ALGEBRA LINIOWA 2

dr Joanna Jureczko

Politechnika Wrocławska
Wydział Elektroniki
Katedra Telekomunikacji i Teleinformatyki

Niniejsza prezentacja stanowi jedynie skrypt do wykładu. Wykład będzie wzbogacony o dodatkowe informacje, tj. dowody wybranych twierdzeń przykłady, wskazówwki do zadań itp. Dodatkowe informacje dotyczące programu znajdują się w Karcie Przedmiotu.

WYKŁAD 1

Liczby całkowite
Algorytm Euklidesa
Rozszerzony algorytm Euklidesa

LICZBY CAŁKOWITE

Przyjmijmy, jak zwykle, że $\mathbb{N} = \{0, 1, 2, 3, ...\}$ jest zbiorem liczb naturalnych, a $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$ zbiorem liczb całkowitych. Oczywiście

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Działaniem dwuargumentowym w zbiorze A nazywamy dowolną funkcję d odwzorowującą zbiór $d\colon A \times A \to A$. Oznaczamy $(a, b) \mapsto c$, gdzie $a, b, c \in A$, (inne oznaczenie $a \circ b = c$).

1. Działanie d musi być określone dla każdej pary elementów ze zbioru A.
2. Wynik działania musi należeć do zbioru A.
3. Wynik działania musi być jednoznacznie określony, (tzn. danej parze elementów przyporządkowujemy dokładnie jeden element z tego zbioru).

Przykłady działań dwuargumentowych.

$A = \mathbb{N}$, to działaniem dwuargumentowym jest $+$ oraz $\cdot$, ale nie jest $-$ ani $:$, (bo np. para $(2, 3)$ nie ma odpowiednika w $\mathbb{N}$).

$A = \mathbb{Z}$, to działaniem dwuargumentowym jest $+, -$ oraz $\cdot$, ale nie jest $:$, (bo np. para $(2, -3)$ nie ma odpowiednika w $\mathbb{Z}$).

$A = \mathbb{Q}$, $A = \mathbb{R}$, to działaniem dwuargumentowym są $+, -$ oraz $\cdot$ ale nie jest $:$, (bo para $(a, 0)$ nie nie ma odpowiednika w A).

Mowimy, że liczba a **dzieli** liczbę b, (inaczej b dzieli się przez a), jeśli istnieje liczba całkowita c taka, że $b = ac$.
Piszemy wtedy
$$a|b.$$
Liczbę a nazywamy wtedy **dzielnikiem** liczby a, a liczbę b **wielokrotnością** liczby a.

Twierdzenie 1.1.

1. Jeśli $a|b$ i $b|c$, to $a|c$.
2. Jesli $a|b$, to $ac|bc$ dla dowolnej liczby $c \neq 0$.
3. Jeśli $c|a$ i $c|b$, to $c|da + eb$ dla dowolnych liczb d i e.
4. Jeśli $a|b$ i $b \neq 0$, to $|a| \leqslant |b|$.
5. Jeśli $a|b$ i $b|a$, to $|a| = |b|$.

Twierdzenie 1.2. Jeśli a i b są liczbami całkowitymi oraz $b > 0$, to istnieją jednoznacznie wyznaczone liczby q i r takie, że

$$a = qb + r \quad 0 \leqslant r < b.$$

Liczbę q w powyższym twierdzeniu nazywamy ilorazem, a liczbę r resztą z dzielenia a przez b. Piszemy wtedy

$$r = a \ (mod \ b).$$

Wspólnym dzielnikiem liczb a i b nazywamy liczbę całkowitą, przez którą obie liczby dzielą się bez reszty.

Wśród wspólnych dzielników dwóch liczb całkowitych a i b, które nie są obie równe zeru, istnieje dokładnie jeden największy (ze względu na relację $\leqslant$). Nazywamy go **największym wspólnym dzielnikiem (NWD)** liczb a i b.

Największy wspólny dzielnik jest zawsze nieujemny. Przyjmujemy $NWD(0,0) = 0$.

Oznaczmy

$$a_1\mathbb{Z} + ... + a_k\mathbb{Z} = \{a_1 z_1 + ... + a_k z_k \colon z_1, ..., z_k \in \mathbb{Z}\}.$$

Jest to zbiór wszystkich **całkowitoliczbowych kombinacji liniowych** liczb $a_1, ..., a_k \in \mathbb{Z}, k \in \mathbb{N}$.

Twierdzenie 1.3. Zbiorem wszystkich całkowitoliczbowych kombinacji liniowych liczb a i b jest zbiór wszystkich wielokrotności $NWD(a,b)$, tzn.

$$a\mathbb{Z} + b\mathbb{Z} = NWD(a,b)\mathbb{Z}.$$

Twierdzenie 1.4. Dla dowolnych liczb a, b i c równanie $ax + by = c$ z niewiadomymi x i y ma rozwiązanie w zbiorze liczb całkowitych, gdy $NWD(a, b)$ jest dzielnikiem c, czyli istnieją liczby całkowite x i y takie, że

$$ax + by = NWD(a, b).$$

ALGORYTM EUKLIDESA

Twierdzenie 1.5. (Algorytm Euklidesa)
1. Jeśli $b = 0$, to $NWD(a, b) = |a|$.
2. Jeśli $b \neq 0$, to $NWD(a, b) = NWD(|b|, a \; mod \; b)$.

