# Ciała skończone i kombinatoryka - zadania kwalifikacyjne

Michał Kotowski

13 czerwca 2015

Zasady oceniania:

- rozwiązania należy przysyłać na adres: `michal.kotowski1@gmail.com`
- zrobienie zadań wymaga przyswojenia sobie niewielkiego kawałka teorii o ciałach i wielomianach - należy przeczytać (np. z Wikipedii), co to jest ciało (wystarczy sama znajomość definicji) oraz zapoznać się z treścią ściągawki o dzieleniu wielomianów (link: `http://www.math.toronto.edu/~michal/sciagawka.pdf`)
- w razie trudności, niejasności, wątpliwości co do treści zadań, znalezienia literówek itd. - piszcie, pojawią się dodatkowe wyjaśnienia i/lub wskazówki
- w przypadku dużej liczby chętnych o kwalifikacji zadecyduje łączna liczba poprawnie zrobionych zadań

**Zadanie 1.** (a) Które z poniższych zbiorów (z naturalnymi działaniami) są ciałami, a które nie (sprawdź tylko te aksjomaty, które nie są od razu oczywiste):

- $\mathbb{N}$ (liczby naturalne)
- $\mathbb{Z}$ (liczby całkowite)
- $\mathbb{Q}$ (liczby wymierne)
- $\mathbb{Q}_+$ (liczby wymierne dodatnie)
- $\mathbb{R}$ (liczby rzeczywiste)
- $\mathbb{Z}_2$ (zbiór 0,1 z dodawaniem modulo 2)
- $\mathbb{Z}_3$ (analogicznie j.w.)
- $\mathbb{Z}_4$ (analogicznie j.w.)

Uogólnij ostatnie trzy przykłady.

(b) Dla $p$ - liczby pierwszej, pokaż wielomian o współczynnikach z $\mathbb{Z}_p$, który nie ma żadnych pierwiastków w $\mathbb{Z}_p$ (wskazówka - co możesz powiedzieć o wielkości $a^p$?).

(c) Rozpatrzmy wielomian $f(x) = x^2 - x - 1$ nad $\mathbb{Z}_2$. Niech $F = \mathbb{Z}_2[x]/(f)$ będzie pierścieniem ilorazowym modulo $f$ (patrz ściągawka). Pokaż, że każdy element $F$ można reprezentować wielomianem nad $\mathbb{Z}_2[x]$ stopnia co najwyżej 1. Ile elementów ma $F$? Pokaż, że $F$ jest ciałem i wypisz tabelkę mnożenia dla $F$.

(d) (podpunkt "z gwiazdką", nieco trudniejszy) Uogólnij konstrukcję z poprzedniego podpunktu,zastępując $\mathbb{Z}_2$ przez $\mathbb{Z}_p$, gdzie $p \neq 2$. (w razie problemów z szukaniem odwrotności w $\mathbb{Z}_p[x]/(f)$ - przypomnieć sobie algorytm Euklidesa w formie $ax + by = NWD(a, b)$, on działa też dla wielomianów; w ostateczności zostawić na później)

(e) Czy nad każdym ciałem skończonym może istnieć wielomian o nie wszystkich współczynnikach zerowych zerujący się na każdym elemencie tego ciała? Pokaż, że dla każdego ciała skończonego $\mathbb{F}$ istnieje wielomian, który nie ma żadnych pierwiastków w $\mathbb{F}$.

**Zadanie 2.**

(a) Kodem poprawiającym błędy nad $\mathbb{Z}_p$ nazwiemy dowolny podzbiór $C \subseteq \mathbb{Z}_p^n$. Dla dowolnych dwóch elementów $x, y \in C$ ich odległością Hamminga $d(x, y)$ nazywamy liczbę pozycji, na których się różnią (gdzie każdy element traktujemy jako ciąg $n$ wyrazów z $\mathbb{Z}_p$). Załóżmy, że kod $C$ ma tę własność, że każde dwa jego elementy znajdują się w odległości co najmniej $d$. Udowodnić, że:

$$|C| \leqslant \frac{p^n}{\sum_{k=0}^{t} \binom{n}{k} (p-1)^k}$$

gdzie $t = \lfloor \frac{d-1}{2} \rfloor$.

(b) Rozpatrzmy kod $C$ nad $\mathbb{Z}_2$ otrzymany w następujący sposób: każdemu możliwemu ciągowi $(x_1, x_2, x_3, x_4) \in \{0, 1\}^4$ przyporządkowujemy ciąg $(x_1, x_2, x_3, x_4, x_2 + x_3 + x_4, x_1 + x_3 + x_4, x_1 + x_2 + x_4)$. Elementami kodu są wszystkie otrzymane w ten sposób ciągi z $\{0, 1\}^7$. Znaleźć minimalną odległość Hamminga między dowolnymi dwoma elementami $C$. Jak ma się rozmiar kodu i minimalna odległość do nierówności z poprzedniego podpunktu?

