M O Ż N A   L E P I E J
M O Ż N A   W I Ę C E J

Wojciech Guzicki

Konferencja SEM (Elementarne, ale niebanalne)
Sielpia, 26 października 2018 r.

WOKÓŁ TWIERDZENIA

MANTELA

Zadanie 1. (II OMG, zadanie 3/II)
W przestrzeni danych jest 6 punktów, z których żadne cztery nie leżą na jednej płaszczyźnie. Łącząc niektóre z tych punktów narysowano 10 odcinków. Wykaż, że w ten sposób uzyskano co najmniej jeden trójkąt.

Inaczej. Dany jest graf G mający 6 wierzchołków i 10 krawędzi. Udowodnij, że ten graf zawiera trójkąt.

Zadanie 2. (XXXVII OM, zadanie 5/III)
W turnieju szachowym uczestniczy $2n$ ($n > 1$) zawodników, przy czym każdych dwóch spośród nich rozgrywa między sobą co najwyżej jedną partię. Udowodnij, że taki przebieg rozgrywek, w którym żadna trójka zawodników nie rozgrywa trzech partii między sobą, jest możliwy wtedy i tylko wtedy, gdy liczba wszystkich partii rozegranych w turnieju nie przekracza n^2.

Inaczej. Udowodnij, że istnieje graf bez trójkątów mający $2n$ wierzchołków i k krawędzi wtedy i tylko wtedy, gdy $k \leq n^2$.

TWIERDZENIE MANTELA

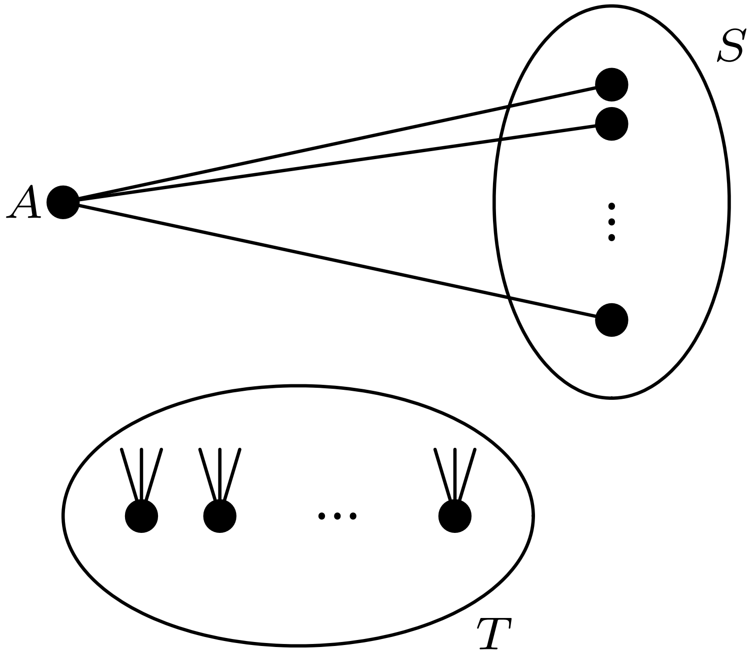
Twierdzenie 1. (Mantel, 1907) Dany jest graf G bez trójkątów, mający n wierzchołków i k krawędzi. Wówczas

$$k \leq \frac{n^2}{4}.$$

Inaczej. Dany jest graf G mający n wierzchołków i więcej niż $\frac{n^2}{4}$ krawędzi. Wówczas graf G zawiera trójkąt.

Dowód twierdzenia Mantela.

- Niech A będzie wierzchołkiem największego stopnia. Oznaczmy $m = d(A)$.
- Niech S będzie zbiorem wierzchołków sąsiadujących z A. Wtedy $|S| = m$.
- Niech T będzie zbiorem wierzchołków niesąsiadujących z A. Wtedy $|T| = n - m - 1$.
- Każda krawędź ma jeden koniec w A lub co najmniej jeden koniec w wierzchołku należącym do zbioru T.



$$k \leq m + m(n - m - 1) = m(n - m).$$

Wystarczy udowodnić, że:

$$m(n-m) \leq \frac{n^2}{4}.$$

Przekształcamy tę nierówność w sposób równoważny:

$$4m(n-m) \leq n^2,$$

$$4mn - 4m^2 \leq n^2,$$

$$0 \leq 4m^2 - 4mn + n^2,$$

$$0 \leq (2m-n)^2.$$

Ile to jest $\dfrac{n^2}{4}$?

- Jeśli $n = 2m$, to $\dfrac{n^2}{4} = m^2$.
- Jeśli $n = 2m + 1$, to $\dfrac{n^2}{4} = m(m+1) + \dfrac{1}{4}$.

Definicja. $$M(n) = \begin{cases} m^2, & \text{jeśli } \ n = 2m, \\ m(m+1), & \text{jeśli } \ n = 2m+1. \end{cases}$$

TWIERDZENIE MANTELA

Inne sformułowanie

Twierdzenie 1. Dany jest graf G mający n wierzchołków i co najmniej

$$M(n) + 1$$

krawędzi. Wówczas graf G zawiera trójkąt.

Ponadto, jeśli $k \leq M(n)$, to istnieje graf G bez trójkątów mający n wierzchołków i k krawędzi.

Różne kierunki uogólnień:

- Jeśli graf ma dużo krawędzi, to zawiera podgraf mający szczególne własności.

- Jeśli graf ma dużo krawędzi, to zawiera wiele podgrafów mających szczególne własności.

Zadanie 3. (V OMG, zawody II stopnia, zadanie 4)
Na przyjęciu spotkało się sześć osób. Okazało się, że każda z nich ma wśród pozostałych dokładnie trzech znajomych. Wykaż, że pewne cztery z tych osób mogą usiąść przy okrągłym stole w taki sposób, aby każda z nich siedziała pomiędzy swoimi dwoma znajomymi.

Zadanie 4. (III Mała OM, zawody III stopnia dla uczniów klas starszych, zadanie 6)
W pewnej konferencji uczestniczy 1995 osób. Każda z nich ma wśród pozostałych co najmniej 45 znajomych. Wykaż, że można znaleźć takich czterech uczestników tej konferencji, którzy mogą usiąść przy okrągłym stole tak, by każdy siedział obok swoich znajomych.

Zadanie 5. (LXVIII OM, zawody I stopnia, zadanie 6)
W balu uczestniczyło 20 kawalerów i 20 dam. W każdym z 99 tańców tańczyła dokładnie jedna para, za każdym razem inna. W każdej parze tańczyła dama z kawalerem. Dowieść, że istnieje takich dwóch kawalerów i takie dwie damy, że każdy z tych dwóch kawalerów zatańczył z obiema tymi damami.

Ostatnie trzy zadania mają wspólną postać:

- Jeśli graf G ma dużo krawędzi, to zawiera czworokąt.

Twierdzenie 2. (Reiman, 1958) Dany jest graf G mający n wierzchołków i k krawędzi. Wówczas, jeśli

$$k > \frac{n}{4} \cdot (1 + \sqrt{4n - 3}),$$

to graf G zawiera czworokąt.

To twierdzenie wystarczy do rozwiązania zadania 3, ale jest za słabe, by rozwiązać zadanie 4.

Mamy bowiem

$$\frac{6}{4}\cdot\left(1+\sqrt{4\cdot 6-3}\right)=\frac{3}{2}\cdot\left(1+\sqrt{21}\right)\approx 8{,}37,$$

więc każdy graf mający 6 wierzchołków i co najmniej 9 krawędzi zawiera czworokąt. Można udowodnić więcej: wystarczy 8 krawędzi.

