Nieparzyste dzielniki i wykładniki p-adyczne

Seminarium Olimpiady Matematycznej dla nauczycieli,
Arkadiusz Męcel
17-18.12.2021 r.

Nieparzyste dzielniki

Jedną z metod rozwiązywania zadań z teorii liczb jest rozważanie największego dzielnika nieparzystego liczby całkowitej. Innymi słowy, każdą liczbę całkowitą dodatnią możemy zapisać w postaci:

$$n = 2^k \cdot m,$$

gdzie m jest liczbą nieparzystą, a dokładniej – największym nieparzystym dzielnikiem liczby n.

Zadanie 1 (W. Sierpiński[1] (5), Zad. 11)**.** *Niech n będzie liczbą naturalną. Ile co najwyżej liczb może zawierać zbiór liczb naturalnych nie większych od $2n$, z których żadna nie jest podzielna przez żadną inną?*

Rozwiązanie. W szukanym zbiorze nie może być dwóch liczb $a > b$ mających ten sam największy dzielnik nieparzysty m, bowiem wtedy $b \mid a$. Rzeczywiście, jeśli dla pewnych $r > s$ mamy $a = 2^r \cdot m > 2^s \cdot m = b$, czyli $\frac{a}{b} = 2^{r-s}$. Liczb nieparzystych nie większych niż $2n$ jest n, a zatem tyle elementów może mieć co najwyżej poszukiwany zbiór. I rzeczywiście, zbiór liczb postaci: $\{n+1, \ldots, 2n\}$ ma szukaną własność. ■

Zadanie 2 ((Wariacja na temat poprzedniego zadania))**.** *Rozważmy zbiór S złożony z n liczb postaci $S = \{n+1, n+2, \ldots, 2n-1, 2n\}$. Pokazać, że suma największych nieparzystych dzielników wszystkich elementów zbioru S równa jest n^2.*

Rozwiązanie. W zbiorze $\mathcal{S}$ nie ma dwóch liczb mających ten sam dzielnik nieparzysty. Argumentujemy niemal identycznie jak wyżej. Gdyby pewne $a > b$ ze zbioru $\mathcal{S}$ miały sam sam nieparzysty dzielnik, wówczas dla pewnych $r > s$ mamy $a = 2^r \cdot m > 2^s \cdot m = b$, czyli $\frac{a}{b} = 2^{r-s} \geqslant 2$. Jednak dla dowolnych elementów $a > b$ ze zbioru $\mathcal{S}$ mamy: $\frac{a}{b} < 2$. Uzyskana sprzeczność pokazuje, że największe nieparzyste dzielniki liczb ze zbioru S są parami różne. Jest ich $n+1$. A zatem są to elementy zbioru $1, 3, \ldots, 2n-1$. Suma tych elementów to oczywiście n^2.■

Zadanie 3 (Węgry, 2003)**.** *Dla liczby całkowitej dodatniej k przez $p(k)$ oznaczamy największy dzielnik nieparzysty k. Wykazać, że dla dowolnego n całkowitego dodatniego mamy:*

$$\frac{2n}{3} < \frac{p(1)}{1} + \frac{p(2)}{2} + \ldots + \frac{p(n)}{n} < \frac{2(n+1)}{3}.$$

Rozwiązanie. Patrz (7), Zad. 3.30. Zauważmy, że

$$p(k) = \begin{cases} k & \text{, gdy k jest liczbą nieparzystą,} \\ p(k/2) & \text{, gdy k jest liczbą parzystą.} \end{cases}.$$

Widać więc, że sensownie jest poprowadzić rozumowanie indukcyjne, przy czym krok indukcyjny będziemy wykonywać w zależności od parzystości n. Rozważamy dalej dwa przypadki.

- Przypadek 1, gdy $n = 2l$. Wówczas

$$\frac{p(1)}{1} + \frac{p(2)}{2} + \ldots + \frac{p(2l)}{2l} = 1 + \frac{p(2)}{2} + 1 + \frac{p(4)}{4} + \ldots + 1 + \frac{p(2l)}{2l} = l + \frac{1}{2}\left(\frac{p(1)}{1} + \ldots + \frac{p(l)}{l}\right).$$

  Z założenia indukcyjnego wiemy, że $\frac{l}{3} < \frac{1}{2} \cdot \left(\frac{p(1)}{1} + \ldots + \frac{p(l)}{l}\right) < \frac{(l+1)}{3}$. A zatem dodając l mamy:

$$\frac{l}{3} + l = \frac{4l}{3} < \frac{p(1)}{1} + \frac{p(2)}{2} + \ldots + \frac{p(n)}{n} < \frac{(l+1)}{3} + l = \frac{4l+1}{3},$$

  ale

$$\frac{2n}{3} = \frac{4l}{3}, \quad \frac{4l+1}{3} < \frac{4l+2}{3} = \frac{2(n+1)}{3}.$$

- Przypadek 2, gdy $n = 2l+1$ rozpatrujemy w sposób analogiczny.

[1] W znanej pozycji Art and Craft of Problem Solving P. Zeitz przypisuje to zadanie P. Erdösowi, patrz Example 3.3.7.

■

Zadanie 4 (XXXIV OM (1982), 2 etap; Olimpiada Matematyczna RFN 1982, 1 etap)**.**
Niech $a(k)$ będzie największą liczbą nieparzystą, przez którą dzieli się k. Udowodnić, że:

$$\sum_{k=1}^{2^n} a(k) = \frac{1}{3}(4^n + 2).$$

Rozwiązanie. **Sposób 1.** Rozumowanie przedstawiane w RFN i zagranicznych książkach cytujących to zadanie. Niech $S(a, b, c, \ldots)$ oznacza sumę największych dzielników nieparzystych liczb $a, b, c \ldots$. W szczególności niech $S_n = S(1, 2, 3, \ldots, 2^n)$ będzie szukaną przez nas sumą.

Korzystamy z obserwacji poczynionej w poprzednim zadaniu, na mocy której otrzymujemy:

$$S_n = S(1,2,3,\ldots,2^n) = S(1,3,5,\ldots,2^n-1) + S(2,4,6,\ldots,2^n) = (1+3+5+\ldots+2^n-1) + S(1,2,3,\ldots,2^{n-1}).$$

Jak zdążyliśmy się przekonać w Zadaniu 2, suma pierwszych k dodatnich liczb nieparzystych równa jest k^2. Skoro $2^n - 1$ jest 2^{n-1}-wszą liczbą nieparzystą, to:

$$S_n = (2^{n-1})^2 + S(1,2,3,\ldots,2^{n-1}) = 4^{n-1} + S_{n-1} \quad \Rightarrow \quad S_n - S_{n-1} = 4^{n-1}.$$

Używając wielokrotnie powyższego warunku mamy:

$$S_n - S_1 = (S_n - S_{n-1}) + (S_{n-1} - S_{n-2}) - \ldots - (S_2 - S_1) = 4 + 4^2 + \ldots + 4^{n-1} \Rightarrow S_n = 2 + \frac{4(4^{n-1}-1)}{4-1} = \frac{4^n+2}{3}.$$

