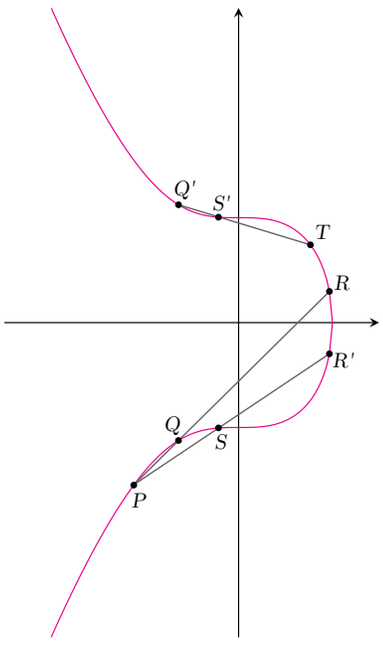
List do redakcji: Jak rysować styczne do krzywej $x^3 + y^2 = 1$



Bardzo lubię *Deltę* (chociaż nie wszystko w niej). Na przykład podobał mi się artykuł z *Delty* 6/2017: *Z samą linijką na okrąg*. Lektura tego tekstu bardzo mnie wciągnęła i zainspirowała. Wiem na przykład, że okręgi, o których jest tam mowa, mogą być opisane równaniami typu $x^2 + y^2 = 1$. I profesor Kordos pięknie pokazuje konstrukcje stycznych do takiego okręgu, przechodzące przez uprzednio zadany punkt. Ale w swoim liście przedstawię metodę rysowania stycznej do krzywej $\mathcal{K}$ danej równaniem $x^3 + y^2 = 1$ w danym punkcie $P \in \mathcal{K}$ i proszę, aby mnie poczytać. W tym celu najpierw pokazuję na rysunku obok, jak taka krzywa w ogóle wygląda (proszę na razie nie przejmować się zaznaczonymi tam punktami, opiszę je później). Widać, że jest ona symetryczna względem osi poziomej, gdyż jeśli $(x, y) \in \mathcal{K}$, to $(x, -y)$ też spełnia równanie $x^3 + y^2 = 1$, czyli rzeczywiście $(x, -y) \in \mathcal{K}$. Dalej często będzie tak, że oprócz punktu Z na płaszczyźnie rozważam również punkt do niego symetryczny względem osi OX – będę go oznaczać symbolem Z'. Przechodzę teraz do konstrukcji stycznej do krzywej $\mathcal{K}$ w punkcie $P \in \mathcal{K}$. Wybieram najpierw punkt $Q \in \mathcal{K}$, dbając tylko o to, aby $Q \neq P$: to chyba mogę, bo na krzywej jest nieskończenie wiele punktów? Teraz mogę poprowadzić prostą PQ i właśnie to robię. Przecina ona krzywą $\mathcal{K}$ jeszcze w trzecim punkcie, nazwę go R. Na mocy wstępnej obserwacji również $R' \in \mathcal{K}$. Prowadzę teraz prostą PR' (jak nie mam pecha, to $R' \neq P$) i literą S oznaczam trzeci punkt przecięcia tej prostej z krzywą $\mathcal{K}$. Teraz dla odmiany prowadzę prostą $S'Q'$. Trzeci punkt przecięcia prostej $S'Q'$ (o ile dalej szczęście mi sprzyja, to raczej $S' \neq Q'$) z krzywą $\mathcal{K}$ oznaczam przez T. Ja uważam teraz, że prosta TP jest szukaną styczną do $\mathcal{K}$ w punkcie P i dlatego tak dokładnie opisałem swoją drogę.

Też słyszałem, że matematycy potrafią udowodnić, że taka konstrukcja jest zawsze poprawna, albo pokazują, że w pewnych przypadkach nie działa. Ale w to drugie to wątpię. Takoż wątpię w sugestie zawarte w artykule pana Mariusza Skałby *Liczby pierwsze jako niewiadome*, również z *Delty* 6/2017 (na lewo od artykułu Marka Kordosa). Ja preferuję taką matematykę, że można sobie coś wyobrazić i ewentualnie dorysować, a nie taką, że nic się nie dzieje i są tylko równania i wzory. Ale jak zobaczę, o co chodzi w tych równaniach, to może coś dorysuję i odezwę się do Państwa.

