Uwagi do zadania 786

Piotr KUMOR

Uwaga 1.

Jest oczywiste, że w obu przykładach *(z rozwiązania Autora – przyp. red.)* otrzymujemy nieskończone ciągi parami różnych (mnogościowo – jako zbiory) czwórek. Ponadto, w przykładzie 2 mamy nieskończenie wiele czwórek parami rozłącznych. Dokładniej – nie twierdzimy, że wszystkie one są parami rozłączne, ale z pewnością istnieje taki nieskończony podciąg. Natomiast czwórki z przykładu 1 mają wszystkie tę wspólną jedynkę.

Można podać wiele (nieskończenie wiele) innych przykładów. Ich konstrukcja nie nastręcza trudności, więc nie warto się nad tym zatrzymywać.

Dużo trudniejsze, ciekawsze i bardzo naturalne są zagadnienia wspomniane w kolejnych uwagach. Mianowicie:

Uwaga 2.

Narzuca się pytanie, czy istnieje czwórka taka, że wszystkie sześć iloczynów jest dobrych?

Hipoteza, że odpowiedź jest negatywna, jest znana jako: ***D*(−1) quadruple conjecture**.

To wciąż hipoteza, jednak wiele wiadomo na ten temat.

a) Liczba ewentualnych takich czwórek jest skończona

Theorem 2.

There are only finitely many $D(-1)$-quadruples. Moreover, if $\{a, b, c, d\}$ is a $D(-1)$-quadruple, then $\max\{a, b, c, d\} < 10^{10^{23}}$.

b) Najmniejszy element każdej takiej czwórki musi być równy jeden.

Theorem 1b.

There does not exist a $D(-1)$-quadruple $\{a, b, c, d\}$ with $2 \leq a < b < c < d$.

c) Nie istnieje piątka (*quintuple*) liczb o tej własności

Corollary 1.

There does not exist a $D(-1)$-quintuple.

Twierdzenia cytowane w b) i c) są udowodnione w pracy Dujella and Fuchs (2005). Natomiast twierdzenie cytowane w a) pochodzi z pracy Dujella et al. (2007). *(Wykaz literatury na końcu komentarzy)*

Uwaga 3.

Dwie podane wyżej prace, a także wiele innych o podobnej tematyce można znaleźć na stronie chorwackiego matematyka Andreja Dujella. Jest on bez wątpienia ekspertem w tych tematach. Andrej Dujella (Zagrzeb). Strona domowa: https://web.math.pmf.unizg.hr/~duje/

Andrej Dujella, publikacje:
https://web.math.pmf.unizg.hr/~duje/papers1.html

Uwaga 4.

Dla danej liczby całkowitej $k \neq 0$, oraz liczby całkowitej dodatniej m, zbiór m parami różnych liczb całkowitych dodatnich jest nazywany diofantycznym m-tuplem typu $D(k)$ wtedy i tylko wtedy, gdy dla każdych dwóch różnych jego

elementów x, y liczba $xy + k$ jest kwadratem liczby całkowitej dodatniej. Powyżej omawialiśmy wyłącznie przypadek $k = -1$ (z treści zadania 786), czyli problem $D(-1)$.

Jednak zagadnienie to jest od dawna znane i badane dla dowolnych wartości k. Historia tych zmagań jest podana w pracach Andreja Dujella oraz w wielu innych źródłach.

Najsławniejszy przypadek, to problem $D(1)$. Jego historia sięga starożytności (Diofantos) i dotyczy wielu znakomitych matematyków (między innymi Fermat). Inaczej niż w przypadku problemu $D(-1)$, czwórek typu $D(1)$ jest nieskończenie wiele, a wzory parametryczne były znane już dawno (XVIII wiek Euler i współcześni) Jednak twierdzenie, że nie ma piątki typu $D(1)$ udowodniono całkiem niedawno: He, Togbé, and Ziegler (2019).

Rozwiązanie i uwagi do zadania 787

Piotr KUMOR

Rozwiązanie.

W punkcie **(I)** udowodnimy fakt nieco mocniejszy, zaś w punkcie **(II)** fakt nieco ogólniejszy.

(I) Niech $\min(M)$ oraz $\max(M)$ będą odpowiednio najmniejszym i największym elementem zbioru M (złożonego z liczb całkowitych, jak w treści zadania). Niech s będzie największą liczbą naturalną taką, że $2^s \leq \max(M) - \min(M)$ (czyli $2^s \leq \max(M) - \min(M) < 2^{s+1}$)

Wówczas elementy zbioru M można ustawić w ciąg $(x_1, \ldots, x_n)$ tak, by dla każdej trójki wskaźników $i, j, k \in \{1, \ldots, n\}$, $i < j < k$ spełniony był warunek: Liczba $x_i + x_k - 2x_j$ nie dzieli się przez 2^s (więc tym bardziej nie może być równa zero).

(II) W treści zadania zamieńmy słowo „całkowitych” słowem „rzeczywistych” lub „zespolonych” Teza pozostaje wtedy prawdziwa. (**podkreślmy**, że w treści **zadania**, nie punktu **(I)** bo oczywiście nie ma wtedy mowy o żadnej podzielności)

Możliwe są też dalsze uogólnienia. Pozostaje to także prawdą gdy jest skończonym podzbiorem pewnej (dowolnego wymiaru!) przestrzeni liniowej nad ciałem liczb wymiernych.

Dowód punktu (I)

Udowodnimy najpierw następujący

Lemat. Dla każdej liczby naturalnej t teza punktu (I) jest prawdziwa dla zbioru $M = \{0, 1, \ldots, 2^t - 1\}$. Wówczas $s = t - 1$.

Dowód lematu.

Dla $t = 0$ i $t = 1$ nie ma czego dowodzić. Dla $t = 2$ mamy $M = \{0, 1, 2, 3\}$. Przyjmijmy ustawienie: 0, 2, 1, 3. Mamy $s = 1$, $2^s = 2$ i teza jest oczywiście prawdziwa. Pierwszy i trzeci wyraz każdej trójki są bowiem różnej parzystości.

Dalej stosujemy indukcję względem t.

Załóżmy, że teza jest prawdziwa dla pewnej liczby naturalnej $t \geq 2$.

Niech $a_0, a_1, \ldots, a_{2^t-1}$ niech będzie permutacją 2^t liczb $0, 1, \ldots, 2^t - 1$, która spełnia tezę lematu dla tej wartości t.

Wtedy ciąg 2^{t+1} liczb $2a_0, 2a_1, \ldots, 2a_{2^t-1}, 2a_0 + 1, 2a_1 + 1, \ldots, 2a_{2^t-1} + 1$ jest permutacją liczb $0, 1, \ldots, 2^{t+1} - 1$, która spełnia tezę lematu dla $t + 1$. (Wtedy $s = t$).