Sposób 2. Rozumowanie przedstawione w Archiwum OM[2]. Jeśli liczba całkowita m jest podzielna przez 2^r, ale nie jest podzielna przez 2^{r+1}, to $a(m) = \frac{m}{2^r}$. Mamy też:

$$a(m) = \frac{m}{2^r} = m - \frac{m}{2} - \frac{m}{4} - \ldots - \frac{m}{2^r}.$$

Pomysł polega na zamianie sumy $a(1) + \ldots + a(2^n)$ na sumę powyższych różnic, branych od $m = 1$ do $m = 2^n$. Wyobraźmy sobie, że w kolejne wiersze wpisujemy kolejne składniki różnic:

$$\begin{array}{rccccccccc}
a(1) = & 1 & & & & & & & & \\
a(2) = & 2 & -1 & & & & & & & \\
a(3) = & 3 & & & & & & & & \\
a(4) = & 4 & -2 & -1 & & & & & & \\
a(5) = & 5 & & & & & & & & \\
a(6) = & 6 & -3 & & & & & & & \\
a(7) = & 7 & & & & & & & & \\
a(8) = & 8 & -4 & -2 & -1 & & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\
a(2^n-2) = & 2^n-2 & -(2^{n-1}-1) & & & & & & & \\
a(2^{n-1}) = & 2^{n-1} & & & & & & & & \\
a(2^n) = & 2^n & -2^{n-1} & -2^{n-2} & -2^{n-3} & -2^{n-4} & -2^{n-5} & \ldots & -1 &
\end{array}$$

Możemy rozłożyć powyższą sumę na sumy częściowe zgodnie z kolumnami powyższej tabeli. W pierwszej kolumnie jest suma liczb od 1 do 2^n. W drugiej odejmujemy połówki wszystkich liczb całkowitych podzielnych przez 2, a więc liczby całkowite od 1 do 2^{n-1}. W kolejnej kolumnie odejmujemy ćwiartki liczb podzielnych przez 4, czyli łącznie kolejne liczby całkowite od 1 do 2^{n-2}, itd. Stąd możemy zapisać sumę $a(1) + \ldots + a(2^n)$ jako:

$$\begin{aligned}
\sum_{k=1}^{2^n} a(k) &= \sum_{k=1}^{2^n} k - \frac{1}{2}\sum_{k=1}^{2^{n-1}} 2k - \frac{1}{4}\sum_{k=1}^{2^{n-2}} 4k - \ldots - \frac{1}{2^{n-1}}\sum_{k=1}^{2} 2^{n-1}k - \frac{2^n}{2^n} = \\
&= \sum_{k=1}^{2^n} k - \sum_{k=1}^{2^{n-1}} k - \sum_{k=1}^{2^{n-2}} k - \ldots - \sum_{k=1}^{2} k - 1 \\
&= \frac{2^n(2^n+1)}{2} - \frac{2^{n-1}(2^{n-1}+1)}{2} - \frac{2^{n-2}(2^{n-2}+1)}{2} - \ldots - \frac{2(2+1)}{2} - 1.
\end{aligned}$$

Dalszy rachunek polega jedynie na zsumowaniu uzyskanych ciągów geometrycznych, co zostawiam Czytelnikowi.
■

[2] `https://archom.ptm.org.pl/?q=node/866`, uwaga na literówki.

Zadanie 5 (USAMO, 1993)**.** *Niech f_1, f_2 będą nieparzystymi liczbami dodatnimi. Dla $n \geqslant 3$ określamy f_n jako największy nieparzysty dzielnik liczby $f_{n-2} + f_{n-1}$. Znaleźć* $\lim_{n\to\infty} f_n$.

Rozwiązanie. Rozwiązanie ma trzy etapy, same w sobie stanowiące dość charakterystyczne typy rozumowań.

- Pokażemy, że jeśli pewne dwa kolejne wyrazy rozważanego ciągu są sobie równe, to wszystkie dalsze też.
- Pokażemy, że pewne dwa kolejne wyrazy ciągu muszą być równe.
- Pokażemy, że NWD kolejnych par wyrazów ciągu są takie same.

Pierwsza uwaga jest taka, że wszystkie elementy rozważanego ciągu są liczbami nieparzystymi. Istotnie, począwszy od dwóch liczb nieparzystych f_1, f_2, każdy kolejny element ciągu jest dzielnikiem nieparzystym sumy dwóch poprzednich wyrazów, a więc jest liczbą nieparzystą.

Przypuśćmy teraz, że trzy kolejne wyrazy naszego ciągu mają postać a, a, b. Wiemy, że b to największy nieparzysty dzielnik liczby $a + a$, gdzie a jest liczbą nieparzystą. W szczególności $b = a$. A zatem jeśli dwa wyrazy naszego ciągu są równe, to wszystkie dalsze też.

Załóżmy teraz, że żadne dwa kolejne wyrazy wypisywanego ciągu nie są równe. Weźmy zatem cztery kolejne wyrazy a, b, c, d. Mamy nierówność:

$$c \leqslant \frac{a+b}{2} < \max\{a, b\}.$$

Rzeczywiście c jest największym dzielnikiem nieparzystym a oraz b, więc jego uzyskanie wymaga podzielenia przez pewną dodatnią potęgę 2, bo suma $a + b$ jest zawsze parzysta. A druga nierówność? Otóż skoro liczby a, b są różne, to ich średnia nie może być równa żadnej z nich, a zatem jest mniejsza od większej z nich. Podobną nierówność dostajemy dla b, c, d:

$$d \leqslant \frac{c+b}{2} < \max\{b, c\} \leqslant \max\{a, b\}.$$

Łącząc uzyskane nierówności otrzymujemy:

$$\max\{a, b\} < \max\{c, d\}.$$

To jest jednak niemożliwe, bo nieskończony ciąg liczb dodatnich

$$\max\{f_n, f_{n+1}\}$$

nie może być ściśle malejący. A zatem rzeczywiście pewne dwa elementy naszego ciągu muszą być równe, a jak pokazaliśmy wyżej, z tego wynika, że od pewnego miejsca ciąg ma tę samą wartość.

Teraz pokażemy, że ta wartość to $\mathrm{NWD}(f_1, f_2)$. Niech a, b, c to trzy kolejne wyrazy naszego ciągu. Niech $\mathrm{NWD}(a, b) = x$, $\mathrm{NWD}(b, c) = y$. Teza jest taka, że $x = y$. Oczywiście

$$c = \frac{a+b}{2^n},$$

dla pewnego n całkowitego dodatniego. A zatem przekształcając to wyrażenie dostajemy

$$2^n c - b = a.$$

Liczby b, c są podzielne przez y. A zatem także a jest podzielna przez y. Wiemy jednak, że to x jest największym wspólnym dzielnikiem a, b, więc $y \leqslant x$.