Z drugiej strony, graf w zadaniu 4 ma co najmniej 44888 krawędzi, ale

$$\frac{1995}{4}\cdot\left(1+\sqrt{4\cdot 1995-3}\right)\approx 45044{,}133.$$

Dla grafów dwudzielnych twierdzenie Reimana ma następującą postać.

Twierdzenie 3. Dany jest graf dwudzielny G o następujących własnościach:

- zbiór wierzchołków jest sumą zbiorów $A \cup B$, gdzie $A \cap B = \varnothing$ oraz $|A| = |B| = n$,
- każda krawędź ma jeden koniec w zbiorze A i drugi w zbiorze B,
- liczba krawędzi jest większa od

$$\frac{n}{2} \cdot (1 + \sqrt{4n - 3}).$$

Wówczas graf G zawiera czworokąt.

Dla przypomnienia:

Zadanie 5. (LXVIII OM, zawody I stopnia, zadanie 6)
W balu uczestniczyło 20 kawalerów i 20 dam. W każdym z 99 tańców tańczyła dokładnie jedna para, za każdym razem inna. W każdej parze tańczyła dama z kawalerem. Dowieść, że istnieje takich dwóch kawalerów i takie dwie damy, że każdy z tych dwóch kawalerów zatańczył z obiema tymi damami.

Ostatnie twierdzenie wystarcza do rozwiązania zadania 5. Mamy bowiem dla $n = 20$:

$$\frac{n}{2} \cdot (1 + \sqrt{4n - 3}) = \frac{20}{2} \cdot (1 + \sqrt{4 \cdot 20 - 3}) = 10(1 + \sqrt{77}) \approx 97{,}75.$$

Wystarczy zatem, by na przyjęciu było 98 tańców.

Na zakończenie tej części wykładu popatrzmy na jeszcze jedno twierdzenie podobnej postaci.

Twierdzenie 4. (Turán, 1941) Dany jest graf G mający n wierzchołków i więcej niż

$$T(n,p)=\left(1-\frac{1}{p-1}\right)\cdot\frac{n^2}{2}$$

krawędzi. Wówczas graf G zawiera podgraf pełny mający p wierzchołków. Ponadto, jeśli $k \leq T(n,p)$, to istnieje graf G mający n wierzchołków i k krawędzi oraz niezawierający podgrafu pełnego mającego p wierzchołków.

Zauważmy, że dla $p=3$ otrzymujemy twierdzenie Mantela.

Inne wzmocnienie twierdzenia Mantela jest zawarte w następującym twierdzeniu:

Twierdzenie 5. (Rademacher, 1941, nieopublikowane) Dany jest graf G mający $n \geq 3$ wierzchołków i $k = M(n)+1$ krawędzi. Wówczas graf G zawiera co najmniej $\left\lfloor \frac{n}{2} \right\rfloor$ trójkątów.

Znany dowód twierdzenia Rademachera, pochodzący od Erdösa, przebiega przez indukcję. Pokażę na przykładzie główny krok tej indukcji.

- **Założenie indukcyjne** (dla $n = 5$): jeśli graf G ma 5 wierzchołków i 7 krawędzi, to zawiera co najmniej dwa trójkąty.

- **Teza indukcyjna:** jeśli graf G ma 6 wierzchołków i 10 krawędzi, to zawiera co najmniej trzy trójkąty.

W dowodzie tezy indukcyjnej będziemy rozpatrywać dwa przypadki:

- Graf G ma wierzchołek v stopnia co najwyżej 2: $d(v) \leq 2$.

- Wszystkie wierzchołki grafu G mają stopień równy co najmniej 3.

Przypadek 1. Graf G ma wierzchołek v stopnia co najwyżej 2: $d(v) \leq 2$.

Usuńmy z grafu wierzchołek v oraz usuńmy dwie krawędzie, w tym wszystkie krawędzie wychodzące z wierzchołka v. Otrzymujemy graf H mający 5 wierzchołków i 8 krawędzi. Z twierdzenia Mantela wynika, że graf H ma co najmniej jeden trójkąt. Niech będzie to trójkąt abc.

Usuńmy teraz z grafu H krawędź ab. Otrzymamy graf K mający 5 wierzchołków i 7 krawędzi. Z założenia indukcyjnego wynika, że graf K ma co najmniej dwa trójkąty.

Oczywiście te dwa trójkąty są także trójkątami grafu G. Wraz z trójkątem abc mamy zatem w grafie G co najmniej trzy trójkąty.

Przypadek 2. Każdy wierzchołek grafu G ma stopień równy co najmniej 3.

Wówczas w grafie G istnieją co najwyżej dwa wierzchołki stopnia co najmniej 4. Przypuśćmy bowiem, że:

$$d(v_1), d(v_2), d(v_3) \geq 4 \quad \text{oraz} \quad d(v_4) = d(v_5) = d(v_6) = 3.$$

Wówczas mamy nierówność

$$20 = d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) + d(v_6) \geq 3 \cdot 4 + 3 \cdot 3 = 21,$$

która jest nieprawdziwa. Teraz korzystamy z twierdzenia Mantela. W grafie G istnieje co najmniej jeden trójkąt, na przykład abc.

Przypadek 2 – cd. Co najmniej jeden wierzchołek trójkąta abc ma stopień równy 3, niech będzie to wierzchołek a.

Usuwamy z grafu G wierzchołek a wraz z wychodzącymi z niego trzema krawędziami. Otrzymujemy graf H, który ma 5 wierzchołków i 7 krawędzi. Z założenia indukcyjnego wynika, że ma on co najmniej 2 trójkąty. Te trójkąty są także trójkątami grafu G.

Wraz z trójkątem abc, który zniszczyliśmy usuwając z grafu G wierzchołek a, graf G ma zatem co najmniej 3 trójkąty. To kończy dowód tezy indukcyjnej.

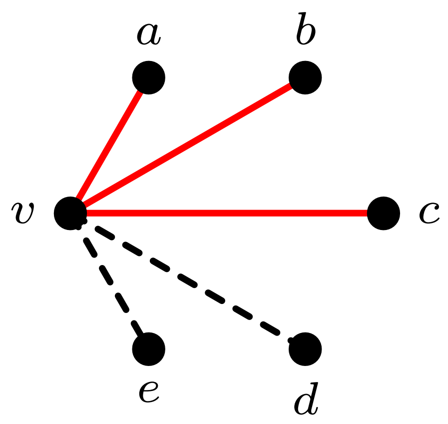
WOKÓŁ TWIERDZENIA

RAMSEYA

Zadanie 6. (XVII OM, zadanie 3/II)
Na płaszczyźnie obrano 6 punktów, z których żadne trzy nie leżą na jednej prostej i wykreślono wszystkie odcinki łączące parami te punkty. Niektóre z odcinków wykreślono przy tym kolorem czerwonym, a inne niebieskim. Dowieść, że któreś trzy z danych punktów są wierzchołkami trójkąta o bokach jednego koloru.

