Teoria liczb to „matematyka matematyki" zajmująca się badaniem własności liczb - głównie całkowitych. Kiedyś wydawało się, że to dziedzina najbardziej abstrakcyjna z możliwych i praktycznych zastosowań mieć nie będzie. Dziś już wiemy, że to nieprawda: na przykład współczesne systemy szyfrowania opierają się właśnie na teorii liczb. Teoria liczb przydaje się też w kompresji danych, tworzeniu kodów, które same wykrywają błędy przy ich wpisywaniu (np. numery kont bankowych, numery kart kredytowych). Stosowana bywała też w tworzeniu muzyki (Brian Eno). Istnieje też całkiem sporo zastosowań teorii liczb we współczesnej fizyce teoretycznej (http://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/physics.htm).
W tym dziale domyślnie zakładamy, że liczby o których mówimy są całkowite, one bowiem są przedmiotem zainteresowania teorii liczb.

I. Podzielność, NWD i algorytmy Euklidesa

Dodawanie, odejmowanie i mnożenie w ramach liczb całkowitych nie ma szczególnie interesujących własności. Jednak ciekawe problemy pojawiają się przy dzieleniu, gdyż wynik dzielenia dwu liczb całkowitych nie musi być całkowity.

Definicja 1. *Jeśli dla pewnych liczb całkowitych a, b istnieją liczby q, r takie, że $a = bq + r$ i $0 \leq r < b$, to q nazywamy* ilorazem *liczb a i b, a r* - resztą *z dzielenia a przez b. Zapisujemy $r = a \mod b$.*

Przykłady

Definicja 2. *Mówimy, że b* dzieli *a (lub a* jest podzielne *przez b, b jest* dzielnikiem *a, a jest* wielokrotnością *b), jeśli istnieje q takie, że $a = bq$, czyli, gdy $a \mod b = 0$. Zapisujemy $b|a$.*

Twierdzenie 1. *Dla dowolnych liczb a, b, c zachodzi:*
a) jeśli $a|b$ to $a|bc$,
b) jeśli $a|b$ i $b|c$ to $a|c$,
c)jeśli $a|b$, $a|c$ to $a|(b + c)$.

Definicja 3. Największy wspólny dzielnik *niezerowych liczb a i b (zapisywany jako $NWD(a, b)$) to największa liczba d taka, że $d|a$ i $d|b$.*

Przykłady
Poniżej algorytm, który ma już około 2300 lat, pochodzący z „Elementów" Euklidesa. Służy do znajdowania największego wspólnego dzielnika dla liczb całkowitych.

Algorytm 1. *EUKLIDES(a, b).*
***Dane**: Liczby całkowite dodatnie a, b.*
***Zmienne**: r - liczba całkowita.*
I. Dopóki $b \neq 0$ wykonuj:
Ia. $r := a \mod b$.
Ib. $a := b$, $b := r$.
***Rezultat**: Na końcu działania algorytmu a jest największym wspólnym dzielnikiem danych na początku liczb.*

Przykład Znaleźć NWD$(888, 1104)$.
W kryptografii przydaje się tzw. rozszerzony algorytm Euklidesa, który znajduje liczby x i y z poniższego twierdzenia.

Twierdzenie 2. *Dla dowolnych liczb całkowitych dodatnich a i b istnieją liczby całkowite x i y takie, że $ax + by = NWD(a, b)$.*

Algorytm 2. *ROZSZ_EUK(a, b).*
***Dane**: Liczby całkowite dodatnie a, b.*
***Zmienne**: r_i, q_i, x_i,y_i - ciągi liczb całkowitych, i-licznik pętli.*

I. $r_0 := a$, $r_1 := b$,$i := 1$.
II. Dopóki $r_i \neq 0$ *wykonuj:*
IIa. $i := i + 1$.
IIb. $r_i := r_{i-2} \mod r_{i-1}$, $q_{i-1} := (r_{i-2} - r_i)/r_{i-1}$.
{Zauważmy, że w momencie zakończenia działania tej pętli $r_i = NWD(a, b)$ *i dla wszystkich* $k < i - 1$ *zachodzi* $r_k - q_{k+1}r_{k+1} = r_{k+2}$*}*
III. $i := i - 1$, $x_i := 0$, $y_i := 1$.
IV. Dopóki $i > 1$ *wykonuj:*
IVa. $i := i - 1$.
IVb. $x_i := y_{i+1}$, $y_i := x_{i+1} - q_i x_i$.
***Rezultat**: (x_1, y_1) są odpowiednią parą z twierdzenia 2.*

Przykład Znaleźć NWD(234, 123) oraz liczby całkowite x, y takie, że $123x+234y =$NWD(234, 123).

i	r_i	q_i	x_i	y_i
0	234			
1	123	?	?	?
2	?	?	?	?
...	...	...	...	...

