Zadanie 1

Rozpatrzmy V — n-wymiarową przestrzeń nad ciałem $\mathrm{GF}(4)$. Niech $\alpha_1, \dots, \alpha_n$ będą wektorami bazy tej przestrzeni. Widać teraz, że każdy wektor V jest jednoznacznie zapisany jako $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$, gdzie $a_i \in \mathrm{GF}(4)$. Stąd istnieje bijekcja między wektorami V a ciągami $(a_1, \dots, a_n)$, tych zaś jest 4^n.

Teraz policzmy, na ile sposobów z przestrzeni n wymiarowej nad tym ciałem można wybrać k wektorów liniowo niezależnych, z uwzględnieniem kolejności. Pierwszy wektor można wybrać na $4^n - 1$ sposobów — może być nim każdy wektor niebędący wektorem zerowym. Drugi zaś już na $4^n - 4$ — nie może być on wielokrotnością pierwszego wektora. Ogólnie wybierając $(s+1)$-szy wektor ξ_{s+1} możemy wybrać go dowolnie pod warunkiem, że $\xi_{s+1} \notin \mathrm{lin}(\xi_1, \xi_2, \dots, \xi_s)$. Jednak $\mathrm{lin}(\xi_1, \xi_2, \dots, \xi_s)$ jest przestrzenią s-wymiarową (gdyż $\xi_1, \dots, \xi_s$ są liniowo niezależne), a więc $(s+1)$-szy wektor można wybrać na $4^n - 4^s$ sposobów (dowolny wektor z danej przestrzeni n-wymiarowej, nienależący do zapisanej przed chwilą przestrzeni s-wymiarowej). Stąd k wektorów liniowo niezależnych można wyznaczyć na $\prod\limits_{s=0}^{k-1}(4^n - 4^s)$ sposobów.

Aby policzyć liczbę podprzestrzeni k-wymiarowych przestrzeni V, zauważmy, że gdy policzyliśmy liczbę liniowo niezależnych k-tek wektorów, to każda taka k-tka rozpinała jakąś przestrzeń k-wymiarową. Jednak wiele k-tek mogło wyznaczać tę samą przestrzeń. Ustalmy więc jakąś przestrzeń k-wymiarową U i policzmy, ile k-tek ją wyznacza. Są to jednak dokładnie k-tki liniowo niezależne w tej przestrzeni. Jest ich więc $\prod\limits_{s=1}^{k-1}(4^k - 4^s)$.

Każdą podprzestrzeń k-wymiarową policzyliśmy więc $\prod\limits_{s=1}^{k-1}(4^k - 4^s)$ razy i uzyskaliśmy $\prod\limits_{s=0}^{k-1}(4^n - 4^s)$, a więc ich liczba wynosi

$$\frac{\prod\limits_{s=0}^{k-1}(4^n - 4^s)}{\prod\limits_{s=0}^{k-1}(4^k - 4^s)}$$

Zadanie 2

Dowód. Łatwo widać, z tw. Steiniza o wymianie, że $n \leqslant m$, a ponadto można dobrać takie wektory (wymierne, ale można przemnożyć przez wspólny mianownik) $\alpha_{n+1}, \dots, \alpha_m$, żeby układ $\alpha_1, \alpha_2, \dots, \alpha_m$ był liniowo niezależny w $\mathbb{Q}^m$. Odtąd możemy więc zakładać, że $n = m$.

Zapiszmy macierz A o wyrazach $a_{i,j}$, której kolejne wiersze będą wektorami $\alpha_1, \dots, \alpha_n$. Wykonajmy na macierzy A nad $\mathbb{Q}$ proces eliminacji Gaussa-Jordana (tzw. schodkowanie), w wyniku czego otrzymamy macierz jednostkową (bo operacje elementarne nie zmieniają liniowej niezależności wektorów, a jedynym możliwym wynikiem eliminacji Gaussa-Jordana dla macierzy o liniowo niezależnych rzędach jest macierz jednostkowa).

Jednak zapisujmy wszystkie liczby wymierne $\frac{u_i}{t_i}$ $(u_i, t_i \in \mathbb{Z} \setminus \{0\})$ przez jakie przemnażaliśmy wiersze macierzy w trakcie wykonywania eliminacji Gaussa-Jordana. Niech $T \in \mathbb{Z} \setminus \{0\}$ będzie równe iloczynowi wszystkich liczb $u_i \cdot t_i$.

