Nieparzyste dzielniki i wykładniki p-adyczne

Obóz naukowy Olimpiady Matematycznej Juniorów
Poziom OM, 12.08.2020 r.

Jednym z interesujących sposobów radzenia sobie z zadaniami olimpijskimi z teorii liczb jest rozważanie dzielników liczb występujących w zadaniu. Opieramy się wówczas na twierdzeniu o jednoznacznym rozkładzie liczby całkowitej na czynniki pierwsze. Często do lepszego zrozumienia sytuacji wystarczy jednak wyodrębnienie pewnego konkretnego dzielnika pierwszego. Dla przykładu, 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. Korzystając z tej i innych podobnych obserwacji można rozwiązać wiele ciekawych zadań. Zacznijmy od prostego zadania ilustrującego to zagadnienie.

Zadanie 1. *Wybrano* 51 *różnych liczb naturalnych mniejszych od* 100*. Udowodnić, że istnieją wśród nich takie dwie liczby, że pierwsza dzieli drugą.*

Rozwiązanie jest następujące: z każdą z wybranych 51 liczb związany jest jej największy dzielnik nieparzysty. Możliwych wartości tego dzielnika jest tyle, ile nieparzystych liczb w zbiorze $\{1, 2, \ldots, 100\}$, a więc 50. Tymczasem wybraliśmy 51 liczb. Wobec tego pewne dwie z nich, nazwijmy je a i b mają ten sam największy dzielnik nieparzysty c. Możemy więc zapisać:

$$a = 2^k \cdot c, \quad b = 2^l \cdot c,$$

gdzie k i l są pewnymi liczbami całkowitymi nieujemnymi. Jeżeli $k < l$, to a dzieli b, jeśli zaś $l < k$, to b dzieli a.

Zadanie o bardzo podobnej idei, a jednak wymagające pomysłowości pochodzi z drugiego etapu 63. Olimpiady Matematycznej.

Zadanie 2. *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.*

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, który pokażę będziemy w dalszej części wykładu intensywnie rozwijać. 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 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 zadania.

Czy widzicie podobieństwo pomiędzy dwoma omówionymi zadaniami? Obydwa opierały się na zastosowaniu zasady szufladkowej Dirichleta i na rozkładzie na czynniki pierwsze. Kolejne zadanie wiąże się z jeszcze jednym pojęciem, które niekiedy pojawia się w rozwiązaniach zadań olimpijskich – tak zwanym największym wspólnym nieparzystym dzielnikiem. Używa się też, na poziomie intuicyjnym, pojęcia ciągu.

Zadanie 3. *Niech f_1, f_2 będą nieparzystymi liczbami dodatnimi. Określamy ciąg liczb: pierwszy wyraz oznaczamy f_1, drugi jako f_2, zaś dla $n \geqslant 3$ wyraz n-ty równy f_n jest największym nieparzystym dzielnikiem sumy dwóch poprzednich wyrazów, czyli największym nieparzystym dzielnikiem liczby $f_{n-2} + f_{n-1}$. Pokazać, że od pewnego momentu wyrazy tego ciągu są identyczne i równe liczbie* $\mathrm{NWD}(f_1, f_2)$.

Dowód jest bardziej złożony niż poprzednie. Po pierwsze pokażemy, że jeśli pewne dwa wyrazy rozważanego ciągu są sobie równe, to wszystkie kolejne wyrazy tego ciągu są równe. Po drugie, pokażemy, że wartość, na której rozważany ciąg się stabilizuje to $\mathrm{NWD}(f_1, f_2)$.

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 jesli dwa wyrazy naszego ciągu są równe, to wszystkie dalsze też.

A może rozważana przed chwilą sytuacja nie jest możliwa? Załóżmy na chwilę, że żadne dwa 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:

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

Z dwóch uzyskanych nierówności wynika, że

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

To by oznaczało, że ciąg liczb postaci $NWD(f_{2n}, f_{2n-1})$ jest ściśle malejący, gdzie f_m jest m-tym elementem rozważanego ciągu. To jest jednak niemożliwe, bo nieskończony ciąg liczb dodatnich 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. Oczywiście

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

dla pewnego n całkowitego dodatniego. A zatem przekształcając to wyrażenie dostajemy $2^n c - b = a$. Niech $\mathrm{NWD}(a, b) = x$, $\mathrm{NWD}(b, c) = y$. 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 $b = xb'$. A zatem c, jako największy dzielnik nieparzysty liczby $a + b$ równa jest iloczynowi x razy największy dzielnik nieparzysty liczby $a' + b'$. W szczególności x jest wspólnym dzielnikiem zarówno b, jak i c. Zatem $x \leqslant y$. Stąd $x = y$. 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 $\mathrm{NWD}(f_1, f_2)$.

