Szereg Leibniza i punkty kratowe

*Michał KRYCH**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Niniejszy artykuł został napisany w oparciu o „Geometrię poglądową” Davida Hilberta i Stefana Cohn-Vossena. To wspaniała książka napisana przez jednego z najwybitniejszych matematyków w historii, na podstawie wykładów Hilberta przy udziale jego ucznia. Nieco zapomniana; dostępna również w języku polskim.

Powiążemy tu wzór Leibniza

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \ldots$$

z geometrią (pola) i teorią liczb. Tekst jest wyraźnie dłuższy od tego, który jest w książce Hilberta i Cohn-Vossena, bo szkicujemy dowód twierdzenia z teorii liczb, na które autorzy jedynie powołują się. Pozostawimy jednak bez dowodu niektóre bardzo znane twierdzenia z teorii liczb, ze względu na ograniczenia miejsca w miesięczniku. Zaznaczyć warto, że podawany zwykle studentom pierwszego roku dowód jest krótszy, ale zdaniem autora tego tekstu, nie pokazuje związku z geometrią, który jest mocno sugerowany obecnością π we wzorze.

Używać będziemy liczb zespolonych. Jak zwykle $i^2 = -1$. Symbol $\mathbb{Z}[i]$ oznacza zbiór liczb zespolonych, których części rzeczywista i urojona są całkowite. Liczby te nazywane są też *punktami kratowymi.*

Istotny dla dalszych rozważań jest fakt:
liczba całkowita n większa od 1 jest sumą kwadratów dwu liczb całkowitych wtedy i tylko wtedy, gdy jest iloczynem dwu sprzężonych elementów $\mathbb{Z}[i]$, o modułach większych od 1, co wynika z równości $n = x^2 + y^2 = (x + yi)(x - yi)$.

W $\mathbb{Z}[i]$ można zajmować się dzieleniem liczb nieomal tak, jak w zbiorze liczb całkowitych. Liczba $z_1 \in \mathbb{Z}[i]$ jest dzielnikiem liczby $z_2 \in \mathbb{Z}[i]$ wtedy i tylko wtedy, gdy istnieje taka liczba $q \in \mathbb{Z}[i]$, że $z_2 = qz_1$. Liczba $1 + i$ jest dzielnikiem liczby 2, bo $2 = (1 - i)(1 + i)$. Jedynymi dzielnikami jedności w $\mathbb{Z}[i]$, czyli dzielnikami liczby 1, są ± 1 oraz $\pm i$, bo z równości $1 = qz_1$ wynika, że $1 = |q|^2|z_1|^2$, i z tego że $q, z_1 \in \mathbb{Z}[i]$ wynika, że $|q|^2 = 1 = |z_1|^2$, a jeśli $x, y \in \mathbb{Z}$ i $x^2 + y^2 = 1$, to $xy = 0$. *Liczbę pierwszą* w $\mathbb{Z}[i]$ można zdefiniować jako taką, której jedynymi dzielnikami są dzielniki jedności oraz ona sama pomnożona przez jeden z dzielników jedności, ale sama nie jest dzielnikiem jedności. Wtedy $2 = (1 - i)(1 + i)$ nie jest liczbą pierwszą, ale 3 już jest (Czytelniku: dlaczego?). Prawdziwe jest, jak w przypadku podzielności w $\mathbb{Z}$,

Twierdzenie (o jednoznaczności rozkładu na czynniki pierwsze)**.** *Jeśli $z \in \mathbb{Z}[i]$ nie jest dzielnikiem jedności, to istnieją liczby pierwsze $p_1, p_2, \ldots, p_k \in \mathbb{Z}[i]$ takie, że $z = p_1p_2\ldots p_k$. Jeśli liczby $\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_\ell \in \mathbb{Z}[i]$ są pierwsze i $z = \tilde{p}_1\tilde{p}_2\ldots\tilde{p}_\ell$, to $k = \ell$ i po ewentualnej zmianie numeracji ilorazy $\frac{p_j}{\tilde{p}_j}$ są dzielnikami jedności w $\mathbb{Z}[i]$.*

Dowód można oprzeć na następującym, nietrudnym do uzasadnienia, fakcie.

Twierdzenie (o dzieleniu z resztą w $\mathbb{Z}[i]$)**.** *Dla dowolnych liczb $w, z \in \mathbb{Z}[i]$, $z \neq 0$ istnieją liczby $\kappa, \varrho \in \mathbb{Z}[i]$ takie, że $w = \kappa z + \varrho$ i $|\varrho| < |z|$. Liczbę κ nazywamy ilorazem,* a *ϱ resztą* z dzielenia liczby w przez liczbę z.

Iloraz i reszta **nie** są zdefiniowane jednoznacznie: $3 = (1 - i)(1 + i) + 1 = (2 - i)(1 + i) - i$, więc resztą z dzielenia 3 przez $1 + i$ jest zarówno 1 jak i $-i$, ilorazami są odpowiednio $1 - i$ oraz $2 - i$.

Obecność π we wzorze Leibniza sugeruje, że w którymś momencie naszych rozważań powinien pojawić się okrąg.