II. NWW i jej własności

Definicja 4. Najmniejsza wspólna wielokrotność *dodatnich liczb a i b (zapisywana jako $NWW(a, b)$) to najmniejsza liczba w taka, że $a|w$ i $b|w$.*

Przykłady

Twierdzenie 3. *Dla dodatnich liczb a, b zachodzi:*

$$a \cdot b = NWD(a, b) \cdot NWW(a, b).$$

W szczególności zachodzi: $NWD(a, b) = \frac{ab}{NWW(a,b)}$ *i* $NWW(a, b) = \frac{ab}{NWD(a,b)}$.

Dzięki powyższemu twierdzeniu możemy wyznaczać NWW algorytmicznie: wystarczy wyznaczyć $NWD(a, b)$ z algorytmu Euklidesa i zastosować wzór: $NWW(a, b) = \frac{ab}{NWD(a,b)}$. Ważne jest następujące twierdzenie:

Twierdzenie 4. *Dla dodatnich liczb a, b zachodzi:*

$$a|c \text{ i } b|c \Leftrightarrow NWW(a, b)|c.$$

Przyda się ono w rozdziale: Kombinatoryka. Oczywiście, twierdzenie to działa również dla większej ilości liczb niż dwie.

III. Liczby pierwsze

Każda liczba $a > 1$ ma przynajmniej 2 dzielniki: 1 i samą siebie.

Definicja 5. Liczba pierwsza *to liczba naturalna posiadająca dokładnie 2 różne dzielniki. Liczbę naturalną większą od 1 nazywamy* złożoną*, gdy nie jest pierwsza.*

Definicja 6. *Jeśli $NWD(a, b) = 1$ to a i b nazywamy* liczbami względnie pierwszymi*. Można to zapisać $a \perp b$.*

Liczby pierwsze są kluczowe dla teorii liczb, gdyż każdą liczbę można rozłożyć na iloczyn liczb pierwszych w dokładnie jeden sposób. Można to porównać do cząsteczek chemicznych, które może utworzyć tylko jeden układ atomów.

Twierdzenie 5 (Fundamentalne twierdzenie arytmetyki)**.** *Każda liczba naturalna $n > 1$ ma jednoznaczny (z dokładnością do kolejności mnożenia) rozkład (czyli faktoryzację) na iloczyn liczb pierwszych.*

Jednakże to twierdzenie nie jest w żaden sposób konstruktywne - i to własnie jest dla informatyków najważniejsze. Obecnie nie jest znany żaden efektywny algorytm faktoryzujący liczby naturalne, tzn. znajdujący rozkład na iloczyn liczb pierwszych, co jest sednem współczesnych systemów kryptograficznych. Oczywiście, niektóre liczby można rozłożyć stosunkowo łatwo - najtrudniejsze zaś wydają się te, które są iloczynami dwu liczb pierwszych podobnej wielkości.
Ciekawostka: za rozkłady pewnych liczb różne firmy (np. RSA) są skłonne płacić setki tysięcy dolarów.
Warto zwrócić uwagę jeszcze na kilka faktów:
Po pierwsze, rozkład liczb a i b na czynniki pierwsze automatycznie zadaje nam ich NWD. Jednak efektywne otrzymanie rozkładów jest niełatwe, a bez tej znajomości możemy znaleźć NWD algorytmem Euklidesa.
Po drugie, choć rozkład liczby na czynniki pierwsze jest algorytmicznie nieosiągalny, to sprawdzenie, czy jakaś liczba jest pierwsza jest dużo prostsze: istnieją algorytmy sprawdzające to w czasie $O(\log^3 m)$, gdzie m jest sprawdzaną liczbą.
I ostatnia informacja o liczbach pierwszych:

Twierdzenie 6. *Liczb pierwszych jest nieskończenie wiele.*

Dowód Załóżmy nie wprost, że liczb pierwszych jest skończenie wiele i są to: $p_1, \ldots, p_k$. Rozważmy liczbę $n = p_1 p_2 \ldots p_k + 1$. Jest ona oczywiście większa od każdej p_i. Ponadto żadna z liczb pierwszych p_i nie dzieli n, bo n przy dzieleniu przez p_i daje resztę 1. A zatem n albo jest nową liczbą pierwszą, albo w rozkładzie n są nowe liczby pierwsze. Sprzeczność.
Ciekawostka Największą **znaną** (tj. taką, której pierwszość udowodniono) liczbą pierwszą (na moment rozpoczęcia tego wykładu tj. 1 X 2017) jest $2^{74207281} - 1$. Liczy sobie 22338618 cyfr w zapisie dziesiętnym. Jej pierwszość udowodnił w styczniu 2016 roku Curtis Cooper.