Sprawdzenie tego jest natychmiastowe : Jest to istotnie permutacja 2^{t+1} liczb $0, 1, \ldots, 2^{t+1} - 1$. Oczywiście dla każdej trójki wskaźników $0 \leq i < j < k \leq 2^{t+1} - 1$ liczba $x_i + x_k - 2x_j$ jest albo nieparzysta, albo równa $2(a_i + a_k - 2a_j)$, gdzie a_i, a_k, a_j jest podciągiem w permutacji $a_0, a_1, \ldots, a_{2^t} - 1$. Zatem $a_i + a_k - 2a_j$ nie dzieli się przez 2^{t-1} (z założenia indukcyjnego), więc $2(a_i + a_k - 2a_j)$ nie dzieli się przez 2^t.

Teza lematu jest więc prawdziwa dla $t + 1$, i dalej przez indukcję dla wszystkich liczb naturalnych t.

Lemat został udowodniony

Niech teraz M będzie skończonym zbiorem liczb całkowitych, zaś s największą liczbą naturalną taką, że $2^s \leq \max(M) - \min(M)$ (czyli $2^s \leq \max(M) - \min(M) < 2^{s+1}$).

Niech $M - \min(M)$ oznacza zbiór liczb postaci $m - \min(M)$ gdzie $m \in M$. Zbiór $M - \min(M)$ oczywiście jest podzbiorem zbioru $\{0, 1, \ldots, 2^{s+1} - 1\}$.

Na podstawie lematu zbiór $\{0, 1, \ldots, 2^{s+1} - 1\}$ posiada permutację, która spełnia tezę. Oczywiście jest to też permutacja dobra dla zbioru $M - \min(M)$ więc także dla zbioru M.

Dowód punktu (I) został zakończony

Dowód punktu (II)

Uogólnienie na liczby wymierne jest natychmiastowe.

Załóżmy, że M jest skończonym podzbiorem pewnej ustalonej (dowolnej!) przestrzeni liniowej W nad ciałem liczb wymiernych. Ponieważ jest to zbiór skończony, więc wymiar najmniejszej podprzestrzeni liniowej $V(M)$, która zawiera zbiór M, też jest skończony (nie większy od mocy zbioru M). Nie ma tu znaczenia wymiar tej dużej przestrzeni W.

Jeżeli wymiar $V(M)$ jest równy jeden (zapisujemy $\dim V(M) = 1$; wszystkie przestrzenie nad ciałem liczb wymiernych) teza zachodzi na podstawie pierwszego zdania dowodu punktu (II).

Dalej stosujemy indukcję względem liczby $\dim V(M)$.

Załóżmy, że dla pewnej liczby naturalnej $n \geq 1$ teza jest prawdziwa dla każdego zbioru M takiego, że $\dim V(M) \leq n$.

Rozważmy pewien zbiór M taki, że $\dim V(M) = n + 1$. Zapiszmy przestrzeń $V(M)$ w postaci sumy prostej: $V(M) = V_0 \oplus V_1$, gdzie $\dim V_0 = n$, $\dim V_1 = 1$. Można to zrobić na nieskończenie wiele sposobów, ustalmy dowolnie jeden z nich. Każdy wektor $m \in M$ ma jednoznaczne przedstawienie w postaci $m = m_0 + m_1$, gdzie $m_0 \in V_0$, $m_1 \in V_1$.

Niech $M_0 = \{m_0 \colon m \in M\}$, $M_1 = \{m_1 \colon m \in M\}$ (M_0 i M_1 to rzuty zbioru M odpowiednio na V_0 i V_1). Ponieważ $M_0 \subset V_0$ oraz $\dim V_0 = n$, więc $V(M_0) \subset V_0$, czyli $\dim V(M_0) \leq n$. Musi też być $V(M_1) = V_1$ (bo $\dim V(M) = n + 1$).

Na podstawie założenia indukcyjnego, elementy zbioru M_0 można ustawić w ciąg, który nie ma podciągu arytmetycznego.

Jednak pojawia się tu pewna przeszkoda. Otóż należałoby mówić raczej o multizbiorze M_0, bowiem rzuty różnych elementów zbioru M na przestrzeń V_0 mogą być równe. Jeżeli jednak dla pewnych różnych elementów zbioru M, powiedzmy dla m i m' mamy $m_0 = m'_0$, to $m_1 \neq m'_1$ (bo $m \neq m'$).

Zatem ustawmy elementy zbioru M w ciąg leksykograficznie: najpierw według współrzędnej V_0, a gdy te współrzędne są równe, według współrzędnej V_1. Oczywiście na współrzędnych V_0 i V_1 stosujemy uporządkowania wolne od ciągów arytmetycznych – takie istnieją na podstawie założenia indukcyjnego.

Otrzymane ustawienie wektorów zbioru M jest wolne od ciągów arytmetycznych. Gdyby bowiem taki ciąg x, y, z się pojawił, to pewne dwie spośród współrzędnych

x_0, y_0, z_0 muszą być równe. Jednak wtedy trzecia też jest im równa (bo jeśli wektory u, w, v spełniają równanie $u + v = 2w$ i dwa z nich są równe, to trzeci też jest im równy). Zatem współrzędne x_1, y_1, z_1 są parami różne i (z naszej konstrukcji) nie tworzą ciągu arytmetycznego.

Teza została więc udowodniona dla zbioru M.

Przez indukcję jest to więc prawda dla każdego skończonego podzbioru M przestrzeni liniowej W.

Dowód punktu (II) został zakończony

Uwagi.

1) Ponieważ liczby rzeczywiste (także zespolone) tworzą przestrzeń liniową nad ciałem liczb wymiernych, więc teza punktu (II) jest prawdziwa dla skończonych zbiorów liczb rzeczywistych (zespolonych).

Można jeszcze nieco uogólnić punkt (II). Teza pozostaje prawdziwa dla skończonych podzbiorów dowolnej grupy, które generują podgrupę przemienną bez elementów skończonego rzędu (czyli abelową grupę wolną). Taka podgrupa jest bowiem naturalnie izomorficzna z podzbiorem przestrzeni liniowej nad ciałem liczb wymiernych.

2) Poruszane tu zagadnienia są bardzo znane.

W wersji dla liczb naturalnych było to przedmiotem zadania z III Olimpiady Informatycznej: Zadanie *Permutacje Antyarytmetyczne* z zawodów 3 stopnia (marzec 1996). Autor zadania: Wojciech Guzicki

Treść i szczegółowe rozwiązanie dostępne w sprawozdaniu z III OI (zwanym dalej [OI 3]):

https://www.oi.edu.pl/static/attachment/20130309/1995_1.pdf

na stronach 106 – 112.

3) Ważna i wczesna praca o tej tematyce Davis et al. (1977) (wspomniana w [OI 3]) pochodzi z lat 70-tych

http://matwbn.icm.edu.pl/ksiazki/aa/aa34/aa3417.pdf

4) Zwróćmy uwagę na znacznie nowszą pracę Ardal et al. (2011). Mam tę pracę na dysku, więc na pewno była ona dostępna „on line free". Niestety nie zapisałem adresu i teraz nie potrafię go odnaleźć. Może jest nieaktualny?