Na razie pozostaję z szacunkiem dla prawej matematyki

Jan DOCIEKLIWY

Odpowiedź Mariusza Skałby

Z dużym zainteresowaniem przeczytałem Pana list i uznałem, że powinienem się do niego ustosunkować. Tym bardziej że naczelną dla mnie zasadą jest poszanowanie różnorodności gustów – również matematycznych. Nic na to nie poradzę, że nie podoba się Panu mój artykuł, ale spróbuję naświetlić przedstawiony w nim problem z nieco innej strony. W rzeczonym tekście tytułowe liczby pierwsze p, q są niewiadomymi w równaniu diofantycznym

$$p^2 - 2q^2 = -1. \tag{1}$$

W zamieszczonej tam tabelce przytoczyłem przykładowe cztery pary liczb pierwszych, które spełniają to równanie – największa z nich to:

$$p = 19175002942688032928599,$$
$$q = 13558774610046711780701.$$

Przyzna Pan, że te liczby są duże – to pożywiło moją naiwność i skłoniło do sformułowania hipotezy, że **równanie (1) ma nieskończenie wiele rozwiązań w liczbach pierwszych** p, q. W pewnym sensie „dorysowałem" dalszą część tabelki rozwiązań, ale ta ekstrapolacja nie musiała się Panu spodobać. Muszę szczerze wyznać, że gdy spojrzałem na tę tabelkę z innej perspektywy, to i mnie wydała się ona marna i nieobiecująca. Ja nie z tych, co dorysowują, ale chętnie coś dopowiem.

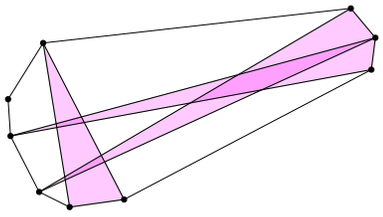
Problemy, w których występują liczby pierwsze, są często bardzo trudne. Tak trudne, że nie ma systematycznych metod ich badania. Dlatego czasem stosuje się namiastki ścisłych metod, czyli tak zwane *heurystyki*. Nie mają one szlachetnego statusu twierdzeń matematycznych, pozwalają jednak na ukształtowanie intuicji i oczekiwań wobec badanego matematycznego problemu – przy pełnej świadomości, że ostatecznie intuicje te mogą okazać się błędne. Jest wśród nich heurystyka następująca:

Załóżmy, że ciąg liczb naturalnych $x_1, x_2, \ldots$ spełnia warunek:

$$\sum_{n=1}^{\infty} \frac{1}{\log x_n} < \infty. \tag{2}$$

Wówczas w ciągu tym występuje co najwyżej skończenie wiele liczb pierwszych.

Rozwiązanie zadania M 1722.
Pokażemy, że jeśli n jest parzyste, to wielokąt $\mathcal{F}$ nie jest zbalansowany. Przekątna A_1A_m, gdzie $m = \frac{n}{2} + 1$, dzieli wielokąt na dwa wielokąty: $H_1 = A_1A_2 \ldots A_m$ i $H_2 = A_mA_{m+1} \ldots A_nA_1$. Punkt P nie może leżeć na przekątnej, gdyż $B_1 \neq A_m$. Jeśli P leży wewnątrz H_2, to punkty $B_1, B_2, \ldots, B_m$ leżą na $m-1$ odcinkach będących jednocześnie bokami wielokątów $\mathcal{F}$ i H_2, zatem któryś z boków $\mathcal{F}$ zawiera dwa punkty B_i – sprzeczność. Następujący rysunek pokazuje, że dziewięciokąt wypukły nie musi być zbalansowany, gdyż punkt P powinien znaleźć się w części wspólnej trzech narysowanych trójkątów.



Najpierw kilka słów uzasadnienia, a właściwie zaledwie motywacji, bo to tylko heurystyka, a nie twierdzenie matematyczne! Na każdym porządnym kursie rachunku prawdopodobieństwa dość szybko pojawia się twierdzenie zwane czasem *lematem Borela–Cantellego.*

Lemat. *Jeśli ciąg zdarzeń A_n ma tę własność, że*

$$\sum_{n=1}^{\infty} \Pr(A_n) < \infty, \tag{3}$$

to z prawdopodobieństwem 1 *zachodzi tylko skończenie wiele spośród nich.*

Również obowiązkowo na każdym wykładzie uniwersyteckim z teorii liczb pojawia się (niekoniecznie z dowodem) trudne i ważne *twierdzenie o liczbach pierwszych*:

Twierdzenie. *Jeżeli $\pi(x)$ oznacza liczbę liczb pierwszych w przedziale $[2, x]$, to:*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

„Wyprowadzimy” teraz z obu powyższych prawdziwych twierdzeń matematycznych naszą heurystykę. Niech mianowicie A_n oznacza „zdarzenie”, że x_n jest liczbą pierwszą. Oczywiście jest to wielkie udawanie, gdyż fakt bycia liczbą pierwszą nie ma nic wspólnego z losowością, np. jeśli $x_8 = 67$, to x_8 jest liczbą pierwszą, a jeśli $x_8 = 68$, to nie. Ale brnijmy dalej! Ponieważ na podstawie twierdzenia o liczbach pierwszych

$$\Pr(A_n) \approx \frac{\pi(x_n)}{x_n} \approx \frac{1}{\log x_n},$$

więc na podstawie (2) mamy (3) i stąd teza.

Chyba najsłynniejszym „zastosowaniem” wyprowadzonej przez nas heurystyki jest przypadek *liczb Fermata*:

$$F_n = 2^{2^n} + 1.$$

Założenia heurystyki są spełnione, gdyż

$$\sum_{n=1}^{\infty} \frac{1}{\log(2^{2^n}+1)} < \frac{1}{\log 2} \sum_{n=1}^{\infty} \frac{1}{2^n} < \infty.$$

Tak więc konsekwentnie wyszło nam, że liczb pierwszych Fermata jest skończenie wiele, co, jak powszechnie wiadomo, stoi w ostrej sprzeczności ze słynnym przypuszczeniem samego Fermata, że ciąg F_n zawiera wyłącznie liczby pierwsze!

O błędności przypuszczenia Fermata wiedział już Euler, który udowodnił złożoność liczby F_5. Pisał o tym Wojciech Guzicki w Δ^3_{22}.

Spróbujmy teraz zastosować heurystykę do naszego problemu. W tym celu na równanie (1) spojrzymy ogólnie i poszukamy jego wszystkich rozwiązań w liczbach naturalnych p, q. Nieskończenie wiele takich rozwiązań dają wzory

$$p_n + q_n\sqrt{2} := (1+\sqrt{2})^n, \text{ gdzie } n = 1, 3, 5, \ldots \tag{4}$$

i dość łatwo wykazać, że uzyskujemy w ten sposób wszystkie rozwiązania. Mamy zatem

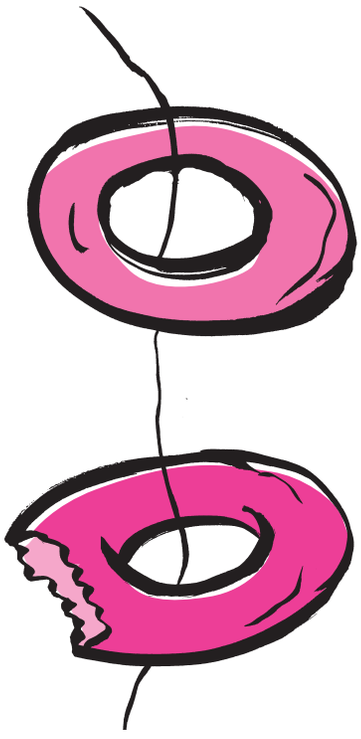
$$\begin{aligned} p_n &= \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}, \\ q_n &= \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}, \ n = 1, 3, 5, \ldots \end{aligned} \tag{5}$$

Niech teraz B_n oznacza „zdarzenie”, że obie liczby p_n, q_n są liczbami pierwszymi. Szacujemy

$$\Pr(B_n) \approx \frac{1}{\log p_n} \cdot \frac{1}{\log q_n}.$$

Skorzystaliśmy jakby z „niezależności” odpowiednich „zdarzeń”, ale jeśli p_n jest liczbą pierwszą, to raczej nie zwiększa to szansy na to, że q_n też jest liczbą pierwszą. Tak więc w powyższym możemy interpretować $\approx$ w sensie $\leqslant$. Ze wzorów (5) dostajemy teraz

$$\log p_n \approx n\log(1+\sqrt{2}), \quad \log q_n \approx n\log(1+\sqrt{2}),$$



zatem ostatecznie dla pewnej stałej C

$$\sum_n \Pr(B_n) < C \cdot \sum_n \frac{1}{n^2} < \infty,$$

co na podstawie heurystyki pozwala wnioskować, że **równanie (1) ma tylko skończenie wiele rozwiązań w liczbach pierwszych** p, q. Być może w tabelce reprodukowanej w artykule *Liczby pierwsze jako niewiadome* są wszystkie rozwiązania (?).