Widzimy jak przydatne może być wydzielanie odpowiedniego typu czynnika w badaniu podzielności. Ważnym narzędziem pozwalającym na formalizację tego typu rozważań jest tak zwany wykładnik p-adyczny.

Definicja 1. *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 oraz p^{k+1} nie jest dzielnikiem n. Piszemy wówczas*

$$v_p(n) = k.$$

A więc dla przykładu $v_3(24) = 1$, $v_7(30) = 0$, zaś $v_5(500) = 3$. Wprowadzenie wykładnika p-adycznego pozwoli nam spojrzeć zupełnie inaczej na podzielność. Odnotujmy najpierw kilka bardzo prostych własności, wynikających bezpośrednio z twierdzenia o rozkładzie liczby całkowitej na czynniki pierwsze.

Twierdzenie 1. *Niech p będzie liczbą pierwszą, zaś a, b niech będą liczbami całkowitymi. Wówczas:*

- *liczba a jest dzielnikiem liczby b wtedy i tylko wtedy, gdy $v_p(a) \leqslant v_p(b)$, dla każdego p,*
- $v_p(ab) = v_p(a) + v_p(b)$,
- $v_p(a/b) = v_p(a) - v_p(b)$,
- $v_p(a^n) = nv_p(a)$,
- $v_p(\mathrm{NWD}(a, b)) = \min\{v_p(a), v_p(b)\}$,
- $v_p(\mathrm{NWW}(a, b)) = \max\{v_p(a), v_p(b)\}$,
- $v_p(a \pm b) \geqslant \min\{v_p(a), v_p(b)\}$, *przy czym równość zachodzi, gdy $v_p(a) \neq v_p(b)$.*

Przykładowe proste zastosowanie powyższych faktów, to dowód znanej dobrze formuły.

Twierdzenie 2. *Dla dowolnych liczb całkowitych dodatnich zachodzi równość:*

$$\mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b) = a \cdot b.$$

Aby sprawdzić czy dwie liczby całkowite dodatnie x, y są równe wystarczy sprawdzić, czy $v_p(x) = v_p(y)$, dla każdej liczby pierwszej p. Policzmy zatem wartość wyrażenia:

$$v_p(\mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b)) - v_p(ab).$$

Zgodnie z własnościami podanymi wyżej wyrażenie to jest równe:

$$\max\{v_p(a), v_p(b)\} + \min\{v_p(a), v_p(b)\} - v_p(a) - v_p(b).$$

Jest jasne, że wyrażenie to jest zawsze równe 0.

Zobaczmy jak pojęcie wykładnika p-adycznego stosuje się do rozwiązywania zadań.

Zadanie 4. *Ile jest par liczb całkowitych dodatnich (a, b) spełniających równanie:*

$$a^2 + b^2 = ab(a + b)?$$

Rozważmy dowolną liczbę pierwszą p oraz wielkości $v_p(a), v_p(b)$. Ze znanych nam własności dostajemy:

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

czyli z założenia podanego w zadaniu mamy:

$$v_p(a) + v_p(b) + v_p(a + b) = v_p(a^2 + b^2).$$

Będziemy korzystać z ostatniej własności opisanej w Twierdzeniu 1, rozważając osobno przypadki, gdy $v_p(a) = v_p(b)$ oraz, gdy $v_p(a) \neq v_p(b)$.

- Jeśli $v_p(a) = v_p(b)$, dla wszystkich liczb pierwszych p, to oczywiście $a = b$, a wtedy mamy równanie $2a^2 = 2a^3$, czyli $a = b = 1$.
- Jeśli $v_p(a) \neq v_p(b)$, to bez straty ogólności można założyć, że $v_p(a) < v_p(b)$, dla pewnej liczby pierwszej p. Wówczas $v_p(a+b) = v_p(a)$ oraz $v_p(a^2+b^2) = v_p(a^2) = 2v_p(a)$, bo $v_p(a^2) = 2v_p(a) < 2v_p(b) = v_p(b^2)$. A zatem założenie z treści zadania na poziomie wykładników p-adycznych przybiera w rozważanym przypadku postać:
$$v_p(a) + v_p(b) + v_p(a) = 2v_p(a),$$
co jest niemożliwe, bo oznacza, że $v_p(b) = 0$. A zatem drugi przypadek nie może mieć miejsca i zadanie jest rozwiązane.