W uwadze 3 (Remark 3) na końcu pracy Ardal et al. (2011) jest podana ciekawa konstrukcja. Ta sama konstrukcja (lecz ograniczona do skończonych podzbiorów liczb naturalnych) występuje też w pracy [OI 3] i jest podstawą efektywnego algorytmu.

Poniżej opiszę tę konstrukcję, w nieco innym języku.

Niech D oznacza zbiór nieujemnych liczb dwójkowo wymiernych, to znaczy liczb postaci $\sum_{-\infty}^{+\infty} \frac{c_k}{2^k}$, gdzie $c_k \in \{0, 1\}$ oraz $\sum_{-\infty}^{+\infty} c_k < +\infty$. (ostatnia nierówność znaczy po prostu, że jedynek jest tylko skończenie wiele).

Określamy funkcję $\varphi\colon D \to D$ wzorem $\varphi\left(\sum_{-\infty}^{+\infty} \frac{c_k}{2^k}\right) = \sum_{-\infty}^{+\infty} \frac{c_k}{2^{-k}}$: (liczba palindromiczna). Np.: $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi\left(\frac{3}{2}\right) = 3$.

Odnotujmy dwie oczywiste własności funkcji φ.

(a) $\varphi\big(\varphi(x)\big) = x$ dla wszystkich $x \in D$

(b) Funkcja φ jest więc permutacją (inaczej bijekcją) zbioru D na ten sam zbiór. Oczywiście zbiór D zawiera zbiór liczb całkowitych nieujemnych $\mathbb{N}_0$. Zachodzi też równość zbiorów $\varphi(\mathbb{N}_0) = D \cap [0, 2)$ ($[0, 2)$ oznacza przedział domknięto–otwarty).

Okazuje się, że funkcja φ ma jeszcze jedną ciekawą i kluczową dla nas własność. Otóż: Dla każdych trzech elementów x, y, z zbioru D: jeżeli $x < y < z$, to $\varphi(x) + \varphi(z) \neq 2\varphi(y)$.

Ponieważ funkcja φ jest swoją własną odwrotnością, więc można ująć to inaczej: funkcja φ nie jest monotoniczna na żadnym ciągu arytmetycznym.

Dowód tej własności funkcji φjest podany w pracy Ardal et al. (2011). W [OI 3] jest mowa co prawda tylko o zbiorach skończonych, jednak stąd też łatwo wynika owa własność funkcji φ.

5) Z podanej wyżej własności funkcji φ wynika natychmiast teza zadania 787 (w wersji oryginalnej, nie tej z punktu (I) z podzielnością). Wystarczyłoby tu nawet nieco mniej. Jeżeli E jest podzbiorem prostej rzeczywistej, który zawiera pewien nieskończony ciąg arytmetyczny, zaś funkcja $g\colon E \to E$ jest permutacją (czyli bijekcją = wzajemnie jednoznaczna) zbioru E, która nie jest monotoniczna na żadnym ciągu arytmetycznym, to też daje ona tezę zadania 787.

6) Problem polega więc na odkryciu takiego zbioru E i jego permutacji g. Takimi są zbiór D i funkcja φ, oraz pewne oczywiste podzbiory zbioru D niezmiennicze dla funkcji φ. Czy są inne przykłady? Nie znalazłem takich, ani dowodu, że nie istnieją. Na pewno żaden podzbiór zbioru liczb całkowitych dodatnich $\mathbb{N}_0$ nie jest dobry. Nie można bowiem ustawić wszystkich liczb naturalnych w permutację antyarytmetyczną. Fakt ten jest niemal oczywisty i łatwo sprawdzić go „na palcach". Odnotujmy jednak jego dowód podany w pracy Davis et al. (1977). Dowód ten jest widoczny na zdjęciu poniżej:

Permutations of the positive integers. Let $A = a_1 a_2 a_3 \ldots$ be a permutation of the set $\boldsymbol{Z}^+$ of positive integers. Denote by $\mathscr{S}_k$ the set of those A which contain no monotone k-term A.P.

FACT 3.

$$\mathscr{S}_3 = \emptyset.$$

Proof. Let $A = a_1 a_2 a_3 \ldots$ be a permutation of $\boldsymbol{Z}^+$. If i denotes the least index for which $a_i > a_1$ then for some $j > i$,

$$a_j = 2a_i - a_1$$

and so we always have, in fact, an increasing 3-term A.P. in A. ■

Zbiorem E nie może też być żaden podzbiór zbioru wszystkich liczb całkowitych (dodatnich i ujemnych). Nie można bowiem ustawić wszystkich liczb naturalnych w „obustronnie nieskończony" ciąg wolny od ciągów arytmetycznych. Formalnie: nie istnieje taka bijekcja zbioru wszystkich liczb całkowitych i zbioru liczb naturalnych.

Fakt ten jest mniej oczywisty niż poprzedni, ale prawdziwy. Jego dwa różne dowody (oba dość skomplikowane) także są podane w pracy Davis et al. (1977) na stronach 85 – 87.

Czy podobne twierdzenie jest prawdziwe dla zbioru wszystkich (lub tylko dodatnich) liczb wymiernych ? Dla zbioru wszystkich (lub tylko dodatnich) liczb rzeczywistych?

Nie mam pojęcia.

7) Nie natrafiłem na żadne inne twierdzenie o nieskończonej permutacji anty–trój–arytmetycznej niż wspomniane wyżej. W pracy Davis et al. (1977) jest podany przykład permutacji liczb naturalnych anty–pięcio–arytmetycznej. Problem istnienia permutacji anty–cztero–arytmetycznej jest tam postawiony jako problem otwarty, i wygląda na to, że pozostał takim do dzisiaj. Jest za to podany przykład permutacji „ obustronnie nieskończonej" anty–cztero–arytmetycznej. Fakt 6 dowód na stronach 87 – 88

8) O permutacjach nie znalazłem więcej informacji. Jednak są dostępne nowe wyniki, które dowodzą istnienia odpowiednich **uporządkowań zbiorów**. Dla zbiorów nieskończonych, to coś innego niż permutacje. W każdym razie teraz nie widzę tutaj związków. (być może z powodu mojej ignorancji w tym temacie).

W pracy Ardal et al. (2011) główny wynik to

Theorem 4.1

The linear ordering $<_{\mathbb{R}}$ of $\mathbb{R}$ (defined above) is chaotic.

Note that in Theorem 4.1, $\mathbb{R}$ can be replaced by any field of characteristic 0.

Wspomniane są ciała charakterystyki zero, ale faktycznie dowód działa dla wszystkich przestrzeni liniowych nad ciałem liczb wymiernych. Zacytujmy tu jeszcze inną, bardzo niedawną pracę Károlyi and Komjáth (2017). Praca jest dostępna tutaj `http://web.cs.elte.hu/~kope/p70.pdf`

9) Z twierdzenia tego wynika natychmiast punkt (II) rozwiązania. Jednak nasz dowód jest elementarny (właściwie poruszamy się wśród zbiorów skończonych), i stanowi on konieczny krok w dowodzie Theorem 4.1. Kolejne kroki dowodu Theorem 4.1 nie są już elementarne, i korzystają z takich narzędzi jak lemat Königa oraz pewnik wyboru.

