redakcyjnych.

M. Z.

I

Euklides, Fermat i kongruencje

Bóg stworzył liczby całkowite, wszystkie inne są dziełem człowieka.

Leopold Kronecker, wg Heinricha Webera

Każda liczba naturalna[2] jest sumą jedynek. Na przykład

$$7 = 1 + 1 + 1 + 1 + 1 + 1 + 1.$$

Z punktu widzenia dodawania jedynki stanowią podstawowe cegiełki, z których zbudowane są wszystkie liczby. Ale ograniczając się do dodawania, trudno o liczbach naturalnych powiedzieć coś ciekawego.

Inaczej jest, gdy przechodzimy do mnożenia. Tu funkcję podstawowych cegiełek pełnią **liczby pierwsze**. Każda liczba naturalna większa od 1 jest albo liczbą pierwszą, albo iloczynem liczb pierwszych. Na przykład

$$1\,001 = 7 \cdot 11 \cdot 13, \qquad 1\,111\,111 = 239 \cdot 4649.$$

Twierdzenie, że rozkład taki jest jednoznaczny jest jednym z fundamentów teorii liczb. Większość osób przyjmuje to za oczywiste. Dopiero Gauss, pod koniec XVIII w. odczuł tu potrzebę dowodu. Nie jest on oczywisty. Po drodze korzystamy z **algorytmu Euklidesa**, pierwszego interesującego algorytmu teorii liczb.

Już Euklides w III w. p.n.e. wiedział, że liczb pierwszych jest nieskończenie wiele. Chyba każdy dowód tego twierdzenia korzysta ze wspomnianej jednoznaczności rozkładu.

[2]Kronecker myślał zapewne wyłącznie o *dodatnich* liczbach całkowitych, gdyż zero i liczby ujemne pojawiły się tak późno — i mają tyle wad (np. nie można przez zero dzielić) — że wyraźnie wyglądają na dzieło człowieka. My również przyjmiemy, że liczby naturalne zaczynają sie od jedynki: 1, 2, 3... W teorii liczb jest to ogólnie przyjęte.

Kongruencje — wprowadzone przez Gaussa — to w zasadzie tylko sposób zapisu, ale będziemy przekonywać się wielokrotnie, że są one nadspodziewanie użyteczne. W języku kongruencji formułowane są niemal wszystkie najważniejsze twierdzenia wykładów 2-4, w tym **małe twierdzenie Fermata** i **chińskie twierdzenie o resztach**.

Arytmetyka kongruencji prowadzi do zainteresowania pierścieniami $\mathbb{Z}_n$. Ich podstawowe własności różnią się w zależności od tego, czy n jest liczbą pierwszą, czy złożoną. Gdy p jest liczba pierwszą, pierścień $\mathbb{Z}_p$ jest ciałem. Pokażemy, że w ciele $\mathbb{Z}_p$ istnieją **pierwiastki pierwotne**, tzn. elementy, których potęgi wyczerpują niezerowe elementy ciała.

Te cztery początkowe wykłady stanowią rodzaj elementarza teorii liczb. Nie ma tu jakiejś idei przewodniej, a żadne z twierdzeń nie jest szczególnie głębokie. Na razie szykujemy narzędzia.

Wykład 1

Liczby pierwsze

. . . postanowiłem ponumerować swoje rozdziały liczbami pierwszymi 2, 3, 5, 7, 11, 13 i tak dalej, ponieważ je lubię.

Mark Haddon, *Dziwny przypadek psa nocną porą*,
Świat Książki, 2003, przekł. Małgorzata Grabowska

Przypomnijmy, że liczba **pierwsza** to liczba, która ma tylko dwa dzielniki: 1 i samą siebie. Liczba **złożona** to liczba, która ma *więcej niż dwa* dzielniki. Zauważmy, że 1 nie jest ani liczbą pierwszą, ani złożoną.

Euklides (ok. 300 p.n.e.) kojarzony jest przede wszystkim z geometrią. Ale jego *Elementy* zawierają też dwa klasyczne wyniki teorii liczb, o których będzie mowa w tym wykładzie: jedno z najważniejszych twierdzeń i najsławniejszy algorytm.

1.1 Twierdzenie Euklidesa i sito Eratostenesa

Zasadnicze twierdzenie arytmetyki - Twierdzenie Euklidesa i sito Eratostenesa - Zadania

Około 2300 lat temu Euklides wykazał, że liczb pierwszych jest nieskończenie wiele, a niedługo potem Eratostenes pokazał, jak „wyłowić" wszystkie liczby pierwsze za pomocą algorytmu znanego dziś jako *sito Eratostenesa*.

Zasadnicze twierdzenie arytmetyki i twierdzenie Euklidesa

Twierdzenie 1.1 (zasadnicze twierdzenie arytmetyki)
Każda liczba naturalna większa od 1 jest albo liczbą pierwszą, albo iloczynem liczb pierwszych. Przedstawienie liczby naturalnej w postaci iloczynu liczb pierwszych jest jednoznaczne z dokładnością do porządku czynników.

Na przykład $600 = 2^3 \cdot 3 \cdot 5^2$. Przedstawienie takie nazywamy **rozkładem na czynniki pierwsze**. Gauss był chyba pierwszym matematykiem, który odczuł potrzebę dowodu, że rozkład jest jednoznaczny. Przez ponad 2000 lat twierdzenie uchodziło za oczywiste. Krótki dowód damy pod koniec wykładu. Ale już teraz skorzystamy z niego w dowodzie jednego z pierwszych głębokich twierdzeń teorii liczb.

Twierdzenie 1.2 (Euklides)
Liczb pierwszych jest nieskończenie wiele.

Znanych jest kilkanaście dowodów tego twierdzenia. Poniższy pochodzi zasadniczo z *Elementów*, choć jego forma jest mocno uwspółcześniona.

Dowód: Załóżmy, że jest tylko skończenie wiele liczb pierwszych: p_1, p_2, ..., p_k. Rozpatrzmy liczbę

$$n = p_1 p_2 ... p_k + 1.$$

Z zasadniczego twierdzenia arytmetyki wynika, że albo n jest sama liczbą pierwszą (oczywiście różną od wszystkich p_i), albo ma rozkład na czynniki pierwsze. Niech p będzie jednym z tych czynników. Ponieważ n przy dzieleniu przez którekolwiek p_i daje resztę 1, więc p jest różna od wszystkich p_i. Tak więc wykazaliśmy, że musi istnieć jeszcze jakaś liczba pierwsza, wbrew założeniu, że p_1, p_2, ..., p_k to *wszystkie* liczby pierwsze.

Sito Eratostenesa

Aby znaleźć wszystkie liczby pierwsze mniejsze od ustalonej liczby M, należy po prostu *odsiać* wszystkie złożone, i oczywiście jedynkę. Służy do tego **sito Eratostenesa**. Eratostenes był aleksandryjskim uczonym z III w. p.n.e. Dziś pamiętamy go przede wszystkim jako tego, który obliczył długość równika. Dla matematyków jest głównie odkrywcą *sita*.