Zadanie 5. *Dane są liczby całkowite dodatnie a, b, c takie, że liczba*

$$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$$

jest całkowita. Udowodnić, że abc jest sześcianem liczby całkowitej.

W normalnych warunkach to zadanie wygląda na bardzo problematyczne. Zauważmy jednak jak eleganckie jest rozwiązanie z użyciem wykładnika p-adycznego. Mamy:

$$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}=\frac{a^2c+b^2a+c^2b}{abc}.$$

Niech p będzie liczbą pierwszą. Oznaczmy $A=v_p(a), B=v_p(b), C=v_p(c)$. Z założenia wynika zatem, że:

$$v_p(a^2c+b^2a+c^2b)\geqslant v_p(abc),$$

czyli równoważnie:

$$v_p(a^2c+b^2a+c^2b)\geqslant A+B+C.$$

Zauważmy, że naszym celem jest po prostu pokazać, że $A+B+C$ jest zawsze podzielna przez 3. To będzie dokładnie znaczyło, że liczba p wchodzi z wykładnikiem podzielnym przez 3 do rozkładu abc na czynniki pierwsze.

Wiemy jak postępować z wykładnikiem modulo p w przypadku sumy $v_p(a^2c+b^2a+c^2b)$. Trzeba osobno rozważyć sytuację, gdy $v_p(a^2c), v_p(b^2a)$ oraz $v_p(c^2b)$ są parami różne, oraz gdy nie są parami różne. Liczby te to po prostu $2A+C, 2B+A, 2C+B$.

- Liczby $v_p(a^2c), v_p(b^2a)$ oraz $v_p(c^2b)$ są parami różne. Wówczas mamy:

  $$\begin{aligned}2A+C&\geqslant\min\{2A+C,2B+A,2C+B\}=v_p(a^2c+b^2a+c^2b)\geqslant A+B+C\\2B+A&\geqslant\min\{2A+C,2B+A,2C+B\}=v_p(a^2c+b^2a+c^2b)\geqslant A+B+C\\2C+B&\geqslant\min\{2A+C,2B+A,2C+B\}=v_p(a^2c+b^2a+c^2b)\geqslant A+B+C\end{aligned}$$

  Z pierwszej nierówności dostajemy $A\geqslant B$, z drugiej $B\geqslant C$, a z trzeciej $C\geqslant A$, co oznacza, że $A=B=C$. A zatem $A+B+C=3A$ jest podzielne przez 3,

- Jeśli zachodzi równość, powiedzmy $2A+C=2B+A$, to $A+C=2B$, więc $v_p(abc)=A+C+B=2B+B=3B$, więc jest podzeine przez 3.

Jednym z najbardziej znanych faktów związanych z wykładnikiem p-adycznym jest jego wartość dla liczby $n!$, czyli iloczynu n pierwszych liczb całkowitych dodatnich, zwana formułą Legendre'a.

Twierdzenie 3. *Niech n będzie liczbą całkowitą dodatnią oraz p – liczbą pierwszą. Wówczas:*

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

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

Powyższa suma napisana jest tak, jakby była nieskończona, ale oczywiście chodzi jedynie o to, że może być dowolnie długa. Oczywiście istnieje k takie, że $p^k>n$, więc od pewnego momentu wszystkie jej składniki sumy napisanej wyżej to zera. Jak to udowodnić? Zobaczmy krótki szkic:

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

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 zastosowaniem wzoru Legendre'a jest 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.

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

Wzór na $v_p(n!)$ przydaje się w wielu zadaniach, w których operujemy na ilorazach silni. W kombinatoryce ilorazy takie mają często istotne znaczenie. Również w teorii liczb wzór ten odgrywa bardzo ważną rolę. Jest kluczowym elementem trudnego dowodu tzw. postulatu Bertranda mówiącego, że dla każdej liczby całkowitej $n > 1$ istnieje liczba pierwsza p taka, że $n < p < 2n$. Pozostańmy jednak przy zadaniach olimpijskich. Rzadko zdarzają się zadania wykorzystujące bezpośrednio formułę Legendre'a. Oto przykład z OM.

