

# Kryptografia Algebra

dr Robert Borowiec

pokój 908, C-5

tel. 3203083

e-mail: [robert.borowiec@ita.pwr.wroc.pl](mailto:robert.borowiec@ita.pwr.wroc.pl)

www: [lstwww.ita.pwr.wroc.pl/~RB/](http://lstwww.ita.pwr.wroc.pl/~RB/)

**Wykład II**

**2-godziny**

## Arytmetyka modularna

**Kongruencja** jest to przystawanie liczb  $a$  i  $b$  według modułu  $m$  (modulo  $m$ ) i jest zapisywana w postaci:

$$a \equiv b \pmod{m} \quad \text{lub} \quad a \equiv_m b,$$

$$\text{gdy } m \mid (a-b)$$

Liczba  $a$  przystaje do  $b$  wtedy, gdy  $m$  dzieli bez reszty  $a-b$

# Elementy algebry

- Pojęcia podstawowe
  - ❑ grupa, pierścień, ciało
  - ❑ arytmetyka modularna
  - ❑ funkcja Eulera
- Przestrzenie wektorowe
  - ❑ wielomiany pierwotne
  - ❑ wielomiany minimalne

## Grupa

**Grupa  $Q$**  jest zbiorem elementów, w którym jest określone pewne jednowartościowe dwuargumentowe działanie, umownie zwane dodawaniem "+", oraz są spełnione cztery aksjomaty dla dowolnych  $a, b, c \in Q$ :

# Grupa-aksjomaty

- 1) suma dowolnych elementów jest elementem grupy (zamkniętość):

$$a + b \in Q; \quad (1a)$$

- 2) wynik sumowania nie zależy od kolejności składników sumy (łączność):

$$a + (b + c) = (a + b) + c; \quad (1b)$$

- 3) istnieje element neutralny  $e$  (prawo identyczności):

$$a + e = e + a = a, \quad e \in Q; \quad (1c)$$

- 4) istnieją elementy odwrotne (prawo odwrotności):

$$a + \bar{a} = e \quad \bar{a} \in Q. \quad (1d)$$

## Grupa cd..

**Przykład 1:** Zbiór wszystkich liczb rzeczywistych (łącznie z zerem) stanowi grupę względem operacji zwyczajnego dodawania.

**Przykład 2:** Zbiór wszystkich liczb rzeczywistych z wyłączeniem zera stanowi grupę względem operacji zwyczajnego mnożenia.

Grupa jest **grupą przemienną** lub **abelową**, jeśli zachodzi równość

$$a + b = b + a. \quad (2)$$

**Przykład grupy nieprzemiennej:** zbiór macierzy stopnia  $n$ , których wyrazami są dowolne liczby rzeczywiste, jest grupą nieprzemianną względem operacji mnożenia macierzowego.

# Pierścień

**Pierścień**  $R$  jest zbiorem elementów, dla których są zdefiniowane dwa działania:

$a + b$  - zwane umownie dodawaniem oraz

$a \cdot b$  - zwane umownie mnożeniem,

przy czym  $a, b$  są elementami  $R$ . Zbiór  $R$  jest pierścieniem, jeśli są spełnione następujące aksjomaty:

## Pierścień-aksjomaty

- 1) zbiór  $R$  jest grupą abelową ze względu na dodawanie

$$a + b = b + a; \quad (3a)$$

- 2) zbiór  $R$  jest zamknięty ze względu na operację mnożenia

$$a \cdot b \in R; \quad (3b)$$

- 3) mnożenie jest łączne, to znaczy dla dowolnych  $a, b, c \in R$  zachodzi

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c; \quad (3c)$$

- 4) obowiązuje prawo rozdzielności dodawania względem mnożenia, to znaczy

$$a \cdot (b + c) = a \cdot b + a \cdot c. \quad (3d)$$

# Pierścień-przykład

Zbiór liczb stanowiących klasy reszt modulo dowolna liczba całkowita  $m$  jest pierścieniem względem operacji dodawania modulo  $m$  i operacji mnożenia modulo  $m$ . Dla  $m = 4$  reguły dodawania i mnożenia są następujące:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

# Ciało

**Ciało**  $C$  jest to pierścień przemienny, w którym istnieje element neutralny względem mnożenia, spełniający prawo identyczności

$$\varepsilon \in C, \quad a \cdot \varepsilon = \varepsilon \cdot a = a, \quad (4a)$$

a każdy niezerowy element ma swój element odwrotny względem mnożenia

$$a^{-1} \in C, \quad a \cdot a^{-1} = a^{-1} \cdot a = \varepsilon. \quad (4b)$$

Przykładem ciała jest zbiór wszystkich liczb rzeczywistych.