Na tym zakończę z obawy, że ciąg uwag stanie się nieskończony ☺.

Uwagi do zadania 796

Piotr KUMOR

Porzućmy założenie, że m jest liczbą parzystą. Prawdziwe są następujące twierdzenia:

Twierdzenie Zsigmondy; wersja R (różnice)

If $a > b > 0$ are comprime integer, then for any integer $n \geq 1$, there is a prime number p (called a *primitive prime divisor*) that divides $a^n - b^n$ and does not divide $a^k - b^k$ for any positive integer $k < n$, with the following exceptions:

- $n = 1$, $a - b = 1$; then $a^n - b^n = 1$ which has no prime divisors
- $n = 2$, $a + b$ a power of two; then any odd prime factor of $a^2 - b^2$ must be contained in $a^1 - b^1$, which is also even
- $n = 6$, $a = 2$, $b = 1$; then $a^6 - b^6 = 63 = 3^2 \times 7 = (a^2 - b^2)^2(a^3 - b^3)$.

Twierdzenie Zsigmondy; wersja S (sumy)

Similarly, $a^n + b^n$ has at least one primitive prime divisor with the eception $2^3 + 1^3 = 9$.

Dowody obu wersji twierdzenia można znaleźć na przykład tutaj :

`https://math.stackexchange.com/questions/660585/elementary-proof-of-zsigmondys-theorem`

Dowód dla różnic (wersja R), choć nazywany tutaj (i wielu innych miejscach) elementarnym, wyraźnie wykracza jednak ponad matematykę szkolną i „olimpijską”. Gdy jednak wersję R mamy już udowodnioną, dowód wersji S jest natychmiastowy:

The proof for the case $a^n + b^n$ can be deduced from the case $a^n - b^n$.

For any positive integer $n > 1$ for which $2n$ does not give an exception on Zsigmondy's theorem, $a^{2n} - b^{2n}$ has a primitive prime divisor p, dividing either $a^n - b^n$ or $a^n + b^n$. However, p can't divide $a^n - b^n$ since then p wouldn't be primitive. Thus we have $p \mid a^n + b^n$ and $p \nmid a^{2k} - b^{2k}$ for all $k < n$. This implies $p \nmid a^k + b^k$ for all $k < n$, hence the theorem. □

Note that the exception $2^6 - 1^6$ is reflected in $2^3 + 1^3$. The case $n = 2$ and $a + b$ a power of 2 disappears because we only consider $n > 1$ here.

Jako zastosowanie twierdzenia Zsigmondy udowodnimy następujący :

Fakt.

Jeżeli $a \geq 1$, $b \geq 1$, $x \geq 2$, $z \geq 2$ są liczbami całkowitymi, spełniającymi równanie

$$a^x + b^x = (a+b)^z, \tag{1}$$

to ma miejsce jeden z dwóch przypadków:
1) $a > b$, $a = 2$, $b = 1$, $x = 3$, $z = 2$ (oraz symetrycznie, gdy $b > a$)
2) $a = b = 2^k$, a liczby całkowite dodatnie k, x, z spełniają równość $kx + 1 = z(k+1)$. Liczba całkowita $k \geq 1$ może być tutaj dowolna, dla ustalonej liczby k istnieje nieskończenie wiele par x, z.

Dowód Faktu:

Jest to niemal natychmiastowa konsekwencja twierdzenia Zsigmondy w wersji S. Załóżmy bowiem, że $a > b \geq 1$ i niech $d = NWD(a,b)$, $a = dt$, $b = dq$, $NWD(t,q) = 1$. Oczywiście musi być $x > z$, więc $d^{x-z}(t^x + q^x) = (t+q)^z$. Jeżeli $t = 2$, $q = 1$ oraz $d = 1$, to mamy przypadek 1). Jeżeli $t = 2$, $q = 1$ oraz $d > 1$, to musi być $d = 3^s$, $s \geq 1$ oraz (na podstawie twierdzenia Zsigmondy w wersji S) musi być $x = 3$, więc $z = 2$ (bo $x > z \geq 2$). To jednak oczywiście niemożliwe gdy $s \geq 1$. Przypadek $t \geq 3$ jest wykluczony przez ponowne zastosowanie twierdzenia Zsigmondy w wersji S.

Jeżeli $a = b$, to twierdzenia Zsigmondy nie można stosować, ale wtedy $NWD(a,b)$ musi być potęgą dwójki i natychmiast otrzymujemy przypadek 2).

Fakt został więc udowodniony.

Oczywiście wynika z niego, że w warunkach zadania 796 implikacja „tylko wtedy” jest prawdziwa również dla nieparzystych wykładników m. (W dowodzie Faktu wykładnik ten był oznaczony jako x).

Przytoczony na początku rozwiązania dowód przy założeniu parzystości m, to w istocie dowód takiej najprostszej (sub)wersji twierdzenia Zsigmondy w wersji S: mianowicie tylko dla sum $x + y$ oraz $x^m + y^m$ (dla parzystych m).

Nie wiem czy dla m nieparzystych odpowiednią wersję twierdzenia Zsigmondy można udowodnić równie prosto?

Natomiast dowód implikacji „wtedy” (z zadania 796) jest oczywiście natychmiastowy, bez względu na parzystość m. Jeżeli bowiem $k(m-n) = n-1$, to równanie (*) jest oczywiście spełnione dla $x = y = 2^k$.

Rozwiązanie i uwagi do zadania 796

Janusz OLSZEWSKI

Rozwiązanie

Niech x, y będą rozwiązaniami równania (1); liczba d niech będzie największym wspólnym dzielnikiem liczb x i y oraz $x = da$, $y = db$, gdzie liczby a i b są

względnie pierwsze. Równanie z zadania zapisujemy w postaci

$$d^{m-n}(a^m + b^m) = (a+b)^n. \tag{2}$$

Ponieważ liczby x, y są całkowite dodatnie, więc $a, b \geq 1$ oraz $a^m + b^m \geq 2$. Czyli, liczba $a^m + b^m$ ma dzielnik pierwszy p. Z równości (2) wynika, że liczba pierwsza p jest również dzielnikiem liczby $a+b$, tj. $b \equiv -a \pmod{p}$. Uwzględniając dodatkowo założenie zadania, że m jest parzyste, otrzymujemy kongruencje

$$0 \equiv a^m + b^m \equiv a^m + (-a)^m = 2a^m \pmod{p}.$$

Jednak liczby a i p są względnie pierwsze[1] , więc $p \mid 2$, tj. $p = 2$. Czyli $a^m + b^m = 2^t$ dla pewnej liczby całkowitej dodatniej t. Liczby a i b są nieparzyste (jako, że są względnie pierwsze i $2 = p \mid a+b$), dlatego liczby $a^{m/2}$ i $b^{m/2}$ są także nieparzyste, a ich kwadraty dają przy dzieleniu przez 4 resztę 1. Zatem, gdyby liczba t była większa niż 1 wówczas

$$0 \equiv 2^t = a^m + b^m = (a^{m/2})^2 + (b^{m/2})^2 \equiv 1 + 1 = 2 \pmod{4}.$$

Mamy sprzeczność. Tak więc $a^m + b^m = 2$, co jest równoważne temu, że $a = b = 1$. Podstawiając otrzymane wartości do równości (2) dostajemy związek $d^{m-n} = 2^{n-1}$. Zatem d jest potęgą liczby 2, tj. $d = 2^\alpha$ oraz $\alpha(m-n) = n-1$, gdzie α jest liczbą całkowitą nieujemną (liczba α może być równa zero). Inaczej mówiąc, jeżeli równanie (1) ma rozwiązania, to liczba $n-1$ dzieli się przez $m-n$.