Z drugiej strony, $a = xa'$ oraz $b = xb'$. Oczywiście x jest liczbą nieparzystą. A zatem c, jako największy dzielnik nieparzysty liczby $a + b$ równe jest iloczynowi x oraz największego dzielnika nieparzystego liczby $a' + b'$. W szczególności x jest wspólnym dzielnikiem zarówno b, jak i c. Zatem $x \leqslant y$. W rezultacie dostajemy $x = y$.

A zatem wszystkie kolejne NWD kolejnych wyrazów rozważanego ciągu są takie same i wynoszą $\mathrm{NWD}(f_1.f_2)$. Skoro, na mocy pierwszej części dowodu od pewnego momentu ciąg ten jest stały, to właśnie owa stała wartość wynosi $\mathrm{NWD}(f_1, f_2)$.

■

Zadanie 6 (LX OM, 1 etap)**.** *Dana jest liczba całkowita $n \geqslant 2$. Niech $r_1, r_2, r_3, \ldots, r_{n-1}$ będą odpowiednio resztami z dzielenia liczb*

$$1, \quad 1+2, \quad 1+2+3, \cdots, \quad 1+2+\ldots+(n-1)$$

przez n. Znaleźć wszystkie takie wartości n, że ciąg $(r_1, r_2, \ldots, r_{n-1})$ jest permutacją ciągu $(1, 2, \ldots, n-1)$.

Rozwiązanie. Rozwiązanie za Archiwum OM[3]. Odpowiedź: $n = 2^k$, dla $k = 1, 2, 3, \ldots$

Wykażemy najpierw, że potęgi dwójki spełniają warunki zadania. W tym celu wystarczy udowodnić, że jeżeli $n = 2^k$, dla pewnego całkowitego $k \geqslant 1$, to reszty $r_1, r_2, r_3, \ldots, r_{n-1}$ są parami różne i żadna z nich nie jest równa zeru. Gdyby któraś z tych reszt, powiedzmy r_m, była równa zeru, to liczba

$$1+2+\ldots+m = \frac{m(m+1)}{2}$$

byłaby podzielna przez 2^k. Zatem dla pewnej wartości $m \in \{1, 2, \ldots, 2^k - 1\}$ iloczyn $m(m+1)$ byłby podzielny przez 2^{k+1}. Lecz jedna z liczb $m, m+1$ jest parzysta, a druga – nieparzysta. Stąd jedna z nich musiałaby być podzielna przez 2^{k+1}, wbrew temu, że obie te dodatnie liczby nie przekraczają 2^k.

Gdyby z kolei dwie z rozważanych reszt były równe – powiedzmy $r_l = r_m$, gdzie $1 \leqslant l < m \leqslant n-1$, wówczas liczba:

$$(1+2+\ldots+m) - (1+2+\ldots+l) = \frac{m(m+1)}{2} - \frac{l(l+1)}{2} = \frac{m^2 - l^2 + m - l}{2} = \frac{(m-l)(m+l+1)}{2}$$

byłaby podzielna przez 2^k. Suma czynników w liczniku to $2m+1$, czyli liczba nieparzysta. Tak jak wcześniej wynika stąd, że jedna z liczb $m-l, m+l+1$ musi być podzielna przez 2^{k+1}. Jednakże liczby l, m są różne, dodatnie i mniejsze niż 2^k, co ponownie daje sprzeczność.

Aby dokończyć rozwiązanie, wystarczy dowieść, że gdy liczba m ma nieparzysty dzielnik pierwszy p, to ciąg $(r_1, r_2, \ldots, r_{n-1})$ nie jest permutacją ciągu $(1, 2, \ldots, n-1)$. Zauważmy w tym celu, że dla dowolnej liczby całkowitej dodatniej t liczby:

$$1+2+\ldots+(tp-2)+(tp-1) = \frac{tp(tp-1)}{2}, \quad 1+2+\ldots+(tp-1)+tp = \frac{tp(tp+1)}{2}$$

są podzielne przez p, gdyż nieparzysty czynnik pierwszy p w liczniku nie skraca się z mianownikiem. W związku z tym reszty:

$$r_{p-1}, r_p, \quad r_{2p-1}, r_{2p}, \quad r_{3p-1}, r_{3p}, \quad \ldots, \quad r_{n-p-1}, r_{n-p}, \quad r_{n-1}$$

są podzielne przez p. Zatem w ciągu $(r_1, r_2, \ldots, r_{n-1})$ co najmniej $2\frac{n}{p} - 1$ liczb jest podzielnych przez p. W ciągu $(1, 2, \ldots, n-1)$ występuje zaś jedynie $\frac{n}{p} - 1$ liczb podzielnych przez p. Tak więc liczba n nie ma żądanej własności. ■

Zadanie 7 (LXIV OM, 1 etap)**.** *Niech n będzie dodatnią liczbą całkowitą. Wykazać, że jeśli suma wszystkich jej dodatnich dzielników jest nieparzysta, to liczba n jest kwadratem lub podwojonym kwadratem liczby całkowitej.*

Rozwiązanie.[4] Niech $n = 2^k \cdot l$, gdzie l jest dodatnią liczbą nieparzystą. Zauważmy, że każdy nieparzysty dzielnik liczby n musi być dzielnikiem liczby l. Ile jest tych nieparzystych dzielników?

Suma parzystych dzielników liczby n jest parzysta, jeśli więc suma wszystkich dodatnich dzielników liczby n jest nieparzysta, to nieparzystych dzielników n jest nieparzyście wiele. A zatem l ma nieparzyście wiele dzielników. Wynika stąd, że l jest kwadratem pewnej liczby całkowitej m. A zatem

$$n = 2^k \cdot m^2.$$

Jeśli k jest parzysta, to $k/2$ jest całkowita nieujemna i n jest kwadratem:

$$n = \left(2^{\frac{k}{2}} \cdot m\right)^2.$$

Jeśli zaś k jest nieparzysta, to liczba $\frac{k-1}{2}$ jest całkowita i wtedy n jest podwojonym kwadratem:

$$n = 2 \cdot \left(2^{\frac{k-1}{2}} \cdot m\right)^2.$$

■

[3] `https://archom.ptm.org.pl/?q=node/9`, uwaga na literówki

[4] J. Jaszuńska, *Kwadraty i dzielniki raz jeszcze*, Gezetka OMJ Kwadrat, nr 12 (2004), `https://omj.edu.pl/gazetka-omj`.

Zadanie 8 (LXIII OM, 2 etap)**.** *Niech m, n będą takimi dodatnimi liczbami całkowitymi, że w zbiorze $\{1, 2, \ldots, n\}$ znajduje się dokładnie m liczb pierwszych. Dowieść, że wśród dowolnych $m+1$ różnych liczb z tego zbioru można znaleźć liczbę, która jest dzielnikiem iloczynu pozostałych m liczb.*

Rozwiązanie. Rozwiązanie za stroną OM. Rozumujemy nie wprost. Załóżmy, że teza zadania jest nieprawdziwa. Oznaczałoby to w przypadku naszego zadania istnienie $m+1$-elementowego zbioru A zawartego w zbiorze $\{1, 2, \ldots, n\}$ (przy czym istnieje dokładnie m liczb pierwszych mniejszych od n) takiego, że żadna liczba $x \in A$ nie jest dzielnikiem iloczynu pozostałych m elementów zbioru A. I co dalej?

