# Spis treści

**1 Operacje** **1**
1.1 Działanie wewnętrzne i zewnętrzne . . . 2
1.2 Własności operacji . . . 2

**2 Grupa** **2**
2.1 Grupa $\mathbb{Z}_n$ . . . 2
2.2 Grupa $\mathbb{Z}_n^\times$ . . . 2

**3 Podgrupa** **2**
3.1 Generowanie . . . 2
3.2 Przystawanie . . . 3

**4 Funkcja Eulera** **3**

**5 Permutacje** **3**
5.1 Rozkład na cykle . . . 3
5.2 Iloczyn transpozycji . . . 3
5.3 Postać macierzowa . . . 3
5.4 Znak permutacji . . . 3

**6 Pierścień** **4**
6.1 Pierścień z jedynką . . . 4
6.2 Pierścień przemienny . . . 4

**7 Ciało** **4**

**8 Wielomiany** **4**
8.1 Przykład ciała wielomianowego . . . 4
8.2 Rozkładalność a ciała . . . 4

**9 Rozszerzony algorytm Euklidesa** **5**

**10 Problem logarytmu dyskretnego** **5**

**11 Test na pierwszość Fermata** **5**

**12 Twierdzenie Eulera** **6**

**13 Chińskie twierdzenie o resztach** **6**

**14 Faktoryzacja wielomianu nad ciałem skończonym** **6**
14.1 Distinct-degree factorization . . . 6

**15 Wspólne miejsca zerowe wielomianów jednej zmiennej** **6**

**16 Wielomiany wielu zmiennych** **6**

**17 Bazy Gröbnera** **6**

Kazali mi to zdawać, choć algebrę miałem jakbym nie miał ciekawszych rzeczy do roboty i potrzebował tej powtórki. Fun times.

# 1 Operacje

Każdą funkcję która ma dwa argumenty i zwraca jeden wynik można nazwać operacją. Teoretycznie zatem można konwencjonalne operatory traktować jako funkcje. $+(1,1) = 2$

### 1.1 Działanie wewnętrzne i zewnętrzne

Działanie wewnętrzne w zbiorze $A$: $* : A \times A \to A$. Działanie zewnętrzne w zbiorze $A$: $* : F \times A \to A$

### 1.2 Własności operacji

Rozróżniamy kilka własności, które mogą mieć operacje.

- **Łączność** - $A * (B * C) = (A * B) * C$
- **Przemienność** - $A * B = B * A$
- **Rozdzielność** - $A * (B + C) = A * B + A * C$
- **Element neutralny** - $A * E = A$
- **Element odwrotny** - $A * A^{-1} = E$

## 2 Grupa

Grupa to zbiór $G$ z działaniem wewnętrznym $*$ jeśli:

- $*$ jest łączne
- $*$ posiada element neutralny
- $*$ posiada element odwrotny

Dodatkowo jeśli $*$ jest przemienne to mamy grupę abelową.

### 2.1 Grupa $\mathbb{Z}_n$

Specyficzna grupa, która jest zbiorem liczb całkowitych od 0 do $n-1$ z działaniem $+$ modulo $n$. Elementem przeciwnym dla $a$ jest $n-a$.

### 2.2 Grupa $\mathbb{Z}_n^\times$

$$\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : NWD(a, n) = 1\}$$

A działanie tej grupy to mnożenie modulo $n$. Element przeciwny oblicza się algorytmem Euklidesa.

## 3 Podgrupa

Podgrupa to podzbiór grupy z odpowiednio dostosowanym działaniem. Na przykład podgrupą $\mathbb{Z}_{12}$ jest $(\{0, 4, 8\}, +)$, ponieważ nie ma pary elementów z podzbioru, które po dodaniu dałyby coś spoza podzbioru.

### 3.1 Generowanie

Niech $(G, *)$ będzie grupą z elementem neutralnym $E$. Wtedy:

$$\langle g \rangle = \{\overbrace{g * g * \cdots * g}^{n} : n \in \mathbb{N}\} \cup \{E\} \cup \{\overbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}^{m} : m \in \mathbb{N}\}$$

Jeśli $G = \langle g \rangle$ dla pewnego $g$ to $G$ jest grupą cykliczną. Rzędem $g$ jest $|\langle g \rangle|$

W $\mathbb{Z}_{12}$ podgrupą generowaną przez 4 jest $\{0, 4, 8\}$, a $rz(4) = |\langle 4 \rangle|$. Z kolei $\langle 1 \rangle = \mathbb{Z}_{12}$ zatem $\nVdash\nvDash$ jest grupą cykliczną. Jeżeli $p$ jest liczbą pierwszą to $\mathbb{Z}_p^\times$ jest grupą cykliczną.