Dodatkowo, otrzymujemy potencjalne rozwiązanie: $x = da = 2^\alpha, y = db = 2^\alpha$.

Łatwo sprawdzamy, że pary $(x, y) = (2^\alpha, 2^\alpha)$, gdzie $\alpha = \frac{n-1}{m-n}$ są rozwiązaniami naszego równania z zadania. Mamy więc dowód implikacji w drugą stronę tj. jeżeli liczba $\alpha = (n-1)/(m-n)$ jest całkowita nieujemna, to równanie (1) ma rozwiązanie (jedyne) $x = 2^\alpha, y = 2^\alpha$.

Uwaga 1.

Pokusimy się o znalezienie rozwiązań x, y równania (1) (danego w zadaniu) dla $m, n \geq 1$.

Bez trudu sprawdzamy trywialne przypadki równania (1), gdy $n = 1$ lub $m = 1$:

- ✓ gdy $n = 1$, wówczas dostajemy równanie $x^m + y^m = x + y$, stąd albo $m = 1$ i wtedy każda para liczb całkowitych dodatnich (x, y) spełnia nasze równanie, albo $m > 1$ i wtedy tylko para $(x, y) = (1, 1)$ spełnia nasze równanie.
- ✓ gdy $m = 1$, wówczas $x + y = (x + y)^n$, czyli $n = 1$ i wracamy do poprzedniego już rozważanego przypadku.

Załóżmy dalej, że m jest nieparzyste (przypadek, gdy liczba m jest parzysta rozwiązano powyżej) oraz $m, n > 1$. Wówczas $m > n > 1$, gdyż $(x+y)^n = x^m + y^m < (x+y)^m$.

Przyjmijmy oznaczenia jak w powyższym rozwiązaniu dla m parzystych, dochodząc do równości

$$d^{m-n}(a^m + b^m) = (a+b)^n. \tag{2}$$

Liczba nieparzysta m jest większa od 1, więc ma dzielnik pierwszy. Weźmy dowolny (oczywiście nieparzysty) dzielnik pierwszy p liczby m tj. $m = p \cdot r$, gdzie r jest dodatnią liczba nieparzystą. Oznaczmy

$$c = a^r,\ d = b^r,\ A = \frac{c^p + d^p}{c+d} = c^{p-1} - c^{p-2}d + \cdots - cd^{p-2} + d^{p-1}.$$

[1] liczby a i p są względnie pierwsze, gdyż w przeciwnym razie $p \mid a$, co na mocy podzielności $p \mid a+b$ oznaczałoby, że $p \mid b$, a więc liczby a i b nie byłyby względnie pierwsze

Liczby c i d są względnie pierwsze (bo a i b są względnie pierwsze). Możemy także założyć, że $c \geq d$ (przypadek $c < d$ jest symetryczny).

Jeśli liczba A jest równa 1, to $c = d = 1$, a więc również $a = b = 1$. Powtarzamy rozumowanie jak dla m parzystych: podstawiając otrzymane wartości do równości (2) dostajemy związek $d^{m-n} = 2^{n-1}$. Zatem d jest potęgą liczby 2, tj. $d = 2^\alpha$ oraz $\alpha(m-n) = n-1$, gdzie α jest liczbą całkowitą nieujemną (liczba α może być równa zero). Dodatkowo,dostajemy rozwiązania: $x = da = 2^\alpha, y = db = 2^\alpha$. Zatem, gdy $A = 1$ dostajemy bez trudu dowód tezy zadania.

Załóżmy dalej, że $A > 1$. Liczba A ma więc dzielnik pierwszy. Zauważmy, że

$$A \big| c^p + d^p = a^m + b^m \big| (a+b)^n \big| (a^r + b^r)^n = (c+d)^n.$$

Niech q będzie dzielnikiem pierwszym liczby A. Na mocy powyższego ciągu podzielności dostajemy $q \big| A \big| (c+d)^n$, czyli $q \big| c+d$. Stąd

$$\begin{aligned} 0 &\equiv A = c^{p-1} - c^{p-2}d + \cdots - cd^{p-2} + d^{p-1} \\ &\equiv c^{p-1} - c^{p-2}(-c) + \cdots - c(-c)^{p-2} + (-c)^{p-1} \\ &= pc^{p-1} \pmod{q}. \end{aligned}$$

Jednak liczby c i q są względnie pierwsze[2], zatem $q \big| p$, a więc $p = q$. Inaczej mówiąc jedynym dzielnikiem pierwszym liczby A jest p. Liczba A jest zatem potęgą liczby pierwszej p o wykładniku naturalnym tj. $A = p^t$, $t \in \mathbb{N}$. Ponadto, ponieważ $p = q \mid c+d$, więc $c+d = sp$, gdzie $s \in \mathbb{N}$. Przy czym liczby c i d są względnie pierwsze z p, skoro były względnie pierwsze z q.

Stosując wzór dwumianowy obliczamy

$$\begin{aligned} c^p + d^p &= [(c+d) - d]^p + d^p = \sum_{i=0}^{p-1} (-1)^i \binom{p}{i} (c+d)^{p-i} d^i - d^p + d^p \\ &= (c+d)\Big(\sum_{i=0}^{p-1} (-1)^i \binom{p}{i} (c+d)^{p-i-1} d^i \Big). \end{aligned}$$

Stąd

$$A = \sum_{i=0}^{p-2} (-1)^i \binom{p}{i} (c+d)^{p-i-1} d^i + pd^{p-1} = \sum_{i=0}^{p-2} (-1)^i \binom{p}{i} (sp)^{p-i-1} d^i + pd^{p-1}.$$

W otrzymanej sumie każdy ze składników $\binom{p}{i}(sp)^{p-i-1}d^i$ jest podzielny przez p^2 (bo $p \mid \binom{p}{i}$ i $p \mid (sp)^{p-i-1}$ dla $1 \leq i \leq p-2$ oraz $p^2 \mid (sp)^{p-1}$). Stąd i z małego twierdzenia Fermata ($d^{p-1} \equiv 1 \pmod{p}$) otrzymujemy

$$p^t = A \equiv pd^{p-1} \equiv p \pmod{p^2}$$

Tak więc $p^t \equiv p \pmod{p^2}$. Jest to jednak możliwe tylko wtedy, gdy $t = 1$. Czyli $A = p$. Jednak dla $p > 3$, $c > d$ i $c \geq 2$ równość $A = p$ nie zachodzi, gdyż wówczas mamy $A = \frac{c^p + d^p}{c+d} > c^{p-1} - c^{p-2}d \geq c^{p-2} \geq p$.