Pomysł opiera się on na ogólnej obserwacji mówiącej, że liczba a jest dzielnikiem liczby b wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p wykładnik, z jakim liczba p wchodzi do rozkładu a na czynniki pierwsze jest nie większy, niż wykładnik, z jakim p wchodzi do rozkładu b na czynniki pierwsze. Co ta obserwacja wnosi do rozważanego problemu? Otóż to, że każdemu elementowi x zbioru A, który ma być świadkiem nieprawdziwości tezy, przypisać można liczbę pierwszą p taką, że $x = p^s x'$ oraz w rozkładzie iloczynu pozostałych m elementów zbioru A na czynniki pierwsze liczba p występuje mniej niż s razy. Innymi słowy każdemu elementowi zbioru A przypisujemy liczbę pierwszą, która jest przyczyną braku podzielności tego elementu przez iloczyn pozostałych m elementów zbioru A.

Zbiór A ma $m+1$ elementów, a wiemy, że zawarty jest w zbiorze $\{1, 2, \ldots, n\}$, w którym jest tylko m liczb pierwszych. W rezultacie pewna liczba pierwsza została przypisana dwóm różnym elementom $x, y \in A$. Niech w oznacza iloczyn $m-1$ elementów zbioru A różnych od x, y. Na mocy określenia liczby p istnieją takie nieujemne całkowite wykładniki k i l, że:

- p^k jest dzielnikiem x, ale p^k nie jest dzielnikiem wy,
- p^l jest dzielnikiem y, ale p^l nie jest dzielnikiem wx.

Zatem w rozkładzie $wx \cdot wy$ liczba p występuje z wykładnikiem niższym niż $k+l$, mimo, że iloczyn ten jest podzielny przez liczbę xy, która z kolei jest podzielna przez p^{k+l}. Uzyskana sprzeczność kończy rozwiązanie. ■

Zadanie 9 (Obóz naukowy OM, 2007)**.** *Rozstrzygnąć, czy dla dowolnych liczb całkowitych $a > b > 0$ istnieje nieskończenie wiele liczb całkowitych dodatnich n, że liczba $a^n + b^n$ jest podzielna przez n.*

Rozwiązanie. Rozwiązanie za stroną OM. Rozpatrujemy przypadki, gdy $a+b$ jest liczbą parzystą i nieparzystą.

- Przypadek 1, gdy $a+b$ jest nieparzysta. Przypuśćmy, że $n \mid a^n + b^n$. Skonstruujemy większą liczbę m, dla której $m \mid a^m + b^m$. Zauważmy w tym celu, że liczba $a^n + b^n$ jest większa od n, więc istnieje dzielnik pierwszy p liczby $\frac{a^n+b^n}{n}$. Mamy wtedy $pn \mid a^n + b^n$, a ponieważ liczba p jest nieparzysta (z zał.), prawdziwa jest podzielność: $a^n + b^n \mid a^{pn} + b^{pn}$. Wystarczy zatem przyjąć $m = pn$. Rozpoczynając od $n = 1$ dostajemy w ten sposób indukcyjnie rosnący ciąg liczb całkowitych dodatnich spełniających tezę.
- Przypadek 2, gdy liczba $a+b$ jest parzysta. Jeśli obie liczby a, b są parzyste, to oczywiście każda z liczb postaci $n = 2^k$, dla $k = 0, 1, 2, \ldots$ spełnia warunek $n \mid a^n + b^n$, gdyż wynika to z podzielności $2^k \mid 2^{2^k}$, która jest natychmiastową konsekwencją nierówności $2^k > k$.

  Załóżmy z kolei, że liczby a i b są nieparzyste. Wówczas $a^2 + b^2 \equiv 2 \bmod 4$, oraz $a^2 + b^2 > 2$, więc istnieje nieparzysty dzielnik pierwszy $p \mid a^2 + b^2$. Dalej rozumujemy jak w przypadku pierwszym, rozpoczynając od przypadku $n = 2$. Przypuśćmy, że liczba parzysta n spełnia podzielność $n \mid a^n + b^n$. Wtedy liczby n oraz $a^n + b^n$ są parzyste i niepodzielne przez 4, więc liczba $\frac{a^n+b^n}{n}$ ma nieparzysty dzielnik pierwszy p. Liczba $m = pn$ jest w tej sytuacji większa od n i również spełnia $m \mid a^m + b^m$.

■

Zadanie 10 (St. Peterburg, 2001)**.** *Pokazać, że istnieje nieskończenie wiele dodatnich liczb całkowitych n takich, że $n^4 + 1$ ma dzielnik pierwszy większy niż $2n$.*

Rozwiązanie. Patrz (3), str. 19 lub (7), Zad. 3.29. Pokażemy, że zbiór $\mathcal{P}$ dzielników pierwszych liczb w ciągu $n^4 + 1$ jest nieskończony. Istotnie, gdyby liczby $p_1, p_2, \ldots, p_k$ były jedynymi elementami zbioru $\mathcal{P}$, to dla dowolnej liczby pierwszej p dzielącej liczbę $(p_1 p_2 \cdot \ldots \cdot p_k)^4 + 1$ mielibyśmy $p \neq p_i$ dla $i \in \{1, 2, \ldots, k\}$ – sprzeczność.

Dla $p \in \mathcal{P}$ istnieje liczba całkowita m taka, że p dzieli $m^4 + 1$. Jeśli r jest resztą z dzielenia liczby m przez p to łatwo widzimy, że p dzieli liczby $r^4 + 1$ oraz $(p-r)^4 + 1$, stąd dla $n = max\{r, p-r\}$ mamy $p > 2n$ oraz p dzieli $n^4 + 1$, co oznacza, że dla $p \in \mathcal{P}$ znaleźliśmy liczbę $n_p =: n$ spełniającą warunki zadania. Wystarczy teraz zauważyć, że nieskończoność zbioru $\mathcal{P}$ oraz nierówność $n_p \geqslant \sqrt[4]{p} - 1$ dla każdego $p \in \mathcal{P}$ daje tezę. ■

Wykładnik p-adyczny i rozkład na czynniki pierwsze

Definicja. Dana jest liczba pierwsza p oraz liczba całkowita dodatnia n. **Wykładnikiem p-adycznym** liczby n nazywamy taką liczbę całkowitą nieujemną k, że:

- p^k jest dzielnikiem n,
- p^{k+1} nie jest dzielnikiem n.

Piszemy wówczas: $v_p(n) = k$.