Twierdzenie 1.6 Wynikiem działania algorytmu Euklidesa jest największy wspólny dzielnik liczb a i b.

Euklides z Aleksandrii (ok. 365r. p.n.e. – ok. 270r. p.n.e.) matematyk grecki pochodzący z Aten, przez większość życia działający w Aleksandrii. Autor jednych z pierwszych prac teoretycznych z matematyki. Główne jego dzieło to ***Elementy*****, które są pierwszą próbą aksjomatycznego ujęcia geometrii i były podstawowym podręcznikiem geometrii do XIX wieku**. *Elementy* przetłumaczono na wiele języków, zaś liczbą wydań ustępują jedynie Biblii. Euklides usystematyzował ówczesną wiedzę matematyczną w postaci aksjomatycznego wykładu. Zachowały się też dzieła z geometrii, optyki, astronomii i teorii muzyki.

ROZSZERZONY ALGORYTM EUKLIDESA

Do wyznaczania liczb x i y z Twierdzenia 1.4. służy **rozszerzony algorytm Euklidesa**.

Oznaczmy przez $r_0, ..., r_k$ ciąg reszt i przez $q_0, ..., q_k$ ciąg ilorazów obliczonych w czasie działania algorytmu Euklidesa. Konstruujemy dwa ciągi (x_k) i (y_k) takich, że $x = (-1)^n x_n$ i $y = (-1)^{n+1} y_n$ są szukanymi współczynnikami.
Przyjmujemy $x_0 = 1,\ x_1 = 0,\ y_0 = 0,\ y_1 = 1$. Następnie definiujemy

$$x_{k+1} = q_k x_k + x_{k-1},\ y_{k+1} = q_k y_k + y_{k-1}, 1 \leqslant k \leqslant n.$$

Prawdziwe są równości

$$r_k = (-1)^k x_k a + (-1)^{k+1} y_k b$$

dla dowolnych $0 \leqslant k \leqslant n+1$.

Odwrotność modulo n też znajdujemy przy pomocy rozszerzonego algorytmu Euklidesa, który oprócz znajdowania NWD(a,b) znajduje również dwie liczby x i y spełniające równość

$$ax + by = NWD(a, b).$$

Jeśli liczby a i b są względnie pierwsze, to liczba x jest odwrotnością modulo b liczby a.

Niech
(1) $a \cdot u + b \cdot v = w$,
(2) $a \cdot x + b \cdot y = z$
takie, że $NWD(a, b) = NWD(w, z)$.
Zaczynamy od równań
$a \cdot 1 + b \cdot 0 = a$,
$a \cdot 0 + b \cdot 1 = b$.
Stąd u, v, w, x, y i z przyjmują odpowiednio wartości:
$u = 1, v = 0, w = a$
$x = 0, y = 1, z = b$.
Teraz będziemy powtarzać transformacje równań (1) i (2) w pętli, aż otrzymamy wynik $w = 0$.

Najpierw sprawdzamy, czy $w < z$. Jeśli tak, to zamieniamy miejscami równania (1) z (2), tzn. wymieniamy ze sobą współczynniki x z u, v z y i w z z. Wtedy $w \geqslant z$.

Korzystamy z następującej własności NWD: jeśli $NWD(a, b) = NWD(w, z)$, to $NWD(a, b) = NWD((w)_z, z)$.

W równaniu (1) zastępujemy w przez $(w)_z$.
Aby równanie (1) było wciąż spełnione, pozostałe współczynniki u i v również należy odpowiednio zmienić.
Wyznaczamy zatem całkowity iloraz $q = w/z$. Następnie równanie (1) zastępujemy różnicą: (1) - q(2):

$$a \cdot (u - q \cdot x) + b \cdot (v - q \cdot y) = w - q \cdot z$$

Otrzymujemy modyfikację współczynników w równaniu (1):
zamiast u jest $u - q \cdot x$
zamiast v jest $v - q \cdot y$
zamiast w jest $w - q \cdot z = (w)_z$

Po wykonaniu powyższych podstawień wracamy do początku pętli i kontynuujemy ją aż do otrzymania $w = 0$.
Ponieważ w i z są modyfikowane tak samo jak w podstawowym algorytmie Euklidesa, to gdy $w = 0$, otrzymamy parę równań:
(1) $a \cdot u + b \cdot v = w = 0$
(2) $a \cdot x + b \cdot y = z = NWD(a, b)$
Jeśli $z = NWD(a, b) = 1$, to istnieje odwrotność modulo b z liczby a i jest ona równa x. Jeśli $x < 0$ sprowadzamy ją do wartości dodatniej dodając b.

Liczbę całkowitą $p > 1$ nazywamy **liczbą pierwszą**, jeśli ma dokładnie dwa dzielniki dodatnie 1 i p.

Twierdzenie 1.7. Każda liczba całkowita $a > 1$ ma dzielnik pierwszy.

Twierdzenie 1.8. Każdą liczbę całkowitą $a > 1$ można przedstawić w postaci iloczynu liczb pierwszych. Z dokładnością do kolejności czynniki tego iloczynu są wyznaczone w sposób jednoznaczny.