Pozostaje sprawdzić przypadki: $p \leq 3$ lub $c = d$ lub $c = 1$.

Każdy z dwóch ostatnich przypadków prowadzi do tego, że $c = d = 1$ (bo liczby c i d są względnie pierwsze i $c \geq d \geq 1$), czyli $p \mid c+d = 2$ tj. $p = 2$, co daje sprzeczność z założeniem, że p jest nieparzyste.

Z pierwszego przypadku dostajemy $p = 3$, gdyż jak pamiętamy p jest nieparzystą liczbą pierwszą. Stąd i z równości $A = p$ otrzymujemy $c^2 - cd + d^2 = 3$, czyli

[2] liczby c i q są względnie pierwsze, gdyż w przeciwnym razie $q \mid c$, co na mocy podzielności $q \mid c+d$ oznaczałoby, że $q \mid d$, a więc liczby c i d nie byłyby względnie pierwsze

$(c-d)^2+cd=3$. Łatwo sprawdzamy, że spośród par liczb względnie pierwszych c i d, gdzie $c \geq d$ tylko para $(c,d)=(2,1)$, spełnia tę równość. Ponieważ $c=a^r, d=b^r$, więc $a=2$, $b=1$, $r=1$ oraz $m=pr=3$. Podstawiając otrzymane wartości do (2) dostajemy związek $d^{3-n}=3^{n-2}$, który przy naszych ograniczeniach: $3=m \geq n \geq 1$, zachodzi jedynie dla $n=2$ i $d=1$.

Reasumując, otrzymaliśmy następujące **twierdzenie**:

Dane są liczby całkowite $m>n>1$. Równanie

$$x^m+y^m=(x+y)^n \tag{1}$$

ma rozwiązanie w liczbach całkowitych dodatnich x,y wtedy i tylko wtedy, gdy $n-1$ dzieli się przez $m-n$.

Ponadto,

- *jeżeli $m=n=1$, to równanie (1) spełnia każda para liczb całkowitych dodatnich (x,y).*
- *jeżeli $m=3$ i $n=2$, to rozwiązaniami (x,y) równania (1) są pary $(2,1)$ i $(1,2)$.*
- *jeżeli (m,n) jest parą liczb całkowitych dodatnich różnych od $(1,1)$ i $(3,2)$ oraz liczba $\alpha=(n-1)/(m-n)$ jest całkowita nieujemna, to równanie (1) ma rozwiązanie (jedyne) $x=y=2^\alpha$.*
- *dla pozostałych par $m,n>1$ równanie (1) nie ma rozwiązań w liczbach całkowitych dodatnich (x,y).*

Uwaga 2.

Najprościej rozwiązać zadanie (bez zakładania, że m jest parzyste) posługując się następującym wnioskiem z twierdzenia Zsigmondy'ego (*Delta 2/2020*) :

Jeżeli a i b $(a>b)$ są względnie pierwszymi liczbami naturalnymi oraz $m \geq 2$, to istnieje dzielnik pierwszy liczby a^m+b^m, który nie jest dzielnikiem pierwszym żadnej z liczb a^i+b^i dla $i=1,2,\ldots,m-1$, za wyjątkiem przypadku, gdy $m=3, a=2, b=1$.

Udowodnimy twierdzenie wypowiedziane w **uwadze 1.**

Trywialne przypadki równania (1), gdy $n=1$ lub $m=1$, sprawdzamy tak jak w uwadze 1. Załóżmy dalej, że $n>1$. Wówczas $m>n>1$, gdyż $(x+y)^n=x^m+y^m<(x+y)^m$.

Niech x, y będą rozwiązaniami równania (1); liczba d niech będzie największym wspólnym dzielnikiem liczb x i y oraz $x=da$, $y=db$, gdzie liczby a i b są względnie pierwsze. Równanie (1) zapisujemy w postaci

$$d^{m-n}(a^m+b^m)=(a+b)^n. \tag{2}$$

- Gdy $a=b$. Wówczas $a=b=1$, gdyż liczby a i b są względnie pierwsze. Podstawiając te wartości do (2) otrzymujemy $d^{m-n}=2^{n-1}$. Zatem d jest potęgą liczby 2, tj. $d=2^\alpha$ oraz $\alpha(m-n)=n-1$, gdzie α jest liczbą całkowitą nieujemną (liczba α może być równa zero). Dodatkowo, otrzymujemy potencjalne rozwiązanie: $x=da=2^\alpha, y=db=2^\alpha$.

  Łatwo sprawdzamy, że pary $(x,y)=(2^\alpha,2^\alpha)$, gdzie $\alpha=\frac{n-1}{m-n}$ są rozwiązaniami naszego równania z zadania.

- Gdy $a>b$ (przypadek $a<b$ jest symetryczny).

  Ponieważ liczby x, y są całkowite dodatnie, więc $a,b \geq 1$ oraz $a^m+b^m \geq 2$. Czyli, liczba a^m+b^m ma dzielnik pierwszy p. Z równości (2) wynika, że każdy dzielnik pierwszy p liczby a^m+b^m jest również dzielnikiem liczby $a+b$.

Ponieważ dodatkowo wiemy, że $m \geq 2$, więc na mocy wniosku z tw. Zsigmondy'ego musi być $m = 3, a = 2, b = 1$. Podstawiając te wartości do (2) otrzymujemy $d^{3-n} = 3^{n-2}$. Ponieważ $m = 3 > n \geq 1$, więc ostatnia równość zachodzi tylko dla $n = 2$ i $d = 1$ Otrzymujemy potencjalne rozwiązania dla $(m, n) = (3, 2)$ $x = da = 2$, $y = db = 1$. Łatwo sprawdzamy, że gdy $(m, n) = (3, 2)$, wówczas para $(x, y) = (2, 1)$ spełnia nasze równanie.

Uwaga 3.

Zobaczmy, co się stanie jeżeli w usuniemy warunek $m, n \geq 1$. Czyli zajmiemy się rozwiązaniami, gdy liczby m i n są całkowite. Mamy zadanie:

Dane są liczby całkowite m, n, przy czym $n \neq 1$. Udowodnić, że równanie

$$x^m + y^m = (x + y)^n \tag{1}$$

ma rozwiązanie w liczbach całkowitych dodatnich x, y wtedy i tylko wtedy, gdy $n - 1$ dzieli się przez $m - n$

Ponadto,

- *jeżeli $m = n = 1$, to równanie (1) spełnia każda para liczb całkowitych dodatnich (x, y).*
- *jeżeli $m = 3$ i $n = 2$, to rozwiązaniami (x, y) równania (1) są pary $(2, 1)$ i $(1, 2)$.*
- *jeżeli (m, n) jest parą liczb całkowitych różnych od $(1, 1)$ i $(3, 2)$ oraz liczba $\alpha = (n - 1)/(m - n)$ jest całkowita nieujemna, to równanie (1) ma rozwiązanie (jedyne) $x = y = 2^\alpha$.*
- *dla pozostałych par (m, n) liczb całkowitych równanie (1) nie ma rozwiązań w liczbach całkowitych dodatnich (x, y).*

Dowód.