Zasadę działania sita Eratostenesa wyjaśnimy na przykładzie. Wypiszmy wszystkie liczby naturalne od 2 do 45:

◇	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45

Pozostawmy 2 (jest liczbą pierwszą) i skreślmy wszystkie pozostałe parzyste, posuwając się krokiem co 2. Otrzymamy wówczas:

◇	**2**	3	◇	5	◇	7	◇	9	◇	11	◇	13	◇	15
◇	17	◇	19	◇	21	◇	23	◇	25	◇	27	◇	29	◇
31	◇	33	◇	35	◇	37	◇	39	◇	41	◇	43	◇	45

Najwcześniejszą liczbą nieskreśloną (oprócz oczywiście dwójki) jest 3. Pozostawmy ją — to kolejna liczba pierwsza — i skreślmy wszystkie krotności trójki, posuwając się krokiem co 3:

◇	**2**	**3**	◇	5	◇	7	◇	◇	◇	11	◇	13	◇	◇
◇	17	◇	19	◇	◇	◇	23	◇	25	◇	◇	◇	29	◇
31	◇	◇	◇	35	◇	37	◇	◇	◇	41	◇	43	◇	◇

Na tym etapie pozostawiamy 5 — kolejna liczba pierwsza, po czym, posuwając się krokiem co 5 skreślamy krotności 5:

◇	**2**	**3**	◇	**5**	◇	7	◇	◇	◇	11	◇	13	◇	◇
◇	17	◇	19	◇	◇	◇	23	◇	◇	◇	◇	◇	29	◇
31	◇	◇	◇	◇	◇	37	◇	◇	◇	41	◇	43	◇	◇

Zauważmy, że liczba złożona n musi mieć dzielnik mniejszy bądź równy $\sqrt{n}$. Jeśli bowiem $n = pq$, a czynnik $p > \sqrt{n}$, to $q < \sqrt{n}$. Dlatego przesiewanie kończymy, gdy osiągniemy $\sqrt{n}$. W tym przypadku opisany krok był już ostatnim, gdyż $7 > \sqrt{45}$. Efektem takiego przesiewania jest zatem lista:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.$$

Algorytm ten nie jest szczególnie praktyczny, ale pewne zaawansowane rozumowania współczesnej teorii liczb — na przykład tzw. *sito Selberga* — wciąż do tej prostej techniki nawiązują. Na szczęście problem znalezienia wszystkich liczb pierwszych z zadanego przedziału nie ma większego znaczenia praktycznego.

Zadania

1. Przedstaw w postaci iloczynu liczb pierwszych: a) 1001; b) 111 111; c) 11!.

2. Znajdź wszystkie liczby pierwsze pomiędzy 1000 a 1010. Korzystając z zad. 1a) możesz istotnie skrócić rachunki.

3. Po ilu iteracjach sita Eratostenesa otrzymamy wszystkie liczby pierwsze poniżej 1000?

$$\diamondsuit \diamondsuit \diamondsuit$$

4. Pokaż, że dla dowolnego n istnieje ciąg długości n kolejnych liczb złożonych.

5. Analizując dowód Euklidesa wykaż, że n-ta liczba pierwsza p_n spełnia nierówność

$$p_n < 2^{2^n}.$$

Wywnioskuj stąd, że poniżej 2^{2^n} jest przynajmniej $n+1$ liczb pierwszych.

6. Dokończ poniższy dowód Stieltjesa (1890) istnienia nieskończenie wielu liczb pierwszych.

"Załóżmy, że istnieje tylko skończenie wiele liczb pierwszych p_1, p_2, ..., p_n. Podzielmy ten zbiór na dwie niepuste części. Niech a będzie iloczynem liczb należących do jednej z tych części, b — drugiej. Rozważmy $m = a + b \ldots$"

7. Wykaż, że dla $n \geqslant 9$ liczba n-cyfrowa ma co najwyżej n różnych dzielników pierwszych.

8. Ile dzielników ma 10!? Ile spośród nich to liczby nieparzyste?

9. (Mersenne 1640) Znajdź liczbę dzielników liczby 49 000 i ich sumę, nie wypisując dzielników.

1.2 Algorytm Euklidesa i jego konsekwencje

Algorytm Euklidesa - Lemat Bezout - Lemat Euklidesa - Dowód zasadniczego twierdzenia arytmetyki - Zadania

Algorytm Euklidesa to szybki sposób znajdowania największego wspólnego dzielnika dwu liczb naturalnych. Ale jego zasadnicze znaczenie wynika z roli, jaką odgrywa w rozważaniach teoretycznych.

Algorytm Euklidesa

Przypomnijmy podstawowe określenia. Dla liczb naturalnych k, m:

$\mathrm{NWD}\,(k,m)$ — największy wspólny dzielnik liczb k, m,
$\mathrm{NWW}\,(k,m)$ — najmniejsza wspólna wielokrotność liczb k, m.

Na przykład $\mathrm{NWD}\,(15,24) = 3$, $\mathrm{NWD}\,(15,24) = 120$.

Liczby a, b, których jedynym (a więc też największym) wspólnym dzielnikiem jest 1, nazywamy **względnie pierwszymi**. Przykładem 15 i 49.

„Szkolny" algorytm wyznaczania największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności dwu liczb wykorzystuje rozkład obu liczb na czynniki pierwsze. Na przykład dla $2002 = 2 \cdot 7 \cdot 11 \cdot 13$, $1628 = 2^2 \cdot 11 \cdot 37$ mamy

$$\begin{aligned} \mathrm{NWD}\,(2002, 1628) &= 2 \cdot 11 = 22, \\ \mathrm{NWW}\,(2002, 1628) &= 2^2 \cdot 7 \cdot 11 \cdot 13 \cdot 37 = 148\,148. \end{aligned}$$

Zauważmy, że zachodzi, łatwy do wykazania (p. zad.12), związek

$$\mathrm{NWD}\,(k, m) \cdot \mathrm{NWW}\,(k, m) = km.$$

Wynika stąd, że gdy znamy jedną z wielkości $\mathrm{NWD}\,(k, m)$ bądź $\mathrm{NWW}\,(k, m)$, to bez trudu wyznaczymy też drugą.

