

$k = 1$, to weryfikator uczy się tylko pewnego izomorfizmu G , a jeśli $k = 2$, to weryfikator poznaje losową permutację liczb $\{1, \dots, n\}$, zupełnie niezależną od G (bo w tym przypadku nie zna $\pi!$).

Co jeszcze?

Pokazaliśmy dwa przykłady protokołów dowodów z wiedzą zerową. Nasuwa się pytanie: jakie inne (i jak bardzo skomplikowane) stwierdzenia możemy podobnie dowodzić? Okazuje się (być może zaskakująco), że... *niemal wszystkie*. Aby się o tym przekonać, potrzebna jest pewna wiedza z teorii złożoności obliczeniowej, a konkretnie: informacja, że problem istnienia cyklu Hamiltona w grafie jest problemem NP-zupełnym. Nie jest ambicją tego artykułu, aby dokładnie wytłumaczyć to pojęcie (patrz na przykład Δ_{13}^1 , Δ_{17}^1 czy Δ_{17}^1), więc siłą rzeczy musimy w tym momencie trochę rozluźnić rygor ścisłej precyzji na rzecz intuicji.

(„Niemal wszystkie” w akapicie wyżej należy rozumieć jako „niemal wszystkie występujące w praktyce”. Dla Prawdziwych Teoretyków klasa NP to wręcz „niemal nic”.)

Otóż fakt, że problem cyklu Hamiltona (CH) jest NP-zupełny, oznacza, że dzięki temu, że pokazaliśmy protokół dowodu z wiedzą zerową dla CH, wiemy jak konstruować protokoły z wiedzą zerową dla **dowolnego innego** problemu z klasy NP! W jaki sposób? Wystarczy zastosować odpowiednią efektywną redukcję do problemu CH (która musi zawsze istnieć) i dalej stosować protokół opisany wyżej.

W szczególności: załóżmy, że udowodniliśmy hipotezę Riemanna. Rozważmy teraz język:

$$L = \{\text{zdanie prawdziwe } \phi \mid \phi \text{ ma dowód długości } \leq k\}.$$

Niewątpliwie $L \in \text{NP}$ (dlaczego?), więc dla każdego $\phi' \in L$ istnieje dowód z wiedzą zerową, w szczególności: dla $\phi' = \text{„Hipoteza Riemanna jest prawdziwa”}$.

A po ludzku: okazuje się, że istnieje graf G_{Riemann}^k (rozmiaru wielomianowego od k) taki, że jeśli hipoteza Riemanna ma dowód długości $\leq k$, to w tym grafie jest cykl Hamiltona, a jeśli nie ma takiego dowodu – to i cyklu Hamiltona w G_{Riemann}^k nie znajdziemy. Więcej: znalezienie grafu G_{Riemann}^k jest efektywnie obliczalną funkcją zdania ϕ' (zapisanego w jakiejś formalnej logice). Jeśli więc rzeczywiście znajdziemy dowód dla hipotezy Riemanna długości k i mamy nieodpartą pokusę pohandryczyć się ze światem, to możemy zawsze przedstawić wyłącznie dowód istnienia cyklu Hamiltona w grafie G_{Riemann}^k . Dowód z wiedzą zerową, rzecz jasna!

Czytelnik Spostrzegawczy zauważy, że jedną rzecz na temat naszego dowodu jednak zdradzamy – mianowicie górne oszacowanie jego długości (wynoszące k).

Czytelnik Niezłोśliwy jest zapewne w stanie uwierzyć, że dowody z wiedzą zerową są ważnym narzędziem całej kryptologii, a nie tylko jej złośliwej części. Są chociażby podstawą anonimowych kryptowalut (np. Zerocash). Inne ciekawe ich zastosowanie przedstawimy w odcinku VI naszej sagi.

Kraty

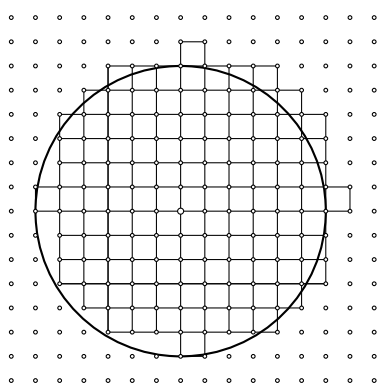
Jarosław GÓRNICKI*

* Wydział Matematyki i Fizyki
Stosowanej, Politechnika Rzeszowska

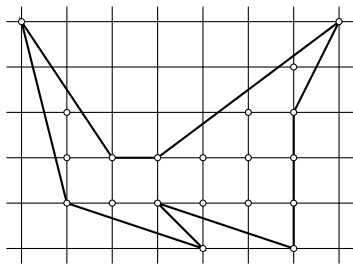
Na płaszczyźnie euklidesowej \mathbb{R}^2 zbiór $\mathbb{Z}^2 = \{(m, n) : m, n \in \mathbb{Z}\}$ nazywamy *kratką*, a jego elementy *punktami kratowymi*.