Zadanie 6. *Dane są liczby całkowite k, n takie, że $1 \leqslant k \leqslant \frac{n^2}{4}$, przy czym k nie ma dzielnika pierwszego większego od n. Udowodnij, że $n!$ dzieli się przez k.*

Gdy mamy obok siebie podzielność i silnię zawsze warto spróbować sprawdzić czy nie uda się skorzystać ze wzoru Legendre'a. Bierzemy zatem dowolną liczbę pierwszą p i żądamy, by $v_p(k)$ było niewiększe niż $v_p(n!)$. To wszystko, czego potrzebujemy. Rozważymy dwa przypadki:

- Niech $v_p(k) = 2x$. Wówczas $p^{2x} \leqslant k \leqslant \frac{n^2}{4}$. Łatwa manipulacja pozwala stwierdzić, ze $2p^x \leqslant n$, czyli

  $$2 \leqslant \frac{n}{p^x}.$$

  Spójrzmy teraz na sumę:

  $$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^x}\right] + \ldots$$

  Szacowanie, które zapisaliśmy pozwala stwierdzić, że pierwsze x składników tej sumy równych to liczby nie mniejsze niż 2. Zatem dowód w tym przypadku jest zakończony, bowiem

  $$v_p(n!) \geqslant 2x = v_p(k).$$

- Niech $v_p(k) = 2x + 1$.. Mamy: $p^{2x+1} \leqslant k \leqslant \frac{n^2}{4}$. Teraz szacowanie będzie bardziej skomplikowane, postaci: $2\sqrt{p}p^x \leqslant n$. A zatem

  $$\frac{n}{p^x} \geqslant 2\sqrt{p}.$$

  Oznacza to, że pierwsze x składników sumy:

  $$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^x}\right] + \ldots$$

  równe jest przynajmniej $2\sqrt{p}$. A zatem

  $$v_p(n!) \geqslant x \cdot 2\sqrt{p} > 2x + 1 = v_p(k).$$

Szacowanie, które wykonaliśmy może wydawać się sztuczne, ale ma również drugie dno. Jeśli ktoś zapoznany jest z pojęciem liczbowego systemu pozycyjnego, może zastanowić się nad interpretacją wzoru Legendre'a w kontekście zapisu liczby n w systemie liczbowym o podstawie równej p, na przykład w systemie dwójkowym.

Jeśli ktoś byłby zainteresowany pogłębieniem tematu wykładnika p-adycznego, to polecam artykuł członka KO OMJ w Tarnowie, Jakuba Węgreckiego, z którego zapożyczyłem kilka prostszych zadań, dostępny pod adresem `https://jagiellonian.academia.edu/JakubW%C4%99grecki`.

Zadania z rozwiązaniami

Zadanie 1. *Na tablicy napisano liczbę pewną liczbę całkowitą dodatnią n. Władek i Robert grają w grę polegającą w każdej turze na odejmowaniu od liczby znajdującej się aktualnie na tablicy jednego z jej dzielników (można odjąć także 1 lub samą liczbę na tablicy) i zastępując liczbę na tablicy uzyskaną różnicą. Gracze wykonują te operacje naprzemienne. Ten z graczy, który będzie musiał zapisać na tablicy 0 przegrywa. Grę zaczyna Władek. Dla jakich n istnieje strategia dająca Władkowi zwycięstwo, niezależnie od ruchów Roberta?*

Rozwiązanie. Taka strategia istnieje tylko dla n parzystych. W takim przypadku Włodek musi w każdym ruchu odejmować 1. W ten sposób Robert za każdym razem otrzymuje liczbę nieparzystą i musi odjąć od niej nieparzysty dzielnik. W skończonej liczbie ruchów Robert otrzyma zatem liczbę pierwszą lub 1, co doprowadzi do jego porażki. Jeżeli n jest nieparzyste, wówczas strategię wygrywającą ma oczywiście Robert. ■

Zadanie 2. *Rozważmy zbiór S złożony z n liczb postaci:*

$$S = \{n+1, n+2, \ldots, 2n-1, 2n\}.$$

Pokaż, że suma największych nieparzystych dzielników wszystkich elementów zbioru S równa jest n^2.