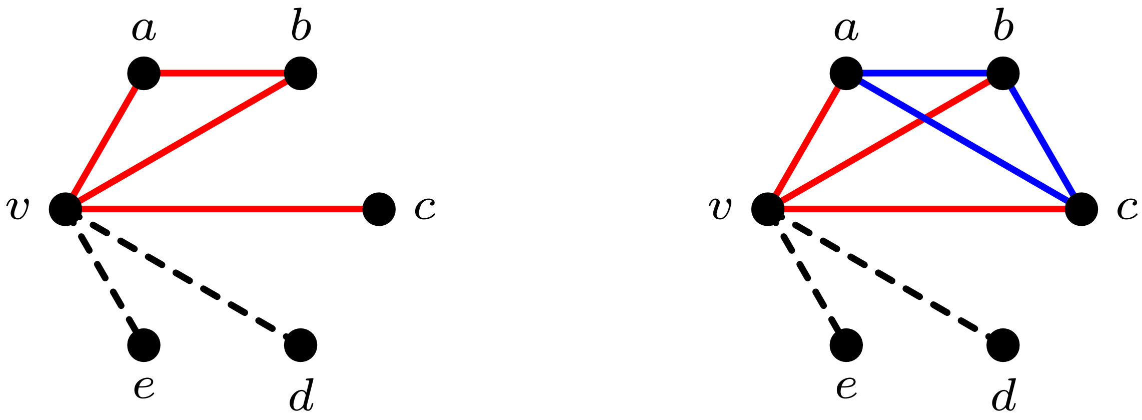
Inaczej. Dany jest graf pełny G o sześciu wierzchołkach, w którym każda krawędź jest czerwona lub niebieska. Udowodnij, że w tym grafie istnieje co najmniej jeden jednokolorowy trójkąt.

Rozwiązanie. Wybieramy wierzchołek v grafu. Wychodzi z niego 5 krawędzi w dwóch kolorach. Z zasady szufladkowej wynika, że co najmniej trzy krawędzie są tego samego koloru. Możemy bez straty ogólności założyć, że krawędzie va, vb i vc są czerwone.



(Krawędzie zaznaczone liniami przerywanymi są dowolnego koloru: czerwone lub niebieskie.)

Przypuśćmy, że któraś z krawędzi ab, ac lub bc jest czerwona; niech na przykład będzie to krawędź ab. Wówczas mamy czerwony trójkąt abv (zob. rysunek po lewej stronie). Jeśli zaś te trzy krawędzie są niebieskie, to mamy niebieski trójkąt abc (zob. rysunek po prawej stronie).



Różne kierunki uogólnień.

Przypuśćmy, że mamy dany graf pełny mający n wierzchołków, którego krawędzi zostały pokolorowane. Wówczas:

- Jeśli liczba n jest duża i mamy dwa kolory, to graf G zawiera spory podgraf pełny jednokolorowy. Podobnie, jeśli liczba n jest duża i mamy więcej kolorów, to graf G zawiera spory podgraf pełny jednokolorowy.
- Jeśli liczba n jest duża i mamy więcej kolorów, to graf G zawiera jednokolorowy trójkąt.
- Jeśli liczba n jest duża i mamy dwa kolory, to graf G zawiera sporo jednokolorowych trójkątów.

Twierdzenie 6. (Ramsey, 1930) Przypuśćmy, że dane są dwie liczby naturalne k i l. Niech następnie

$$n = \binom{k+l-2}{k-1}.$$

Przypuśćmy następnie, że każda krawędź grafu K_n (tzn. grafu pełnego mającego n wierzchołków) została pokolorowana jednym z dwóch kolorów: czerwonym lub niebieskim. Wówczas graf K_n zawiera:

- jednokolorowy czerwony podgraf pełny mający k wierzchołków

lub

- jednokolorowy niebieski podgraf pełny mający l wierzchołków.

Twierdzenie 6 — ogólnie. (Ramsey, 1930) Przypuśćmy, że dane są liczby naturalne $m \geq 2$ oraz $k_1, \ldots, k_m$. Wówczas istnieje liczba naturalna n o następującej własności:

- jeśli każdą krawędź grafu K_n (tzn. grafu pełnego mającego n wierzchołków) pokolorujemy jednym z m kolorów $C_1, \ldots, C_m$, to graf K_n będzie zawierał:

$\star$ jednokolorowy podgraf pełny koloru C_1 mający k_1 wierzchołków

lub … lub

$\star$ jednokolorowy podgraf pełny koloru C_m mający k_m wierzchołków.

Zadanie 7. (VI MOM, zadanie 4)
Siedemnaście osób wymienia pomiędzy sobą listy, przy czym każda osoba koresponduje z każdą z pozostałych. Przedmiotem korespondencji są trzy różne zagadnienia, a każda para osób omawia korespondencyjnie tylko jedno z tych zagadnień. Udowodnij, że są takie trzy osoby, których wzajemna korespondencja dotyczy jednego i tego samego zagadnienia.

Inaczej. Każda krawędź grafu pełnego K_{17} jest pokolorowana jednym z trzech kolorów: czerwonym, niebieskim lub zielonym. Udowodnij, że w tym grafie istnieje jednokolorowy trójkąt.

Rozwiązanie. Weźmy dowolny wierzchołek v grafu K_{17}. Ten wierzchołek sąsiaduje z 16 wierzchołkami; krawędzie wychodzące z wierzchołka v są pokolorowane co najwyżej trzema różnymi kolorami. Z zasady szufladkowej wynika, że co najmniej sześć z tych krawędzi ma ten sam kolor; bez straty ogólności możemy przyjąć, że krawędzie va, vb, vc, vd, ve i vf są czerwone. Mamy teraz dwa przypadki.

Przypadek 1. Co najmniej jedna krawędź łącząca dwa wierzchołki spośród a, b, c, d, e i f jest czerwona. Niech na przykład będzie to krawędź ab. Wówczas trójkąt abv jest czerwony.

Przypadek 2. Wszystkie krawędzie łączące wierzchołki a, b, c, d, e i f są niebieskie lub zielone. Te sześć wierzchołków wraz z łączącymi je krawędziami tworzą graf pełny K_6, którego każda krawędź jest pokolorowana jednym z dwóch kolorów: niebieskim lub zielonym.

Wystarczy teraz skorzystać z zadania 6, by stwierdzić, że ten graf ma jednokolorowy trójkąt (niebieski lub zielony). Zatem nasz graf K_{17} także i w tym przypadku zawiera trójkąt jednokolorowy.

Zadanie 8. (XXXVII OM, zadanie 2/II)
W turnieju szachowym uczestniczy 66 zawodników, każdy z każdym rozgrywa jedną partię, rozgrywki odbywają się w czterech miastach. Udowodnij, że pewna trójka zawodników rozgrywa wszystkie partie między sobą w tym samym mieście.

Inaczej. Każda krawędź grafu pełnego K_{66} jest pokolorowana jednym z czterech kolorów: czerwonym, niebieskim, zielonym lub żółtym. Udowodnij, że w tym grafie istnieje jednokolorowy trójkąt.

Rozwiązanie. Weźmy dowolny wierzchołek v grafu K_{66}. Ten wierzchołek sąsiaduje z 65 wierzchołkami; krawędzie wychodzące z wierzchołka v są pokolorowane co najwyżej czterema różnymi kolorami. Z zasady szufladkowej wynika, że co najmniej 17 z tych krawędzi ma ten sam kolor; bez straty ogólności możemy przyjąć, że krawędzie $va_1, \ldots, va_{17}$ są czerwone. Mamy teraz dwa przypadki.

