Największy wspólny dzielnik

Seminarium OMJ dla nauczycieli matematyki
Arkadiusz Męcel
18-19.09.2020 r.

Tytułowe zagadnienie może na pierwszy rzut oka wydawać się niedopasowanym do działu „Początki z OMJ". Czy rzeczywiście początkującego olimpijczyka warto uczyć akurat o największym wspólnym dzielniku? Jest to pojecie, które na poziomie definicji matematycznej wymaga pewnej dojrzałości i wprawy, a jego używanie w kontekście konkursowym bywa dla uczniów trudne. Jednocześnie jednak intuicje dotyczące znaczenia pojęcia największego wspólnego dzielnika wywodzić można z bardzo różnych prostych zagadnień praktycznych. Najbardziej podstawowe to: zadania dotyczące grupowania obiektów różnego rodzaju w zestawy (czy też drużyny, grupy, paczki) zawierające tyle samo obiektów tego samego rodzaju. Zobaczmy proste przykłady.

- Mając 15 czekoladek i 5 batonów zrobimy maksymalnie 5 zestawów, z których każdy zawiera tyle samo czekoladek (trzy) i batonów (jeden).
- W grupie 15 chłopców i 6 dziewczynek wskazać można maksymalnie 3 drużyny, z których każda zawiera ustaloną liczbę dziewczynek (pięć) i ustaloną liczbę chłopców (dwóch).
- Zestawu 15 kredek i 7 ołówków nie można rozdzielić „sprawiedliwie" w żadnej grupie dzieci (innej niż jednoosobowa) tak, by każdy otrzymał ustaloną liczbę kredek i ustaloną liczbę ołówków.

Owa „maksymalna liczba zestawów/drużyn/paczek" zawierających tyle samo obiektów jednego i drugiego rodzaju, przy czym obiektów jednego rodzaju jest n, a drugiego jest m wynosi właśnie $\mathrm{NWD}(n, m)$. Definicja ta może być w sposób bardzo prosty rozszerzona do większej liczby obiektów. Jeśli chcemy przygotować paczki zawierające jednakową liczbę czekoladek, batonów i pomarańczy, przy czym liczba tych obiektów wynosi odpowiednio p, q, r, to paczek takich można przygotować maksymalnie $\mathrm{NWD}(p, q, r)$.

Powyższa ilustracja pojęcia NWD jest, jak sądzę, przydatna w szkole – motywuje wprowadzenie określonego pojęcia i daje poczucie, że można je praktycznie stosować. Brakuje jej jednak, moim zdaniem, elementu budzącego zaskoczenie czy zaciekawienie, który motywowałby zainteresowanie własnościami NWD i pokazywało nieoczywisty sposób wykorzystania tego pojęcia. Z pomocą przychodzi jednak inny, znany od starożytności problem, na tyle atrakcyjny, że przed ćwierćwieczem trafił nawet w pewnej postaci do Hollywood.

Zadanie 1. *Zeus i McClane muszą rozbroić bombę ukrytą w walizce przez obciążenie jej pojemnikiem z czterema litrami wody. Dysponują jedynie dwoma pojemnikami: jeden ma objętość 3 litrów, a drugi ma objętość 5 litrów. Mogą pobierać wodę z pobliskiej fontanny do tych pojemników, mogą ją wylewać oraz przelewać między pojemnikami. W jaki sposób odmierzyć mogą* 4 *litry wody?*

Rysunek autorstwa Laury Lannes, źródło: https://www.popsci.com/solve-water-puzzle-die-hard-3/

Rozwiązanie jest oczywiście banalne. Można je wykonać na więcej niż jeden sposób.

- Rozwiązanie pierwsze. Napełniamy pojemnik 5-litrowy. Następnie odlewamy 3-litry do drugiego pojemnika, pozostawiając 2-litry w większym pojemniku. Opróżniamy pojemnik 3-litrowy i przelewamy do niego 2 litry z większego. Napełniamy teraz ponownie pojemnik 5-litrowy i wlewamy z niego wodę do mniejszego, aż się napełni. W ten sposób odlejemy z większego pojemnika litr wody i w większym pojemniku pozostaną nam 4 litry.
- Rozwiązanie drugie. Napełniamy pojemnik 3-litrowy i przelewamy następnie jego zawartość do pojemnika 5-litrowego. Następnie napełniamy ponownie mniejszy pojemnik i przelewamy z niego wodę do większego tak, aż się wypełni. W ten sposób w mniejszym pojemniku mamy 1 litr. Opróżniamy teraz większy pojemnik i wlewamy do niego 1 litr z mniejszego. Następnie napełniamy ponownie mniejszy zbiornik i przelewamy jego zawartość do większego, dostając w ten sposób ponownie 4 litry.