# Ciało skończone

Niech  $q$  oznacza liczbę elementów ciała. Jeśli  $q \neq \infty$ , to takie ciało nazywamy *ciałem skończonym* lub *ciałem Galois* i oznaczamy symbolem  $CG(q)$ . Wielkość  $q$  jest nazywana *rzędem ciała*. Na przykład  $CG(5)$  oznacza ciało skończone utworzone przez zbiór pięciu elementów całkowitych  $\{0,1,2,3,4\}$ , w którym są określone operacje dodawania i mnożenia modulo 5.

## Ciało skończone cd..

- Podstawowe ciało Galois-ciało proste
  - ✓  $q=p$ , gdzie  $p$  jest liczbą pierwszą
  - ✓ jest zbiorem wszystkich elementów całkowitych od 0 do  $p-1$
  - ✓ operacje  $+$ ,  $\cdot$ , są operacjami modulo  $p$ 
    - $\Rightarrow S \equiv a + b \pmod{p}$
    - $\Rightarrow P \equiv a \cdot b \pmod{p}$
- Rozszerzone ciało Galois
  - ✓  $q=p^m$ , gdzie  $p$  jest liczbą pierwszą, a  $m$  jest liczbą naturalną

# Przykład ciała prostego- $\text{CG}(5)$

## ➤ Tablice dodawania i mnożenia

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

## $\text{CG}(5)$ - cd..

- Ciało  $\text{CG}(5)$  zawiera:
  - ☐ element neutralny wobec dodawania – 0;
  - ☐ element neutralny wobec mnożenia – 1.
- Każdy element ciała –oprócz zera –zawiera:
  - ☐ element odwrotny wobec dodawania
  - ☐ element odwrotny wobec mnożenia
- Przykład działań z wykorzystaniem elementu odwrotnego
  - ☐ odejmowanie  $2-3=2+(-3)=2+2=4$
  - ☐ dzielenie  $2/3=2\cdot 3^{-1}=2\cdot 2=4$

# Przykład ciała prostego- $CG(2)$

## ➤ Tablice dodawania i mnożenia

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

0 – element neutralny  
względem dodawania

1 – element neutralny  
względem mnożenia

Dodawanie i odejmowanie w  $GF(2)$ , a także mnożenie i dzielenie są sobie równoważne, ponieważ odpowiednio  $1+1=0 \Rightarrow 1=-1$ ,  $1 \cdot 1^{-1}=1 \Rightarrow 1=1^{-1}$ .

## Algebra

### Obliczanie odwrotności liczby

- Jeżeli mamy daną liczbę  $a$  i istnieje taka liczba  $x$  z przedziału  $[0, n-1]$ , że  $ax \bmod n = 1$ , to liczba  $x$  jest odwrotnością liczby  $a$ .
- Liczba  $a \in [0, n-1]$  ma unikalną odwrotność modulo  $n$ , gdy  $a$  i  $n$  są liczbami wzajemnie pierwszymi  
 $NWD(a, n) = 1$  *NWD-największy wspólny dzielnik*

$n = 5, a = 3$

$3 \cdot 0 \bmod 5 = 0$

$3 \cdot 1 \bmod 5 = 3$

$3 \cdot 2 \bmod 5 = 1$

$3 \cdot 3 \bmod 5 = 4$

$3 \cdot 4 \bmod 5 = 2$

$n = 4, a = 2$

$2 \cdot 0 \bmod 5 = 0$

$2 \cdot 1 \bmod 5 = 2$

$2 \cdot 2 \bmod 5 = 0$

$2 \cdot 3 \bmod 2 = 2$



# Arytmetyka modularna

**Zredukowany zbiór residuów mod  $n$**  jest podzbiorem residuów  $\{0, 1, \dots, n-1\}$  względnie pierwszych z  $n$ . Liczba 0 nigdy nie wchodzi w skład zredukowanego zbioru residuów.

*Na przykład:* dla  $n=10$  to zredukowany zbiór residuów zawiera  $\{1, 3, 7, 9\}$ .

Gdy  $n$  jest liczbą pierwszą to zredukowany zbiór residuów zawiera  $n-1$  elementów  $\{1, \dots, n-1\}$ .

# Funkcja Eulera

**Funkcja Eulera  $\phi(n)$**  określa ilość liczb naturalnych w zbiorze  $\{1, 2, \dots, n-1\}$  względnie pierwszych z  $n$ . Lub inaczej określa liczbę elementów w zredukowanym zbiorze residuów modulo  $n$ .