Przypadek 1. Co najmniej jedna krawędź łącząca dwa wierzchołki spośród $a_1, \ldots, a_{17}$ jest czerwona. Niech na przykład będzie to krawędź a_1a_2. Wówczas trójkąt a_1a_2v jest czerwony.

Przypadek 2. Wszystkie krawędzie łączące wierzchołki $a_1, \ldots, a_{17}$ są niebieskie, zielone lub żółte. Te 17 wierzchołków wraz z łączącymi je krawędziami tworzą graf pełny K_{17}, którego każda krawędź jest pokolorowana jednym z trzech kolorów.

Wystarczy teraz skorzystać z zadania 7, by stwierdzić, że ten graf ma jednokolorowy trójkąt (niebieski, zielony lub żółty). Zatem nasz graf K_{66} także i w tym przypadku zawiera trójkąt jednokolorowy.

Zdefiniujmy teraz liczby M_n wzorami rekurencyjnymi:

$$\begin{aligned} M_1 &= 3, \\ M_n &= n \cdot M_{n-1} - n + 2 \quad \text{dla } n \geq 2. \end{aligned}$$

Niech teraz $m = M_n$ dla pewnej liczby naturalnej n.

Można łatwo udowodnić przez indukcję, że jeśli każdą krawędź grafu pełnego K_m pokolorujemy jednym z n kolorów, to w tym grafie istnieje jednokolorowy trójkąt, tzn. istnieją wierzchołki a, b i c takie, że krawędzie ab, ac i bc mają ten sam kolor.

W szczególności mamy:

$$M_1 = 3, \quad M_2 = 6, \quad M_3 = 17, \quad M_4 = 66, \quad M_5 = 327$$

oraz

$$M_6 = 1958.$$

Ciekawostka:

$$M_n = \lfloor \mathrm{e} \cdot n! \rfloor + 1.$$

Zadanie 9. (XX MOM, zadanie 6)
Członkowie pewnego stowarzyszenia międzynarodowego pochodzą z 6 różnych krajów. Lista członków zawiera 1978 nazwisk ponumerowanych liczbami $1, 2, \ldots, 1978$. Udowodnij, że pewien członek ma na liście numer równy sumie numerów dwóch członków pochodzących z tego, co on kraju lub równy podwojonemu numerowi członka również z tego kraju.

Inaczej. Każdą liczbę ze zbioru $\{1, 2, \ldots, 1978\}$ pokolorowano jednym z sześciu kolorów. Udowodnij, że istnieją w tym zbiorze liczby a, b i c tego samego koloru takie, że $a + b = c$ (przy czym liczby a i b nie muszą być różne).

Rozwiązanie zadania 9.

Wystarczy 1957 osób. Weźmy dowolne kolorowanie

$$c : \{1, 2, \ldots, 1957\} \to \{1, 2, 3, 4, 5, 6\}$$

liczb ze zbioru $\{1, 2, \ldots, 1957\}$ sześcioma kolorami.

Rozważamy graf $G = K_{1958}$, którego wierzchołkami są liczby ze zbioru

$$\{0, 1, 2, \ldots, 1957\}.$$

Kolorujemy krawędzie tego grafu sześcioma kolorami.

Niech $0 \leq i, j \leq 1957$. Wówczas przyjmujemy

$$c^*(ij) = c(|i-j|).$$

Ponieważ $M_6 = 1958$, więc graf G zawiera jednokolorowy trójkąt ijk (gdzie $i < j < k$).

$$c^*(ij) = c^*(jk) = c^*(ik),$$

czyli

$$c(j-i) = c(k-j) = c(k-i).$$

Wystarczy przyjąć

$$a = j - i, \quad b = k - j \quad \text{oraz} \quad c = k - i,$$

by otrzymać jednokolorową trójkę (a, b, c) taką, że

$$a + b = c.$$

Twierdzenie 7. (Schur, 1916) Dana jest liczba naturalna $n \geq 2$. Wówczas istnieje liczba naturalna M o następującej własności:

- jeśli każdą liczbę ze zbioru $A = \{1, 2, \ldots, M\}$ pokolorujemy jednym z n kolorów, to w zbiorze A istnieją liczby a, b i c tego samego koloru takie, że
$$a + b = c$$
(przy czym liczby a i b nie muszą być różne).

Tak jak w zadaniu 9 wystarczy przyjąć

$$M = M_n - 1 = \lfloor \mathrm{e} \cdot n! \rfloor.$$

Znalezienie najmniejszej liczby M o własności podanej w twierdzeniu Schura jest poważnym problemem otwartym. Można łatwo udowodnić, że jeśli $n = 2$, to $M = 5$. Podobnie można udowodnić, że jeśli $n = 3$, to $M = 14$. Nietrudne obliczenia komputerowe (przeprowadzone w latach 60-tych XX w.) pokazały, że jeśli $n = 4$, to $M = 45$.

W 2017 roku udowodniono (tym razem za pomocą wielkich obliczeń komputerowych), że jeśli $n = 5$, to $M = 161$. Wykazano także, że istnieje $2\,447\,113\,088$ kolorowań zbioru $\{1, 2, \ldots, 160\}$ bez jednokolorowej trójki (a, b, c) spełniającej równanie $a + b = c$.

Twierdzenie 8. (Goodman, 1959) Przypuśćmy, że każdą krawędź grafu pełnego K_6 pokolorowano jednym z dwóch kolorów: czerwonym lub niebieskim. Wówczas w tym grafie istnieją co najmniej dwa trójkąty jednokolorowe.

Dowód. Zauważmy najpierw, że graf K_6 zawiera

$$\binom{6}{3} = 20$$

trójkątów. Wykażemy, że zawiera co najwyżej 18 trójkątów różnokolorowych (tzn. takich, które mają wierzchołki dwóch kolorów). To oczywiście zakończy dowód.

Niech teraz v będzie dowolnym wierzchołkiem grafu K_6. Wówczas symbolem $d_c(v)$ oznaczymy liczbę czerwonych krawędzi wychodzących z wierzchołka v:

$$d_c(v) = \big|\{w : \text{ krawędź } vw \text{ jest czerwona}\}\big|.$$

Liczba niebieskich krawędzi wychodzących z wierzchołka v jest wówczas równa

$$5 - d_c(v).$$

Następnie przypuśćmy, że a, b i c są wierzchołkami różnokolorowego trójkąta w naszym grafie.

Niech na przykład krawędź ab będzie czerwona, a krawędzie ac i bc będą niebieskie.

Wtedy z wierzchołków a i b wychodzą dwie krawędzie tego trójkąta różnych kolorów, natomiast z wierzchołka c wychodzą dwie krawędzie tego trójkąta tego samego koloru.

Popatrzmy teraz na dowolny wierzchołek v naszego grafu i przypuśćmy, że wychodzą z niego dwie krawędzie vx i vy różnych kolorów.

Wtedy oczywiście trójkąt vxy jest różnokolorowy. Stąd wynika, że liczba trójkątów różnokolorowych zawierających ustalony wierzchołek v, będący końcem krawędzi różnych kolorów w tym trójkącie, jest równa

$$d_c(v) \cdot (5 - d_c(v)).$$

Zatem liczba trójkątów różnokolorowych jest równa

$$\frac{1}{2} \cdot \sum_{v} d_c(v) \cdot (5 - d_c(v)).$$

Ponieważ dla każdej liczby całkowitej x mamy nierówność

$$(x-2)(x-3) \geq 0,$$

czyli

$$x(5-x) \leq 6,$$

więc liczba trójkątów różnokolorowych jest niewiększa od

$$\frac{1}{2} \cdot \sum_{v} 6 = \frac{1}{2} \cdot 6 \cdot 6 = 18.$$

To kończy dowód.