Czy istnieje więcej rozwiązań? Jakie znaczenie ma rozmiar pojemników? Czy umiemy zapisać matematycznie czynności, które opisaliśmy wyżej słownie? Za tymi pytaniami kryje się moim zdaniem wartość dydaktyczna tego zadania. W rozwiązaniu pierwszym wypełniliśmy dwukrotnie pojemnik 5-litrowy i dwa razy przelewaliśmy jego zawartość do pojemnika 3-litrowego. W ten sposób uzyskaliśmy 4 litry, bo

$$4 = 2 \cdot 5 - 2 \cdot 3.$$

W drugim rozwiązaniu trzykrotnie napełniamy pojemnik 3-litrowy i przelewamy jego zawartość do zbiornika 5-litrowego. Uzyskany wynik pochodzi zatem od równości:

$$4 = 3 \cdot 3 - 1 \cdot 5.$$

W podobny sposób wykonać można zadanie, które zaproponowałem Państwu przed zajęciami.

Zadanie 2. *Dany jest pełen zbiornik mleka o dużej objętości (np. ponad 100 litrów). Jaś jest w posiadaniu dwóch pojemników: jeden ma objętość 5 litrów, a drugi 9 litrów. Jaś może wykonywać następujące operacje:*

- *nabierać mleka ze zbiornika do każdego z pojemników,*
- *odlewać mleko z pojemników z powrotem do zbiornika,*
- *przelewać mleko pomiędzy pojemnikami.*

Czy przy pomocy tych operacji Jaś jest w stanie odmierzyć 2 litry mleka (pojemniki nie mają podziałki)?

Nietrudno przekonać się, że Jaś jest w stanie odliczyć 2 litry mleka. Oto przykładowa procedura:

$$(0,0) \to (5,0) \to (0,5) \to (5,5) \to (1,9) \to (1,0) \to (0,1) \to (5,1) \to (0,6) \to (5,6) \to (2,9),$$

gdzie (x, y) oznacza liczbę litrów w zbiornikach w kolejnych krokach: x to liczba litrów mleka w pojemniku 5-litrowym, zaś y to liczba litrów mleka w zbiorniku 9-litrowym.

W rozwiązaniu tym czterokrotnie napełniliśmy zbiornik 5-litrowy oraz dwukrotnie opróżniliśmy pojemnik 9-litrowy. Poniższe równanie wyjaśnia zatem całą sytuację:

$$2 = 4 \cdot 5 - 2 \cdot 9.$$

W jaki sposób rozwiązywać takie zadania? W istocie rozwiązujemy tu problem, który przekracza program szkolny. Rozwiązujemy bowiem równanie z dwoma niewiadomymi całkowitymi x, y postaci:

$$2 = 5x + 9y.$$

Liczby x, y spełniające powyższe równanie całkowite to oczywiście liczby różnych znaków. To równanie nazywane jest liniowym równaniem diofantycznym. Oczywiście znajdowanie różnych par (x, y) spełniających to równanie można interpretować w języku zadania postawionego wyżej. Równania tego typu mają (dwa dwóch i więcej niewiadomych) ciekawą cechę – albo nie mają rozwiązania, albo mają nieskończenie wiele rozwiązań. Pierwszą sytuację łatwo zobaczyć próbując uzyskać 2 litry mleka mając do dyspozyci zbiorniki 4-litrowe i 8-litrowe. Problem ten sprowadza się do znalezienia takich liczb całkowitych x, y, że

$$4x + 8y = 2.$$

Widzimy jednak, że równania napisanego wyżej nie da się rozwiązać. Istotnie, prawa strona tego równania jest, niezależnie od x oraz y liczbą podzielną przez 4. Natomiast 2 nie jest podzielna przez 4. Czy widzimy kiedy istnieje, a kiedy nie istnieje rozwiązanie postawionego problemu? Na poziomie intuicji nietrudno to widzieć: rozwiązanie istnieje, gdy poszukiwana objętość wody/mleka jest wielokrotnością największego wspólnego dzielnika objętości pojemników, ktorymi wolno odmierzać wodę. Czy można rozszerzać problem na większą liczbę pojemników o różnych objętościach? Oczywiście można. Uzyskamy wtedy równania o trzech i więcej niewiadomych, związane z pojęciem największego wspólnego dzielnika układu liczb.