IV. Arytmetyka modularna

Definicja 7. *Mówimy, że dwie liczby a i b* przystają do siebie modulo *n, jeśli ich różnica $a-b$ jest wielokrotnością n (lub innymi słowy, jeśli liczby te dają tę samą resztę z dzielenia przez n). Zapisujemy to symbolem $a \equiv b (mod\ n)$ lub $a \equiv_n b$.*

Łatwo sprawdzić, że relacja przystawania modulo jest równoważnością na zbiorze liczb całkowitych. Ponadto spełnione są własności:

Twierdzenie 7. *Dla dowolnych a, b, c, d oraz $n > 0$ mamy:*
a) jeśli $a \equiv_n b$ i $c \equiv_n d$, to $a + c \equiv_n b + d$,
b) jeśli $a \equiv_n b$ i $c \equiv_n d$, to $a - c \equiv_n b - d$,
c) jeśli $a \equiv_n b$ i $c \equiv_n d$, to $ac \equiv_n bd$.

Na przykład, jeśli jakaś liczba daje resztę 5 z dzielenia przez 17, a druga liczba z dzielenia przez 17 daje resztę 3, to ich suma da resztę 8, ich iloczyn resztę 15, a ich różnica (w podanej kolejności) resztę 2.
Dzięki temu, można zdefiniować działania na klasach abstrakcji relacji modulo tak samo jak na liczbach.
Przez $\mathbb{Z}_n$ będziemy oznaczać zbiór reszt z dzielenia przez n z działaniami arytmetycznymi modulo n.
Przykład $3 + 5 \equiv_6 2$, $3 - 5 \equiv_6 4$, $3 \cdot 5 \equiv_6 3$.
Przykład Zegar, zjawiska cykliczne, koła zębate, algorytmy samokorygujące.

Twierdzenie 8 (Reguła skracania)**.** *Dla $n > 0$ jeśli $ad = bd (mod\ n)$ i $d \perp n$ to $a = b (mod\ n)$.*

V. Kongruencje liniowe i ich układy

Definicja 8. Kongruencją liniową *nazywamy przystawanie postaci* $ax \equiv_n b$, *gdzie* $a, b \in \mathbb{Z}$, *zaś* $x \in \mathbb{Z}_n$ *jest niewiadomą, zwaną też* rozwiązaniem *tej kongruencji.* Układem k kongruencji liniowych *będziemy nazywać zbiór* k *przystawań postaci* $Ax \equiv_n b$, *gdzie* A *jest macierzą* $k \times k$ *o współczynnikach z* $\mathbb{Z}$, $b \in \mathbb{Z}^k$ *jest wektorem złożonym z* k *liczb całkowitych, zaś* $x \in \mathbb{Z}_n^k$ *jest wektorem niewiadomych, zwanym też* rozwiązaniem *tej kongruencji.*

Przykład

$$7x \equiv_{10} 6.$$

Przykład

$$\begin{cases} 3x - 5y \equiv_{13} 1 \\ 9x - 4y \equiv_{13} 10. \end{cases}$$

Przykład

$$2x \equiv_4 3.$$

Twierdzenie 9. *Kongruencja liniowa* $ax \equiv_n b$ *ma co najmniej jedno rozwiązanie wtedy i tylko wtedy gdy* $NWD(a, n)|b$.

Przykład

$$\begin{cases} 3x + y \equiv_{17} 1 \\ x + 6y \equiv_{17} 2. \end{cases}$$

Twierdzenie 10 (Kroneckera-Capellego dla kongruencji)**.** *Jeśli* $\det A \perp n$ *to układ kongruencji liniowych* $Ax \equiv_n b$ *ma dokładnie jedno rozwiązanie.*

Przykład Modularny wiedźmin.

VI. Funkcja φ-Eulera

Na zakończenie - funkcja podstawowa dla koncepcji nowoczesnego kodowania RSA.

Definicja 9. *Funkcja* φ*-Eulera to* $\varphi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$ *zdefiniowana wzorem:*

$$\varphi(n) = |\{1 \leq a \leq n \quad : \quad \mathsf{NWD}(a, n) = 1\}|,$$

czyli jest to odwzorowanie przyporządkowujące liczbie n *moc zbioru liczb naturalnych dodatnich nie większych od niej i względnie pierwszych z nią.*

Przykład $\varphi(6)$.

Twierdzenie 11. *Dla dowolnej liczby pierwszej* p *zachodzą związki:*
a) $\varphi(p) = p - 1$
b) $\varphi(p^k) = p^k(1 - \frac{1}{p})$.

Twierdzenie 12. *Dla dowolnych dwóch dodatnich liczb względnie pierwszych* m *i* n *zachodzi:*
$\varphi(mn) = \varphi(m)\varphi(n)$.

Przykład $\varphi(600)$.
Ogólnie, obliczenie wartości funkcji Eulera jest równie trudne jak rozkład na czynniki pierwsze.

Twierdzenie 13 (Eulera)**.** *Jeśli* $NWD(a, n)=1$ *to* $a^{\varphi(n)} \equiv_n 1$.

Wniosek 14 (Małe Twierdzenie Fermata)**.** *Dla dowolnej liczby pierwszej* p *i dowolnego* n *zachodzi* $n^p \equiv_p n$.

Przykład $19^{74} \mod 28 =$.