Tupot małych kroczków albo żart historii

Mariusz SKAŁBA

Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Z chałupy na salony – tak najkrócej można by opisać karierę menueta w europejskiej muzyce użytkowej. Zasięg *drobnych kroków* (po francusku *menu pas* oznacza właśnie „drobny krok") okazał się jednak znacznie większy: menuet nie tylko przekroczył ramy barokowej suity, ale za sprawą klasyków wiedeńskich zajął poczesne miejsce jako trzecia część sonaty, najważniejszej formy muzycznej. Wreszcie Beethoven, a potem Chopin dokonali dalekosiężnej transformacji menueta do scherza (po włosku „żart"): już u pierwszego jest ono tylko chwilami żartobliwe, u drugiego zaś scherzo jest w pełni samodzielne i zawsze dramatyczne.

Podobnie było z karierą równań w matematyce. Wyszły one z opłotków arytmetycznej praktyki, trafiając na salony wyrafinowanych spekulacji: równania algebraiczne wzbogacone o równania różniczkowe stały się potężnym i systematycznym narzędziem poznawania świata i jednym z najintensywniej uprawianych i żyznych poletek matematyki. Z tej działki wymieńmy trzech gigantów: Newton, Euler i Gauss. Ponoć pierwszy z nich mawiał, że widział dalej niż inni, gdyż stał na barkach poprzedników – olbrzymów.

Pomiędzy teoriami poszczególnych rodzajów równań istnieją potężnie płodne sprzężenia zwrotne, ale w sensie, który podniesiemy w tym artykule, wszystko obraca się cały czas wokół równań pojęciowo najprostszych, czyli *diofantycznych.* Dla dowolnego wielomianu $F(x_1, x_2, \ldots, x_n)$ o współczynnikach całkowitych możemy mianowicie zająć się równaniem

$$F(x_1, \ldots, x_n) = 0$$

i szukać jego rozwiązań tylko w liczbach całkowitych $x_1, \ldots, x_n$. Możemy ewentualnie dopuścić wymierne wartości niewiadomych. W obu przypadkach mówimy o *równaniu diofantycznym.* Jak zilustrujemy poniżej, trudność konkretnego równania zależy zarówno od liczby niewiadomych, jak i stopnia wielomianu F. Przypadki, gdy stopień F jest mniejszy od 3, można skwitować krótko i pozytywnie: dzisiaj istnieją zadowalające teorie zarówno dla równań diofantycznych liniowych, jak i kwadratowych dowolnej liczby zmiennych. Tytułem przykładów przytoczymy po jednym klasycznym twierdzeniu dla stopnia 1 i 2.

- Równanie $a_1x_1 + \ldots + a_nx_n = b$, gdzie $a_1, \ldots, a_n, b$ są dane całkowite, ma rozwiązania w liczbach całkowitych $x_1, \ldots, x_n$ wtedy i tylko wtedy, gdy liczba b dzieli się przez $\mathrm{NWD}(a_1, \ldots, a_n)$.
- Jeśli liczba naturalna d nie jest kwadratem, to równanie $x^2 - dy^2 = 1$ (zwane *równaniem Pella*) ma nieskończenie wiele rozwiązań w liczbach naturalnych x, y, przy czym jeśli x_1, y_1 jest rozwiązaniem z najmniejszym naturalnym x_1, to wszystkie rozwiązania otrzymamy poprzez potęgowanie liczby $x_1 + y_1\sqrt{d}$, a dokładniej: para liczb naturalnych x, y jest rozwiązaniem tego równania wtedy i tylko wtedy, gdy istnieje takie $n \in \mathbb{N}$, że
$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Dla potrzeb dalszej części artykułu rozważmy dokładniej przypadek $d = 2$. Para liczb $(3, 2)$ jest tu najmniejszym rozwiązaniem, a więc wszystkie rozwiązania zawarte są w ciągu (x_n, y_n):

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n.$$

Ponieważ $x_n - y_n\sqrt{2} = (3 - 2\sqrt{2})^n$, więc możemy wypisać wzory explicite na x_n, y_n:

$$x_n = \frac{(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n}{2}, \quad y_n = \frac{(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n}{2\sqrt{2}}.$$

Jak szybko rosną kolejne rozwiązania równania

$$x^2 - 2y^2 = 1? \tag{1}$$

Na mocy powyższych wzorów:

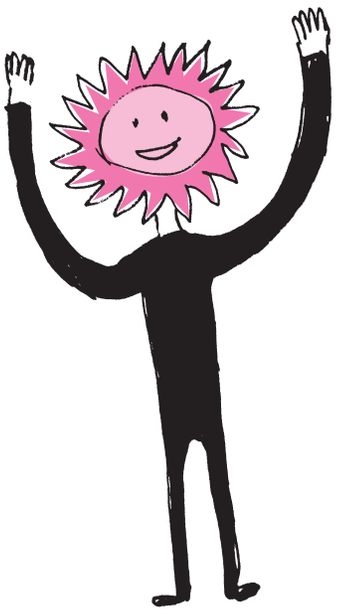
$$\log(x_n) \approx n\log(3 + 2\sqrt{2}) - \log(2), \quad \log(y_n) \approx n\log(3 + 2\sqrt{2}) - \frac{3}{2}\log(2),$$

gdyż potęgi liczby $0 < 3 - 2\sqrt{2} < 1$ są zaniedbywalnie małe dla dużych n. Można to zinterpretować tak, że liczba cyfr w liczbach x_n, y_n jest rzędu cn, gdzie c jest pewną stałą dodatnią.

Wspomnimy teraz o równaniach diofantycznych, w których rozwiązania rosną jeszcze szybciej. Niech mianowicie

$$F(x, y) = y^2 - x^3 - ax - b = 0, \tag{2}$$

gdzie $a, b \in \mathbb{Q}$ spełniają warunek $\Delta = 4a^3 + 27b^2 \neq 0$. Ten warunek gwarantuje, że zbiór punktów (x, y) spełniających równanie (2) jest krzywą gładką, tzn. taką, która ma styczną w każdym punkcie. Krzywe zadane równaniami typu (2) nazywamy *eliptycznymi.* Podobnie jak w przypadku równania Pella, okazuje się, że każde rozwiązanie w liczbach wymiernych (o ile w ogóle takie rozwiązania



istnieją) można wygenerować ze skończenie wielu rozwiązań za pomocą odpowiedniej procedury geometrycznej: prowadząc sieczne lub styczne przez dane punkty wymierne. Mówi o tym słynne twierdzenie Mordella z 1922 roku. Wnikliwa analiza każdej konkretnej krzywej eliptycznej prowadzi do wniosku, że maksimum licznika i mianownika współrzędnej x generowanych punktów ma około cn^2 cyfr! Tak więc chociaż rozwiązań może być nieskończenie wiele, to na pewno niewiele jest rozwiązań „małych” (przy czym „rozmiar” liczby wymiernej r/s, gdzie $r,s\in\mathbb{Z}$ oraz $\mathrm{NWD}(r,s)=1$, rozumiemy tu jako $\max(|r|,|s|)$). Równania krzywych eliptycznych to nieliczne równania diofantyczne 3 stopnia, dla których istnieje bogata, głęboka i piękna teoria – jeden z problemów milenijnych: hipoteza Bircha–Swinnertona-Dyera, dotyczy zresztą rozwiązań wymiernych równania (2).

Ale czy rozwiązania mogą rosnąć jeszcze szybciej? Rozważmy w tym celu równanie diofantyczne z 1. etapu 68 Olimpiady Matematycznej:

$$(x^2+2y^2)^2-2(z^2+2t^2)^2=1.$$

Zadanie polegało na udowodnieniu, że to równanie ma nieskończenie wiele rozwiązań w liczbach całkowitych. Niech dalej S oznacza zbiór wszystkich liczb całkowitych postaci x^2+2y^2, gdzie $x,y\in\mathbb{Z}$. Załóżmy najpierw, że dla pewnego n mamy