Nie pokazuję Państwu powyższych zadań po to, by nauczyć rozwiązywania równań diofantycznych. Ważna jest raczej idea, jaka stoi za samym **sformułowaniem** tych równań. Okazuje się, że w wielu zadaniach, nawet bardzo prostych, warto jest operować wyrażeniami, które pojawiają się w tych równaniach. Nazywają się one kombinacjami liniowymi.

Definicja 1. *Niech a, b będą liczbami całkowitymi. Dowolną liczbę postaci $ax + by$, gdzie x, y są liczbami całkowitymi nazywamy* ***kombinacją liniową*** *liczb a, b.*

A zatem, patrząc na przykłady wcześniej:

- 2 jest kombinacją liniową liczb 5 oraz 9
- 2 nie jest kombinacją liniową liczb 4 oraz 8

Podstawowe pytanie, kluczowe dla nowego spojrzenia na największy wspólny dzielnik jest nastepujące:

Kiedy liczba całkowita n jest kombinacją liniową liczb całkowitych a oraz b?

Dokładnie to pytanie stawialiśmy sobie rozwiązując problem z mlekiem. Odnotujmy teraz dwie prościutkie obserwacje, które mają ogromne znaczenie.

Obserwacja 1. *Jeśli liczba d jest dzielnikiem zarówno liczby a, jak i liczby b, to jest również dzielnikiem dowolnej kombinacji liniowej liczb a oraz b.*

Obserwacja 2. *Liczba* $\mathrm{NWD}(a, b)$ *jest dzielnikiem* ***każdej*** *liniowej kombinacji liczb a oraz b.*

Dowody obydwu tych obserwacji są niemal oczywiste, jeśli umiemy posługiwać się abstrakcyjną notacją związaną z podzielnością. Jeśli, zgodnie z tezą pierwszej obserwacji, liczba d jest dzielnikiem zarówno a, jak i b, to istnieją liczby całkowite a' oraz b' takie, że $a = d \cdot a'$ oraz $b = d \cdot b'$. W szczególności biorąc dowolną kombinację liniową $ax + by$ liczb a, b mamy:

$$ax + by = (da')x + (db'y) = d(a'x) + d(b'y) = d(a'x + b'y).$$

A zatem d jest dzielnikiem $ax + by$. Skoro każdy wspólny dzielnik liczb a, b jest dzielnikiem każdej kombinacji liniowej tych liczb, to także $\mathrm{NWD}(a, b)$ ma tę własność.

Powyższe obserwacje są niemal oczywiste, a mają bardzo eleganckie skutki. Oto przykłady zadań z konkursów, które można stosunkowo łatwo rozwiazać za pomocą tej obserwacji.

Zadanie 3. *Suma liczba całkowitych a, b jest podzielna przez 3, zaś różnica $a - b$ jest podzielna przez 4. Pokazać, że liczba $13a + b$ jest podzielna przez 6.*

Zauważmy najpierw, że liczba $a + b = (a - b) + 2b$ jest parzysta, a zatem liczba $a + b$ jest podzielna przez 2 i przez 3, czyli jest podzielna przez 6. A zatem liczba $13a + b = 12a + (a + b)$ jest podzielna przez 6.

Zauważmy, że w istocie mamy $a + b = 6k$ oraz $a - b = 4q$, dla pewnych k i q, z czego wynika, że $a = 3k + 2q$ oraz $b = 3k - 2q$, dla pewnych k, q całkowitych.

Zadanie 4. *Pokazać, że każda liczba całkowita większa od 6 może być zapisana jako suma dwóch względnie pierwszych liczb całkowitych większych niż 1.*

Niech $m > 6$ będzie liczbą całkowitą. Jeśli m jest nieparzysta, to oczywiście $m = n + (n + 1)$. Jeśli m jest podzielna przez 4, to $4n = (2n - 1) + (2n + 1)$, a dwie kolejne liczby nieparzyste są względnie pierwsze. Wreszcie gdy m jest liczbą parzystą, ale niepodzielną przez 4, wówczas $m = (n-2)+(n+2)$, gdzie n jest liczbą nieparzystą. Dwie liczby nieparzyste różniące się o 4 są względnie pierwsze. Dlaczego? Podpowiedź: dzielnik różnicy.

Zadanie 5. *Udowodnij, że ułamki*

$$\frac{21n+4}{14n+3} \quad \textit{oraz} \quad \frac{30n+1}{12n+1}$$

są nieskracalne dla każdego n naturalnego.