Carl Gauss zauważył, że jeśli liczba punktów kratowych w kole $x^2 + y^2 \leq r^2$ wynosi $L(r)$, to $\frac{L(r)}{r^2} \rightarrow \pi$, gdy $r \rightarrow \infty$ (rys. 1). Empirycznie wyznaczył $L(100) = 31\,417$, więc $\pi \approx 3,1417$. Precyzyjnie, Gauss pokazał, że $L(r) = \pi r^2 + E(r)$, gdzie błąd $|E(r)| \leq 2\sqrt{2}\pi r$. Do dziś nie wiemy, jakie jest najlepsze oszacowanie tego błędu.

Szybko okazało się, że kraty to ciekawy obiekt badań matematycznych. Na przykład, na płaszczyźnie łatwo wykreślić prostą, która nie przecina zbioru \mathbb{Z}^2 . Jeśli na prostej znajdują się dwa punkty kratowe, to jest ich na tej prostej nieskończenie wiele i są one rozmieszczone w równych odstępach. Istnieją też proste, które zawierają dokładnie jeden punkt kratowy. Gdyby prosta przechodząca przez punkty $(0, 0)$ i $(1, \sqrt{2})$ zawierała punkt kratowy $(m, n) \neq (0, 0)$, to z twierdzenia Talesa uzyskalibyśmy, że $\sqrt{2} = \frac{n}{m}$, a to jest niemożliwe, bo $\sqrt{2}$ jest liczbą niewymierną.



Rys. 1. Liczba $L(r)$ jest równa powierzchni pokrytej przez kwadraty jednostkowe, których dolny lewy wierzchołek leży wewnątrz lub na brzegu koła



Rys. 2. $|W| = 9 + \frac{1}{2} \cdot 11 - 1 = \frac{27}{2}$

Konsekwencją twierdzenia Blichfeldta jest sławny wynik Hermanna Minkowskiego:

Twierdzenie (H. Minkowski, 1889) *Jeżeli zbiór $M \subset \mathbb{R}^n$, $n \geq 2$, jest ograniczony, wypukły, symetryczny względem początku układu współrzędnych i o objętości większej od 2^n , to zbiór M zawiera niezerowy punkt kraty \mathbb{Z}^n .*

Analizując pola wielokątów o wierzchołkach w punktach kraty \mathbb{Z}^2 , Georg Pick wykazał niespodziewanie, że wiedza o liczbie i położeniu punktów kratowych w wielokącie określa jego pole.

Twierdzenie 1. (G. Pick, 1899) *Pole wielokąta W , którego wierzchołki są punktami kraty \mathbb{Z}^2 , a boki nie przecinają się, jest równe*

$$|W| = p_w + \frac{1}{2}p_b - 1,$$

gdzie p_w i p_b oznaczają, odpowiednio, liczbę punktów kratowych we wnętrzu i na brzegu wielokąta (rys. 2).

Jednym z istotniejszych wyników o punktach kratowych jest rezultat Hansa Blichfeldta:

Twierdzenie 2. (H. Blichfeldt, 1914) *Dla dowolnej liczby naturalnej k , dowolny zbiór ograniczony $M \subset \mathbb{R}^n$, $n \geq 2$, o objętości większej od k można tak przesunąć, by zawierał co najmniej $k + 1$ elementów kraty \mathbb{Z}^n .*

Część I. Problem i rozwiązanie

W 1957 r. Hugo Steinhaus w *Matematyce* 10 (2), str. 58–59, przedstawił kilka zadań konkursowych dotyczących kraty \mathbb{Z}^2 :

Zadanie A. *Udowodnić, że dla każdej liczby naturalnej n istnieje koło, zawierające wewnątrz dokładnie n punktów kratowych.*

Zadanie B. *Znaleźć największe koło zawierające wewnątrz dokładnie:*

- (a) 0 punktów kratowych, (b) 1 punkt kratowy, (c) 2 punkty kratowe, (d) 3 punkty kratowe, (e) 4 punkty kratowe, (f) 5 punktów kratowych. *Podać średnice tych kół.*

Zadanie C. *Największe koło zawierające wewnątrz dokładnie 4 punkty kratowe można tak przesunąć, żeby wewnątrz miało dokładnie 9 punktów kratowych, a także dokładnie 8 lub 7 punktów kratowych. Czy można je tak przesunąć, żeby w jego wnętrzu było dokładnie 5, 6 lub 10 punktów kratowych?*

Rozwiązania Steinhausa znajdzie Czytelnik w książce *Jeszcze 105 zadań Hugona Steinhausa* opracowanej przez Edwarda Piegata, Oficyna Wydawnicza GiS, Wrocław 2000.