**Zadanie 3.**

Skończoną płaszczyzną rzutową rzędu $q$ nazwiemy zbiór $X$ o $q^2 + q + 1$ elementach, zwanych punktami, wraz z rodziną podzbiorów $X$, oznaczaną $\mathcal{L}$ i zwaną rodziną prostych, o następujących własnościach:

(1) Każda prosta zawiera dokładnie $q + 1$ punktów

(2) Dowolne dwa punkty leżą na dokładnie jednej prostej

(a) Udowodnić, że każdy punkt leży na dokładnie $q + 1$ prostych, prostych jest dokładnie $q^2 + q + 1$ oraz dowolne dwie proste przecinają się w dokładnie jednym punkcie.

(b) Podać przykład płaszczyzny rzutowej rzędu 2.

(c) (zrób tylko, jeśli rozwiązałeś/aś już pozostałe zadania) Rozpatrzmy trójki elementów $(x_0, x_1, x_2)$, gdzie $x_i \in \mathbb{Z}_q$ i $q$ jest liczbą pierwszą. Rozpatrzmy zbiór $X$ złożony z elementów oznaczanych $[x_0 : x_1 : x_2]$ zdefiniowanych jako:

$$[x_0 : x_1 : x_2] = \{(cx_0, cx_1, cx_2) : c \in \mathbb{Z}_q, c \neq 0\}$$

gdzie zakładamy, że nie wszystkie $x_0, x_1, x_2$ są jednocześnie równe 0. Innymi słowy, dla każdej trójki $(x_0, x_1, x_2)$ utożsamiamy z nią wszystkie trójki otrzymane z niej przez pomnożenie przez niezerowy element z $\mathbb{Z}_q$.

Określamy zbiór $\mathcal{L}$ jako złożony z elementów oznaczanych $L(a_0, a_1, a_2)$ i zdefiniowanych jako:

$$L(a_0, a_1, a_2) = \{[x_0 : x_1 : x_2] : a_0x_0 + a_1x_1 + a_2x_2 = 0\}$$

dla wszystkich trójek takich, że nie wszystkie $a_0, a_1, a_2$ są jednocześnie równe 0.

Udowodnić, że zbiór punktów $X$ wraz ze zbiorem prostych $\mathcal{L}$ tworzy płaszczyznę rzutową rzędu $q$.

**Zadanie 4.**

Niech $\mathbb{F}_q$ będzie ciałem skończonym mocy $q$. Niech $X = \{X_1, \ldots, X_m\}$ będą losowo wybranymi elementami $\mathbb{F}_q$ (być może z niejednostajnym rozkładem) - rodzinę $X$ nazwiemy 2-niezależną, jeśli dla dowolnych $i \neq j$ i dowolnych $a, b \in \mathbb{F}_q$ mamy:

$$\mathbb{P}(X_i = a \cap X_j = b) = \mathbb{P}(X_i = a)\mathbb{P}(X_j = b)$$

gdzie $\mathbb{P}(A)$ oznacza prawdopodobieństwo zajścia zdarzenia $A$. Innymi słowy, wszystkie elementy $X_i$ (dalej: zmienne losowe) są parami niezależne - jest to własność słabsza od łącznej niezależności.

Analogicznie, rodzinę zmiennych losowych nazywamy $k$-niezależną, jeśli dla dowolnych $i_1, \ldots, i_k$ oraz dowolnych $a_1, \ldots, a_k \in \mathbb{F}_q$ zachodzi:

$$\mathbb{P}(\bigcap_{j=1}^{k} X_{i_j} = a_j) = \prod_{j=1}^{k} \mathbb{P}(X_{i_j} = a_j)$$

Niech $X_0, X_1$ będą niezależnie i jednostajnie wylosowanymi elementami $\mathbb{F}_q$. Rozpatrzmy rodzinę zmiennych $Y_1, \ldots, Y_q$ określoną jako:

$$Y_k = X_0 + X_1k$$

(a) pokaż, że $Y_k$ tworzą rodzinę 2-niezależnych zmiennych - jaki płynie pożytek z wprowadzenia takich zmiennych, jeśli naszym celem jest otrzymanie jak największej rodziny 2-niezależnych zmiennych przy użyciu jak najmniejszej liczby losowych bitów? (porównaj np. z sytuacją, gdy wszystkie $Y_k$ losujemy niezależnie)

(b) pokaż, że $Y_k$ nie są 3-niezależne

(c) uogólnij tę konstrukcję na rodzinę zmiennych $k$-niezależnych dla dowolnego $k$

**Zadanie 5.**

Przypuśćmy, że $n$ osób posiada pewien sekret (losowo wybraną liczbę $x \in \mathbb{Z}_p$), który chcą podzielić na $n$ części tak, aby:

- każde $k$ osób na podstawie swoich części mogło odtworzyć sekret
- części posiadane przed dowolny podzbiór $i < k$ osób nie dawały żadnej informacji o sekrecie (tzn. z punktu widzenia tych osób każda wartość sekretu jest równie prawdopodobna)

Jak można tego dokonać? (wskazówka: rozpatrz wielomian stopnia $k-1$ nad $\mathbb{Z}_p$ o losowych współczynnikach)