Dla dużych liczb znalezienie rozkładu na czynniki pierwsze bywa bardzo trudne. Algorytm Euklidesa pozwala tę trudność obejść. Sprowadza on obliczanie największego wspólnego dzielnika do wielokrotnego *dzielenia z resztą*. W zbiorze liczb całkowitych wykonalne są dodawanie, odejmowanie i mnożenie. Dzielenie liczb całkowitych zazwyczaj wyprowadza poza ten zbiór. Przy dzieleniu z resztą wynik (dokładniej: obydwa wyniki) są liczbami całkowitymi. Na przykład, dzieląc 31 przez 7, otrzymujemy iloraz 4 i resztę 3:

$$31 : 7 = 4 \text{ reszta } 3, \quad \text{tzn.} \quad 31 = 4 \cdot 7 + 3.$$

Ogólnie, mówimy, że liczba całkowita n daje przy dzieleniu przez liczbę naturalną k iloraz q oraz resztę r, jeżeli

$$n = qk + r, \quad \text{przy czym } 0 \leqslant r \leqslant k - 1.$$

Zasadę działania algorytmu Euklidesa wyjaśnimy na przykładzie. Spójrzmy, jak za jego pomocą wyznaczyć $\mathrm{NWD}\,(2002, 1628)$:

$$\begin{aligned} 2002 : 1628 &= 1 \text{ reszta } 374 \\ 1628 : 374 &= 4 \text{ reszta } 132 \\ 374 : 132 &= 2 \text{ reszta } 110 \\ 132 : 110 &= 1 \text{ reszta } 22 \\ 110 : 22 &= 5 \text{ reszta } 0. \end{aligned}$$

Ostatnia niezerowa reszta — tutaj 22 — jest największym wspólnym dzielnikiem badanych liczb. Aby zrozumieć, *dlaczego* tak się dzieje, spójrzmy na inny zapis wykonywanych działań:

$$\begin{aligned} 2002 &= 1 \cdot 1628 + 374 \\ 1628 &= 4 \cdot 374 + 132 \\ 374 &= 2 \cdot 132 + 110 \\ 132 &= 1 \cdot 110 + 22 \\ 110 &= 5 \cdot 22 + 0. \end{aligned}$$

Z pierwszej równości wynika, że każdy dzielnik dwu spośród liczb 2002, 1628, 374 jest też dzielnikiem trzeciej, a stąd

$$\mathrm{NWD}\,(2002, 1628) = \mathrm{NWD}\,(1628, 374).$$

Podobnie

$$\mathrm{NWD}\,(1628, 374) = \mathrm{NWD}\,(374, 132) = \mathrm{NWD}\,(132, 110) = \mathrm{NWD}\,(110, 22).$$

A stąd $\mathrm{NWD}\,(2002, 1628) = \mathrm{NWD}\,(110, 22) = 22$.

Lemat Bézout

Spójrzmy jeszcze raz na rozważany przykład, ale tym razem rachunki będziemy prowadzić wstecz:

$$22 = 132 - 110 = 132 - (374 - 2 \cdot 132) = 3 \cdot 132 - 374 = 3(1628 - 4 \cdot 374) - 374 =$$

$$= 3 \cdot 1628 - 13 \cdot 374 = 3 \cdot 1628 - 13(2002 - 1628) = 14 \cdot 1628 + (-13) \cdot 2002.$$

Podobne rachunki można przeprowadzić dla dowolnej pary liczb całkowitych a, b. Zachodzi zatem następujące:

Twierdzenie 1.3 (lemat Bézout)
Niech d będzie największym wspólnym dzielnikiem liczb a, b. Wówczas istnieją liczby całkowite k, l takie, że

$$d = ka + lb.$$

Można wykazać, że prawie wszystkie krotności $\mathrm{NWD}\,(a, b)$ (tzn. wszystkie oprócz skończenie wielu) dadzą się przedstawić w postaci takiej kombinacji o współczynnikach całkowitych *nieujemnych*. Analogiczny lemat (wraz z tą uwagą) zachodzi też dla $\mathrm{NWD}\,(a_1, a_2, \ldots, a_n)$.

Lemat Euklidesa

Zauważmy, że choć 12 dzieli $6 \cdot 8$, to *nie jest prawdą*, że 12 dzieli 6 lub 8. Dla liczb pierwszych jest inaczej:

Twierdzenie 1.4 (lemat Euklidesa)
Jeżeli liczba pierwsza p dzieli iloczyn ab, to dzieli przynajmniej jeden z czynników. W szczególności, jeżeli p dzieli a^2, to dzieli także a.

Dowód: Załóżmy, że p dzieli ab, ale nie dzieli a. Wykażemy, że p dzieli b. Skoro p jest liczbą pierwszą nie dzielącą a, to NWD $(a, p) = 1$. Z lematu Bézout mamy zatem $1 = ka + lp$ dla pewnych liczb całkowitych k, l. Pomnóżmy obie strony równości przez b:

$$b = kab + lpb.$$

Z założenia p dzieli ab, a więc dzieli obydwa składniki, a w takim razie także ich sumę b.

Dowód zasadniczego twierdzenia arytmetyki

Mamy udowodnić, że dla dowolnej liczby naturalnej n rozkład na czynniki pierwsze istnieje i jest jedyny. Skorzystamy z zasady indukcji matematycznej.

Dowód istnienia: Dla $n = 2$ twierdzenie jest oczywiste. Załóżmy, że twierdzenie jest prawdziwe dla wszystkich liczb naturalnych od 1 do n włącznie. Pokażemy je dla $n + 1$. Gdy $n + 1$ jest liczbą pierwszą, to nie ma czego dowodzić. Załóżmy zatem, że $n + 1 = ab$, gdzie a, b liczby naturalne większe od 1.

Z założenia indukcyjnego

$$a = p_1 p_2 \dots p_k, \quad b = q_1 q_2 \dots q_m,$$

przy czym liczby p_i, q_i mogą się powtarzać. Stąd $ab = p_1 p_2 \dots p_k q_1 q_2 \dots q_m$.

Dowód jednoznaczności: Dla $n = 2$ twierdzenie jest oczywiste. Załóżmy, że zachodzi ono dla wszystkich liczb naturalnych od 1 do n włącznie. Rozważmy dwa rozkłady

$$n + 1 = p_1 p_2 \dots p_k = q_1 q_2 \dots q_m.$$

Pokażemy, że różnić się mogą tylko kolejnością czynników.

Skoro p_1 dzieli iloczyn $q_1 q_2 \dots q_m$, to z lematu Euklidesa p_1 dzieli któryś z czynników q_i. Zmieniając ich kolejność możemy przyjąć, że p_1 dzieli q_1. Ale q_1 jest liczbą pierwszą, więc $p_1 = q_1$. Z założenia indukcyjnego $(n + 1)/p_1 = (n + 1)/q_1$ ma rozkład jednoznaczny, a stąd to samo odnosi się do $n + 1$.

Niewymierność pierwiastków

Jedną z podstawowych konsekwencji zasadniczego twierdzenia arytmetyki jest poniższe:

TWIERDZENIE 1.5 *Jeżeli d nie jest kwadratem liczby naturalnej, to $\sqrt{d}$ jest liczbą niewymierną.*

DOWÓD: Możemy przyjąć, że każdy dzielnik pierwszy p liczby d występuje w rozkładzie d na czynniki w pierwszej potędze. Ewentualne wyższe potęgi można wyciągnąć przed pierwiastek, co nie wpłynie na wymierność/niewymierność rozważanej liczby.