### 3.2 Przystawanie

Jeśli dwa elementy $a, b$ są przystające w Grupie $G$ to $a \equiv b$. Na przykład $32 \equiv 4$ w $\mathbb{Z}_7$, ponieważ $32 \mod 7 = 4$. Przystawanie $(\mod n)$ implikuje:

- że $a$ i $b$ przy dzieleniu przez $n$ mają tę samą resztę
- $n$ dzieli $a - b$
- $a = b + nk$ dla pewnego $k \in \mathbb{Z}$

## 4 Funkcja Eulera

$$\varphi(n) = \begin{cases} 1 : n = 1 \\ |\mathbb{Z}_n^\times| : n > 1 \end{cases}$$

Jeśli $p$ jest liczbą pierwszą to $\varphi(p^k) = p^k - p^{k-1}$ oraz $\varphi(p) = p - 1$. Jeśli $NWD(m, n) = 1$ to $\varphi(mn) = \varphi(m)\varphi(n)$.

## 5 Permutacje

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

$$a_n = \pi(n)$$

### 5.1 Rozkład na cykle

$$\pi = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix} = (a_1, a_2, a_3, \ldots, a_n)$$

$$\pi' = \begin{pmatrix} a_1 & a_2 & b_1 & b_2 \\ a_2 & a_1 & b_2 & a_1 \end{pmatrix} = (a_1, a_2) \cdot (b_1, b_2)$$

### 5.2 Iloczyn transpozycji

$$(a_1, a_2, a_3, \ldots, a_k) = (a_1, a_k) \cdot (a_1, a_{k-1}) \cdot \cdots \cdot (a_1, a_3) \cdot (a_1, a_2)$$

### 5.3 Postać macierzowa

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 4 & 3 \end{pmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

### 5.4 Znak permutacji

Ilość czynników w iloczynie transpozycji określa parzystość permutacji.

$$(-1)^n$$

gdzie $n$ to ilość transpozycji

# 6 Pierścień

Pierścień to uporządkowana trójka $R(A, +, \cdot)$, gdzie $A$ to zbiór, a $+$ i $\cdot$ to działania spełniające następujące warunki:

- $(A, +)$ jest grupą abelową
- $+$ i $\cdot$ są są wewnętrzne dla $A$
- Dla każdego $a, b, c \in A$ zachodzi rozdzielność mnożenia względem dodawania: $a \cdot (b + c) = a \cdot b + a \cdot c$ oraz $(a + b) \cdot c = a \cdot c + b \cdot c$
- Istnieje element neutralny mnożenia $1 \in A : \forall a \in A : a \cdot 1 = 1 \cdot a = a$

## 6.1 Pierścień z jedynką

Pierścień z jedynką to pierścień, w którym istnieje element neutralny mnożenia oraz $A \neq \emptyset$

## 6.2 Pierścień przemienny

Pierścień przemienny to pierścień, w którym mnożenie jest przemienna

# 7 Ciało

Ciało $\mathbb{C}(K, +, \cdot)$ to pierścień przemienny z jedynką, oraz $(K \setminus \{0\}, \cdot)$ jest grupą. Innymi słowy: jest to niepusty zbiór $K$ z działaniami $+$ i $\cdot$, które są przemienne, łączne, posiadają elementy neutralne i odwrotne, oraz istnieją takie pary $(a, b)$ dla których:

$$a + b = 0 \text{ oraz } a \cdot b = 1$$

Przykładami ciał są: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

# 8 Wielomiany

Mówimy, że liczba $z$ jest pierwiastkiem $n$-tego stopnia liczby $w$ jeśli

$$z^n = w$$

Każdy wielomian $f \in \mathbb{C}[x]$ stopnia $n$ ma $n$ pierwiastków. Jeśli $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ to

$$f(x) = a_n (x - z_1)(x - z_2) \ldots (x - z_n)$$

## 8.1 Przykład ciała wielomianowego

Zbiór $\{0, 1, x, x + 1\}$ z dodawaniem i mnożeniem modulo $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ jest ciałem.