Oto rozwiązanie. Dla każdego n naturalnego rozważmy następujące kombinacje liniowe:

$$3(14n+3) - 2(21n+4) = 1 \quad \text{oraz} \quad 5(12n+1) - 2(30n+1) = 3.$$

Z pierwszej równości wynika, że pewna kombinacja liniowa liczb $14n+3$ oraz $21n+4$, niezależnie od n, równa jest 1. Zgodnie jednak z obserwacją drugą, liczba $\mathrm{NWD}(14n+3, 21n+4)$ jest dzielnikiem każdej kombinacji liniowej tych liczb. W szczególności $\mathrm{NWD}(14n+3, 21n+4)$ jest dzielnikiem liczby 1, czyli samo wynosi 1. To oznacza, że ułamek $(21n+4)/(14n+3)$ jest zawsze nieskracalny.

A jak jest w drugim przypadku? Tu potrzeba dodatkowej prostej obserwacji. Wiemy, że $\mathrm{NWD}(12n+1, 30n+1)$ jest dzielnikiem każdej kombinacji liniowej liczby $12n+1, 30n+1$. A zatem jest to też dzielnik liczby 3. A zatem $\mathrm{NWD}(12n+1, 30n+1)$ równe jest 1 lub 3. Widać jednak, że liczby $12b+1, 30n+1$ dają, niezależnie od n, resztę 1 z dzielenia przez 3. A zatem ich wspólnym dzielnikiem nie jest nigdy 3. Zatem także drugi rozważany ułamek jest dla każdego n nieskracalny.

Zadanie 6. *Liczby a, b są całkowite. Pokazać, że:*

(a) Jeśli 13 *jest dzielnikiem $a+4b$, to* 13 *jest dzielnikiem $10a+b$,*

(b) Jeśli 19 *jest dzielnikiem $3a+7a$, to* 19 *jest też dzielnikiem $43a+75a$,*

(c) Jeśli 17 *jest dzielnikiem $3a+2b$, to* 17 *jest też dzielnikiem $10a+b$.*

Rozwiązanie korzysta po raz kolejny z kombinacji liniowych. Mamy:

$$\begin{aligned} 10(a+4b) - (10a+b) &= 39b, \\ 43(3a+7b) - 3(43a+75b) &= 38b, \\ 10(3a+2b) - 3(10a+b) &= 17b. \end{aligned}$$

Zadanie 7. *Liczby $2n+1$ oraz $3n+1$ są kwadratami, dla pewnego całkowitego dodatniego n. Pokazać, że liczba $5n+3$ nie jest pierwsza.*

Znów szukamy kombinacji liniowej. Mamy:

$$5n+3 = 4(2n+1) - (3n+1).$$

A zatem jeśli $2n+1 = a^2$ oraz $3n+1 = b^2$, to

$$5n+3 = 4a^2 - b^2 = (2a+b)(2a-b).$$

Zatem $2a-b = 1$, jeśli różnica ta ma być liczbą pierwszą. Wówczas jednak $b = 2a-1$, czyli $5n+3 = (2a+2a-1)$, czyli $5n+3 = 4a-1$, a więc $5n = 4a-4$. Zatem $a^2 - 4a + 4 = (a-2)^2 = 1-3n$, co jest niemożliwe.

Czas wreszcie wyjaśnić w jaki sposób największy wspólny dzielnik wiąże się z kombinacjami liniowymi. Mówi o tym następujący wynik.

Twierdzenie 1 (Lemat Bezout)**.** *Dla każdych liczb całkowitych niezerowych a, b istnieją liczby całkowite x, y takie, że*

$$ax + by = \mathrm{NWD}(a, b).$$

Ten fakt może być zaskakujący. Okazuje się, że nie tylko każda kombinacja liniowa liczb całkowitych nieujemnych jest podzielna przez największy wspólny dzielnik (z tego już skorzystaliśmy), ale po prostu jedna z tych kombinacji **jest** największym wspólnym dzielnikiem. Fakt ten ma olbrzymie znaczenie w teorii liczb. Można z niego wyprowadzić szereg fundamentalnych rezultatów, na czele z twierdzeniem o rozkładzie (i jego jednoznaczności) dowolnej liczby całkowitej różnej od $-1, 0, 1$ na czynniki pierwsze. Spróbuje pokazać dowód tego wyniku. W tym celu użyjemy techniki bardzo często wykorzystywanej w teorii liczb, która ma też ogromne znaczenie w trudniejszych zadaniach. Jest to tak zwana zasada dobrego porządku.