Załóżmy, że $\sqrt{d}$ jest liczbą wymierną. Istnieją zatem liczby naturalne k, m takie, że

$$\sqrt{d} = \frac{k}{m}, \qquad \text{czyli} \qquad k^2 = dm^2.$$

Można przyjąć, że ułamek k/m jest nieskracalny.

Niech p będzie dzielnikiem pierwszym d. Skoro p dzieli dm^2, to na mocy zasadniczego twierdzenia arytmetyki dzieli też $k^2 = dm^2$, a więc także k. Zatem lewa strona ostatniej równości dzieli się przez p^2. Ponieważ w rozkładzie d na czynniki, p występuje w pierwszej potędze, więc p dzieli m. Tak więc p jest wspólnym dzielnikiem k, m, wbrew założeniu, że ułamek k/m jest nieskracalny. Otrzymana sprzeczność kończy dowód.

Zadania

10. Znajdź największy wspólny dzielnik liczb 2849 i 5291 za pomocą algorytmu:
a) „szkolnego"; b) Euklidesa.

11. Znajdź największy wspólny dzielnik podanej pary i przedstaw go jako kombinację całkowitych dwu liczb:

a) 1001 i 1331; b) 2849 i 5291; c) 12 345 i 123 456.

12. Zbadaj, czy są względnie pierwsze:

a) 2001, 3001; b) 12357, 75321; c) $2n+1$, $4n^2+1$; d) $(n+1)!+1$, $n!+1$.

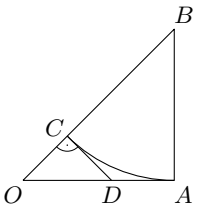
♢ ♢ ♢

13. Wykaż, że $\mathrm{NWD}\,(k,m) \cdot \mathrm{NWW}\,(k,m) = km$.

14. **Liczbami Fermata** nazywamy liczby postaci $F_n = 2^{2^n}+1$.
a) Wykaż, że $F_{n+1} = F_0F_1...F_n + 2$.
b) Uzasadnij, że liczby Fermata są parami względnie pierwsze.
c) Wyprowadź stąd kolejny dowód istnienia nieskończenie wielu liczb pierwszych.

15. W roku 2000 Tom Apostol przedstawił nowy dowód niewymierności $\sqrt{2}$.

Załóżmy, że $\sqrt{2} = p/q$, zatem $p^2 = q^2 + q^2$. Wynika stąd, że istnieje równoramienny trójkąt prostokątny o bokach całkowitych. Niech OAB będzie najmniejszym takim trójkątem.



Okrąg o środku B i promieniu AB przecina przeciwprostokątną w punkcie C. Styczna do okręgu poprowadzona w punkcie C przecina przyprostokątną w punkcie D.
a) uzasadnij, że odcinki CO i CD mają długość całkowitą;
b) to samo dla odcinka OD.
Wywnioskuj stąd sprzeczność z założeniem.

16. Gra Euklides
Dwu graczy na przemian wymienia liczbę naturalną większą od 1, przy czym nie można wymieniać liczb wcześniejszych ani ich sum. Przegrywa ten, kto nie może podać żadnej liczby spełniającej te warunki. Np. jeśli gracz rozpoczynający grę wymieni 4, a jego przeciwnik 5, to w kolejnym ruchu nie można już podać ani 4, ani 5, ani żadnej z liczb

$$8 = 4 + 4, \quad 9 = 4 + 5, \quad 10 = 5 + 5, \quad 12 = 4 + 4 + 4, \quad 13 = 4 + 4 + 5, \ \ldots$$

Pozostały tylko liczby 2, 3, 6, 7, 11, a więc gra po kilku ruchach się skończy.
a) Gracze rozpoczęli partię Euklidesa od liczb 4, 5, 11. Który z graczy ma w tym momencie strategię zwycięską?
b) Który z graczy ma strategię zwycięską, gdy gra zaczęła się od liczb 4, 6?
c)* Wykaż, że każda partia kończy się po skończonej liczbie ruchów.
Wsk. Niech

$$d_n = \mathrm{NWD}\,(a_1, a_2, \ldots, a_n),$$

gdzie $a_1, a_2, \ldots$ to liczby kolejno wymieniane przez graczy. Wykaż, że żaden wyraz tego ciągu nie może powtarzać się nieskończenie wiele razy.

1.3 Euklides

Żył na przełomie IV i III w. p.n.e. Urodził się prawdopodobnie w Aleksandrii, która w owym czasie była najważniejszym ośrodkiem naukowym na świecie. Poza tym niewiele o nim wiadomo, choć jego *Elementy* przez ponad 2000 lat były — po rozmaitych cięciach i uproszczeniach — podstawowym podręcznikiem geometrii wszędzie tam, gdzie docierała klasyczna cywilizacja grecka.

Elementy składają się z 13 ksiąg. W istocie tylko część dotyczy geometrii. Księgi V oraz VII-X poświęcone są arytmetyce, choć rozważania prowadzone są w języku geometrii: mówi się raczej o długościach odcinków niż o liczbach. Algorytm Euklidesa pojawia się w księdze VII, twierdzenie o istnieniu nieskończenie wielu liczb pierwszych w księdze IX.

Euklides jest też autorem ważnego traktatu o optyce i kilku innych dzieł poświęconych geometrii.

Wykład 2

Kongruencje i ich zastosowania

Kongruencje wprowadził do matematyki Gauss, w swym sławnym dziele *Disquisitiones arithmeticae* (1801). Rzadko się zdarza, by tak prosty pomysł dawał tak duże korzyści.

2.1 Kongruencje

Kongruencja jako równoważność - Arytmetyka kongruencji - Odwracalność i dzielenie kongruencji - Zadania

W arytmetyce zegarowej, gdzie np. $19 + 8 = 27 = 3$ (bo 8 godzin po godzinie dziewiętnastej jest godzina trzecia) operujemy wyłącznie resztami z dzielenia przez 24. Z kolei przy obliczaniu dnia tygodnia operujemy resztami z dzielenia przez 7. Wszędzie, gdzie operujemy resztami, wygodnym narzędziem są kongruencje.

Niech n będzie dowolną liczbą naturalną. Mówimy, że liczby całkowite a, b **przystają modulo** n, jeżeli ich różnica $a - b$ dzieli się przez n. Symbolicznie zapisujemy to tak:

$$a \equiv b \bmod n.$$

Zapis taki nazywamy **kongruencją**. Na przykład

$$7 \equiv 1 \bmod 3, \qquad 31 \equiv 11 \bmod 5, \qquad 9 \equiv -7 \bmod 4.$$

Kongruencja jako równoważność

Łatwo sprawdzić, że dla dowolnych liczb całkowitych a, b, c:

$$\begin{aligned} a &\equiv a \bmod n && \text{(zwrotność)},\\ a \equiv b \bmod n &\Longrightarrow b \equiv a \bmod n && \text{(symetria)},\\ (a \equiv b \bmod n \text{ i } b \equiv c \bmod n) &\Longrightarrow a \equiv c \bmod n && \text{(przechodniość)}. \end{aligned}$$

Oznacza to, że przy ustalonym n kongruencja modulo n jest relacją równoważności na zbiorze liczb całkowitych.