| $+$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $x$ | $x+1$ |
| $1$ | $1$ | $0$ | $x+1$ | $x$ |
| $x$ | $x$ | $x+1$ | $0$ | $1$ |
| $x+1$ | $x+1$ | $x$ | $1$ | $0$ |

Tabela 1: Dodawanie w wyżej zdefiniowanym ciele

## 8.2 Rozkładalność a ciała

Dlaczego zbiór $\{0, 1, x, x + 1\}$ z dodawaniem i mnożeniem modulo $f(x) = x^2 + 1 \in \mathbb{Z}_2[x]$ nie jest ciałem? Ponieważ $x^2 + 1$ jest rozkładalny w $\mathbb{Z}_2[x]$.

Mówimy, że wielomian $f(x)$ jest rozkładalny w $\mathbb{Z}_p[x]$ jeśli gdy istnieją wielomiany $g_1, g_2 \in \mathbb{Z}_p[x]$ stopnia co najmniej 1 takie, że $f(x) = g_1(x) g_2(x)$.

Dla każdego $n \in \mathbb{N}$ i każdej liczby pierwszej $p$ istnieje wielomian stopnia $n$ w $\mathbb{Z}_p[x]$ który jest nierozkładalny.

# 9 Rozszerzony algorytm Euklidesa

Dla $a, b \in \mathbb{Z}$ wyznacza $NWD(a, b)$ oraz $x, y \in \mathbb{Z} : ax + by = NWD(a, b)$. Jest on zdefiniowany w następujący sposób:

$$(r_0, s_0, t_0) = (a, 1, 0), (r_1, s_1, t_1) = (b, 0, 1)$$
$$(r_{i+1}, s_{i+1}, t_{i+1}) = (r_{i-1}, s_{i-1}, t_{i-1}) - \lfloor \frac{r_{i-1}}{r_i} \rfloor (r_i, s_i, t_i)$$

Równanie $ax + by = c$ ma rozwiązanie w $\mathbb{Z}$ tylko jeśli $NWD(a, b)|c$. Na przykład: dla $30, 45$ mamy:

1. (45, 1, 0), (30, 0, 1)
2. (45, 1, 0) - 1 * (30, 0, 1) = (15, 1, -1)
3. (30, 0, 1) - 2 * (15, 1, -1) = (0, -2, 3)
4. $NWD(30, 45) = 15$
5. $15 = -1 * 30 + 1 * 45$

Albo inaczej: $61^{-1} \in \mathbb{Z}_{130} =?$

$$61^{-1} \in \mathbb{Z}_{130} \rightarrow 61x \equiv 1 \mod 130 \rightarrow 61x + 130y = 1$$

1. (130, 1, 0), (61, 0, 1)
2. (130, 1, 0) - 2 * (61, 0, 1) = (8, 1, -2)
3. (61, 0, 1) - 7 * (8, 1, -2) = (5, -7, 15)
4. (8, 1, -2) - 1 * (5, -7, 15) = (3, 8, -17)
5. (5, -7, 15) - 1 * (3, 8, -17) = (2, -15, 32)
6. (3, 8, -17) - 1 * (2, -15, 32) = (1, 23, -49)
7. (2, -15, 32) - 2 * (1, 23, -49) = (0, -61, 130)
8. $NWD(61, 130) = 1$
9. $1 = (-49) * 61 + 23 * 130$

# 10 Problem logarytmu dyskretnego

Dane: $a, c \in \mathbb{Z}, n \in \mathbb{N}$. Cel: znaleźć $x \in \mathbb{Z}_n$ takie, że $a^x = c \in \mathbb{Z}_n$. Alternatywnie można zdefiniować postać ogólną, gdzie mamy grupę $G$ oraz $|G| \in \mathbb{P}$, i chcemy znaleźć $x \in G : g^x = h$.

# 11 Test na pierwszość Fermata

Jeśli $p \in \mathbb{P}$ to $\forall_{a \in \mathbb{Z}_p \setminus \{0\}} a^{p-1} = 1 \in \mathbb{Z}_p$.