Zadanie 1 (XVIII OM, 3 etap)**.** *Znaleźć najwyższą potęgę liczby* 2 *będącą dzielnikiem liczby*

$$L_n = (n+1)(n+2)\cdot\ldots\cdot 2n,$$

gdzie n jest liczbą naturalną.

Rozwiązanie. Rozwiązanie za Archiwum OM.[5]. Zauważmy, że

$$n!\cdot L_n = (2n)!.$$

Zatem

$$L_n = \frac{(2n)!}{n!} = \frac{1\cdot 2\cdot 3\cdot\ldots\cdot 2n}{1\cdot 2\cdot 3\cdot\ldots\cdot n} = 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot\frac{2\cdot 4\cdot 6\cdot\ldots\cdot 2n}{1\cdot 2\cdot 3\cdot\ldots\cdot n} = 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot 2^n.$$

Stąd wynika, że L^n jest podzielne przez 2^n, ale nie jest podzielne przez 2^{n+1}. ■

Zadanie 2. *Niech n będzie liczbą naturalną. Wyznaczyć $v_3(2^n+1)$.*

Rozwiązanie. Patrz (2), Zad. 1. Rozważmy najpierw problem podzielności 2^n+1 przez 3 oraz przez 9.

- Jeśli $n = 2m$ jest parzyste, to $2^n = 4^m \equiv 1 \bmod 3$ i zatem $v_2^n + 1$ nie jest podzielne przez 3, tzn. $v_3(2^n+1) = 0$.
- Jeśli n jest nieparzyste oraz niepodzielne przez 3, to mamy $n = 6m+1$ lub $n = 6m+5$, czyli

  $$2^n = 2^{6m+1} = 64^m\cdot 2 \equiv 2 \bmod 9 \quad \text{lub } 2^n = 2^{6m+5} = 64^m\cdot 32 \equiv 5 \bmod 9,$$

  zatem 2^n+1 jest podzielne przez 3, ale nie jest podzielne przez 9, czyli $v_3(2^n+1) = 1$.

  Ogólnie natomiast należy zauważyć, że:

$$\frac{2^{3n}+1}{2^n+1} = 2^{2n} - 2^n + 1.$$

Zauważmy, że mamy $2^{6n+k} = 64\cdot 2^k \equiv 2^k \bmod 2^k$, oraz:

k	0	1	2	3	4	5
$2^k \bmod 9$	1	2	4	8	7	5

czyli gdy n jest nieparzyste mamy

$$\frac{2^{3n}+1}{2^n+1} = 2^{2n} - 2^n + 1 \equiv 3 \bmod 9.$$

Oznacza to, że

$$v_3(2^{3n}+1) = v_3(2^n+1) + 1.$$

W szczególności gdy $n = 3^{v_3(n)}\cdot m$ jest nieparzyste, gdzie $3 \nmid m$, to zgodnie z drugim punktem wyżej mamy

$$v_3(2^{3^{v_3(n)}\cdot m}+1) = v_3(2^m+1) + v_3(n) = 1 + v_3(n).$$

■

* * *

[5] https://archom.ptm.org.pl/?q=node/1324

Własności wykładnika p-adycznego

Niech p będzie liczbą pierwszą, zaś a, b niech będą liczbami całkowitymi. Wówczas:

- $a \mid b$ wtedy i tylko wtedy, gdy $v_p(a) \leqslant v_p(b)$, dla każdej liczby pierwszej p,
- $v_p(ab) = v_p(a) + v_p(b)$,
- $v_p(a/b) = v_p(a) - v_p(b)$,
- $v_p(a^n) = nv_p(a)$,
- $v_p(\mathrm{NWD}(a,b)) = \min\{v_p(a), v_p(b)\}$,
- $v_p(\mathrm{NWW}(a,b)) = \max\{v_p(a), v_p(b)\}$,
- $v_p(a \pm b) \geqslant \min\{v_p(a), v_p(b)\}$, a równość zachodzi, gdy $v_p(a) \neq v_p(b)$.

Zadanie 3. *Dane są liczby całkowite x, y takie, że suma*

$$\frac{x^2}{y} + \frac{y^2}{x}$$

jest liczbą całkowitą. Udowodnić, że obydwa składniki powyższej sumy są liczbami całkowitymi.

Rozwiązanie. Patrz (6), Zad. 1. Wykażemy, że dla dowolnej liczby pierwszej p zachodzi $v_p(y) \leqslant v_p(x^2) = 2v_p(x)$. Ułamek:

$$\frac{x^2}{y} + \frac{y^2}{x} = \frac{x^3 + y^3}{xy}$$

jest liczbą całkowitą, więc dla dowolnej liczby pierwszej p zachodzi:

$$v_p(xy) = v_p(x) + v_p(y) \leqslant v_p(x^3 + y^3).$$

Rozważamy dwa przypadki:

- Liczby $v_p(x^3)$ oraz $v_p(y^3)$ są różne. Wtedy:

$$v_p(x^3) \geqslant v_p(x^3 + y^3) = \min\{v_p(x^3), v_p(y^3)\} = \min\{3v_p(x), 3v_p(y)\} \geqslant v_p(x) + v_p(y).$$

  czyli $v_p(x^3) = 3v_p(x) \geqslant v_p(x) + v_p(y)$, a zatem $2v_p(y) \geqslant v_p(x)$.
- Jeśli $v_p(x^3) = v_p(y^3)$, to $v_p(x) = v_p(y)$, a zatem nierówność $2v_p(x) \geqslant v_p(y)$ jest równoważna nierówności $v_p(x) \geqslant 0$.

■

Zadanie 4. *Niech a, b, c będą liczbami całkowitymi dodatnimi takimi, że $a^b \mid b^c$ oraz $a^c \mid c^b$. Udowodnić, że $a^2 \mid bc$.*

Rozwiązanie. Patrz (6) Zad. 6. Niech p będzie dowolną liczbą pierwszą. Z warunków zadania mamy $c \cdot v_p(a) \leqslant b \cdot v_p(c)$ oraz $b \cdot v_p(a) \leqslant c \cdot v_p(b)$, co równoważnie daje:

$$\frac{c}{b} \cdot v_p(a) \leqslant v_p(c), \quad \frac{b}{c} \cdot v_p(a) \leqslant v_p(b).$$

Po dodaniu stronami otrzymujemy:

$$\left(\frac{b}{c} + \frac{c}{b}\right) v_p(a) \leqslant v_p(b) + v_p(c) = v_p(bc).$$

Nierówność $2 \leqslant \frac{b}{c} + \frac{c}{b}$ jest oczywiście znanym folklorem dla $b, c > 0$:

$$2 \leqslant \frac{b}{c} + \frac{c}{b} \quad \Longleftrightarrow \quad 2bc \leqslant b^2 + c^2 \quad \Longleftrightarrow \quad 0 \leqslant (b-c)^2.$$

■

Zadanie 5. *Największy wspólny dzielnik liczb naturalnych a, b, c jest równy 1. Udowodnić, że jeżeli zachodzi równość $ab = c(b-a)$, to liczba $b-a$ jest kwadratem liczby całkowitej.*

Rozwiązanie. Trzeba pokazać, że dla każdej liczby pierwszej p liczba $v_p(b-a)$ jest parzysta. Równość postawiona w zadaniu implikuje, że:

$$v_p(a) + v_p(b) = v_p(ab) = v_p(c(b-a)) = v_p(c) + v_p(b-a).$$

Rozważamy przypadki:

- Niech $v_p(a) \neq v_p(b)$, np. $v_p(a) > v_p(b)$. Wówczas wypisana wyżej równość ma postać

  $$v_p(a) + v_p(b) = v_p(c) + v_p(b),$$

  czyli $v_p(a) = v_p(c)$. Jednak $NWD(a, b, c) = 1$, więc albo $v_p(a) = v_p(c) = 0$, albo $v_p(b) = 0$. Pierwsza możliwość nie może zajść, bo $0 = v_p(a) > v_p(b)$, zaś druga oznacza $v_p(b-a) = v_p(b) = 0$.