Arytmetyka kongruencji

Kongruencje można stronami dodawać, odejmować i mnożyć. Tak więc pod wieloma względami kongruencja przypomina równość.

Twierdzenie 2.1 *Jeżeli* $a \equiv b \mod n$ *oraz* $c \equiv d \mod n$, *to*

$$\begin{aligned} a + c &\equiv b + d \bmod n,\\ a - c &\equiv b - d \bmod n,\\ ac &\equiv bd \bmod n. \end{aligned}$$

Ponadto dla dowolnego naturalnego wykładnika k

$$a^k \equiv b^k \bmod n.$$

Dowód: Rozważmy najpierw dodawanie stronami. Należy pokazać, że jeśli $a - b$ oraz $c - d$ dzielą się przez n, to także $(a + c) - (b + d)$ dzieli się przez n. Ale

$$(a + c) - (b + d) = (a - b) + (c - d),$$

a suma liczb podzielnych przez n też dzieli się przez n.

Dla różnicy rachunki są niemal identyczne. W przypadku iloczynu stosowne przekształcenie różnicy $ac - bd$ wymaga pewnej pomysłowości:

$$ac - bd = ac - bc + bc - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d).$$

Dowód dla potęgowania otrzymujemy, k-krotnie mnożąc stronami kongruencję $a \equiv b \bmod n$.

Przykład 2.1 Znajdź ostatnią cyfrę liczby 2^{1000}.

Rozwiązanie: Ponieważ $2^5 = 32 \equiv 2 \bmod 10$, więc mnożąc obie strony tej kongruencji przez 2^{k-1} otrzymamy

$$2^{k+4} \equiv 2^k \bmod 10.$$

Zatem ostatnie cyfry 2^k powtarzają się w cyklu czteroelementowym. Ponieważ $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, więc dla k podzielnego przez 4 ostatnią cyfrą będzie 6.

W dalszym ciągu, mówiąc o kongruencjach będziemy czasem używali terminu **arytmetyka zegarowa** albo **modularna**. Zauważmy, że w arytmetyce modulo 24 używamy tylko liczb

$$0,\ 1,\ 2,\ \ldots, 23$$

i dość niekonsekwentnie 24, gdyż 24 i 0 oznaczają tę samą godzinę. Podobnie w arytmetyce modulo n używamy zasadniczo liczb 0, 1, 2, ..., $n-1$, ale czasem także n, równego w tej arytmetyce zeru. Zazwyczaj piszemy też -1 zamiast równoważnego zapisu $n-1$. Te drobne niekonsekwencje nie powinny tworzyć problemów.

W dalszym tekście $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ oznacza zbiór reszt modulo liczba pierwsza p. W ogólnym przypadku stosujemy symbol $\mathbb{Z}_n$.

Odwracalność i dzielenie kongruencji

Wiemy już, że kongruencje można dodawać, odejmować i mnożyć stronami. Pokażemy, że przy pewnych założeniach kongruencje można też stronami dzielić. Ponieważ *dzielenie* to mnożenie przez odwrotność, więc zacznijmy od kwestii, czy zawsze istnieje odwrotność.

Odwrotnością elementu a **modulo** n nazywamy taki element, oznaczany przez a^{-1}, że

$$aa^{-1} \equiv 1 \bmod n.$$

Zazwyczaj, gdy mówimy o odwrotności a zakładamy, że sam element a, jak też odwrotność, należą do zbioru 1, 2, ..., $n-1$. Na przykład odwrotnością liczby 3 modulo 10 jest 7, gdyż $3 \cdot 7 \equiv 1 \bmod 10$. Elementy 2, 5 (oraz oczywiście zero) odwrotności modulo 10 nie mają.

Zbiór elementów odwracalnych w $\mathbb{Z}_n$ oznaczamy symbolem $\mathbb{Z}_n^*$.

Twierdzenie 2.2 (kryterium odwracalności w arytmetyce zegarowej)
Liczba naturalna a jest odwracalna modulo n wtedy i tylko wtedy, gdy a oraz n są względnie pierwsze. W szczególności, dla liczby pierwszej p każdy niezerowy element $\mathbb{Z}_p$ jest odwracalny.

Dowód: Załóżmy, że a oraz n są względnie pierwsze. Na mocy lematu Bézout dla pewnych k, l zachodzi równość $ka + ln = 1$. Zatem

$$ka \equiv 1 \bmod n,$$

co oznacza, że k jest odwrotnością a modulo n.

Na odwrót: odwracalność a modulo n oznacza, że dla pewnego k zachodzi kongruencja $ka \equiv 1 \bmod n$. Wówczas istnieje l takie, że $ka - 1 = ln$. Równoważnie $ka + (-l)n = 1$, a to oznacza, że a oraz n są względnie pierwsze.

Twierdzenie 2.3 (prawo skracania)
Jeżeli a jest względnie pierwsze z n, to zachodzi prawo skracania

$$ab \equiv ac \bmod n \Longrightarrow b \equiv c \bmod n.$$

Dla dowodu wystarczy obie strony kongruencji pomnożyć przez $a^{-1} \bmod n$.

Obliczanie odwrotności

Odwrotność modulo n znajdujemy za pomocą odwrotnego algorytmu Euklidesa. Procedurę pokażemy na przykładzie szukania $37^{-1} \bmod 99$.

Zastosujemy algorytm Euklidesa do liczb 37 i 99.

$$\begin{aligned} 99 &= 2 \cdot 37 + 25, \\ 37 &= 1 \cdot 25 + 12, \\ 25 &= 2 \cdot 12 + 1. \end{aligned}$$

Stąd

$$1 = 25 - 2 \cdot 12 = 25 - 2 \cdot (37 - 25) = 3 \cdot 25 - 2 \cdot 37 = 3 \cdot (99 - 2 \cdot 37) - 2 \cdot 37 = 3 \cdot 99 - 8 \cdot 37,$$

zatem

$$37 \cdot (-8) \equiv 1 \bmod 99, \qquad \text{czyli} \qquad 37^{-1} \equiv -8 \equiv 91 \bmod 99.$$

Pierścienie i ciała

Pierścieniem nazywamy zbiór, w którym wykonalne jest dodawanie, odejmowanie i mnożenie, przy czym dodawanie i mnożenie są łączne i przemienne oraz zachodzi prawo rozdzielności mnożenia względem dodawania. W teorii liczb najważniejszymi przykładami pierścieni są zbiór liczb całkowitych $\mathbb{Z}$ (ze zwykłymi działaniami) oraz zbiory $\mathbb{Z}_n$ z działaniami modulo n.

Ciało to pierścień, w którym wykonalne jest też dzielenie. Oczywiście każde ciało jest także pierścieniem. Przykładami ciał są $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, a także ciała skończone $\mathbb{Z}_p$ dla p będącego liczbą pierwszą, z działaniami modulo p. Istnieją też ciała skończone o liczebności p^k, ale w naszych rozważaniach nie pojawiają się.