Ogólnie:

Liczba trójkątów jednokolorowych w dowolnie pokolorowanym grafie K_n jest równa:

$$T = \frac{n(n-1)(n-2)}{6} - \frac{1}{2} \cdot \sum_v d_c(v) \cdot (n - 1 - d_c(v)).$$

Twierdzenie 9. (Goodman, 1959) Dany jest graf pełny K_n, w którym każda krawędź jest czerwona lub niebieska. Wówczas w tym grafie istnieje co najmniej $T(n)$ jednokolorowych trójkątów, gdzie:

$$T(n) = \begin{cases} \frac{n(n-2)(n-4)}{24}, & \text{jeśli } 2 \mid n, \\ \frac{n(n-1)(n-5)}{24}, & \text{jeśli } 4 \mid n-1, \\ \frac{(n+1)(n-3)(n-4)}{24}, & \text{jeśli } 4 \mid n+1. \end{cases}$$

W szczególności mamy:

$$\begin{aligned} T(6) &= 2, \\ T(7) &= 4, \\ T(8) &= 8, \\ T(9) &= 12, \\ T(10) &= 20, \\ T(11) &= 28, \\ T(12) &= 40. \end{aligned}$$

TWIERDZENIE EGZ

P. Erdös, A. Ginzburg, A. Ziv

Zadanie 10. (Singapore Secondary Schools Math Olympiad, 1990) Mamy danych 5 liczb całkowitych. Udowodnij, że istnieją wśród nich dokładnie 3 liczby, których suma jest podzielna przez 3.

Zadanie 11. (Singapore Secondary Schools Math Olympiad, 1990) Mamy danych 17 liczb całkowitych. Udowodnij, że istnieje wśród nich dokładnie 9 liczb, których suma jest podzielna przez 9.

Rozwiązanie zadania 10 wynika łatwo z zasady szufladkowej Dirichleta.

W rozwiązaniu zadania 11 skorzystamy sześciokrotnie z zadania 10.

Bierzemy dowolne 5 liczb spośród danych 17 liczb. Wśród nich znajdują się 3 liczby a_1, a_2, a_3, których suma dzieli się przez 3:

$$a_1 + a_2 + a_3 = 3k_1.$$

Te 3 liczby odkładamy na bok. Pozostało 14 liczb.

Powtarzamy tę konstrukcję: bierzemy dowolne 5 liczb i wśród nich znajdujemy 3 liczby a_4, a_5, a_6, których suma dzieli się przez 3:

$$a_4 + a_5 + a_6 = 3k_2.$$

Te trzy liczby także odkładamy na bok. Pozostało 11 liczb.

W podobny sposób, jeszcze trzykrotnie korzystając z zadania 10, znajdujemy następne trzy takie trójki liczb:

$$a_7 + a_8 + a_9 = 3k_3, \quad a_{10} + a_{11} + a_{12} = 3k_4, \quad a_{13} + a_{14} + a_{15} = 3k_5.$$

Wśród pięciu liczb k_1, k_2, k_3, k_4, k_5 znajdują się 3 liczby, których suma dzieli się przez 3.

Bez straty ogólności (w razie potrzeby zmienimy numerację wybranych liczb) możemy założyć, że

$$k_1 + k_2 + k_3 = 3m.$$

Wówczas

$$a_1+a_2+a_3+\ldots+a_9 = 3k_1+3k_2+3k_3 = 3(k_1+k_2+k_3) = 3\cdot 3m = 9m.$$

To kończy rozwiązanie zadania.

Własność $EGZ(n)$

Spośród dowolnych $2n-1$ liczb całkowitych można wybrać dokładnie n liczb, których suma jest podzielna przez n.

Zadania 10 i 11 dowodzą własności

$$EGZ(3) \quad \text{oraz} \quad EGZ(9).$$

Twierdzenie 10. Przypuśćmy, że dane są liczby naturalne $m, n \geq 2$ takie, że prawdziwe są własności $EGZ(m)$ oraz $EGZ(n)$. Wówczas prawdziwa jest też własność $EGZ(mn)$.

Dowód. Powtarzamy rozumowanie z rozwiązania zadania 11. Przypuśćmy, że mamy $2mn - 1$ liczb całkowitych.

Wybieramy z nich dowolne $2m - 1$ liczb i wśród nich znajdujemy m liczb, których suma jest podzielna przez m:

$$a_1 + a_2 + \ldots + a_m = k_1 \cdot m$$

dla pewnej liczby całkowitej k_1. Te m liczb odkładamy na bok. Pozostaje $2mn - m - 1$ liczb.

Ponieważ $n \geq 2$, więc $2mn - m - 1 \geq 2m - 1$.

Zatem spośród pozostałych liczb możemy wybrać $2m-1$ liczb i wśród nich znajdujemy m liczb, których suma jest podzielna przez m:

$$a_{m+1} + a_{m+2} + \ldots + a_{2m} = k_2 \cdot m$$

dla pewnej liczby całkowitej k_2.

Te liczby znów odkładamy na bok. Pozostaje $2mn - 2m - 1$ liczb.

Ponieważ $n \geq 2$, więc $2mn - 2m - 1 \geq 2m - 1$.

Zatem spośród pozostałych liczb znów możemy wybrać $2m - 1$ liczb i wśród nich jeszcze raz znajdujemy m liczb, których suma jest podzielna przez m:

$$a_{2m+1} + a_{2m+2} + \ldots + a_{3m} = k_3 \cdot m$$

dla pewnej liczby całkowitej k_3.

Te liczby także odkładamy na bok. Pozostaje $2mn - 3m - 1$ liczb.

Tę czynność możemy wykonać $2n-1$ razy.

Przypuśćmy bowiem, że wykonaliśmy ją już co najwyżej $2n-2$ razy. Wybraliśmy zatem co najwyżej $m \cdot (2n-2)$ liczb.

Zostało zatem co najmniej

$$(2mn-1)-m(2n-2)=2mn-1-2mn+2m=2m-1$$

liczb. Zatem spośród nich jeszcze co najmniej jeden raz będziemy mogli wybrać m liczb, których suma jest podzielna przez m.

W ten sposób możemy wybrać $2n-1$ zestawów po m liczb takich, że w każdym zestawie suma wybranych m liczb jest podzielna przez m. Mamy zatem:

$$\begin{aligned} a_1 + a_2 + \ldots + a_m &= k_1 \cdot m, \\ a_{m+1} + a_{m+2} + \ldots + a_{2m} &= k_2 \cdot m, \\ a_{2m+1} + a_{2m+2} + \ldots + a_{3m} &= k_3 \cdot m, \\ \ldots \quad \ldots \quad \ldots \quad &\quad \ldots \\ a_{(2n-2)m+1} + a_{(2n-2)m+2} + \ldots + a_{(2n-1)m} &= k_{2n-1} \cdot m. \end{aligned}$$

Mamy teraz $2n-1$ liczb $k_1, k_2, \ldots, k_{2n-1}$. Wśród nich jest n liczb, których suma jest podzielna przez n. Po odpowiednim przenumerowaniu tych liczb można założyć, że

$$k_1 + k_2 + \ldots k_n = l \cdot n$$

dla pewnej liczby całkowitej l. Wówczas

$$(a_1 + \ldots + a_m) + (a_{m+1} + \ldots + a_{2m}) + \ldots + (a_{(n-1)m+1} + \ldots + a_{nm}) =$$
$$= k_1 m + k_2 m + \ldots + k_n m = m(k_1 + k_2 + \ldots + k_n) = mnl.$$

Znaleźliśmy więc mn liczb, których suma jest podzielna przez mn. To kończy dowód twierdzenia.