**Przykład.**  $\phi(8)=4$ , ponieważ w zbiorze liczb mniejszych od 8 tylko 1, 3, 5 i 7 są względnie pierwsze z 8.

**Przykład.** Dla liczby pierwszej  $p$   $\phi(p)=p-1$ ,

## Twierdzenia

**Twierdzenie.** Dla  $n=p \cdot q$ , gdzie  $p, q$  są liczbami pierwszymi, słuszne jest równanie:

$$\phi(n) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1)$$

## Twierdzenia

**Twierdzenie Fermata.** Niech  $p$  będzie liczbą pierwszą. Wówczas dla każdej liczby  $a$  spełniającej warunek  $\text{NWD}(a, p)=1$  zachodzi

$$a^{p-1} \bmod p = 1$$

**Uogólnienie Eulera.** Dla każdego  $a$  i  $n$  takich, że  $\text{NWD}(a, n)=1$ , zachodzi równanie:

$$a^{\phi(n)} \bmod n = 1$$

# Algebra

## Obliczanie odwrotności liczby

- Podane przez *Eulera* uogólnienie *Fermata* dostarcza algorytmu do rozwiązywania równania  $(a \cdot x) \bmod n = 1$ , gdy  $\text{NWD}(a, n) = 1$ . Rozwiązanie to ma postać:

$$x = a^{\phi(n)-1} \bmod n$$

- Jeżeli  $n$  jest liczbą pierwszą, to:

$$x = a^{(n-1)-1} \bmod n = a^{n-2} \bmod n$$



## Przestrzenie wektorowe

Przestrzeń liniowa  $V$  rozpięta nad ciałem liczbowym  $C$  jest to zbiór elementów, dla którego są spełnione odpowiednie aksjomaty. *Przestrzeń liniowa* jest nazywana również *przestrzenią wektorową*, a jej elementy - *wektorami*. Elementy ciała  $C$  są *skalarami*.

# Aksjomaty przestrzeni liniowej

- (1) zbiór  $V$  jest grupą abelową względem dodawania;
- (2) dla dowolnego wektora  $\mathbf{v} \in V$  i dowolnego skalaru  $c \in C$  zachodzi
$$c \cdot \mathbf{v} \in V; \quad (5a)$$
- (3) dla dowolnych wektorów  $\mathbf{v}, \mathbf{u} \in V$  i dowolnego skalaru  $c \in C$  zachodzi
$$c \cdot (\mathbf{v} + \mathbf{u}) = c \cdot \mathbf{v} + c \cdot \mathbf{u}; \quad (5b)$$
- (4) dla dowolnego wektora  $\mathbf{v} \in V$  i dowolnych skalarów  $c, d \in C$  zachodzi
$$(c + d) \cdot \mathbf{v} = c \cdot \mathbf{v} + d \cdot \mathbf{v}; \quad (5c)$$
- (5) dla dowolnego wektora  $\mathbf{v} \in V$  i dowolnych skalarów  $c, d \in C$  zachodzi
$$(c \cdot d) \cdot \mathbf{v} = c \cdot (d \cdot \mathbf{v}). \quad (5d)$$

## Wektory liniowo niezależne

Jeżeli  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$  są wektorami w przestrzeni liniowej  $V$  rozpiętej nad ciałem liczbowym  $C$ , to dowolną sumę o postaci

$$\mathbf{u} = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \dots + a_k \mathbf{v}_k, \quad (8)$$

w której są elementami ciała  $C$ , nazywamy *liniową kombinacją* wektorów. O zbiorze  $k$  wektorów  $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$  mówimy, że jest *liniowo niezależny* jeśli dla dowolnie wybranego zbioru skalarów  $\{a_1, a_2, \dots, a_k\}$  zależność

$$a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \dots + a_k \mathbf{v}_k = \mathbf{0} \quad (9)$$

zachodzi wtedy i tylko wtedy, gdy wszystkie są równe zeru, tzn.

$$a_1 = a_2 = \dots = a_k = 0.$$

# Wymiar przestrzeni

Największa liczba liniowo niezależnych wektorów w przestrzeni stanowi *wymiar przestrzeni*. Wymiar przestrzeni jest nazywany również *liczbą stopni swobody przestrzeni*. Dowolny zbiór  $n$  liniowo niezależnych wektorów tworzy *bazę przestrzeni  $n$ -wymiarowej*.

*Przykład:* Trzy wektory binarne  $(0,0,1)$ ,  $(0,1,0)$  i  $(1,0,0)$  są liniowo niezależne i tworzą bazę przestrzeni wektorowej  $V_3$ , zawierającej osiem wektorów binarnych:  $(0,0,0)$ ,  $(0,0,1)$ , ...,  $(1,1,1)$ , będących kombinacjami liniowymi wektorów bazy nad ciałem  $CG(2)$ .

# KONIEC

## Dziękuję za uwagę