Zadania

1. Sprawdź, że $7^4 \equiv 1 \bmod 100$. Znajdź dwie ostatnie cyfry liczby 7^{777}.

2. Znajdź: a) $23^{-1} \bmod 51$; b) $35^{-1} \bmod 144$; c) $10^{-1} \bmod 9999$.

3. Uzasadnij, że dla nieparzystej liczby naturalnej n liczba $5^n + 8^n$ dzieli się przez 13.

4. Wykaż, że zachodzi równoważność

$$(a \equiv b \bmod m) \Longleftrightarrow (ak \equiv bk \bmod mk).$$

5. Uzasadnij, że jeżeli zachodzą kongruencje $a \equiv b \bmod m$ oraz $a \equiv b \bmod n$, przy czym m, n są względnie pierwsze, to zachodzi też kongruencja $a \equiv b \bmod mn$.

6. Wykaż, że:
a) jeżeli $a \equiv 1 \bmod 2$, to $a^2 \equiv 1 \bmod 8$;
b) jeżeli $p > 3$ jest liczbą pierwszą, $p \equiv 1 \bmod 3$, to $p^2 \equiv 1 \bmod 24$.

7. Uzasadnij, że jeżeli p jest liczbą pierwszą, to dla $k = 1, 2, \ldots, p-1$ zachodzi

$$\binom{p}{k} \equiv 0 \bmod p.$$

$$\diamondsuit \diamondsuit \diamondsuit$$

8. Uzasadnij, że prawie wszystkie liczby Fermata $F_n = 2^{2^n} + 1$ kończą się siódemką.

9.* Fermat przypuszczał, że wszystkie liczby $F_n = 2^{2^n} + 1$ są pierwsze. Nie korzystając z kalkulatora wykaż, że 641 dzieli F_5. Wsk.: $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$.

10.* Prestidigitator prezentuje zadziwiającą sztuczkę z kartami. Publiczność wybiera losowo z pełnej talii 52 kart pięć, po czym jego asystentka podaje mu cztery z nich. Po chwili zastanowienia bezbłędnie odgaduje piątą. Jak on to robi?

Wsk. Pośród 5 kart zawsze są przynajmniej dwie w tym samym kolorze. Przyjmijmy, że są to trefle. Asystentka poda wówczas karty w kolejności:

$$\clubsuit - ? - ? - ?.$$

Tak więc za pomocą pierwszej karty przekaże informację o kolorze karty odgadywanej, a za pomocą kolejności trzech pozostałych — jedną z liczb 1, 2, ..., 6. Dlaczego to już wystarczy?

2.2 Dwa klasyczne twierdzenia: Wilsona i Fermata

Twierdzenie Wilsona - Małe twierdzenie Fermata - Zadania

Póki obracamy się w świecie małych liczb, póty łatwo rozstrzygnąć, czy dana liczba n jest pierwsza czy złożona. Wystarczy sprawdzić, czy ma ona jakikolwiek dzielnik pierwszy mniejszy bądź równy $\sqrt{n}$. W kryptografii, gdzie operuje się liczbami rzędu 10^{300} i większymi, tak proste metody są nieskuteczne.

W tym wykładzie zajmiemy się dwoma twierdzeniami, które *potencjalnie* mogą pomóc w szybkim rozstrzygnięciu, czy liczba jest pierwsza czy złożona.

Twierdzenie Wilsona

TWIERDZENIE 2.4 (Wilson, ok. 1770)
Liczba naturalna $p > 1$ jest pierwsza wtedy i tylko wtedy, gdy

$$(p-1)! + 1 \equiv 0 \bmod p.$$

Za odkrywcę uchodzi John Wilson, opublikował je (1770) Edward Waring. Wcześniej znał je al-Hajsam (X/XI w.), Leibniz (XVII w.), a pierwszy dowód pochodzi od Lagrange'a (1777).

DOWÓD: Pokażemy najpierw, że jeśli p jest liczbą pierwszą, to zachodzi żądana kongruencja. Dla $p = 2$ twierdzenie jest oczywiste. Możemy więc ograniczyć się do przypadku, gdy p jest liczbą pierwszą nieparzystą.

Rozważmy liczby 1, 2, 3, ..., $p-2$, $p-1$. Ponieważ p jest liczbą pierwszą, więc każda z tych liczb ma swoją odwrotność modulo p. Zbadajmy najpierw, dla jakich a spośród tych liczb zachodzi

$$a \equiv a^{-1} \bmod p, \qquad \text{tzn.} \qquad a^2 \equiv 1 \bmod p.$$

Ten ostatni warunek oznacza, że p dzieli

$$a^2 - 1 = (a-1)(a+1).$$

Z lematu Euklidesa wynika, że p dzieli $a-1$ lub $a+1$, a to oznacza, że $a = 1$ lub $a = p-1$.

Pomińmy na razie te dwie liczby. Zatem liczby 2, 3, ..., $p-2$ dzielą się na pary, liczba i jej odwrotność modulo p, a stąd

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \bmod p.$$

Mnożąc obie strony tej kongruencji stronami przez $p-1$ otrzymamy

$$(p-1)! \equiv p-1 \equiv -1 \bmod p,$$

skąd teza twierdzenia.

Pozostaje pokazać, że jeśli n jest liczbą złożoną, to

$$(n-1)! + 1 \not\equiv 0 \bmod n.$$

Niech p będzie dzielnikiem pierwszym n. Wówczas p dzieli $(n-1)!$, a więc nie może dzielić $(n-1)! + 1$.

Twierdzenie Wilsona ma postać równoważności, daje zatem ładne *kryterium pierwszości*. Niestety sprawdzanie warunku $(p-1)! + 1 \equiv 0 \bmod p$ wymaga obliczania silni. Nie ma żadnych sposobów, aby uniknąć przy tym długich rachunków. Wzór Stirlinga, z którego korzystamy przy obliczaniu silni, daje tylko wartość przybliżoną.

Małe twierdzenie Fermata

TWIERDZENIE 2.5 (małe twierdzenie Fermata, 1640)
Jeżeli p jest liczbą pierwszą, a liczbą całkowitą niepodzielną przez p, to

$$a^{p-1} \equiv 1 \bmod p.$$

Niezależnie od Fermata twierdzenie to odkrył Leibniz. Z typową dla owych czasów dezynwolturą żaden z tych wielkich matematyków nie opublikował dowodu, choć samo twierdzenie należy do najważniejszych w teorii liczb.

DOWÓD: Jeśli liczba pierwsza p nie dzieli a, to ciąg liczb 1, 2, 3, ..., $p-1$ oraz ciąg liczb

$$(*) \quad a,\ 2a,\ 3a, \ldots (p-1)a \bmod p$$

różnią się jedynie kolejnością.