- Niech $v_p(a) = v_p(b)$. Wówczas albo $v_p(a) = v_p(b) = 0$, albo $v_p(c) = 0$. W pierwszym przypadku $v_p(c) = v_p(b-a) = 0$. W drugim zaś dostajemy równość

  $$v_p(a) + v_p(a) = v_p(b-a),$$

  czyli $v_p(b-a)$ jest liczbą parzystą.

■

Formuła Legendre'a

Niech n będzie liczbą całkowitą dodatnią oraz p – liczbą pierwszą. Wówczas:

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots,$$

gdzie $[x]$ jest najmniejszą liczbą całkowitą nie większą niż x.

Zobaczmy krótki szkic dowodu. Mamy:

$$v_p(n!) = v_p(1) + v_p(2) + \ldots + v_p(n-1) + v_p(n).$$

Jedynie dzielniki liczby p są niezerowymi składnikami tej sumy. Niech r będzie największą liczbą całkowitą dodatnią taką, że $rp \leqslant n$. Wówczas:

$$v_p(n!) = v_p(p)+v_p(2p)+\ldots+v_p(rp) = v_p(1)+v_p(2)+\ldots+v_p(r)+r\cdot v_p(p) = v_p(1)+v_p(2)+\ldots+v_p(r)+r = v_p(r!)+r.$$

Oczywiście $r = \left[\frac{n}{p}\right]$. Postępując analogicznie jak dla n widzimy, że $v_p(r) = v_p(1) + \ldots + v_p(s) + s$, gdzie

$$s = \left[\frac{r}{p}\right] = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right].$$

Wzór powyżej trzeba by oczywiście uzasadnić, podobnie jak wzór $[[n/p^k]/p] = [n/p^{k+1}]$, dla $k > 1$, co zostawiam jako ćwiczenie. Postępując w ten sposób dalej uzyskujemy kolejne składniki sumy występującej we wzorze Legendre'a. Po pewnej liczbie kroków zostanie nam do obliczenia $v_p(q!)$, gdzie $q < p$, co jest równe 0.

Typowym (i zapewne jednym z prostszych) zastosowaniem wzoru Legendre'a jest wyznaczanie liczby zer, którą kończy się rozwinięcie dziesiętne liczb typu $n!$, i podobnych.

Na przykład dla 2020! chodzi o przedstawienie jej w postaci $10^x \cdot y$, gdzie y jest liczbą niepodzielną przez 10. Zauważmy, że $x = v_5(2020)$. Istotnie, nietrudno sprawdzić, że $v_2(2020!) > v_5(2020!)$, porównując ze sobą kolejne składniki $[2020/2^k]$ oraz $[2020/5^k]$ sum opisujących te wielkości. A zatem liczba 2020! ma na końcu 503 zera, zgodnie z poniższym rachunkiem.

$$v_5(2020!) = \left[\frac{2020}{5}\right] + \left[\frac{2020}{25}\right] + \left[\frac{2020}{125}\right] + \left[\frac{2020}{625}\right] = 404 + 80 + 16 + 3 = 503.$$

Zadanie 6. *Pokazać, że dla żadnej liczby całkowitej dodatniej n liczba 2^n nie jest dzielnikiem liczby $n!$.*

Rozwiązanie. Musimy pokazać, że dla każdego $n > 0$ mamy $v_2(2^n) > v_2(n!)$. Ze wzoru Legendre'a

$$v_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \ldots + \left[\frac{n}{2^k}\right],$$

gdzie $2^k \leqslant n < 2^{k+1}$. A zatem mamy:

$$v_2(n!) \leqslant \frac{n}{2} + \frac{n}{2^2} + \ldots + \frac{n}{2^k} = \frac{n}{2}\left(1 + \frac{1}{2} + \ldots + \frac{1}{2^{k-1}}\right).$$

Ze wzoru skróconego mnożenia (trzeba się ich już na tym etapie uczyć):

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1),$$

mamy:

$$1 + \frac{1}{2} + \ldots + \ldots + \frac{1}{2^{k-1}} = \frac{1 - \frac{1}{2^k}}{1 - \frac{1}{2}} = 2 - \frac{1}{2^{k-1}}.$$

A zatem mamy:

$$v_2(n!) \leqslant \frac{n}{2}\left(2 - \frac{1}{2^{k-1}}\right) < n = v_2(2^n).$$

■

Zadanie 7 (Obóz naukowy OM, 2012)**.** *Udowodnić, że dla dowolnej dodatniej liczby całkowitej n liczba*

$$(2^n - 2^0)(2^n - 2^1)(2^n - 2^2)\ldots(2^n - 2^{n-1})$$

jest podzielna przez $n!$

Rozwiązanie. Korzystając z formuły Legendre'a wiemy, że dla dowolnej liczby pierwszej p mamy:

$$v_p(n!) \leqslant \frac{n}{p} + \frac{n}{p^2} + \ldots = \frac{n}{p}\left(1 + \frac{1}{p} + \ldots\right) = \frac{n}{p} \cdot \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1}.$$

A zatem należy udowodnić, że wykładnik, z jakim dowolna liczba pierwsza p wchodzi ro rozkładu liczby $M = (2^n - 2^0)(2^n - 2^1)(2^n - 2^2)\ldots(2^n - 2^{n-1})$ to co najmniej $\left[\frac{n}{p-1}\right]$.

Liczba M jest podzielna przez

$$2^0 \cdot 2^1 \cdot 2^2 \cdot \ldots \cdot 2^{n-1} = 2^{n(n-1)/2},$$

a wykładnik $\frac{1}{2}n(n-1)$ jest równy co najmniej n dla każdej wartości $n \geqslant 3$. To oznacza, że ostatnie zdanie poprzedniego akapitu jest prawdziwe dla liczby pierwszej $p = 2$ i dowolnej liczby $n \geqslant 3$. Bezpośrednie sprawdzenie dowodzi, że teza zadania jest prawdziwa także dla $n = 1$ i $n = 2$.