Rozwiązanie. Rozważmy największy dzielnik nieparzysty liczby $n+i$, postaci a_i, dla $i = 1, \ldots, n$. Jest to jedna z liczb $1, 3, 5, \ldots, 2n-1$. Pokażmy, że dla $i \neq j$ mamy $a_i \neq a_j$. Załóżmy przeciwnie. Niech

$$n + i = a \cdot 2^x, \quad n + j = a \cdot 2^y,$$

dla $i \neq j$ oraz $x, y \geqslant 0$. Oczywiście $x \neq j$, bo inaczej $n + i = n + j$, a założyliśmy coś innego. Niech $x > y$. Wówczas $n + i > 2(n + j)$. To jest jednak niemożliwe, bo najmniejsza liczba w S to $n + 1$, a największa to $2n$. 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. *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?*

Dowód. W szukanym zbiorze nie może być dwóch liczb mających ten sam największy dzielnik nieparzysty. 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 4. *Udowodnij, że zbiór liczb całkowitych dodatnich można podzielić na nieskończenie wiele podzbiorów $A_1, A_2, A_3, \ldots$, z których żadne dwa nie mają elementu wspólnego, przy czym podzbiory te mają następującą własność: jeśli pewne liczby całkowite dodatnie a, b, c, d należą do tego samego zbioru A_n, dla pewnego n, to nastepujące warunki są równoważne:*

- *$a - b$ oraz $c - d$ należą do pewnego zbioru A_m (przy czym niekoniecznie $m = n$),*
- *$\frac{a}{b} = \frac{c}{d}$.*

Rozwiązanie. Niech A_k będzie zbiorem wszystkich liczb postaci

$$(2k-1) \cdot 2^n,$$

czyli zbiorem liczb, których największy nieparzysty dzielnik równy jest $2k-1$. Sprawdźmy, że wymagania zadania wobec zbiorów A_m są spełnione. Niech a, b, c, d należą do A_k, przy czym $x > y$ oraz $z > w$. Możemy zatem napisać:

$$x = (2k-1) \cdot 2^{a+b}, \quad y = (2k-1) \cdot 2^a, \quad z = (2k-1)2^{c+d}, \quad w = (2k-1) \cdot 2^c.$$

Wówczas:

$$x - y = (2k-1)(2^b - 1)(2^a), \quad z - w = (2k-1)(2^d - 1)(2^c).$$

Mamy pokazać, że przynależność $x - y$ oraz $z - w$ do tego samego zbioru A_m, dla pewnego n, jest równoważna warunkowi $x/y = z/w$. Załóżmy więc, że $x-y$ oraz $z-w$ mają ten sam największy dzielnik nieparzysty. Wówczas $(2k-1)(2^b-1) = (2k-1)(2^d-1)$, czyli $b = d$. Tymczasem $x/y = 2^b$ oraz $z/w = 2^d$. Jasne jest więc, że żądana równoważność ma miejsce.

■

Zadanie 5. *Dane są liczby całkowite x, y takie, że suma*

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

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

Rozwiązanie. 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, na przykład $v_p(x^3) > v_p(y^3)$. Wtedy z nierówności wyżej oraz ostatniego punktu Twierdzenia z wykładu mamy $v_p(x^3) \geqslant v_p(x^3+y^3) = 3v_p(y) \geqslant v_p(x)+v_p(y)$, czyli $2v_p(y) \geqslant v_p(x)$. Jeśli zaś $v_p(x^3) < v_p(y^3)$, to $v_p(x^3 + y^3) = v_p(x^3) = 3v_p(x) \geqslant v_p(x) + v_p(y)$ i rezultat jest ten sam.
- 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 prawdziwej nierówności $v_p(x) \geqslant 0$. Zatem teza zadania jest prawdziwa.

■

Zadanie 6. *Największy wspólny dzielnik liczb naturalnych a, b, c jest równy 1. Udowodnij, 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.

■

Zadanie 7. *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 8. *Na płaszczyźnie z układem współrzędnych umieszczono pionek w punkcie (1,1). Pionkiem tym poruszać wolno według następujących zasad:*

- *z każdego punktu o współrzędnych (a, b) można przejść do $(2a, b)$ lub $(a, 2b)$,*
- *z każdego punktu o współrzędnych (a, b) można przejść do $(a-b, b)$, o ile $a > b$ lub do $(a, b-a)$, jeśli $a < b$.*

Opisz wszystkie pola o współrzędnych (x, y), do których można się dostać z pola $(1, 1)$.