Rzeczywiście, zauważmy przede wszystkim, że skoro p nie dzieli a, to nie jest możliwe, aby $ka \equiv 0 \bmod p$ dla $k = 1, 2, \ldots, p-1$. Tak więc wszystkie reszty $ka \bmod p$ to liczby naturalne od 1 do $p-1$. Ponieważ jest ich dokładnie $p-1$, więc wystarczy wykazać, że są one parami różne.

Przypuśćmy, że dla różnych $i, j < p$ mamy $ai \equiv aj \bmod p$. Ponieważ p nie dzieli a, więc obie strony możemy podzielić przez a, co daje nam $i \equiv j \bmod p$. Obie liczby są mniejsze od p, więc $i = j$, wbrew założeniu.

Skoro liczby $(*)$ modulo p to 1, 2, ..., $p-1$ tylko zapisane w innej kolejności to

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \bmod p,$$

czyli

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

Ponieważ $(p-1)!$ jest względnie pierwsze z p, więc obie strony kongruencji można skrócić, co daje nam żądaną kongruencję.

Zauważmy, że $2^{10} = 1024 \equiv 1 \bmod 343$, a więc $2^{340} = \left(2^{10}\right)^{34} \equiv 1 \bmod 341$, choć $341 = 11 \cdot 31$. Tak więc twierdzenie odwrotne nie zachodzi. Dalszych przykładów dostarczają liczby Carmichaela (p. zad. 15.)

Zadania

11. Znajdź resztę z dzielenia:

a) 100! przez 101; b) 99! przez 101; c) 999! przez 1001.

12. Korzystając z małego twierdzenia Fermata znajdź resztę z dzielenia 2^{1000} przez 17.

13. Pokaż, że dla liczby pierwszej p i dowolnej liczby całkowitej a zachodzi kongruencja $a^p \equiv a \bmod p$. W istocie jest to inna wersja małego twierdzenia Fermata.

14. Wykaż, że dla dowolnej liczby pierwszej p

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

$$\diamondsuit \quad \diamondsuit \quad \diamondsuit$$

15. Z małego twierdzenia Fermata wynika, że dla dowolnej liczby a względnie pierwszej z 561 zachodzą kongruencje

$$a^2 \equiv 1 \bmod 3, \qquad a^{10} \equiv 1 \bmod 11, \qquad a^{16} \equiv 1 \bmod 17.$$

Wywnioskuj stąd, że dla każdej liczby a względnie pierwszej z 561 zachodzi $a^{560} \equiv 1 \bmod 561$. Liczby o takiej własności nazywamy liczbami **Carmichaela**.

16. Wyprowadź małe twierdzenie Fermata dla naturalnych n korzystając z kongruencji w zadaniu 14.

17. Wykaż, że istnieje nieskończenie wiele liczb złożonych postaci:

a) $n! + 1$; b) $n! - 1$; c)* $(n!)^2 + 1$.

18.* Dla dowolnej liczby naturalnej $k \geqslant n$ zachodzi tożsamość

$$n! = k^n - \binom{n}{1}(k-1)^n + \binom{n}{2}(k-2)^n - \binom{n}{3}(k-3)^n + \ldots + (-1)^n \binom{n}{n}(k-n)^n.$$

a) udowodnij twierdzenie Wilsona korzystając z tej tożsamości;
b) udowodnij wykorzystywaną tożsamość.

2.3 Myśl lokalnie - wnioskuj globalnie

Liniowe równania diofantyczne - Sumy kwadratów - Cechy podzielności - Liczby Mersenne'a - Zadania

Z kongruencjami stykać się będziemy niemal we wszystkich wykładach. Tu pokażemy kilka przykładów zastosowań, jednocześnie akcentując zasadniczą ideę ogólną, która tkwi w przedstawianych rozumowaniach.

Liniowe równania diofantyczne

Pokażemy, jak znaleźć rozwiązania całkowite równania postaci

$$ax + by = c,$$

gdzie a, b, c są liczbami całkowitymi, przy czym a, b są względnie pierwsze. To ostatnie założenie nie jest istotnym ograniczeniem. Jeżeli d jest wspólnym

dzielnikiem a, b i dzieli c, to obie strony równania można podzielić przez d. Jeżeli d nie dzieli c, to równanie jest oczywiście sprzeczne.

Przekształćmy równanie do postaci $by = c - ax$. Przy ustalonym x warunkiem koniecznym i dostatecznym rozwiązalności równania jest podzielność $c - ax$ przez b. Zatem x można wyznaczyć z kongruencji

$$c - ax \equiv 0 \bmod b, \qquad \text{czyli} \qquad x \equiv ca^{-1} \bmod b.$$

Niech x_0 będzie jedynym rozwiązaniem tej kongruencji modulo b. Wówczas

$$x = x_0 + kb, \qquad y = \frac{c - a(x_0 + kb)}{b} = \frac{c - ax_0}{b} - ak, \qquad k \in \mathbb{Z}.$$

Rozumowanie to ilustruje ogólną zasadę podaną w tytule podrozdziału. Znajdujemy rozwiązanie modulo b (problem lokalny), a wyciągamy wniosek dla całego zbioru $\mathbb{Z}$ (problem globalny).

Przykład 2.2 *Rozwiąż w liczbach całkowitych równanie* $5x + 13y = 2$.

Rozwiązanie: Mamy tu $13y = 2 - 5x$, więc $5x \equiv 2 \bmod 13$. Zatem

$$x \equiv 5^{-1} \cdot 2 \equiv 8 \cdot 2 \equiv 3 \bmod 13.$$

Stąd

$$x = 3 + 13k, \qquad y = \frac{2 - 5x}{13} = \frac{2 - 5(3 + 13k)}{13} = -1 - 5k, \qquad k \in \mathbb{Z}.$$

Sumy kwadratów

Pokażemy, że 3 nie jest sumą kwadratów dwu liczb wymiernych. Załóżmy, że

$$3 = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2, \qquad \text{czyli} \qquad a^2 + b^2 = 3c^2,$$

gdzie a, b, c są pewnymi liczbami naturalnymi. Możemy przyjąć, że przynajmniej jeden z ułamków a/c, b/c jest nieskracalny.

Z ostatniej równości wynika, że zachodzi kongruencja

$$a^2 + b^2 \equiv 3c^2 \equiv 0 \bmod 3.$$

Przy dzieleniu przez 3 kwadrat dowolnej liczby daje resztę 0, gdy jest ona postaci $3k$ albo 1, gdy jest postaci $3k \pm 1$. Zatem powyższa kongruencja może

zachodzić tylko wówczas, gdy a oraz b są podzielne przez 3. Niech $a = 3k$, $b = 3l$. Mamy $(3k)^2 + (3l)^2 = 3c^2$, skąd $3(k^2 + l^2) = c^2$. Zatem c jest podzielne przez 3, wbrew założeniu o nieskracalności ułamków a/c, b/c.

Uzyskaliśmy tu wynik dotyczący nieskończonego zbioru liczb całkowitych $\mathbb{Z}$ (świat globalny), analizując jego odbicie w lokalnym świecie $\mathbb{Z}_3$. W podobny sposób otrzymuje się w teorii liczb wiele wyników *negatywnych*.