Niech p będzie nieparzystą liczbą pierwszą. Wtedy na mocy małego twierdzenia Fermata liczba

$$p \,|\, 2^{p-1} - 1.$$

Dla dowolnej nieujemnej liczby całkowitej $k < n$ mamy

$$2^n - 2^k = 2^k(2^{n-k} - 1).$$

Jeśli ponadto różnica $n - k$ jest podzielna przez $p - 1$, to $n - k = l(p-1)$ dla pewnej liczby całkowitej l, a więc liczba

$$2^{n-k} - 1 = (2^{p-1})^l - 1$$

jest podzielna przez $2^{p-1} - 1$ i tym bardziej przez p. Inaczej mówiąc z podzielności $n - 1 \,|\, n - k$ wynika, że czynnik $2^n - 2^k$ występujący w iloczynie definiującym liczbę M jest podzielny przez p. Zatem $v_p(M)$ równy jest co najmniej liczbie wartości $k \in \{0, 1, \ldots, n-1\}$, dla których różnica $n - k$ jest podzielna przez $p - 1$, czyli — co najmniej liczbie elementów zbioru $\{1, 2, 3, \ldots, n\}$ podzielnych przez $p - 1$. Ta ostatnia liczba jest oczywiście równa $\left[\frac{n}{p-1}\right]$, co kończy rozwiązanie. ■

Zadanie 8 (LVIII OM, 1 etap)**.** *Niech $F(k)$ będzie iloczynem wszystkich dodatnich dzielników liczby całkowitej k. Rozstrzygnąć, czy istnieją różne liczby całkowite dodatnie m, n, dla których $F(m) = F(n)$.*

Rozwiązanie. Niech $1 = d_1 < d_2 < \ldots < d_k = n$ będą wszystkimi dodatnimi dzielnikami ustalonej liczby całkowitej dodatniej n. Wówczas n/d_1, n/d_2, …, n/d_k także są wszystkimi dodatnimi dzielnikami liczby n, zatem możemy napisać:

$$F(n) = d_1 \cdot d_2 \cdot \ldots \cdot d_k = \frac{n}{d_1} \cdot \frac{n}{d_2} \cdot \ldots \cdot \frac{n}{d_k}.$$

Stąd wynika, że:

$$F(n) = \sqrt{d_1 \cdot d_2 \cdot \ldots \cdot d_k \cdot \frac{n}{d_1} \cdot \frac{n}{d_2} \cdot \ldots \cdot \frac{n}{d_k}} = \sqrt{n^k} = n^{d(n)/2},$$

gdzie $d(n)$ oznacza liczbę wszystkich dzielników liczby n.

Przypuśćmy teraz, że dla pewnych liczb całkowitych dodatnich m, n zachodzi równość $F(m) = F(n)$. Wtedy $m^{d(m)/2} = n^{d(n)/2}$, więc

$$m^{d(m)} = n^{d(n)}.$$

Twierdzimy, że m, n jest dodatnimi potęgami pewnej liczby całkowitej. Po ewentualnym wzięciu pierwiastka stopnia $NWD(d(m), d(n))$ mamy równość $m^a = n^b$, gdzie $NWD(a, b) = 1$. Teraz dla dowolnej liczby pierwszej p mamy:

$$b \cdot v_p(n) = a \cdot v_p(m).$$

Skoro a, b są względnie pierwsze, to $b \,|v_p(m)$. Zatem każdy dzielnik pierwszy liczby m wchodzi do rozkładu m z wielokrotnością b, czyli m jest b-tą potęgą pewnej liczby całkowitej r. A zatem wobec $m^a = r^{ab} = n^b$ dostajemy, że m, n są potęgami r.

Niech $m = r^A, n = r^B$, dla pewnych A, B całkowitych. Niech $A < B$. Stąd wynika, że $m < n$ oraz, ponieważ każdy dzielnik liczby m jest (teraz) dzielnikiem liczby n zachodzi $d(m) \leqslant d(n)$. Wobec tego $m^{d(m)} < n^{d(n)}$ i otrzymujemy sprzeczność. Podobna sprzeczność powstaje przy założeniu $B > A$. Stąd $A = B$, co oznacza, że $m = n$. ■

Zadanie 9 (LVIII OM, 3 etap)**.** *Liczbę całkowitą dodatnią nazwiemy białą, jeżeli jest równa* 1 *lub jest iloczynem parzystej liczby liczb pierwszych (niekoniecznie różnych). Pozostałe liczby całkowite dodatnie nazwiemy czarnymi. Zbadać, czy istnieje taka liczba całkowita dodatnia, że suma jej białych dzielników jest równa sumie jej czarnych dzielników.*

Rozwiązanie. Dla liczby całkowitej $k > 1$ niech $B(k)$ oznacza sumę białych dzielników liczby k, $C(k)$ – liczbę czarnych dzielników liczby k oraz niech $D(k) = B(k) - C(k)$. Szukamy takiego k, by $D(k) = 0$. Pokażemy najpierw, że dla dowolnych względnie pierwszych liczb całkowitych dodatnich l, m prawdziwa jest równość:

$$D(lm) = D(l) \cdot D(m).$$

Zobaczymy najpierw co wynika z tej równości, a potem ją pokażemy. Przypuśćmy, że dla pewnej $n >$ mamy $D(n) = 0$. Rozłóżmy n na iloczyn potęg różnych liczb pierwszych:

$$n = p_1^{r_1} \cdot \ldots \cdot p_j^{r_j}.$$

Na mocy uzyskanego wzoru mamy:

$$D(n) = D(p_1^{r_1}) \cdot D(p_j^{r_j}) = 0.$$

Wobec tego istnieje liczba pierwsza p i liczba całkowita dodatnia r, dla których $D(p^r) = 0$. Jest to jednak niemożliwe: wszystkimi białymi dzielnikami p^r są liczby $1, p^2, p^4, \ldots$, a wszystkimi czarnymi dzielnikami – liczby $p, p^3, p^5, \ldots$, i w konsekwencji zachodzi równość

$$D(p^r) = 1 - p + p^2 - p^3 + \ldots + (-1)^r p^r,$$

zaś liczba stojąca po prawej stronie równości nie jest podzielna przez p, więc nie może być zerem.

Dowodzimy $D(lm) = D(l) \cdot D(m)$., dla $NWD(l, m) = 1$. Wyrazimy $B(lm)$ oraz $C(lm)$ przez liczby $B(l), B(m), C(l), C(m)$. Oczywiście każdy dodatni dzielnik d iloczynu lm ma jednoznaczne przedstawienie w postaci $d = ab$, gdzie a jest dzielnikiem liczby l, zaś b jest dzielnikiem liczby m.