$$x_n=a^2+2b^2,\quad y_n=c^2+2d^2,\quad \text{gdzie } a,b,c,d\in\mathbb{Z}$$

i oczywiście x_n,y_n oznaczają n-te rozwiązanie równania Pella (1). Wówczas

$$x_{2n}+y_{2n}\sqrt{2}=(x_n+y_n\sqrt{2})^2=(x_n^2+2y_n^2)+2x_ny_n\sqrt{2}.$$

Mamy ponadto

$$2x_ny_n=(2ad+2bc)^2+2(ac-2bd)^2.$$

Zatem jeśli $x_n,y_n\in S$, to również $x_{2n},y_{2n}\in S$. Wychodząc od rozwiązania $x_1=3=1^2+2\cdot 1^2, y_1=2=0^2+2\cdot 1^2$, otrzymamy ciąg nieskończony $x_{2^n},y_{2^n}\in S$, co kończy rozwiązanie zadania z olimpiady. Ciąg x_{2^n} rośnie bardzo szybko – liczba x_{2^n} ma około $c2^n$ cyfr! Powstaje jednak naturalne pytanie, czy w ten sposób wytworzymy wszystkie rozwiązania? Okazuje się, że nie: można sprawdzić na komputerze, że $x_{257},y_{257}\in S$, i stąd powstaje druga seria nieskończona: $x_{257\cdot 2^n},y_{257\cdot 2^n}$. Czy są jeszcze inne serie? Wiadomość z ostatniej chwili: mamy $x_{937},y_{937}\in S$, co generuje trzecią serię $x_{937\cdot 2^n},y_{937\cdot 2^n}$ – być może są inne serie z rozwiązaniem „startowym” $x_n,y_n\in S$, gdzie $n<937$ jest nieparzyste. Czy liczba serii jest skończona? To drugie pytanie jest ekstremalnie trudne i na pewno nie nadaje się na olimpiadę. Przy okazji zajmowania się 10. problemem Hilberta Martin Davis badał równanie podobnego typu:

$$9(x^2+7y^2)^2-7(z^2+7t^2)^2=2,$$

i wysunął hipotezę, że ma ono tylko rozwiązania pochodzące z równości $9\cdot 1^2-7\cdot 1^2=2$. Z prawdziwości tej hipotezy wynikałoby łatwo dokończenie negatywnego rozstrzygnięcia 10. problemu Hilberta, ale niestety są jeszcze inne rozwiązania. Do rozwiązania problemu Hilberta wystarczyłaby osłabiona wersja hipotezy Davisa twierdząca, że rozwiązań jest skończenie wiele, ale nikomu nie udało się udowodnić (ani obalić) nawet tego. Ostatecznie Jurij Matiasiewicz znalazł odpowiednią formułę diofantyczną o wykładniczym wzroście na innej drodze, badając wnikliwie i dogłębnie ciąg Fibonacciego, i w ten sposób dokończył rozwiązanie (negatywne) 10. problemu Hilberta.

O 10. problemie Hilberta pisaliśmy w Δ^{12}_{19}

Podsumujmy nasze rozważania: niektóre równania czwartego stopnia z czterema niewiadomymi są tak trudne, że nie sposób przy obecnym stanie wiedzy i metod opisać ich *wszystkich* rozwiązań całkowitych, ale... Pomarzmy przez chwilę: może ktoś kiedyś wymyśli przynajmniej jednolity algorytm rozstrzygania, czy dane równanie czwartego stopnia ma w ogóle jakiekolwiek rozwiązanie całkowite? Przywołajmy teraz anegdotyczną tasmańską metodę liczenia: *Jeden, dwa,..., mnóstwo*, i parafrazując Newtona, wyraźmy swoje najskrytsze życzenie – jako matematycy stojący wysoko na gigantycznym i olbrzymim podeście matematyki współczesnej chcemy podskoczyć jeszcze wyżej – przynajmniej na stopień *czwarty*!

Wykażemy na koniec, że nie ma na to szans! Skorzystamy oczywiście z negatywnego rozstrzygnięcia 10. problemu Hilberta: *nie ma algorytmu, który odpowiadałby na pytanie o istnienie rozwiązań dowolnego równania diofantycznego*. Wykażemy teraz, że gdyby taki algorytm istniał dla równań stopnia $\leqslant 4$ (o dowolnej liczbie niewiadomych), to dałoby się go przerobić na algorytm uniwersalny: działający dla równania diofantycznego dowolnego stopnia. Tytułem ilustracji pokażemy teraz, jak zakodować równanie Fermata stopnia n:

$$x^n + y^n = z^n$$

za pomocą równania

$$F_n(x_1, x_2, \ldots, x_k) = 0$$

stopnia $\leqslant 4$. Określamy najpierw ciąg zmiennych $x_1, x_2, \ldots, x_n$ przyjmujących wartości całkowite dodatnie w następujący sposób: $x_1 = x$ oraz

