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, wskazówki do zadań itp. Dodatkowe informacje dotyczące programu znajdują się w Karcie Przedmiotu.

WYKŁAD 3

Pierścień
Pierścienie klas reszt
Pierścień $\mathbb{Z}_n$
Małe twierdzenie Fermata
Chińskie twierdzenie o resztach

PIERŚCIEŃ
PIERŚCIEŃ KLAS RESZT
PIERŚCIEŃ $\mathbb{Z}_n$

Niech P będzie niepustym zbiorem, na którym określone są działania $+$ i $\cdot$ oraz jest wyróżniony element 0. Mówimy, że $(P,+,\cdot,0)$ jest **pierścieniem**, gdy $(P,+)$ jest grupą abelową oraz dla wszelkich $a,b,c \in P$ spełnione są warunki:

$$(b+c)\cdot a = b\cdot a + c\cdot a$$

$$a\cdot(b+c) = a\cdot b + a\cdot c$$

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c.$$

Pierścienie, w których

$$a \cdot b = b \cdot a$$

nazywamy **pierścieniami przemiennymi**.

Pierścienie, w których oprócz elementu 0 jest też wyróżniony element 1 taki, że dla każdego $a \in P$

$$a \cdot 1 = 1 \cdot a = a$$

nazywamy **pierścieniem z jedynką.**

W dalszej części będziemy zajmować się tylko pierścieniami przemiennymi z jedynką.

Przykłady pierścieni przemiennych z jedynką

$(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$.

$(\mathbb{Z}[i],+,\cdot)$, gdzie $\mathbb{Z}[i]=\{a+bi\colon a,b\in\mathbb{Z}\}$

$(\mathbb{Z}_n,\oplus,\odot)$, gdzie $\oplus,\odot$ są odpowiednio dodawaniem i mnożeniem modulo n.

$M(n,K,+,\cdot)$, gdzie $M(n,K)$ jest zbiorem macierzy stopnia n nad $K\in\{\mathbb{R},\mathbb{C}\}$ (na ogół nieprzemienny).

$(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ jest pierścieniem przemiennym z jedynką $1+m\mathbb{Z}$. Nazywamy go **pierścieniem klas reszt** modulo m. Jest on izomorficzny z $\mathbb{Z}_n$, gdy $n=m$.

Twierdzenie 3.1. Klasa reszt $a + m\mathbb{Z}$ jest odwracalna w pierścieniu $\mathbb{Z}/m\mathbb{Z}$ wtedy i tylko wtedy, gdy kongruencja

$$ax \equiv 1 (mod\ m)$$

ma rozwiązanie.

Twierdzenie 3.2. Klasa reszt $a+m\mathbb{Z}$ jest odwracalna w pierścieniu $\mathbb{Z}/m\mathbb{Z}$, (tzn. kongruencja $ax \equiv 1$ $(mod\ m)$ ma rozwiązanie) wtedy i tylko wtedy, gdy $NWD(a,m)=1$. Jeśli $NWD(a,m)=1$, to element odwrotny do klasy $a+m\mathbb{Z}$ jest wyznaczony jednoznacznie, (tzn. rozwiązanie x kongruencji $ax \equiv 1(mod\ m)$ jest wyznaczone jednoznacznie modulo m).

Twierdzenie 3.3. Zbiór wszystkich odwracalnych klas reszt modulo m z działaniem mnożenia jest skończoną grupą abelową.

FUNKCJA EULERA

Rozważmy zbiór $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ reszt z dzielenia modulo n. Każde z tych elementów z łacińskiego nazywamy **residuem**. Wtedy **zredukowanym zbiorem residuów mod n** nazywać będziemy podzbiór $\mathbb{Z}_n$ residuów względnie pierwszych z n. Zauważmy, że dla $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą, taki zbiór jest równy $\mathbb{Z}_p^* = \{1, ..., p-1\}$.