Suma wszystkich iloczynów postaci ab, gdzie a, b są białymi dzielnikami równa jest $B(l)B(m)$, zaś suma wszystkich takich iloczynów, w których dzielniki a, b są czarne wynosi $C(l)C(m)$. Licząc $B(lm)$ zauważamy, że dzielnik d liczby lm jest biały wtedy i tylko gdy l i m mają taki sam kolor. Zatem:

$$B(lm) = B(l)B(m) + C(l)C(m).$$

Skoro $B(lm) + C(lm) = B(l)B(m) + C(l)C(m) + B(l)C(m) + C(l)B(m)$, to mamy także:

$$C(lm) = B(l)C(m) + C(l)B(m).$$

Zatem

$$D(lm) = (B(l) - C(l))(B(m) - C(m)) = D(l)D(m).$$

■

Zadanie 10 (Wietnam, 1992)**.** *Niech n będzie liczbą całkowitą dodatnią. Oznaczmy przez $f(n)$ liczbę dzielników dodatnich liczby n, których cyfra jedności to 1 lub 9, zaś przez $g(n)$ oznaczmy liczbę dzielników dodatnich liczby n, których cyfrą jedności jest 3 lub 7. Pokazać, że $f(n) \geqslant g(n)$.*

Rozwiązanie. Po pierwsze niech $n = 2^x \cdot 5^y \cdot k$, gdzie x, y są całkowite nieujemne oraz k jest nieparzysta, niepodzielna przez 5. Zauważmy, że $f(n) = f(k)$ oraz $g(n) = g(k)$. Istotnie, dzielniki n o cyfrach jedności $1, 3, 7, 9$ są nieparzyste i niepodzielne przez 5, więc są względnie pierwsze z 2 i 5. W rezultacie są też dzielnikami k, i to wszystkimi możliwymi. A zatem możemy zakładać, że n jest liczbą nieparzystą, niepodzielną przez 5.

Niech A będzie zbiorem liczb całkowitych o cyfrach jedności 1 lub 9, zaś B niech będzie zbiorem liczb całkowitych o cyfrach jedności 3 lub 7.

Rozważmy przypadek, gdy n należy do B. Wówczas biorąc dowolny jej dzielnik m z B mamy, że $\frac{n}{m}$ jest elementem A. W szczególności każdemu dzielnikowi n z B odpowiada dokładnie jeden dzielnik z A, czyli $f(n) = g(n)$.

Pozostaje rozważyć trudniejszy przypadek, gdy n jest elementem A, a więc ma cyfrę jedności 1 lub 9. Niestety podzielenie elementu z A przez dzielnik ze zbioru A może dać zarówno dzielnik z A, jak i z B, więc analogiczny argument jak wyżej nie zadziała. Musimy zbadać rozkład n na czynniki. Pokażemy, że w tym przypadku $f(n) > g(n)$.

Weźmy dowolny dzielnik pierwszy p liczby n i oznaczmy przez a liczbę $p^{v_p(n)}$, czyli najwyższą potęgę p dzielącą n. Liczbę n/a oznaczamy jako b. Będziemy zliczać dzielniki n, osobno ze zbioru A i osobno ze zbioru B. Skoro $n = ab$, to każdy dzielnik d liczby n można przedstawić w sposób jednoznaczny jako iloczyn dzielnika d_a liczby a i dzielnika d_b liczby b. Jeśli d_a oraz d_b są z A, to d też. Jeśli d_a oraz d_b są z B, to d jest z A. Jeśli d_a należy do A oraz d_b należy do B, to d należy do B, i odwrotnie – jeśli d_a należy do B oraz d_b nalezy do A, to d należy do A. Wynikają stąd wzory:

$$f(n) = f(a)f(b) + g(a)g(b), \quad g(n) = f(a)g(b) + f(b)g(a).$$

Istotnie, aby jednak dostać dzielnik z A trzeba przemnożyć dwa dzielniki typu A lub dwa dzielniki typu B, zaś aby dostać dzielnik z B trzeba przemnożyć dwa dzielniki różnych typów. Na ile sposobów? Dzielnik liczby a ze zbioru A można wybrać na $f(a)$ sposobów, a dzielnik b ze zbioru A można wybrać na $f(b)$ sposobów. Zatem iloczyn tych dzielników można wybrać na $f(a)f(b)$ różnych sposobów. Osobno zliczamy dzielniki n typu A powstające przez przemnożenie dzielników typu B: te iloczyny można uformować na $g(a)g(b)$ sposobów. Stąd wzór na $f(n)$. Aby dostać dzielnik typu B trzeba przemnożyć dzielnik typu A z dzielnikiem typu B, stąd wzór na $g(n)$. A zatem:

$$f(n) - g(n) = f(a)f(b) + g(a)g(b) - f(a)g(b) - f(b)g(a) = (f(a) - g(a))(f(b) - g(b)).$$

W szczególności teza $f(n) - g(n) > 0$ jest równoważna temu, że $f(a) - g(a) > 0$ oraz $f(b) - g(b) > 0$. Wystarczy więc, że rozstrzygniemy zadanie dla $n = p^k$, gdzie n jest elementem A, bo wtedy zadanie sprowadza się do rozstrzygnięcia nierówności $f(b) - g(b) > 0$, którą możemy wykonać analogicznie, jak dla a, wydzielając kolejny czynnik pierwszy.

Czym jest $f(p^k)$, gdzie $p \in A$? Jest to $k+1$. Czym jest $g(p^k)$, gdy $p \in A$? Jest to 0. Tu więc nierówność zachodzi. Czym jest $f(p^k)$, jeśli p należy do B? Wówczas pamiętamy, że k musi być parzyste i wtedy dzielniki z A to $1, p^2, p^4, \ldots, p^{[k/2]}$, czyli $f(p^k) = [k/2] + 1$. Natomiast $g(p^k)$ zlicza dzielniki postaci $g, g^3, \ldots, g^{k-1}$, których jest $[k/2]$. A zatem w obydwu przypadkach $f(n) > g(n)$, co kończy dowód.

■

Źródła rozwiązań (czasami nieco zmodyfikowanych lub poprawionych, a czasami całkowicie zapożyczonych).

(1) Archiwum OM oraz strona OM: `https://archom.ptm.org.pl/`, `https://om.mimuw.edu.pl/`.

(2) Byszewski J. *Lemat o podnoszeniu wykładnika oraz twierdzenie Zsigmondy'ego*.

(3) Burek D., *Obóz przygotowawczy do Olimpiady Matematycznej*, III Liceum Ogólnokształcące im. Adama Mickiewicza w Tarnowie Krynica Zdrój, 22 – 25 września 2015.

(4) Bzdęga B., *Wykładniki p-adyczne*, Czasopismo *Delta*, 11.2020 r.

(5) Sierpiński W. *Teoria liczb*, Monografie Matematyczne 19, 1950, `http://matwbn.icm.edu.pl/ksiazki/mon/mon19/mon1`

(6) Węgrecki J., *Wykładniki p-adyczne*, `Academia.edu`.

(7) Andreescu T„ Andrica D., Feng Z., *104 Number Theory Problems: From the Training of the USA IMO Team*, Birkhäuser Boston, Year: 2006.

(8) Art of Problem Solving, `https://artofproblemsolving.com`.