Wskazówka 1 (Zasada dobrego porządku)**.** *W każdym niepustym podzbiorze S liczb całkowitych nieujemnych wskazać można najmniejszy element, czyli taki element n, że dla każdego elementu m zbioru S mamy: $n \leqslant m$.*

Zauważmy, że ta prosta zasada korzysta bardzo mocno z założeń. Gdybyśmy zamienili liczby całkowite nieujemne, na dowolne liczby całkowite, to twierdzenie nie byłoby prawdziwe, ponieważ biorąc za S zbiór coraz mniejszych liczb ujemnych:

$$-1, -2, -3, \ldots,$$

nie znajdziemy w S najmniejszego elementu. Również samo założenie nieujemności liczb to za mało. W poniższym ciągu ułamków nie ma elementu najmniejszego:

$$\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$$

Żeby dobrze zrozumieć działanie tej zasady udowodnimy najpierw prostszy fakt niż lemat Bezout, mianowicie twierdzenie o dzieleniu z resztą.

Twierdzenie 2. *(O dzieleniu z resztą) Niech a, b będą liczbami całkowitymi dodatnimi, przy czym $b \geqslant a$ oraz $a \neq 0$. Wówczas istnieją liczby q, r, przy czym $q \geqslant 1$ oraz $0 \leqslant r < a$ takie, że:*

$$b = qa + r.$$

Liczbę r nazywamy resztą z dzielenia b przez a.

Rozważamy podzbiór liczb całkowitych postaci

$$b - a, b - 2a, b - 3a, b - 4a, \ldots$$

Zauważmy, że pierwszy element tego ciągu jest nieujemny (bo $b \geqslant a$) i każdy kolejny element jest mniejszy, niż poprzedni (bo $a > 0$). Wybierzmy z tego ciągu wszystkie elementy nieujemne i nazwijmy uzyskany zbiór przez S. Zauważmy, że zbiór S jest niepusty i składa się jedynie z liczb całkowitych nieujemnych. A zatem istnieje w nim najmniejszy element, który nazwiemy:

$$b - ta,$$

dla pewnego t. Zauważmy, że:

$$b = ta + (b - ta).$$

Twiedzimy, ze $0 \leqslant b - ta < a$. Innymi słowy, twierdzimy, że ów najmniejszy element zbioru S jest resztą z dzielenia b przez a. Rzeczywiście, jest to liczba nieujemna zgodnie z założeniem, że to najmniejszy element zbioru S, złożonego z nieujemnych liczb całkowitych. Pozostaje pokazać, że $b - ta < a$. Gdyby było inaczej, czyli $b - ta \geqslant a$, wówczas liczba $b - ta - a = b - (t + 1)a$ byłaby nieujemna i należałaby do zbioru S! Jednak $b - ta > b - (t + 1)a$, co by oznaczało, że $b - ta$ nie było elementem najmniejszym w S. Otrzymana sprzeczność dowodzi, że $b - ta < a$. A zatem dowód jest zakończony.

Bardzo podobną technikę wykorzystamy w dowodzie Lematu Bezout, przy czym ograniczymy się do przypadku, gdy liczby a, b są dodatnie, dla większej czytelności argumentów. Rozważmy zbiór L wszystkich wyrażeń typu $ax + by$, gdzie x, y są liczbami całkowitymi oraz $ax + by > 0$. Są tu więc wszystkie na przykład wyrażenia $a+b, 2a+b, a+2b$, a także mogą być wyrażenia postaci $a-b$, czy też $2a-3b$, o ile tylko są dodatnie. Oczywiście a, b są dodatnie, więc ten zbiór jest niepusty, zawiera choćby $a + b$. Zgodnie z zasadą dobrego porządku istnieje zatem **najmniejsza dodatnia kombinacja liniowa** liczb a, b. Nazwijmy ten element jako d. Twiedzimy, że $d = \mathrm{NWD}(a, b)$. Aby to pokazać, użyjemy poprawnej, matematycznej definicji NWD, która ma postać:

Definicja 2. *Niech a, b liczbami całkowitymi, z których co najmniej jedna jest niezerowa. Przez* $\mathrm{NWD}(a, b)$ *oznaczamy największy wspólny dzielnik liczb a, b, czyli taką liczbę całkowitą n, że:*

- *n jest dzielnikiem zarówno a, jak i b,*
- *jeśli liczba m jest również dzielnikiem zarówno a, jak i b, to $m \leqslant n$.*