Do określenia ilości liczb w $\mathbb{Z}_n$ względnie pierwszych z n służy **funkcja Eulera** $\phi(n)$. Niech $m, n, p \in \mathbb{N}$ oraz p będzie liczbą pierwszą. Wtedy

$$\phi(p) = p - 1,$$

$$\phi(m \cdot n) = \phi(m)\phi(n),$$

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1).$$

Leonhard Euler (1707-1783) szwajcarski matematyk i fizyk; był pionierem w wielu obszarach obu tych nauk. Dokonał licznych odkryć w tak różnych gałęziach matematyki jak **rachunek różniczkowy i całkowy** oraz **teoria grafów**. Wniósł duży wkład w rozwój terminologii i notacji matematycznej. Jako pierwszy w historii użył pojęcia i oznaczenia funkcji. Opublikował wiele ważnych prac z zakresu mechaniki, optyki i astronomii. Euler jest uważany za czołowego matematyka XVIII wieku i jednego z najwybitniejszych w całej historii.

Przykład Dla $n = 10$ mamy $\phi(n) = 4$. Zbiór zredukowany to $\{1, 3, 7, 9\}$.
Dla $n = 15$ mamy $\phi(n) = 8$. Zbiór zredukowany to $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

MAŁE TWIERDZENIE FERMATA

Twierdzenie 3.4. [Małe twierdzenie Fermata] Jeśli $NWD(a, m) = 1$, to $a^{\varphi(m)} \equiv 1 \ (mod \ m)$.

Wniosek 3.5. Liczba x taka, że $x \equiv a^{\varphi(m)-1} \ (mod \ m)$ jest rozwiązaniem kongruencji $ax \equiv 1 (mod \ m)$.

Pierre de Fermat (1601-1665) matematyk (samouk) francuski, z wykształcenia prawnik i lingwista. Większość jego prac matematycznych została opublikowana dopiero po śmierci przez syna, Samuela. Pierre de Fermat dokonał wielu odkryć w teorii liczb, m.in. sformułował słynne **wielkie twierdzenie Fermata**. Wykazał, że **wszystkie krzywe drugiego stopnia da się uzyskać przez odpowiednie przecinanie płaszczyzną powierzchni stożka;** podał metodę znajdowania ekstremum funkcji. Jego prace wraz z pracami Blaise Pascala stworzyły też podstawy pod późniejszy rozwój rachunku prawdopodobieństwa. Fermat już w 1636 wprowadził metodę **prostokątnego układu współrzędnych**, przeprowadził dowód, że **równaniom pierwszego stopnia odpowiadają proste, a równaniom drugiego stopnia linie odpowiadające przecięciu stożka płaszczyzną** (np. elipsy, hiperbole, parabole).

Szybkie potęgowanie Aby szybko i efektywnie obliczać wyrażenie a^b należy zastosować wzór

$$a^b = a^{\Sigma_{i=0}^{k} e_i 2^i} = \Pi_{i=0}^{k} (a^{2^i})^{e_i} = \Pi_{0 \leqslant i \leqslant k, e_i = 1} a^{2^i},$$

gdzie $\Sigma_{i=0}^{k} e_i 2^i$ oznacza rozwinięcie dwójkowe liczby b.

CHIŃSKIE TWIERDZENIE O RESZTACH

Twierdzenie 3.6. [Chińskie twierdzenie o resztach] Niech $m_1, ..., m_n$ będą parami względnie pierwszymi liczbami całkowitymi dodatnimi i niech $a_1, ..., a_n$ będą liczbami całkowitymi. Wtedy układ kongruencji

$$x \equiv a_1 (mod\ m_1), ..., x \equiv a_n (mod\ m_n)$$

ma rozwiązanie x modulo $m = \Pi_{k=1}^{n} m_k$.

Rozwiązanie układu z Twierdzenia 3.6 jest postaci

$$x = \Sigma_{k=1}^{n} a_k y_k M_k,$$

gdzie $M_k = \frac{m}{m_k}$, a y_k jest rozwiązaniem kongruencji

$$y_k M_k \equiv 1 \ (mod \ m_k) \text{ dla } 1 \leqslant k \leqslant n.$$

Z Wniosku 3.5 mamy, że $y_k = M_k^{\varphi(m_k)-1}$.

Chińskie Twierdzenie o resztach znali już starożytni chińscy astronomowie, którzy używali go do określenia dat zdarzeń rozmaitych zjawisk astronomicznych, znanych z obserwacji. W dobie komputerów to samo twierdzenie służy do znajdowania całkowitych rozwiązań równań o współczynnikach całkowitych oraz do przyspieszania operacji arytmetycznych na komputerze.