Przyjmijmy oznaczenia jak w rozwiązaniu zadania, dochodząc do równości

$$d^{m-n}(a^m + b^m) = (a + b)^n. \tag{2}$$

Rozważmy dwa przypadki:

- Gdy $n \leq 0$.

  Wówczas $x^m + y^m = (x + y)^n < x^n + y^n$, czyli $m < n \leq 0$.

  Oznaczmy $m_1 = -m$, $n_1 = -n$. Równość (2) przybiera postać

  $$(a + b)^{n_1}(a^{m_1} + b^{m_1}) = (ab)^{m_1} d^{m_1 - n_1}. \tag{2'}$$

  Jeżeli a lub b ma dzielnik pierwszy p, to na mocy równości (2') oraz tego, że $m_1 \geq 1$ liczba pierwsza p dzieli jedną z liczb $(a + b)^{n_1}$ lub $(a^{m_1} + b^{m_1})$ tj. $p \mid a + b$ lub $p \mid a^{m_1} + b^{m_1}$. Każdy z tych przypadków prowadzi do stwierdzenia, że liczba pierwsza p dzieli obie liczby a i b, co przeczy temu, że liczby te są względnie pierwsze. Tak więc liczby a i b nie mają dzielników pierwszych, czyli $a = b = 1$. Podstawiając otrzymane wartości do równości (2') dostajemy związek $d^{m_1 - n_1} = 2^{n_1 + 1}$. Zatem d jest potęgą liczby 2, tj. $d = 2^\alpha$ oraz $\alpha(m_1 - n_1) = n_1 + 1$, tj. $\alpha(m - n) = n - 1$, gdzie α jest liczba całkowitą dodatnią. Inaczej mówiąc, jeżeli równanie (1) ma rozwiązania, to liczba $n - 1$ dzieli się przez $m - n$.

  Łatwo sprawdzamy, że pary $(x, y) = (2^\alpha, 2^\alpha)$, gdzie $\alpha = \frac{n-1}{m-n}$ są rozwiązaniami naszego równania z zadania. Mamy więc dowód implikacji w drugą stronę tj. jeżeli liczba $\alpha = (n - 1)/(m - n)$ jest naturalna, to równanie (1) ma rozwiązanie (jedyne) $x = 2^\alpha, y = 2^\alpha$.

- Gdy $n > 0$.

  Wówczas dostajemy przypadek już rozwiązany w zadaniu i w **Uwagach 1 i 2**.

Rozwiązanie i uwagi do zadania 798 (b)

Piotr KUMOR

(b) Udowodnimy, że są to wiersze, których numery są potęgami dwójki (o wykładniku całkowitym dodatnim) i tylko te wiersze.

Niech: $(1+x+x^2)^n = \sum_{k=0}^{2n} a_k x^k$ będzie rozwinięciem wielomianu $(1+x+x^2)^n$ względem potęg zmiennej x. W n–tym wierszu naszego trójkąta występują kolejno liczby a_k. Zaczynając od lewej i numerując identycznie, czyli od zera do $2n$. To tak zwane „współczynniki trójmianowe" (*trinomial coefficients*). Dowodzimy tego faktu przez natychmiastową indukcję względem n (i uznajmy to za udowodnione).

Mamy oczywiście: $(1+x+x^2)^n = \sum_{k=0}^{n} \binom{n}{k}(x+x^2)^k$, gdzie jest $\binom{n}{k}$ jest współczynnikiem dwumianowym Newtona.

Niech $0 < k_n \leq n$ będzie **najmniejszą** liczbą całkowitą k taką, że liczba $\binom{n}{k}$ jest nieparzysta. To znaczy liczby $\binom{n}{1}, \binom{n}{2}, \ldots \binom{n}{k_n-1}$ są parzyste, zaś liczba $\binom{n}{k_n}$ jest nieparzysta.

Wiadomo, że $k_n = n$ wtedy i tylko wtedy, gdy jest potęgą dwójki.

Jest to fakt ogólnie znany, z pewnością wystąpił jako zadanie Austriacko–Polskich Zawodów Matematycznych.

Dowód na pewno można też znaleźć w tomie 7 Zadań z Olimpiad Matematycznych (Maciej Bryński) albo w książce Andrzeja Nowickiego „Podróże po Imperium Liczb", część 11 „Silnie i symbole Newtona". Książka wydana przez Olsztyńską Wyższą Szkołę Informatyki i Zarządzania w Olsztynie w roku 2011. Dowód podany na stronie 90, punkt 8.1.1 i 8.1.3 (szczególny przypadek twierdzenia Glaishera z roku 1899).

Z równości $(1+x+x^2)^n = \sum_{k=0}^{n} \binom{n}{k}(x+x^2)^k = \sum_{k=0}^{2n} a_k x^k$ jest widoczne, że najmniejsza **dodatnia** wartość k taka, że liczba a_k jest nieparzysta, jest równa k_n.

Jeżeli więc liczba n jest potęgą dwójki, to $k_n = n$ więc dla dodatnich k mniejszych od n liczby a_k są parzyste. Dla k większych od n wygląda to symetrycznie, więc dokładnie trzy wartości a_k są nieparzyste: obie skrajne i środkowa.

Oczywiście te trzy wartości a_k zawsze są nieparzyste (trywialne). Jednak gdy liczba n nie jest potęgą dwójki, to wystąpią jeszcze co najmniej dwie inne nieparzyste wartości a_k, mniejsza wartość k jest równa $k_n < n$ (w tym przypadku). W tym wierszu jest więc co najmniej pięć liczb nieparzystych.

Teza punktu (b) została udowodniona.

Uwagi.

1) Zadanie jest bardzo znane. Dawno temu występowało na rosyjskich (i nie tylko rosyjskich) olimpiadach matematycznych. Na przykład „Kwant" 4/1972 lub „Zarubieżnyje matiematiczieskije olimpiady" Moskwa Nauka 1987 (zad. 1.3). Chodzi tu raczej o punkt (a), ale punkt (b) też jest dobrze zbadany.

2) Obszerne informacje znajdują się w pliku T. Sillke, *Odd trinomials*, dostępnym pod adresem:

https://www.math.uni-bielefeld.de/~sillke/PUZZLES/trinomials

w którym udowodniono między innymi:

W żadnym wierszu trójkąta (modulo dwa) nie występują cztery kolejne jedynki, co stanowi znaczne wzmocnienie punktu (a).

Jeżeli $z(n)$ oznacza liczbę jedynek w n–tym wierszu, to prawdziwe są równania rekurencyjne:

$$z(2n) = z(n), \quad z(4n+1) = 3z(n), \quad z(4n+3) = z(2n+1) + 2z(n).$$

Są one tam udowodnione, a dowód nie jest nadmiernie trudny. Na podstawie tych równań można łatwo uzyskać tezę punktu (b) także w wersji znacznie wzmocnionej.