Weźmy dowolną liczbę pierwszą p, która nie dzieli T. Wtedy nie dzieli ona żadnej z liczb t_i, u_i. Stąd gdy zaczniemy wykonywać proces eliminacji Gaussa-Jordana na macierzy A nad cialem $\mathbb{Z}_p$, możemy wykonywać dokładnie takie same operacje elementarne w dokładnie tej samej kolejności jak wykonywaliśmy nad $\mathbb{Q}$. Nigdy nie będziemy wtedy wykonywać mnożenia przez zerowy skalar (gdyż $p \nmid u_i$) oraz zawsze dzielenie będzie wykonalne, gdyż $p \nmid t_i$. To zaś oznacza, że w każdej chwili eliminacji Gaussa-Jordana jeśli nad $\mathbb{Q}$ było $a_{i,j} = \frac{x}{y}$, to nad $\mathbb{Z}_p$ będzie $a_{i,j} = xy^{-1} \pmod p$. Można to łatwo zobaczyć indukcyjnie, po liczbie zrobionych operacji elementarnych.

Stąd niezmiennik ten zachodzi także po zakończeniu eliminacji Gaussa-Jordana, gdzie daje on, że i nad $\mathbb{Z}_p$ macierz A jest schodkowalna do macierzy jednostkowej, co zaś oznacza, że nad $\mathbb{Z}_p$ układ $\alpha_1, \alpha_2, \dots, \alpha_n$ jest liniowo niezależny (co było na ćwiczeniach).

Jednak zauważmy, że jedynym warunkiem na p było to, żeby $p \nmid T$, gdzie T zależy jedynie od wektorów $\alpha_1, \dots, \alpha_n$. Jednak $T \neq 0$, więc ma jedynie skończenie wiele dzielników pierwszych, czyli prawie wszystkie liczby pierwsze go nie dzielą, czyli dla prawie wszystkich liczb pierwszych p układ $\alpha_1, \dots, \alpha_n$ jest liniowo niezależny nad $\mathbb{Z}_p$. $\square$

Zadanie 4

Dowód. Zauważmy, że skoro $W_1, \ldots, W_n$ są podprzestrzeniami właściwymi, to istnieją wektory $\xi_i \in V$, że $\xi_i \notin W_i$. Niech $U = \text{lin}(\xi_1, \xi_2, \ldots, \xi_n)$. Wtedy skoro $V = W_1 \cup W_2 \cup \ldots \cup W_n$, to $V \cap U = (W_1 \cup \ldots \cup W_n) \cap U = (W_1 \cap U) \cup (W_2 \cap U) \cup \ldots \cup (W_n \cap U)$, jednakże $V \cap U$ oraz $W_i \cap U$ są skończeniewymiaarowe, więc jeśli udowodnimy tezę dla przestrzeni skończeniewymiarowych, udowodnimy ją też dla przestrzeni nieskończeniewymiarowych.

Od teraz więc wszystkie przestrzenie są skończeniewymiarowe. Niech $d = \dim V$. Skoro $\dim W_i < \dim V$ (na mocy zadania 5a, gdyby $\dim V \leqslant \dim W_i$, a przecież $W_i \subset V$, to $W_i = V$ — sprzeczność), to $\dim W_i \leqslant d - 1$. Na mocy zadania 1a, $|W_i| \leqslant |k|^{d-1}$.

Załóżmy, że $n \leqslant |k|$ i zauważmy, że możemy oszacować z góry $|V|$ przez $|W_1| + \ldots + |W_n| - (n-1)$. Ten odjęty wyraz $n-1$ pochodzi stąd, że na pewno wektor zerowy należy do każdej z przestrzeni W_i, więc go policzyliśmy n-krotnie.

Stąd $|k|^d = |V| \leqslant |W_1| + |W_2| + \ldots + |W_n| - (n-1) \leqslant n|k|^{d-1} - (n-1) \leqslant |k|^d - (n-1)$. Gdyby $n = 1$, to $V = W_1$, czyli W_1 byłoby podprzestrzenią niewłaściwą. A więc $n > 1$ i oczywiście prawa strona jest mniejsza od lewej, co jest sprzecznością.