1. Losujemy $a \in \mathbb{Z}_p \setminus \{0\}$
2. Obliczamy $a^{p-1} \mod p$
3. Jeśli $a^{p-1} \neq 1$ to $p$ nie jest liczbą pierwszą

Na przykład: $p = 7$, $a = 2$:

$$2^{7-1} = 2^6 = 64 \mod 7 = 1$$

Zatem 7 może być liczbą pierwszą.
Albo $p = 4$, $a = 2$:

$$2^{4-1} = 2^3 = 8 \mod 4 = 0$$

Zatem 4 nie jest liczbą pierwszą.

# 12 Twierdzenie Eulera

Niech $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : NWD(a,n) = 1\}$, $\varphi(n) = |\mathbb{Z}_n^\times|$. Dla każdego $a \in \mathbb{Z}_n^\times$: $a^{\varphi(n)} \equiv 1(\mod n)$

# 13 Chińskie twierdzenie o resztach

Niech $m_1, \ldots m_k \in \mathbb{N}$ będą parami względnie pierwsze ($NWD = 1$), oraz $M = \prod m$. Wtedy dla dowolnych $a_1, \ldots a_k \in \mathbb{Z}$ istnieje $x < M$ takie, że:

$$x \equiv a_i \mod m_i$$

# 14 Faktoryzacja wielomianu nad ciałem skończonym

## 14.1 Distinct-degree factorization

Wielomian $f(x) = a_0 + a_1x^1 \ldots$ nazywamy unormowanym jeśli $a_n = 1$. Współczynniki $a_n$ nazywamy wiodącym. Ponieważ dla każdego $a \in \mathbb{F}_q \setminus \{0\}$ mamy $a^{q-1}$ więc:

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

Dla każdego $d \geq 1$, $x^{q^d} - x \in \mathbb{F}_q[x]$ jest iloczynem wszystkich nierozkładalnych unormowanych wielomianów w $\mathbb{F}_q[x]$ stopnia $k|d$.

# 15 Wspólne miejsca zerowe wielomianów jednej zmiennej

Mając wielomiany $f_1 \ldots f_s \in \mathbb{F}[x]$ o współczynnikach z ciała $\mathbb{F}$, chcemy znaleźć $V = \{x \in \mathbb{F} : f_{1\ldots s}(x) = 0\}$.

$$f(a) = 0 \leftrightarrow x - a|f(x)$$

Aby znaleźć $V$ musimy obliczyć $NWD(f_1, \ldots, f_s)$.

# 16 Wielomiany wielu zmiennych

$$\mathbb{F}[x_1, \ldots, x_n] = \text{zbiór wielomianów zmiennych } x_1, \ldots, x_n$$

$$f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n] = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

Konstrukcje typu $x_1^{i_1} \ldots x_n^{i_n}$ można utożsamić z wektorami $(i_1, \ldots, i_n)$, a te z kolei uporządkować. Na przykład można użyć porządku leksykograficznego gdzie $i \prec j \leftrightarrow$ pierwszy niezerowy współczynnik $j - a$ jest dodatni

Mając ustalony porządek, można zdefiniować dzielenie wielomianów wielu zmiennych. Każdy wielomian $f \in \mathbb{F}[x_1, \ldots x_n]$ można przedstawić w postaci:

$$f = a_1 f_1 + \cdots + a_k f_k + r$$

Na przykład dla $f(x, y) = x^2y + xy^2 + y^2$:

$$f(x, y) = (x + y)(xy) + (y^2 - 1) + x + y + 1$$

# 17 Bazy Gröbnera

Dla porządku $\prec$ na $\mathbb{Z}^\ltimes$ oraz $f_1 \ldots f_n \in \mathbb{F}[x_1, \ldots x_n]$ to:

$$\langle f_1, \ldots, f_n \rangle = \{a_1 f_1 + \cdots + a_n f_n : a_i \in \mathbb{F}[x_1, \ldots, x_n]\}$$

nazywamy idealem generowanym przez $f_1, \ldots, f_n$. Skończony podzbiór ideału, względem porządku $\prec$ nazywamy bazą Gröbnera, jeśli:

$$\langle LT(g) : g \in G \rangle = \langle LT(f) : f \in I \rangle$$