Twierdzenie 11. Dla każdej liczby pierwszej p prawdziwa jest własność $EGZ(p)$.

Wniosek. (Erdös, Ginzburg, Ziv, 1961) Dla każdej liczby naturalnej $n \geq 2$ prawdziwa jest własność $EGZ(n)$.

Pokażę dwa dowody twierdzenia 11. Pierwszy dowód pokażę na dwóch przykładach: $p = 3$ oraz $p = 5$.

Najpierw udowodnię własność $EGZ(3)$. Bierzemy 5 dowolnych liczb całkowitych

$$a_1, \quad a_2, \quad a_3, \quad a_4 \quad \text{oraz} \quad a_5.$$

Patrzymy następnie na zbiór liczb od 1 do 9:

$$K = \{1, 2, 3, 4, 5\}.$$

Zbiór K ma 10 podzbiorów trzyelementowych.

Oto te 10 podzbiorów:

$$\begin{aligned} P_1 &= \{1,2,3\}, & P_6 &= \{1,4,5\},\\ P_2 &= \{1,2,4\}, & P_7 &= \{2,3,4\},\\ P_3 &= \{1,2,5\}, & P_8 &= \{2,3,5\},\\ P_4 &= \{1,3,4\}, & P_9 &= \{2,4,5\},\\ P_5 &= \{1,3,5\}, & P_{10} &= \{3,4,5\}. \end{aligned}$$

Każdemu podzbiorowi P_n zbioru K odpowiada suma pewnych trzech liczb spośród liczb a_1, a_2, a_3, a_4, a_5.

Jeśli
$$P_n = \{i, j, k\},$$
to przyjmujemy
$$S(n) = a_i + a_j + a_k$$

Naszym celem jest wykazanie, że istnieje liczba n taka, że
$$1 \leq n \leq 10 \quad \text{oraz} \quad 3 \mid S(n).$$

Teraz każdemu podzbiorowi P_n przyporządkowujemy w pewien sposób (który pokażę dalej) pewną liczbę naturalną $T(n)$ w taki sposób, że:

- jeśli $3 \mid S(n)$, to $\quad T(n) \equiv 0 \pmod 3$,
- jeśli $3 \nmid S(n)$, to $\quad T(n) \equiv 1 \pmod 3$,
- $T(1) + T(2) + \ldots + T(10) \equiv 0 \pmod 3$.

To zakończy dowód twierdzenia.

Przypuśćmy, że dla każdej liczby naturalnej n takiej, że $1 \leq n \leq 10$ mamy

$$3 \nmid S(n).$$

Wówczas dla każdej takiej liczby n mamy

$$T(n) \equiv 1 \pmod{3},$$

skad wynika, że

$$0 \equiv T(1) + T(2) + \ldots + T(10) \equiv 10 \cdot 1 = 10 \equiv 1 \pmod{1}.$$

To jest niemożliwe. Otrzymana sprzeczność dowodzi, że co najmniej jedna suma $S(n)$ jest podzielna przez 3.

Musimy teraz zdefiniować liczby $T(n)$. Przyjmujemy

$$T(n) = S(n)^2.$$

Wówczas mamy:

- jeśli $3 \mid S(n)$, to $3 \mid S(n)^2$, więc

$$T(n) \equiv 0 \pmod 3,$$

- jeśli $3 \nmid S(n)$, to można łatwo pokazać, że

$$S(n)^2 \equiv 1 \pmod 3,$$

  czyli

$$T(n) \equiv 1 \pmod 3.$$

Do udowodnienia pozostaje tylko kongruencja

$$T(1) + T(2) + \ldots + T(10) \equiv 0 \pmod 3.$$

Przyjrzyjmy się teraz dokładniej liczbom $T(n)$. Przypuśćmy, że

$$P(n) = \{i, j, k\},$$

oraz

$$S(n) = a_i + a_j + a_k.$$

Popatrzmy, jak wówczas wygląda wyrażenie

$$(a_i + a_j + a_k)^2.$$

Mamy mianowicie

$$(a_i + a_j + a_k)^2 = a_i^2 + a_j^2 + a_k^2 + 2a_ia_j + 2a_ia_k + 2a_ja_k.$$

Zatem to wyrażenie jest sumą jednomianów postaci

$$a_i^2 \quad \text{oraz} \quad 2a_ia_j,$$

gdzie $1 \leq i, j \leq 5$.

Weźmy jeden przykładowy jednomian: a_1^2. Pojawi się on w sześciu wyrażeniach postaci $S(n)^2$; są to:

$$(a_1 + a_2 + a_3)^2, \quad (a_1 + a_2 + a_4)^2, \quad (a_1 + a_2 + a_5)^2,$$

$$(a_1 + a_3 + a_4)^2, \quad (a_1 + a_3 + a_5)^2, \quad (a_1 + a_4 + a_5)^2.$$

Stąd wynika, że w całej sumie

$$S_1^2 + S_2^2 + \ldots + S_{10}^2$$

jednomian a_1^2 pojawi się ze współczynnikiem 6.

Weźmy inny przykładowy jednomian: $2a_1a_2$. Pojawi się on w trzech wyrażeniach postaci $S(n)^2$; są to:

$$(a_1 + a_2 + a_3)^2, \quad (a_1 + a_2 + a_4)^2 \quad \text{oraz} \quad (a_1 + a_2 + a_5)^2.$$

Stąd wynika, że w całej sumie

$$S_1^2 + S_2^2 + \ldots + S_{10}^2$$

jednomian a_1a_2 pojawi się także ze współczynnikiem 6.

Podsumujmy. Wyrażenie

$$S_1^2 + S_2^2 + \ldots + S_{10}^2$$

ma zatem postać

$$6 \cdot (a_1^2 + \ldots + a_5^2 + a_1a_2 + a_1a_3 + \ldots + a_3a_4 + a_3a_5 + a_4a_5).$$

Stąd wynika, że dla dowolnych liczb całkowitych a_1, a_2, a_3, a_4, a_5 suma

$$S_1^2 + S_2^2 + \ldots + S_{10}^2$$

jest podzielna przez 3. To kończy dowód twierdzenia.

Powtórzmy to rozumowanie dla $p = 5$. Bierzemy 9 dowolnych liczb całkowitych

$$a_1, \quad a_2, \quad a_3, \quad a_4, \quad a_5, \quad a_6, \quad a_7, \quad a_8 \quad \text{oraz} \quad a_9.$$

Patrzymy następnie na zbiór liczb od 1 do 9:

$$K = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Zbiór K ma 126 podzbiorów pięcioelementowych.