Rozwiązanie Zadania A podał też Waclaw Sierpiński w czasopiśmie *L'Enseignement Mathématique* (2) 4 (1958), str. 25–31. Pomysł Sierpińskiego opierał się na następującej obserwacji:

każde dwa różne punkty kraty \mathbb{Z}^2 mają różne odległości od punktu $w = \left(\sqrt{2}, \frac{1}{3}\right)$, tj. nie ma okręgu o tym środku przechodzącego przez dwa lub więcej punktów kraty.

Istotnie, niech $a = (a_x, a_y)$, $b = (b_x, b_y) \in \mathbb{Z}^2$ i $a \neq b$. Jeżeli $|a - w| = |b - w|$, to

$$(a_x - \sqrt{2})^2 + \left(a_y - \frac{1}{3}\right)^2 = (b_x - \sqrt{2})^2 + \left(b_y - \frac{1}{3}\right)^2,$$

czyli

$$a_x^2 + a_y^2 - b_x^2 - b_y^2 - \frac{2}{3}(a_y - b_y) = 2(a_x - b_x)\sqrt{2}.$$

Prawa strona jest więc liczbą wymierną, zatem $a_x = b_x$, ale wówczas

$$a_y^2 - b_y^2 - \frac{2}{3}(a_y - b_y) = (a_y - b_y) \left(a_y + b_y - \frac{2}{3}\right) = 0.$$

Jest to możliwe jedynie, gdy $a_y = b_y$. Zatem $a = b$, sprzeczność.

Rozwiązanie Sierpińskiego. Krata \mathbb{Z}^2 jest zbiorem przeliczalnym, więc korzystając z powyższej obserwacji, wszystkie jej elementy możemy ustawić w ciąg $\mathbb{Z}^2 = \{a_1, a_2, a_3, \dots\}$ tak, że

$$|a_i - w| < |a_{i+1} - w| \quad \text{dla } i = 1, 2, \dots$$

Wówczas koło otwarte

$$\{x \in \mathbb{R}^2 : |x - w| < |a_{n+1} - w|\}$$

zawiera wszystkie punkty kratowe a_1, a_2, \dots, a_n i żadnych innych. *Voilà!*



Wiele punktów może pełnić rolę środka koła w twierdzeniu Sierpińskiego, ale żaden z nich nie może mieć obu współrzędnych wymiernych. Jeśli

$\bar{w} = \left(\frac{p}{q}, \frac{r}{q}\right)$, to punkty kratowe $(r, -p)$

i $(-r, p)$ są tak samo odległe od punktu \bar{w} , gdyż

$$\begin{aligned} \left(r - \frac{p}{q}\right)^2 + \left(-p - \frac{r}{q}\right)^2 &= \\ &= \left(-r - \frac{p}{q}\right)^2 + \left(p - \frac{r}{q}\right)^2. \end{aligned}$$

Wówczas, jeśli we wnętrzu takiego koła o środku \bar{w} jest n punktów kratowych, to żadne koło o środku w punkcie \bar{w} nie zawiera $n + 1$ punktów kratowych.

Mamy więc:

Twierdzenie 3. Dla każdej liczby naturalnej n istnieje koło o środku $\left(\sqrt{2}, \frac{1}{3}\right)$, którego wnętrze zawiera dokładnie n punktów kratowych.

Podobne rozumowanie (szczegóły pozostawiamy Czytelnikom) pokazuje, że dla każdej liczby naturalnej n istnieje kula o środku w punkcie $\left(\sqrt{2}, \sqrt{3}, \frac{1}{3}\right)$

zawierająca wewnątrz dokładnie n punktów kraty \mathbb{Z}^3 .

Część II. Pokłosie

Naturalne jest pytanie o istnienie okręgów przechodzących dokładnie przez n punktów kraty \mathbb{Z}^2 . Łatwo rysujemy okręgi przechodzące przez 1, 2, 3, 4 punkty kratowe. A jak jest dla większej liczby punktów kratowych?