Jednak najważniejsze pytanie, jakie sobie teraz zadaję, jest takie: Czy teraz bardziej się Panu podoba?

Na koniec odniosę się do Pana metody rysowania stycznych do krzywej $\mathcal{K} : x^3 + y^2 = 1$. Zacznę od gratulacji: Ma Pan świetną intuicję! Przedstawiona przez Pana metoda nigdy nie zawodzi, a oto uzasadnienie.

Rozpatrywana krzywa $x^3 + y^2 = 1$ jest *eliptyczna*. Ma to szalone konsekwencje. Przede wszystkim pozwala określić sumę dwóch punktów P oraz Q naszej krzywej. Mianowicie, niech najpierw R oznacza trzeci punkt przecięcia prostej PQ z krzywą $\mathcal{K}$. Określamy

$$P \oplus Q = R', \tag{6}$$

używając Pana oznaczeń. Oczywiście w przypadku $Q = P$ zamiast prostej PQ trzeba poprowadzić styczną przez P. Ponadto do krzywej $\mathcal{K}$ dokładamy „punkt w nieskończoności" ∞, przyjmując $P \oplus \infty = P$ oraz $P \oplus P' = \infty$ dla każdego $P \in \mathcal{K}$.

Używając takiego dodawania punktów, operacje z Pana instrukcji można zakodować tak:

1. $P \oplus Q = R'$
2. $P \oplus R' = S'$
3. $S' \oplus Q' = T'$

To, że TP jest szukaną styczną, jest równoważne równości:

$$P \oplus P = T',$$

którą uzasadniamy, sumując równości 1–3, gdyż działanie dodawania punktów na krzywej $\mathcal{K}$, określone przez (6), jest przemienne, w cudowny sposób łączne i dopuszcza skracanie!

Jeśli powyższa odpowiedź zainteresowała Pana tematem krzywych eliptycznych, polecam Panu artykuł Tomasza Kazany *Krzywe eliptyczne w kryptografii* z *Delty* 8/2018. Tymczasem dziękuję za Pański list i życzę wiele radości z odkrywania matematyki.

Mariusz SKAŁBA
Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Niebo we wrześniu

We wrześniu Słońce kontynuuje szybką wędrówkę na południe, obniżając przez 30 dni miesiąca wysokość swojego górowania o ponad 11°. Przełoży się to na wydłużenie czasu trwania nocy o prawie 100 minut. Słońce przetnie w drodze na południe równik niebieski 23 września i na naszej półkuli Ziemi zacznie się astronomiczna jesień.

Głównymi wydarzeniami września w tym roku są opozycje Jowisza 26. dnia miesiąca oraz Neptuna 10 dni wcześniej. Jowisz wędruje na tle gwiazdozbioru Ryb i zbliży się do Neptuna na niecałe 10°. Ostatnia planeta od Słońca wędruje zaś na tle gwiazdozbioru Wodnika 2° na zachód od gwiazdy 20 Psc. Niestety w tym roku Jowisz nie stanie się bardzo dobrą wskazówką do odszukania Neptuna, jak to było w lipcu 2009 r., gdy obie planety na krótko dzielił dystans mniejszy niż 1°.

Obecnie przypada wielka opozycja Jowisza, gdyż 20 stycznia przyszłego roku planeta przejdzie przez peryhelium swojej orbity i w opozycji zbliży się do nas na mniej niż 4 *AU*. Jak łatwo zauważyć, w tym roku Jowisz ma największe rozmiary kątowe i jasność. Porównując te wielkości w czasie wielkiej i małej opozycji, otrzymamy znaczną różnicę. W tym roku tarcza Jowisza osiągnie średnicę kątową $50''$ i jasność $-2{,}9^m$. Podczas gdy za 6 lat w momencie opozycji planeta zbliży się do nas tylko na 5,2 *AU* i jej średnica kątowa urośnie do $44''$, jasność natomiast zwiększy się do $-2{,}5^m$.

Orbita Neptuna znacznie bardziej przypomina okrąg i położenie tej planety na orbicie podczas opozycji nie ma wpływu na wielkość i jasność jego tarczy. Neptun, jak co roku, świeci blaskiem $+7{,}8^m$ i do jego dostrzeżenia potrzebna jest jedynie lornetka.