Jeśli chcemy sprawdzić czy jakaś liczba d jest największym wspólnym dzielnikiem liczb a, b, to musimy pokazać, że jest wspólnym dzielnikiem tych liczb oraz, że jest nie mniejsza niż pozostałe dzielniki Skoro liczba d jest kombinacją liniową liczb a, b, to istnieją liczby całkowite x, y, że:

$$d = ax + by.$$

Wiemy, że NWD(a, b) jest dzielnikiem każdej kombinacji liniowej liczb a, b. A zatem $NWD(a, b)$ jest również dzielnikiem d. Dzielnik jest nie większy niż liczba dodatnia, którą dzielimy, a zatem NWD$(a, b) \leqslant d$. Jeżeli pokażemy, że d jest zarówno dzielnikiem a, jak i b, to dowó będzie zakończony. Wykorzystamy założenie, że d jest najmniejszym elementem zbioru L.

Załóżmy, wbrew temu co oczekujemy, że d nie jest dzielnikiem a. Zatem na mocy twierdzenia o dzieleniu z resztą istnieje liczba $0 < r < d$ oraz $k \geqslant 1$ taka, że:

$$a = kd + r.$$

To oznacza, że $r = a - kd$. To jest niemożliwe, bo przecież:

$$r = a - kd = a - k(ax + by) = a(1 - lkx) - kby,$$

jest również elementem zbioru L, i to mniejszym niż d, sprzeczność. A zatem d jest dzielnikiem a. Analogicznie pokazujemy, że d jest dzielnikiem b. A zatem d rzeczywiście jest wspólnym dzielnikiem a oraz b, co oznacza, że $d \leqslant g$. Dowód jest zakończony.

Lemat Bezout ma niezliczone zastosowania. Jednym z najprostszych, bardzo przydatnych na olimpiadach wnioskiem jest fakt:

Twierdzenie 3. *Jeśli liczba pierwsza p jest dzielnikiem iloczynu ab liczb całkowitych a, b, to p jest dzielnikiem a lub p jest dzielnikiem b.*

Znowu rozumować będziemy nie wprost. Załóżmy, wbrew tezie twierdzenia, ze liczba pierwsza p nie dzieli ani a, ani b. Skoro p nie jest dzielnikiem a, to liczby a oraz p są względnie pierwsze. Innymi NWD$(a, p) = 1$. W szczególności, na mocy Lematu Bezout istnieją liczby całkowite x, y takie, że:

$$px + ay = 1.$$

Wykorzystamy teraz założenie, że p jest dzielnikiem ab. Przemnóżmy strony powyższej równości przez b, otrzymując:

$$pxb + ayb = pxb + \mathbf{ab}y = b.$$

Zapisaliśmy zatem liczbę b jako sumę dwóch liczb całkowitych, z których każda jest wielokrotnością p. A zatem b jest wielokrotnością p, wbrew założeniu, że nie jest ani dzielnikiem a, ani b. A zatem teza twierdzenia jest prawdziwa.

Zobaczmy rozwiązanie czterech zadań diametralnie różnej trudności, które korzystają z udowodnionego twierdzenia. Bardzo często zadania te opierają się o nastepujący wariant tego faktu:

Wniosek 1. *Jeśli liczba a^2 jest podzielna przez liczbę pierwszą p, to także liczba a jest podzielna przez p.*

Zadanie 8. *Liczby całkowite a, b spełniają własność $NWD(a, b) = 2$. Pokazać, że liczby te nie mogą być obydwie kwadratami liczb całkowitych.*

Rozwiązanie jest oczywiste. Każda z liczb a, b jest podzielna przez 2. Gdyby jednak $a = x^2$ oraz $b = y^2$, dla pewnych x, y, wówczas z faktu powyżej liczba 2 byłaby również dzielnikiem x oraz y. To by jednak znaczyło, że a oraz b są podzielne przez 4, co prowadzi do sprzeczności, bo $NWD(a, b) = 2$.

Zadanie 9. *Liczby całkowite x oraz y są względnie pierwsze. Pokaż, że również liczby y^2 oraz $x + y$ są względnie pierwsze.*

Przypuśćmy, że liczba pierwsza p jest dzielnikiem y^2 oraz $x + y$. Oznacza to, że p jest dzielnikiem y, a zatem także dzielnikiem $(x + y) - y$, czyli x. Ale liczby x, y są względnie pierwsze, więc doszliśmy do sprzeczności.