$$x_2 = x_1 \cdot x_1,\ x_3 = x_2 x_1,\ \ldots,\ x_n = x_{n-1} x_1$$

i analogicznie $y_1, y_2, \ldots, y_n$ oraz $z_1, z_2, \ldots, z_n$. W tych nowych zmiennych oryginalne równanie Fermata zapisujemy tak: $x_n + y_n = z_n$. Ale powiązanie wszystkich $3n$ zmiennych też wymaga zakodowania. Ostateczne równanie wygląda tak:

$$\sum_{j=1}^{n-1}(x_{j+1} - x_j x_1)^2 + \sum_{j=1}^{n-1}(y_{j+1} - y_j y_1)^2 + \sum_{j=1}^{n-1}(z_{j+1} - z_j z_1)^2 + (x_n + y_n - z_n)^2 = 0.$$

Do dzisiaj nie wiadomo, czy istnieje algorytm, który rozstrzyga dla dowolnego równania diofantycznego stopnia 3, czy ma ono jakiekolwiek rozwiązanie całkowite.

Oczywiście każde równanie diofantyczne można zakodować w analogiczny sposób. Zatem: nie ma szans na jednolitą algorytmiczną teorię równań diofantycznych stopnia $\leqslant 4$!

Zakończmy więc skromnie i z pewną taką nieśmiałością:

Jeden, dwa, trzy (?), . . . , mnóstwo!

W głąb struktury materii

Szymon CHARZYŃSKI

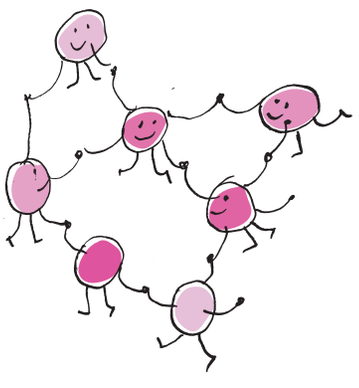
Gdyby cała nauka miała ulec zniszczeniu w jakimś kataklizmie i tylko jedno zdanie można by uratować od zagłady i przekazać następnym pokoleniom, jakie zdanie zawierałoby największą ilość informacji w możliwie najmniejszej liczbie słów? W moim przekonaniu byłoby to zdanie formułujące hipotezę (lub rzeczywistość, jeśli wolicie tak to nazwać) atomistyczną, że wszystko składa się z atomów – w tym jednym zdaniu zawarto ogromną porcję wiadomości o świecie; trzeba tylko posłużyć się odrobiną wyobraźni i inteligencji, aby je dobrze zrozumieć.

Richard Feynman

Cytat pochodzi z podręcznika „Feynmana wykłady z fizyki", tom 1, tłum. Zofia Królikowska (1963).

Hipoteza mówiąca o tym, że materia składa się z niepodzielnych cząstek zwanych atomami, jest znana od starożytności. Jednak przez tysiące lat nie było absolutnie żadnych możliwości doświadczalnego jej potwierdzenia ani obalenia. Tym bardziej nie było możliwości poznania właściwości tych mitycznych atomów. Co więcej, to, co obecnie nazywamy atomami, istotnie różni się od pojęcia, które stworzyli starożytni. Atomy starożytnych filozofów miały być niepodzielne, natomiast nasze, współczesne, atomy składają się z wielu mniejszych cząstek.

Więcej o historii idei atomistycznej można przeczytać w artykułach Grzegorza Białkowskiego Δ^1_{74} i Krzysztofa Rejmera Δ^{11}_{17}.



Pierwszych pośrednich dowodów na istnienie atomów dostarczyło systematyczne badanie reakcji chemicznych. Zaobserwowano, że aby reakcja chemiczna pomiędzy dwoma substratami przebiegała w taki sposób, aby w jej wyniku poza produktem reakcji nie pozostała nadwyżka żadnego z substratów, to należy łączyć te substraty w ściśle określonych proporcjach. Tego typu właściwości świetnie tłumaczy istnienie podstawowych drobin, różnych typów, których zidentyfikowano w XIX wieku kilkadziesiąt i nazwano *pierwiastkami*. Chemicy zauważyli pewne prawidłowości we właściwościach pierwiastków, co doprowadziło do ułożenia z nich pierwszej wersji układu okresowego, w którym było wówczas jeszcze trochę dziur. Wyjaśnienie całej ogromnej mnogości znanych