Stąd mamy, że $n > |k|$. □

Zadanie 5

Część a

Dowód. Niech $\sigma_1, \ldots, \sigma_{\dim B}$ będzie bazą przestrzeni B. Skoro $B \subseteq A$, to $\sigma_i \in A$ i są to wektory liniowo niezależne. To zaś na mocy tw. Steiniza daje, że $\dim A \geqslant \dim B$, co wraz z warunkiem zadania daje, że $\dim A = \dim B$, a więc $\sigma_1, \ldots, \sigma_{\dim B}$ jest bazą A, czyli $A = B$. □

Część b

Dowód. Niech $d = \dim(A \cap B)$. Oczywiście (używając twierdzenia Steiniza) $d = \dim(A \cap B) \leqslant \dim A \leqslant \dim B \leqslant \dim(A + B) = d + 1$. Stąd mamy trzy możliwości: 1) $\dim A = \dim B = d$, 2) $\dim A = \dim B = d + 1$, 3) $\dim A = d, \dim B = d + 1$.

Pierwsza z nich daje sprzeczność, gdyż wtedy $\dim(A \cap B) = \dim A = \dim B$, $A \cap B \subseteq A, B$, a więc $A = B = A \cap B$, a wtedy $A + B = A$, co się nie zgadza z tym, że $\dim(A + B) = 1 + \dim(A \cap B)$.

Druga z nich daje sprzeczność, gdyż wtedy $\dim(A + B) = \dim A = \dim B$, $A, B \subseteq (A + B)$, a więc $A = B = A + B$, ale wtedy $A \cap B = A$, co znów nie zgadza się z warunkiem zadania.

Tak więc $\dim A = d$, $\dim B = d + 1$. Jednak $\dim B = \dim(A + B)$ oraz $B \subseteq A + B$, a więc $B = A + B$. Z drugiej strony $\dim A = \dim(A \cap B)$, $A \cap B \subseteq A$, a więc $A = A \cap B$. □

Część c

Dowód. Niech $d = \dim(B \cap C)$. Oczywiście $d = \dim(B \cap C) \leqslant \dim B < \dim C \leqslant \dim(B + C) = d + 2$. Stąd mamy trzy możliwości: 1) $\dim B = d, \dim C = d + 1$, 2) $\dim B = d + 1, \dim C = d + 2$, 3) $\dim B = d, \dim C = d + 2$.

Pierwsza z nich daje, że $\dim(B + C) = \dim B + \dim C - \dim(B \cap C) = d + d + 1 - d = d + 1 \neq d + 2 = \dim(B + C)$ — sprzeczność.

Druga z nich daje, że $\dim(B + C) = \dim B + \dim C - \dim(B \cap C) = d + 1 + d + 2 - d = d + 3 \neq d + 2 = \dim(B + C)$ — sprzeczność.

Stąd $\dim B = d$, $\dim C = d + 2$. Jednak wtedy $\dim B = \dim(B \cap C)$ i $B \cap C \subseteq B$, więc $B \cap C = B$. Ponadto $\dim C = \dim(B + C)$, jednak $C \subseteq B + C$, więc $C = B + C$. □

Zadanie 6

Dowód. Załóżmy, że istnieje algorytm $\mathfrak{Alg}$ uruchamiany na liczbie n, mogący wykonywać zapytania o porównania pewnych dwóch rozłącznych podzbiorów monet o nieznanych mu masach $a_1, \ldots, a_n$, który po wykonaniu zawsze mniej niż $n - 1$ ważeń odpowiada prawidłowo czy wszystkie monety mają parami równą masę. Dla uproszcznia będę mówił o uruchomieniu algorytmu $\mathfrak{Alg}$ na wejściu $a_1, \ldots, a_n$, mimo że algorytm ten nie poznaje tego wejścia.

Można założyć, że algorytm ten wykona zawsze $n-2$ ważenia: jeśli w pewnym momencie zna już wynik, może i tak wykonać pewną ilość bezsensownych pomiarów, tak, żeby łącznie wykonał $n-2$ porównania.

Przygotujmy wejście $A = (a_1, \ldots, a_n)$, w którym $a_i = 1$ i uruchommy algorytm $\mathfrak{Alg}$. Oczywiście powinien on wykonać $n-2$ ważenia i zwrócić odpowiedź twierdzącą.

Niech i-te pytanie będzie postaci: „Czy zbiór $(a_{l_{i,1}}, \ldots, a_{l_{i,p_i}})$ jest lżejszy, cięższy czy ma równą masę ze zbiorem $(a_{r_{i,1}}, \ldots, a_{r_{i,q_i}})$?". Ułóżmy równanie ξ_i brzmiące: $f_{l_{i,1}} + f_{l_{i,2}} + \ldots + f_{l_{i,p_i}} = f_{r_{i,1}} + f_{r_{i,2}} + \ldots + f_{r_{i,q_i}}$.