Rozwiązanie zadania 798 (b)

Mikołaj PATER

(b) Rozważmy ciąg liczb $a(k,n)$, gdzie $k \in \mathbb{Z}$, $n \in \mathbb{Z} \setminus \mathbb{Z}_-$, spełniający równania

$$\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-}\forall_{x\in\mathbb{R}}(1+x+x^2)^n = \sum_{k=0}^{2n} a(k,n)\cdot x^k,$$

$$\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-}\forall_{k\in\mathbb{Z}\setminus\{0,1,\ldots,2n\}} a(k,n) = 0.$$

Nietrudno wykazać, że k-ta liczba w n-tym wierszu trójkątnego diagramu z treści zadania jest równa $a(k,n)$, gdzie $k \in \{0,1,...,2n\}$, $n \in \mathbb{Z} \setminus \mathbb{Z}_-$.

Dla wielomianów $f(x)$, $g(x)$ będziemy pisać $f(x) \sim g(x)$, jeśli wszystkie współczynniki wielomianu $f(x) - g(x)$ są parzyste oraz $f(x), g(x) \in \mathbb{Z}[x]$.

Z definicji wynika, że wielomiany $f(x)$, $g(x)$ spełniające $f(x) \sim g(x)$ mają równą liczbę współczynników nieparzystych.

Niech $b(n)$ będzie liczbą liczb nieparzystych w n-tym wierszu. Wykażemy następujące równania

(1) $\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-} b(2n) = b(n)$,

(2) $\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-} b(4n+1) = 3b(n)$,

(3) $\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-} b(4n+3) = b(2n+1) + 2b(n)$.

Dowód (1). Ze wzoru dwumianowego Newton'a

$$(1+x^2+x^4)^n \sim (1+x^2+x^4+2x+2x^3+2x^2)^n = (1+x+x^2)^{2n}.$$

Oczywiście wielomiany $(1+x+x^2)^n$, $(1+x^2+x^4)^n$ posiadają tyle samo współczynników nieparzystych. □

Dowód (2). Pod falą jest „ukryte" jak wyżej dwukrotne zastosowanie dwumianu Newtona, dalej korzystamy z definicji ciągu.

$$(1+x+x^2)^{4n+1} \sim (1+x^4+x^8)^n \cdot (1+x+x^2) = \sum_{k=0}^{2n} a(k,n)\cdot(x^{4k}+x^{4k+1}+x^{4k+2}).$$

Powyższy wielomian zapisany w postaci sumy ma trzykrotnie więcej współczynników nieparzystych niż wielomian $(1+x+x^2)^n$, ponieważ zbiory

$$\{4k : k \in \{0,1,...,2n\}\}, \{4k+1 : k \in \{0,1,...,2n\}\}, \{4k+2 : k \in \{0,1,...,2n\}\}$$

nie mają elementów wspólnych. □

Dowód (3). Na początek zauważmy, że

$$(1+x^2+x^4)^{2n+1} \sim (1+x^4+x^8)^n \cdot (1+x^2+x^4) = \sum_{k=0}^{2n} a(k,n)\cdot(x^{4k}+x^{4k+2}+x^{4k+4}).$$

Postępując podobnie jak wcześniej

$$(1+x+x^2)^{4n+3} \sim (1+x^4+x^8)^n \cdot (1+x+x^3+x^5+x^6) =$$
$$\sum_{k=0}^{2n} a(k,n)\cdot(x^{4k}+x^{4k+6}) + \sum_{k=0}^{2n} a(k,n)\cdot x(x^{4k}+x^{4k+2}+x^{4k+4}).$$

Niebieski wielomian ma dwukrotnie więcej współczynników nieparzystych niż wielomian $(1+x+x^2)^n$, z kolei zielone wielomiany mają ich po tyle samo. Pozostaje zaobserwować, że współczynniki nieparzyste niebieskiego wielomianu nigdy nie będą dodawane ze współczynnikami nieparzystymi zielonego wielomianu z powodu rozdziału wykładników potęg przy zmiennej x na rozłączne ciągi. □

Spójrzmy ponownie na nasz trójkąt (mod 2). Jest on symetryczny względem swojej „wysokości". Wobec tego każda liczba na pozycji równej liczbie porządkowej danego niezerowego wiersza (czyli leżąca na wysokości) jest równa 1, bo stoi nad nią jedynka i dwie równe liczby obok. Każdy niezerowy wiersz ma jeszcze dwie jedynki na swoich krańcach. To dowodzi

$$\forall_{n\in\mathbb{Z}_+} b(n) \geq 3.$$

Stąd

$$\forall_{n\in\mathbb{Z}_+} b(4n+1) \geq 9 > 3,$$
$$\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-} b(4n+3) > b(2n+1) \geq 3.$$

To daje

$$\forall_{n\in\mathbb{Z}_+} b(2n+1) > 3. \tag{4}$$

Jeżeli liczba całkowita $m \in \mathbb{Z}_+$ może być zapisana w postaci

$$m = 2^{\nu_2(m)} \cdot p, \quad \text{gdzie } p \in \mathbb{Z}_+ \setminus \{1,2\} \wedge 2|p+1,$$

to na mocy (1) oraz (4) otrzymamy

$$b(m) = b\Big(2^{\nu_2(m)} \cdot p\Big) = b(p) > 3.$$

Pamiętając o $b(0) = 1$ wykazaliśmy, że jedyne liczby n, dla których $b(n) = 3$, mogą być postaci 2^s, gdzie $s \in \mathbb{Z} \setminus \mathbb{Z}_-$. Pozostaje zauważyć, że $b(1) = 3$, więc równanie (1) potwierdza, że jest to również warunek wystarczający. Podsumowując

$$\forall_{n\in\mathbb{Z}\setminus\mathbb{Z}_-} \Big(b(n) = 3 \Leftrightarrow \exists_{s\in\mathbb{Z}\setminus\mathbb{Z}_-} n = 2^s\Big).$$

Literatura

Hayri Ardal, Tom Brown, and Veselin Jungić. Chaotic orderings of the rationals and reals. *The American Mathematical Monthly*, 118(10):921–925, 2011.

J Davis, R Entringer, R Graham, and G Simmons. On permutations containing no long arithmetic progressions. *Acta Arithmetica*, 1(34):81–90, 1977.

Andrej Dujella and Clemens Fuchs. Complete solution of a problem of Diophantus and Euler. *Journal of the London Mathematical Society*, 71(1):33–52, 2005.

Andrej Dujella, Alan Filipin, and Clemens Fuchs. Effective solution of the $D(-1)$-quadruple conjecture. *Acta Arithmetica*, 128(4):319–338, 2007.

Bo He, Alain Togbé, and Volker Ziegler. There is no Diophantine quintuple. *Transactions of the American Mathematical Society*, 371(9):6665–6709, 2019.

Gyula Károlyi and Péter Komjáth. Well ordering groups with no monotone arithmetic progressions. *Order*, 34(2):299–306, 2017.