Rozwiązanie. Najpierw przekonajmy się, że z $(1, 1)$ można dotrzeć tylko do punktów (x, y) takich, że $\mathrm{NWD}(x, y) = 2^s$, dla pewnego nieujemnego s. Po pierwsze wiemy, że $\mathrm{NWD}(x, y) = \mathrm{NWD}(x, y-x) = \mathrm{NWD}(x-y, y)$, a zatem żadne nieparzyste dzielniki wspólne x, y nie zmieniają się przy wykonywaniu operacji, bo największy dzielnik nieparzysty liczby $2a$ oraz b jest taki sam, jak największy dzielnik nieparzysty liczb $a, 2b$ oraz liczb a, b. Skoro na starcie, w punkcie $(1, 1)$ największy wspólny dzielnik nieparzysty wynosi 1, to fakt ten pozostaje prawdą niezależnie od tego do którego punktu się udamy. A zatem $\mathrm{NWD}(x, y)$ musi być potęgą 2.

Teraz sprawdźmy, że rzeczywiście da się z $(1, 1)$ dojść do pola (x, y) takiego, że $\mathrm{NWD}(x, y) = 2^s$, dla pewnego s. W tym celu skorzystamy z zasady ekstremum. Rozważmy podzbiór zbioru liczb całkowitych złożony z wartości wyrażenia $p+q$, gdzie (p, q) to punkt, z którego można dojść do (x, y). Ten zbiór ma element minimalny, a więc dla pewnego (p, q) suma $p + q$ jest najmniejsza możliwa. Zauważmy, że ani p, ani q nie może być parzyste, bo jeśli do (x, y) można dojść z punktu (p, q) to można też dojść z punktów $(p/2, q)$ oraz $(p, q/2)$, a to przeczyłoby minimalności sumy $p + q$. A zatem p, q są nieparzyste. Jeśli $p > q$, to do (p, q) można dotrzeć z $(p + q/2, q)$ poprzez punkt $(p+q, q)$, co znowu przeczy minimalności $p+q$. Podobnie dla $p < q$. A zatem $p = q$. Ale przecież zakładaliśmy, że $\mathrm{NWD}(x, y) = 2^s$, czyli p, q nie mają wspólnych dzielników nieparzystych. Zatem $p = q = 1$, więc można dotrzeć do (x, y) z $(1, 1)$. ■

Zadanie 9. *Pokaż, że liczba różnych rozkładów liczby całkowitej dodatniej n na sumę nieparzystej liczby składników będących kolejnymi liczbami całkowitymi równa jest (licząc z dokładnością do kolejności składników) liczbie nieparzystych dzielników liczby n mniejszych niż $\sqrt{2n}$, zaś liczba rozkładów liczby n na sumę parzystej liczby składników będących kolejnymi liczbami całkowitymi równa jest (licząc z dokładnością do kolejności składników) liczbie nieparzystych dzielników liczby n większych niż $\sqrt{2n}$.*

Rozwiązanie. Przypuśćmy, że n jest sumą nieparzystej liczby kolejnych liczb całkowitych dodatnich. A zatem środkowy wyraz tej sumy jest liczbą całkowitą i średnią wszystkich składników. Niech element ten będzie równy a. Mamy zatem:

$$n = (a-k) + \ldots + a + \ldots + (a+k) = (2k+1)a.$$

Problem w tym, że taki napis można wykonać nawet i bez założenia, że a jest liczbą całkowitą, a taka sytuacja nas nie interesuje. Ważne jest, by okazało się, ze $2k+1$ to dzielnik całkowity liczby n. Wówczas oczywiście dla różnych k będziemy mieli różne rozkłady na sumy kolejnych liczb całkowitych. Pokażemy teraz, że konieczne jest by $2k+1 \leqslant \sqrt{2n}$. Z założenia mamy $a - k \geqslant 1$, a zatem $2a - (2k+1) > 0/$ W konsekwencji

$$2k+1 < 2a = \frac{2n}{2k+1},$$

czyli $(2k+1)^2 < 2n$.

Rozwiązanie części drugiej uzyskuje się analogicznie. Przypuśćmy, że n jest sumą $2k$ kolejnych liczb całkowitych. Oczywiście dla różnych k dostajemy różne rozkłady postaci:

$$n = \underbrace{(a+1-k) + \ldots + a}_{k} + (a+1) + \ldots + (a+k) = 2k(a + \frac{1}{2}) = k(2a+1),$$

ale chodzi o to, by a było liczbą całkowitą. I teraz można pokazać, że $(2a+1)^2 > 2n$. Rzeczywiście $a - k \geqslant 0$ (bo najmniejszy składnik naszej sumy jest o 1 większy), więc $(2a+1) - 2k > 0$, czyli $2a + 1 > \frac{2n}{2a+1}$. ■

Zadanie 10. *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. Pokaż, 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 przemnożyc 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.

■