Zadanie 10. *Załóżmy, że liczba a^2+ab+b^2 jest podzielna przez 9, przy czym liczby a, b są całkowite. Pokazać, że zarówno a, jak i b są wielokrotnościami liczby 3.*

Zauważmy, że

$$a^2+ab+b^2=(a^2-2ab+b^2)+3ab=(a-b)^2+3ab.$$

Skoro a^2+ab+b^2 jest podzielne przez 9, to jest też podzielne przez 3. A zatem także liczba $(a-b)^2$ jest podzielna przez 3. A zatem na mocy wniosku także $a-b$ jest podzielna przez 3, czyli $(a-b)^2$ jest podzielna przez 9. To oznacza, że również $3ab$ jest podzielna przez 9, a zatem ab jest podzielna przez 3. A zatem na mocy twierdzenia jedna z liczba a, b jest podzielna przez 3. Ustaliliśmy jednak, że również $a-b$ jest podzielna przez 3. A zatem obydwie z liczb a, b są podzielne przez 3.

Zadanie 11. *Niech a, b, c, d będą liczbami całkowitymi dodatnimi takimi, że $ad=bc$. Pokazać, że liczba $a+b+c+d$ nie może być pierwsza.*

Pomysł jest taki: załóżmy wbrew tezie, że liczba $a+b+c+d=p$ jest pierwsza. Mamy zatem $d=p-a-b-c$, czyli z założenia:

$$ad=a(p-a-b-c)=bc.$$

W rezultacie

$$ap=ad+a^2+ab+ac=(a+b)(a+c).$$

Oznacza to, że liczba pierwsza p jest dzielnikiem iloczynu $(a+b)(a+c)$. W szczególności, zgodnie z Twierdzeniem wyżej, liczba pierwsza p jest dzielnikiem $a+b$ lub $a+c$. To jest jednak niemożliwe, bo skoro a, b, c, d są dodatnie oraz $p=a+b+c+d$, to $p>a+b$ oraz $p>a+c$. Otrzymana sprzeczność pokazuje, że suma $a+b+c+d$ nie może być liczbą pierwszą.

Opisane metody oczywiście w żadnym stopniu nie wyczepują zagadnień dotyczących NWD. Chciałem skupić się na zagadnieniach wyrastających z równań diofantycznych liniowych, choć i tu nie powiedziałem wszystkiego. Dopiero zaznajomienie się z algorytmem Euklidesa pozwala na pełne operowanie powyższymi pojęciami i na rozwiązywanie kolejnych zadań. Opiera się on o następującą obserwację:

Twierdzenie 4. *Niech a, b będą niezerowymi liczbami całkowitymi. Wówczas:*

$$NWD(a,b)=NWD(a-b,a)=\mathrm{NWD}(a,b-a),$$

przy czym przyjmujemy, że $\mathrm{NWD}(x,y)=\mathrm{NWD}(x,-y)$.

Na własności tej oparte jest mnóstwo ćwiczeń dotyczących NWD, przy czym nie wprowadzałem jej w trakcie seminarium dość celowo. Bardzo często wykorzystuje się tą własność w połączeniu z różnymi algebraicznymi i teorioliczbowymi sztuczkami, na których omówienie nie ma za wiele miejsce w seminarium pokazującym podstawy działania na największym wspólnym dzielniku. W bardzo wielu problemach dotyczących NWD należy wprowadzić tę wielkość jako zmienną i wykonywać na niej rozmaite rachunki. Przykładem zadania tego typu jest Zadanie 1 z finału V OMJ. Ja również chciałbym pokazać jeden przykład zadania tego typu, trudniejszy niż pozostałe. Zawsze jednak trafia nam się uczeń, który potrafi wszystko zrobić. Takie zadanie może być dla niego sporym wyzwaniem (nawet dla licealisty to mógłby być zabójczy problem, choć raczej nie dla olimpijczyka).