Oto te podzbiory:

$$
\begin{array}{ll}
P_1 = \{1,2,3,4,5\}, & P_{10} = \{1,2,3,6,7\}, \\
P_2 = \{1,2,3,4,6\}, & \ldots \quad \ldots \\
P_3 = \{1,2,3,4,7\}, & P_{100} = \{2,4,7,8,9\}, \\
P_4 = \{1,2,3,4,8\}, & \ldots \quad \ldots \\
P_5 = \{1,2,3,4,9\}, & P_{123} = \{4,5,6,8,9\}, \\
P_6 = \{1,2,3,5,6\}, & P_{124} = \{4,5,7,8,9\}, \\
P_7 = \{1,2,3,5,7\}, & P_{125} = \{4,6,7,8,9\}, \\
\ldots \quad \ldots & P_{126} = \{5,6,7,8,9\}.
\end{array}
$$

Dlaczego 126 podzbiorów? Dlatego, że

$$\binom{9}{5} = \frac{9!}{5! \cdot 4!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2 \cdot 1} = 9 \cdot 2 \cdot 7 = 126.$$

Każdemu podzbiorowi P_n zbioru K odpowiada suma pewnych pięciu liczb spośród liczb $a_1, a_2, \ldots, a_9$. Jeśli

$$P_n = \{i, j, k, l, m\},$$

to przyjmujemy

$$S(n) = a_i + a_j + a_k + a_l + a_m.$$

Naszym celem jest wykazanie, że istnieje liczba naturalna n taka, że

$$1 \leq n \leq 126 \quad \text{oraz} \quad 5 \mid S(n).$$

Teraz każdemu podzbiorowi P_n przyporządkowujemy pewną liczbę naturalną $T(n)$ w taki sposób, że:

- jeśli $5 \mid S(n)$, to $\quad T(n) \equiv 0 \pmod 5$,
- jeśli $5 \nmid S(n)$, to $\quad T(n) \equiv 1 \pmod 5$,
- $T(1) + T(2) + \ldots + T(126) \equiv 0 \pmod 5$.

Tak jak poprzednio, to wystarczy do zakończenia dowodu.
Przypuśćmy, że dla każdej liczby naturalnej n takiej, że $1 \leq n \leq 126$ mamy

$$5 \nmid S(n).$$

Wówczas dla każdej takiej liczby n mamy

$$T(n) \equiv 1 \pmod 5,$$

skad wynika, że

$$0 \equiv T(1) + T(2) + \ldots + T(126) \equiv 126 \cdot 1 = 126 \equiv 1 \pmod 5.$$

To jest niemożliwe. Otrzymana sprzeczność dowodzi, że co najmniej jedna suma $S(n)$ jest podzielna przez 5.

Musimy teraz zdefiniować liczby $T(n)$. Przyjmujemy

$$T(n) = S(n)^4.$$

Wówczas mamy:

- jeśli $5 \mid S(n)$, to $5 \mid S(n)^4$, więc

$$T(n) \equiv 0 \pmod{5},$$

- jeśli $5 \nmid S(n)$, to z małego twierdzenia Fermata wynika, że

$$S(n)^4 \equiv 1 \pmod{5},$$

  czyli

$$T(n) \equiv 1 \pmod{5}.$$

Do udowodnienia pozostaje tylko kongruencja

$$T(1)+T(2)+\ldots+T(126)\equiv 0 \pmod 5.$$

Przyjrzyjmy się teraz dokładniej liczbom $T(n)$. Przypuśćmy, że

$$P_n=\{i,j,k,l,m\},$$

oraz

$$S(n)=a_i+a_j+a_k+a_l+a_m.$$

Popatrzmy, jak wówczas wygląda wyrażenie

$$(a_i+a_j+a_k+a_l+a_m)^4.$$

Otóż jest ono sumą jednomianów postaci

$$c \cdot a_i^{\alpha_1} \cdot a_j^{\alpha_2} \cdot a_k^{\alpha_3} \cdot a_l^{\alpha_4} \cdot a_m^{\alpha_5},$$

gdzie c jest tzw. współczynnikiem wielomianowym

$$c = \binom{4}{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5} = \frac{4!}{\alpha_1! \cdot \alpha_2! \cdot \alpha_3! \cdot \alpha_4! \cdot \alpha_5!},$$

a wykładniki $\alpha_1, \ldots, \alpha_5$ mają następujące własności:

- $0 \leq \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \leq 4$,
- $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 4$.

Weźmy teraz jeden przykładowy jednomian: $a_1^2a_3a_7$. Pojawi się on w wielu wyrażeniach postaci $S(n)^4$, na przykład w wyrażeniach

$$(a_1{+}a_2{+}a_3{+}a_7{+}a_9)^4,\ (a_1{+}a_3{+}a_4{+}a_7{+}a_8)^4,\ (a_1{+}a_3{+}a_7{+}a_8{+}a_9)^4.$$

Dokładniej, pojawi się on w wyrażeniach postaci

$$(a_1 + a_3 + a_7 + a_i + a_j)^4,$$

gdzie $i, j \in \{2, 4, 5, 6, 8, 9\}$.

Istnieje

$$\binom{6}{2}$$

takich wyrażeń, bo istnieje tyle par różnych liczb i oraz j takich, że

$$i, j \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \setminus \{1, 3, 7\} = \{2, 4, 5, 6, 8, 9\}.$$

Stąd wynika, że w całej sumie

$$S_1^4 + S_2^4 + \ldots + S_{126}^4$$

ten jednomian pojawi się ze współczynnikiem

$$\binom{6}{2} \cdot \binom{4}{2, 1, 1} = \frac{6 \cdot 5}{2} \cdot \frac{4!}{2! \cdot 1! \cdot 1!} = 15 \cdot 12 = 180.$$

Ten współczynnik jest podzielny przez 5.

Podobne rozumowanie można przeprowadzić ogólnie. Przypuśćmy, że w rozważanym jednomianie znajduje się t czynników (z niezerowymi wykładnikami), gdzie $1 \leq t \leq 4$. Wtedy liczba tych wyrażeń

$$(a_i + a_j + a_k + a_l + a_m)^4,$$

w których wystąpi rozważany jednomian, jest równa

$$\binom{9-t}{5-t}.$$

Można łatwo pokazać, że jeśli $1 \leq t \leq 4$, to

$$5 \mid \binom{9-t}{5-t}.$$

Stąd następnie wynika, że każdy jednomian postaci

$$c \cdot a_i^{\alpha_1} \cdot a_j^{\alpha_2} \cdot a_k^{\alpha_3} \cdot a_l^{\alpha_4} \cdot a_m^{\alpha_5}$$

wchodzi w skład sumy

$$S = S_1^4 + S_2^4 + \ldots + S_{126}^4$$

ze współczynnikiem c podzielnym przez 5.

A więc cała suma S jest podzielna przez 5. Ponieważ

$$T(1)+T(2)+\ldots+T(126)=S_1^4+S_2^4+\ldots+S_{126}^4=S,$$

więc

$$T(1)+T(2)+\ldots+T(126)\equiv 0 \pmod 5.$$

To kończy dowód.

Rozumowanie ogólne dla dowolnej liczby pierwszej p wygląda podobnie. Definiujemy

$$T(n) = S(n)^{p-1}.$$

Musimy tylko wykazać dwie własności współczynników dwumianowych:

- jeśli p jest liczbą pierwszą oraz $1 \leq t \leq p-1$, to

$$p \mid \binom{2p-1-t}{p-t},$$

- jeśli p jest liczbą pierwszą, to

$$p \nmid \binom{2p-1}{p}.$$

Pokażę teraz drugi dowód twierdzenia 11. Najpierw kilka definicji.