Cechy podzielności

Większość cech podzielności ma charakter lokalny: o własnościach liczby wnioskujemy na podstawie jej ostatnich cyfr. Spośród najbardziej znanych cech wyjątkiem są cechy podzielności przez 3 i przez 9. Pokażemy, skąd bierze się ta ostatnia.

Ponieważ $10 \equiv 1 \bmod 9$, więc dla naturalnego k mamy $10^k \equiv 1 \bmod 10$. Stąd

$$a_k \cdot 10^k + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_k + \ldots + a_2 + a_1 + a_0 \bmod 9,$$

gdzie a_k, $\ldots$, a_2, a_1, a_0 to kolejne cyfry liczone od lewej strony Skoro liczba przystaje modulo 9 do sumy swoich cyfr, to jest ona podzielna przez 9 wtedy i tylko wtedy, gdy suma cyfr dzieli się przez 9.

Liczby Mersenne'a

Porównamy teraz dwa podejścia — lokalne i globalne — do tego samego problemu. Wykażemy, że jeżeli $2^p - 1$ jest liczbą pierwszą, to także p jest liczbą pierwszą.

Załóżmy, że p nie jest liczbą pierwszą. Niech $p = km$, gdzie $k > 1$, $m > 1$. Wówczas

$$2^p - 1 = \left(2^k\right)^m - 1 = \left(2^k - 1\right)\left(2^{k(m-1)} + \ldots + 2^{2m} + 2^m + 1\right),$$

więc liczba $2^k - 1$ jest dzielnikiem właściwym $2^p - 1$.

Spójrzmy na to samo rozumowanie prowadzone z użyciem kongruencji. Mamy

$$2^k \equiv 1 \bmod \left(2^k - 1\right),$$

więc

$$2^p = \left(2^k\right)^m \equiv 1 \bmod \left(2^k - 1\right).$$

Liczby postaci $2^p - 1$ nazywamy **liczbami Mersenne'a**. Z powyższego wynika, że liczba Mersenne'a może być pierwszą tylko wówczas, gdy p jest liczbą pierwszą. Ale nie jest to warunek wystarczający, np. $2^{11} = 2047 = 43 \cdot 89$.

Zadania

19. Znajdź wszystkie rozwiązania całkowite równania:

a) $11x + 5y = 1$; b) $4x + 17y = 3$; c) $51x - 21y = 111$.

20. Uzasadnij, że prosta przechodząca przez dwa punkty kratowe płaszczyzny (tzn. punkty o współrzędnych całkowitych) przechodzi przez nieskończenie wiele takich punktów.

21. Wykaż, że żadna z liczb 11, 111, 1111, ... nie jest kwadratem liczby naturalnej.

22. Na zwykłym kalkulatorze nie da się bezpośrednio sprawdzić, że 19 dzieli $18! + 1$ (wniosek z twierdzenia Wilsona). Pokaż, jak łatwo zrobić to za pomocą kongruencji.

23. Wykaż, że żadna liczba postaci $3n - 1$ nie da się przedstawić w postaci $x^2 + 3y^2$.

24. Wykaż, że liczba naturalna dzieli się przez 11 wtedy i tylko wtedy, gdy różnica sumy jej cyfr na pozycjach parzystych i sumy cyfr na pozycjach nieparzystych przystaje modulo 11.

25. Liczby Fibonacciego określamy warunkami $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$. Ciąg jego ostatnich cyfr powtarza się cyklicznie. Znajdź długość tego cyklu.
Wsk.: Rozważ osobno długość cyklu dla reszt modulo 2 i reszt modulo 5. To znacznie skróci rachunki.

♢ ♢ ♢

26. Liczbę naturalną nazywamy **doskonałą**, jeżeli jest ona równa sumie wszystkich swoich dzielników właściwych, np. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$. Wykaż, że jeżeli liczba $2^p - 1$ jest pierwsza, to $2^{p-1}(2^p - 1)$ jest doskonała. Nie wiadomo, czy istnieją liczby doskonałe nieparzyste.

27. ISBN (International Standard Book Numbering) niniejszej książki to 978-83-62780-49-5. Trzy pierwsze cyfry to prefiks (dodany do dawnego, 10-cyfrowego kodu), 83 — kraj wydania (Polska), 62780 — wydawca (Oficyna Wydawnicza GiS), 49 — konkretny tytuł, wreszcie ostatnia cyfra to symbol kontrolny. Symbol kontrolny kodu $a_1a_2a_3 \ldots a_{13}$ (kreski pominięte) określony jest warunkiem

$$a_1 + 3a_2 + a_3 + 3a_4 + \ldots + a_{11} + 3a_{12} + a_{13} \equiv 0 \bmod 10.$$

Uzasadnij, że cyfra kontrolna wykrywa:
a) pojedynczy błąd; b) każdy czeski błąd (zamianę sąsiednich cyfr) z jednym wyjątkiem.

2.4 Fermat

Pierre de Fermat (1601-1665), matematyk francuski, niemal całe życie spędził w Tuluzie i jej okolicach. Nigdy nie był w Paryżu. Ze szkoły wyniósł dobrą znajomość łaciny i greki, znał też biegle włoski i hiszpański. W roku 1631 uzyskał na uniwersytecie w Orleanie stopień bakałarza w zakresie prawa cywilnego. Przez większą część życia pełnił funkcję radcy lokalnego sądu w Tuluzie (stanowisko — zgodnie z ówczesnym obyczajem — kupione za niemałe pieniądze). Matematyką zajmował się prywatnie — nie pełnił żadnych funkcji

akademickich i prawie niczego nie opublikował. Co prawda kwestię uporządkowania swych wyników i ich publikacji rozważał, ale związany z tym trud wyraźnie go zniechęcił. Większość jego wyników znana jest z korespondencji z licznymi matematykami — w tym z Kartezjuszem, Pascalem, Wallisem, Huygensem, Mersennem i Carcavim — część z rękopisów opublikowanych pośmiertnie.

Uchodzi za najwybitniejszego matematyka-amatora wszech czasów, ale traktowanie go jak amatora jest mocno niefortunne. Jest to specyfika epoki — w XVII w. tylko nieliczni utrzymywali się głównie z pracy naukowej, a nawet oni rzadko ograniczali się do jednej dyscypliny.

Fermat jest (wraz z Pascalem) współtwórcą rachunku prawdopodobieństwa, współtwórcą (z Kartezjuszem) geometrii analitycznej i jednym z twórców rachunku różniczkowego. W fizyce znana jest zasada Fermata.

W dziejach teorii liczb jego rola jest zupełnie wyjątkowa. Od czasów Diofantosa (III w. n.e.) był pierwszym wielkim matematykiem, który intensywnie zajmował się tą tematyką. Próbował nią zainteresować Pascala i Huygensa, ale bez powodzenia. Prawdziwym kontynuatorem Fermata w tej dziedzinie stał się dopiero Leonhard Euler, niemal sto lat później.