W 1958 r. Andrzej Schinzel, korzystając z twierdzenia teorii liczb: *liczba $r(n)$ rozwiązań równania $x^2 + y^2 = n$ w liczbach całkowitych (= ilość rozkładów liczby naturalnej n na sumę kwadratów dwóch liczb całkowitych) jest równa $4(d_1 - d_2)$, gdzie d_1 jest liczbą dzielników liczby n postaci $4k + 1$, a d_2 jest liczbą dzielników liczby n postaci $4k + 3$ (dowód w tym numerze, w artykule Michała Krycha), udowodnił:*

Twierdzenie 4. (A. Schinzel, 1958) Dla każdej liczby naturalnej n na okręgu opisanym równaniem

$$\begin{cases} \left(x - \frac{1}{2}\right)^2 + y^2 = \frac{1}{4}5^{k-1} & \text{dla } n = 2k, \\ \left(x - \frac{1}{3}\right)^2 + y^2 = \frac{1}{9}5^{2k} & \text{dla } n = 2k + 1 \end{cases}$$

leży dokładnie n punktów kraty \mathbb{Z}^2 .

Korzystając z rezultatu Schinzla, Tadeusz Kulikowski wykazał:

Twierdzenie 5. (T. Kulikowski, 1959) Dla każdej liczby naturalnej n istnieje sfera, która zawiera dokładnie n punktów kraty \mathbb{Z}^3 .

Dowód. Ustalmy $n \in \mathbb{N}$. Z twierdzenia Schinzla na płaszczyźnie $z = 0$ istnieje okrąg $(x - a)^2 + (y - b)^2 = c$, na którym leży dokładnie n punktów $(x, y, 0) \in \mathbb{Z}^3$.

Rozważmy sferę o środku w punkcie $(a, b, \sqrt{2})$ i promieniu $\sqrt{c + 2}$, gdzie $a = \frac{1}{2}$ lub $\frac{1}{3}$, $b = 0$, a c to kwadrat odpowiedniego promienia z twierdzenia 4:

$$(*) \quad (x - a)^2 + (y - b)^2 + (z - \sqrt{2})^2 = c + 2,$$

$$\text{skąd} \quad (x - a)^2 + y^2 + z^2 - c = 2z\sqrt{2}.$$

Liczby całkowite x, y, z mogą spełniać to równanie tylko wtedy, gdy $z = 0$. Oznacza to, że wszystkie punkty $(x, y, z) \in \mathbb{Z}^3$ leżące na sferze $(*)$ leżą na przecięciu tej sfery z płaszczyzną $z = 0$. Zatem jedyne punkty kratowe na sferze $(*)$ to n punktów kratowych należących do okręgu Schinzla. \square

W tym samym czasie Jerzy Browkin zauważył, że funkcja

$$f(a) = \left|a_x + a_y\sqrt{3} - \frac{1}{3}\right| + \left|a_x\sqrt{3} - a_y - \frac{1}{\sqrt{3}}\right|,$$

(gdzie $a = (a_x, a_y) \in \mathbb{Z}^2$) przyjmuje różne wartości dla każdego dwóch różnych punktów kraty \mathbb{Z}^2 , oraz dowiódł, że dla każdej liczby naturalnej n :

- istnieje kwadrat zawierający wewnątrz (odpowiednio: na brzegu) dokładnie n punktów kraty \mathbb{Z}^2 ,

- istnieje sześcián zawierający wewnątrz dokładnie n punktów kraty \mathbb{Z}^3 .

Podobne problemy można rozważać dla figur o innych kształtach – trójkątów, elips. Oczywiście największe zainteresowanie budzą problemy, które mimo wysiłków nadal pozostają bez odpowiedzi.

Problem 1. Czy istnieje prostopadłościan, którego krawędzie, przekątne ścian, przekątna wewnętrzna mają długości całkowite?

Historia tego problemu sięga 1719 roku, gdy Paul Halcke wskazał prostopadłościan $44 \times 117 \times 240$, którego przekątne ścian też są całkowitej długości.

Problem 2. (H. Steinhaus) Czy istnieje taki podzbiór A płaszczyzny, że każdy zbiór przystający do A zawiera dokładnie jeden punkt kratowy?

Spacer po kracie \mathbb{Z} , \mathbb{Z}^2 lub \mathbb{Z}^3 polegający na tym, że w każdym kolejnym kroku przechodzimy o jedną jednostkę do sąsiedniego punktu kratowego (mając równe szanse poruszania się w każdym możliwym kierunku) nazywamy *symetrycznym błędzeniem przypadkowym*. George Pólya pokazał w 1921 roku, że w przypadku takiego błędzenia w kracie \mathbb{Z} lub \mathbb{Z}^2 z prawdopodobieństwem równym 1 powrócimy do położenia początkowego. W kracie \mathbb{Z}^3 prawdopodobieństwo to wynosi około 0,35. Tak więc naprawdę zabłądzić możemy w kratach \mathbb{Z}^n , gdzie $n \geq 3$, ale to temat na inne spotkanie.