Zauważmy, że układ równań $\xi_1, \xi_2, \ldots, \xi_{n-2}$ jest jednorodny, a więc przestrzeń jego rozwiązań jest liniowa. Jednak łatwo widać, że wymiar tej przestrzeni wynosi conajmniej 2 (np. wynika to z rank-nullity theorem). Można to też zobaczyć, dokonując eliminacji Gaussa na macierzy tego układu, i łatwo widać, że będzie conajwyżej $n-2$ schodków (gdyż w każdym wierszu może być conajwyżej jeden schodek), a więc przynajmniej 2 kolumny nie będą miały schodków, będą więc one odpowiadały zmiennym, które czynimy parametrami (być może będą też jakieś inne, gdy rząd macierzy jest mniejszy niż $n-2$, ale na pewno będą conajmniej dwa parametry). Łatwo więc widać (było na ćwiczeniach), że przestrzeń rozwiązań będzie przynajmniej wymiaru 2.

Niech więc α, β będą dwoma elementami bazy tej przestrzeni rozwiązań. Zauważmy, że conajwyżej jeden z nich może być wielokrotnością wektora $(1, 1, 1, \ldots, 1)$. Załóżmy więc, że wektor $\alpha = (f_1, f_2, \ldots, f_n)$ nie jest wielokrotnością $(1, 1, 1, \ldots, 1)$.

Teraz ustalmy ciąg wag monet $B = (b_1, \ldots, b_n) := (f_1 + M, f_2 + M, \ldots, f_n + M)$, gdzie $M = 2013 + \max(|f_1|, \ldots, |f_n|)$. Oczywiście $f_i + M > 0$.

Uruchommy algorytm $\mathfrak{Alg}$ dla wejścia B. Jeśli algorytm ten jest randomiowany, niech generator liczb losowych zwraca dokładnie te same wartości, co dla naszego pierwotnego wywołania $\mathfrak{Alg}(A)$.

Wtedy zauważmy, że odpowiedzi na zapytania:

- „Czy zbiór $(a_{l_{i,1}}, \ldots, a_{l_{i,p_i}})$ jest lżejszy, cięższy czy ma równą masę ze zbiorem $(a_{r_{i,1}}, \ldots, a_{r_{i,q_i}})$?"
- „Czy zbiór $(b_{l_{i,1}}, \ldots, b_{l_{i,p_i}})$ jest lżejszy, cięższy czy ma równą masę ze zbiorem $(b_{r_{i,1}}, \ldots, b_{r_{i,q_i}})$?"

są identyczne. Istotnie:

$$\begin{aligned}
\left(a_{l_{i,1}} + \ldots + a_{l_{i,p_i}}\right) - \left(a_{r_{i,1}} + \ldots + a_{r_{i,q_i}}\right) &= p_i - q_i \\
\left(b_{l_{i,1}} + \ldots + b_{l_{i,p_i}}\right) - \left(b_{r_{i,1}} + \ldots + b_{r_{i,q_i}}\right) &= \left(f_{l_{i,1}} + \ldots + f_{l_{i,p_i}} + Mp_i\right) - \left(f_{r_{i,1}} + \ldots + f_{r_{i,q_i}} + Mq_i\right) \\
&= M(p_i - q_i) + \left(f_{l_{i,1}} + \ldots + f_{l_{i,p_i}}\right) - \left(f_{r_{i,1}} + \ldots + f_{r_{i,q_i}}\right) \\
&= M(p_i - q_i)
\end{aligned}$$

Jednak $M > 0$, więc wielkości te mają jednakowy znak.

Stąd indukcyjnie (po liczbie zapytań) widzimy, że algorytm $\mathfrak{Alg}$ uruchomiony na wejściu A i na wejściu B zadaje dokładnie takie same pytania i uzyskuje dokładnie takie same odpowiedzi.

Stąd musi on dla wejścia B odpowiedzieć tak jak dla wejścia A, czyli stwierdzić, że wszystkie monety z B mają równą masę. Ale jednak tak nie jest, gdyż $(b_1, \ldots, b_n) = (\varpi, \varpi, \ldots, \varpi) \implies (f_1, \ldots, f_n) = (\varpi - M, \ldots, \varpi - M) = (\varpi - M)(1, 1, 1, \ldots, 1)$, a jednak tak wybraliśmy f_i, żeby to nie było prawdą.

Stąd algorytm $\mathfrak{Alg}$ odpowiedział błędnie dla wejścia B, czyli nie jest poprawny. $\square$