Zadanie 12. *Liczby całkowite dodatnie a, b mają tę własność, że suma*

$$\frac{a+1}{b}+\frac{b+1}{a}$$

jest liczbą całkowitą. Pokaż, że

$$\mathrm{NWD}(a,b)\leqslant\sqrt{a+b}.$$

Rozwiązanie. Wykorzystamy kilka prostych trików (wykorzystanie ich w jednym zadaniu nie jest oczywiste). Po pierwsze zauważmy, że nierówność:

$$\mathrm{NWD}(a,b)\leqslant\sqrt{a+b}$$

jest równoważna nierówności:

$$\frac{a+b}{\mathrm{NWD}(a,b)^2}\geqslant 1.$$

Druga sztuczka polega na zauważeniu, że skoro $\frac{a}{\mathrm{NWD}(a,b)}$ oraz $\frac{b}{\mathrm{NWD}(a,b)}$ są liczbami całkowitymi, to ma sens patrzenie na wyrażenie typu $\frac{ab}{\mathrm{NWD}(a,b)^2}$, które jest liczbą całkowitą. Rozpatrzmy wyrażenie:

$$\frac{a+b}{\mathrm{NWD}(a,b)^2} = \frac{a+b}{\mathrm{NWD}(a,b)^2} \cdot \frac{ab}{ab} = \frac{a+b}{ab} \cdot \frac{ab}{\mathrm{NWD}(a,b)^2}.$$

Pierwszy z czynników wygląda jakby miał coś wspólnego z założeniem dotyczącym całkowitości liczby

$$n = \frac{a+1}{b} + \frac{b+1}{a} = \frac{a^2+a+b^2+b}{ab}.$$

Teraz potrzeba odrobiny algebraicznego geniuszu. Niech $d = \mathrm{NWD}(a,b)$. Mamy:

$$\begin{aligned}\frac{a+b}{d^2} &= \frac{a^2+a}{d^2} + \frac{b^2+b}{d^2} - \frac{a^2}{d^2} - \frac{b^2}{d^2} \\ &= \left(\frac{a+1}{b} + \frac{b+1}{a}\right) \cdot \frac{a}{d} \cdot \frac{b}{d} - \frac{a^2}{d^2} - \frac{b^2}{d^2}.\end{aligned}$$

Prawa strona jest liczbą całkowitą, jako iloczyn dwóch liczb całkowitych $\frac{a+1}{b} + \frac{b+1}{a}$ oraz $\frac{a}{d} \cdot \frac{b}{d}$ pomniejszony o sumę $\frac{a^2}{d^2} - \frac{b^2}{d^2}$. A zatem $\frac{a+b}{\mathrm{NWD}(a,b)^2}$ jest liczbą całkowitą. jest to iloraz liczb dodatnich, a więc liczba całkowita dodatnia. Stąd

$$\frac{a+b}{\mathrm{NWD}(a,b)^2} \geqslant 1,$$

co jest równoważne wyjściowej nierówności. ■

* * *

Na koniec chciałbym wrócić na chwilę do równań diofantycznych postaci $ax + by = d$, od ktorych zaczęliśmy nasze rozważania. Myślę, że warto wiedzieć, że istnieje ciekawa dziedzina zagadnień i problemów otwartych wywodzących się od następującego problemu.

Pytanie 1. *Załóżmy, że dysponujemy nieograniczonymi zasobami monet o nominałach* 5 *i* 9. *Czy jest jakaś kwota, której nie zapłacimy przy użyciu tych monet? Jaka jest największa możliwa kwota tego rodzaju?*

Zauważmy, że owa kwota musi nie być rozwiązaniem równania $5x + 9y = n$, przy czym tym razem zakładamy, że x oraz y są liczbami nieujemnymi! Problemy te rozważane były już w XIX wieku, a w wieku XX zostały spopularyzowane na przykład w postaci tzw. McNuggets Problem. Dla liczb 5 i 9 największa kwota, której nie można zapłacić do 31. To kolejny sympatyczny temat na rozmowę edukacyjną. Tu pojawia się już sporo trudnych zagadnień i twiedzień, choć da się o nich mówić zupełnie przyziemnie. Na przykład liczba 31 to nie przypadek, ale wielkość wzięta z formuły:

$$31 = 5 \cdot 9 - 5 - 9.$$

Ogólny wynik, który pokazuje, że dla monet o nomilałach (całkowitych) x, y najmniejszą kwotą, której nie można zapłacić jest $xy - x - y$ należy do znanego brytyjskiego algebraika Sylvestera. Dowód zrozumie już bardzo dobry uczeń szkoły podstawowej, na poziomie laureata OMJ. Ale to opowieść na inny referat. Dla trzech nominałów takiego wzoru opisującego największą możliwą „nierealizowalną kwotę" (nazywaną często liczbą Frobeniusa) nie znamy do dziś. Można o tych sprawach poczytać na przykład w dostępnym online artykule autorstwa Kamili Łyczek z czasopisma Delta (4/2014): *Kraina dwóch monet* (pisany z przeznaczeniem dla dzieci).