Dla dowolnych skończonych zbiorów A i B liczb całkowitych definiujemy:

$$A + B = \{a + b : \ a \in A \quad \text{oraz} \quad b \in B\}$$

oraz

$$\begin{aligned} A \oplus_p B &= \{n \ \mathbf{mod}\ p : \ n \in A + B\} = \\ &= \{(a + b) \ \mathbf{mod}\ p : \ a \in A \quad \text{oraz} \quad b \in B\}. \end{aligned}$$

W podobny sposób definiujemy zbiory

$$A_1 + A_2 + \ldots + A_n \quad \text{oraz} \quad A_1 \oplus_p A_2 \oplus_p \ldots \oplus_p A_n.$$

Przykład 1. Niech

$$A = \{1, 2\} \quad \text{oraz} \quad B = \{1, 3\}.$$

Wówczas

$$A + B = \{2, 3, 4, 5\} \quad \text{oraz} \quad A \oplus_5 B = \{0, 2, 3, 4\}.$$

Przykład 2. Niech

$$A = \{1, 2\} \quad \text{oraz} \quad B = \{3, 4\}.$$

Wówczas

$$A + B = \{4, 5, 6\} \quad \text{oraz} \quad A \oplus_5 B = \{0, 1, 4\}.$$

Przykład 3. Niech

$$A = \{1, 2\} \quad \text{oraz} \quad B = \{0, 4\}.$$

Wówczas

$$A + B = \{1, 2, 5, 6\} \quad \text{oraz} \quad A \oplus_5 B = \{0, 1, 2\}.$$

- Dana jest liczba pierwsza p oraz zbiór $A \subseteq \mathbb{Z}_p$. Ponadto $x \in \mathbb{Z}_p$. Wówczas:
$$|A \oplus_p \{x\}| = |A|.$$

- Dana jest liczba pierwsza p oraz zbiór $A \subseteq \mathbb{Z}_p$. Ponadto $x, y \in \mathbb{Z}_p$, przy czym $x \neq y$. Niech $B = \{x, y\}$. Wówczas:
$$A \oplus_p B = (A \oplus_p \{x\}) \cup (A \oplus_p \{y\}).$$

- Jeśli $x \in \mathbb{Z}_p$, to: $\quad \mathbb{Z}_p \oplus_p \{x\} = \mathbb{Z}_p$.

- Jeśli $B \subseteq \mathbb{Z}_p$, to: $\quad \mathbb{Z}_p \oplus_p B = \mathbb{Z}_p$.

- Dana jest liczba pierwsza p oraz taki zbiór $A \subseteq \mathbb{Z}_p$, że $|A| < p$. Ponadto $x, y \in \mathbb{Z}_p$, gdzie $x \neq y$. Niech $B = \{x, y\}$. Wówczas:

$$(A \oplus_p \{x\}) \neq (A \oplus_p \{y\}).$$

- Dana jest liczba pierwsza p oraz zbiory $A, B \subseteq \mathbb{Z}_p$. Ponadto $|A| < p$ oraz $|B| = 2$. Wówczas:

$$|A \oplus_p B| > |A|.$$

Ostatnia własność jest szczególnym przypadkiem lematu ogólniejszego, udowodnionego przez Cauchy'ego.

- Dana jest liczba pierwsza p, liczba naturalna n taka, że $1 \leq n < p$ oraz zbiory $A_1, A_2, \ldots, A_n \subseteq \mathbb{Z}_p$. Ponadto $|A_k| = 2$ dla każdej liczby $k = 1, 2, \ldots, n$. Wówczas:

$$|A_1 \oplus_p A_2 \oplus_p \ldots \oplus_p A_n| > n.$$

- Dana jest liczba pierwsza p oraz zbiory $A_1, A_2, \ldots, A_{p-1} \subseteq \mathbb{Z}_p$. Ponadto $|A_k| = 2$ dla każdej liczby k takiej, że $1 \leq k \leq p-1$. Wówczas:

$$|A_1 \oplus_p A_2 \oplus_p \ldots \oplus_p A_{p-1}| = p,$$

  czyli

$$A_1 \oplus_p A_2 \oplus_p \ldots \oplus_p A_{p-1} = \mathbb{Z}_p.$$

Dowód twierdzenia 11. Oczywiście możemy założyć, że dane liczby są elementami zbioru $\mathbb{Z}_p$.

Zamiast danych liczb możemy bowiem rozpatrywać ich reszty z dzielenia przez p.

Uporządkujmy dane liczby w kolejności niemalejącej:

$$0 \leq a_1 \leq a_2 \leq a_3 \leq \ldots \leq a_{2p-2} \leq a_{2p-1} < p.$$

Popatrzmy teraz na liczby a_1 oraz a_p. Oczywiście $a_1 \leq a_p$.

Gdyby okazało się, że $a_1 = a_p$, to mielibyśmy ciąg równości

$$a_1 = a_2 = \ldots = a_p.$$

Wówczas

$$a_1 + a_2 + \ldots + a_p = p \cdot a_1 \equiv 0 \pmod{p}.$$

Przypuśćmy zatem, że $a_1 < a_p$.

W podobny sposób popatrzmy na liczby a_2 i a_{p+1}. Gdyby $a_2 = a_{p+1}$, to mielibyśmy ciąg równości

$$a_2 = a_3 = \ldots = a_{p+1}$$

i wtedy

$$a_2 + a_3 + \ldots + a_{p+1} = p \cdot a_2 \equiv 0 \pmod{p}.$$

Zatem możemy przypuścić, że także $a_2 < a_{p+1}$.

Postępując analogicznie:

- albo w ciągu liczb $(a_1, a_2, \ldots, a_{2p-1})$ znajdziemy p kolejnych jednakowych liczb i wtedy ich suma będzie podzielna przez p,

- albo otrzymamy $p-1$ nierówności

$$a_1 < a_p,\ a_2 < a_{p+1},\ \ldots,\ a_{p-2} < a_{2p-3} \quad \text{oraz} \quad a_{p-1} < a_{2p-2}.$$

W takim przypadku możemy utworzyć $p-1$ zbiorów dwuelementowych:

$$\begin{aligned} A_1 &= \{a_1, a_p\}, \\ A_2 &= \{a_2, a_{p+1}\}, \\ A_3 &= \{a_3, a_{p+2}\}, \\ \ldots &\qquad \ldots \\ A_{p-2} &= \{a_{p-2}, a_{2p-3}\}, \\ A_{p-1} &= \{a_{p-1}, a_{2p-2}\}. \end{aligned}$$

Stąd wynika, że

$$A_1 \oplus_p A_2 \oplus_p \ldots \oplus_p A_{p-1} = \mathbb{Z}_p.$$

W szczególności liczba $p - a_{2p-1}$ jest elementem zbioru

$$A_1 \oplus_p A_2 \oplus_p \ldots \oplus_p A_{p-1}.$$

To znaczy, że istnieją liczby $b_1, b_2, \ldots, b_{p-1}$ należące odpowiednio do zbiorów $A_1, A_2, \ldots, A_{p-1}$ takie, że

$$b_1 + b_2 + \ldots + b_{p-1} = p - a_{2p-1}$$

w $\mathbb{Z}_p$.

Inaczej mówiąc

$$b_1 + b_2 + \ldots + b_{p-1} \equiv p - a_{2p-1} \pmod{p},$$

czyli

$$b_1 + b_2 + \ldots + b_{p-1} + a_{2p-1} \equiv p \equiv 0 \pmod{p}.$$

Zatem znaleźliśmy dokładnie p liczb wśród danych $2p-1$ liczb, których suma jest podzielna przez p. To kończy dowód twierdzenia.

K O N I E C