Twierdzenie (o podwajaniu sumy kwadratów)**.** *Na okręgu o promieniu $\sqrt{m}$ i środku 0 znajduje się tyle samo punktów kratowych, co na okręgu o promieniu $\sqrt{2m}$ i środku 0.*

Dowód. Jeśli $m = a^2 + b^2 = (a + bi)(a - bi)$, to

$$2m = (1 + i)(1 - i)(a + bi)(a - bi) = (1 + i)(a - bi)(1 - i)(a + bi) =$$
$$= \big((a + b) + (a - b)i\big)\big((a + b) - (a - b)i\big) = (a + b)^2 + (a - b)^2.$$

Jeśli zaś $2m = c^2 + d^2$, to obie liczby c, d są parzyste albo obie są nieparzyste. W obu sytuacjach liczby $a = \frac{c+d}{2}$ i $b = \frac{c-d}{2}$ są całkowite i oczywiście $a^2 + b^2 = = \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = m$. Innymi słowy, przypisując każdemu punktowi kratowemu (a, b) punkt $(a + b, a - b) = (c, d)$, określamy różnowartościowe przekształcenie zbioru wszystkich punktów kratowych **na** zbiór wszystkich punktów kratowych, których obydwie współrzędne dają tę samą resztę z dzielenia przez 2. Przy tym punktom z okręgu o promieniu $\sqrt{m}$ przypisywane są punkty z okręgu o promieniu $\sqrt{2m}$. $\square$

Z tego twierdzenia wynika, że liczba punktów kratowych na okręgu o środku w punkcie 0 i promieniu $r > 0$ zależy wyłącznie od nieparzystych dzielników pierwszych liczby r^2. Opiszemy teraz w kilku krokach, w jaki sposób.

Twierdzenie. *Każda liczba pierwsza $p \in \mathbb{Z}$, która z dzielenia przez 4 daje resztę 1, jest sumą kwadratów dwu liczb całkowitych.*

Liczne dowody tego twierdzenia, sformułowanego przez Pierre'a de Fermata, znajdują się w wielu podręcznikach do teorii liczb oraz, rzecz jasna, w *Delcie* (artykuł *Jedno zdanie* Wojciecha Czerwińskiego, numer 7/2017).

Zauważmy, że z twierdzenia o jednoznaczności rozkładu w $\mathbb{Z}$ wynika, że jeśli $p = x^2 + y^2$ jest liczbą pierwszą w $\mathbb{Z}$ i $x, y \in \mathbb{Z}$, to liczba $x + yi$ jest pierwsza w $\mathbb{Z}[i]$ i wybór liczb $x, y \in \mathbb{Z}$ jest jednoznaczny z dokładnością do pomnożenia liczby $x + yi$ przez ± 1 lub $\pm i$ oraz zmiany kolejności składników. Oznacza to, że jeśli $p = 4m + 1$ $(m \in \mathbb{Z})$ jest liczbą pierwszą w $\mathbb{Z}$, to na okręgu o promieniu $\sqrt{p}$ znajduje się 8 punktów kratowych.

Ponieważ kwadrat liczby całkowitej daje z dzielenia przez 4 (w $\mathbb{Z}$) resztę 0 lub 1, więc liczby postaci $4m + 3$, $m \in \mathbb{Z}$ nie są sumami dwóch kwadratów. Stąd wynika, że liczby pierwsze postaci $4m + 3$ są również pierwsze w $\mathbb{Z}[i]$. Co najmniej jeden z dowodów tego faktu wykorzystuje następujący lemat:

Lemat (o liczbach pierwszych, które są sumami dwóch kwadratów)**.** *Jeśli liczba pierwsza $p > 2$ jest dzielnikiem sumy kwadratów liczb całkowitych niepodzielnych przez p, to sama też jest sumą kwadratów liczb całkowitych.*

Dowód tego lematu zajmuje kilka wierszy, ale go opuszczamy. Z tego lematu wynika:

Wniosek (o dzielnikach pierwszych sumy kwadratów dwu liczb całkowitych)**.** Jeśli liczba n jest sumą dwóch kwadratów liczb całkowitych, to każdy jej dzielnik pierwszy postaci $4m + 3$ wchodzi w jej rozkład na czynniki pierwsze z parzystym wykładnikiem.

Lemat (o liczbie dzielników liczby bez dzielników pierwszych postaci $4m + 1$)**.** *Jeśli $n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_\ell^{\beta_\ell}$ i $q_1, q_2, q_3, \ldots, q_\ell$ są liczbami pierwszymi postaci $4m + 3$, a $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ są dodatnimi liczbami całkowitymi, to:*

- *jeśli wszystkie liczby $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ są parzyste, to liczba dzielników naturalnych postaci $4m + 1$ liczby n jest większa o 1 od liczby jej dzielników postaci $4m + 3$;*
- *jeśli co najmniej jedna z liczb $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ jest nieparzysta, to liczba dzielników naturalnych postaci $4m + 1$ liczby n jest równa liczbie jej dzielników postaci $4m + 3$.*

Dowód. Iloczyn dowolnie wielu liczb postaci $4m + 1$ jest też liczbą tej postaci. Podobnie iloczyn parzystej liczby czynników postaci $4m + 3$. Natomiast iloczyn nieparzystej liczby czynników postaci $4m + 3$ jest liczbą postaci $4m + 3$.

Jeśli $2 \mid \beta_j$, to dzielnikami liczby $q_j^{\beta_j}$ postaci $4m + 1$ są liczby $q_j^0, q_j^2, \ldots, q_j^{\beta_j}$, więc jest ich $1 + \frac{\beta_j}{2}$. Dzielnikami postaci $4m + 3$ są liczby $q_j, q_j^3, \ldots, q_j^{\beta_j - 1}$, więc jest ich $\frac{\beta_j}{2}$.

Jeśli $2 \nmid \beta_j$, to dzielnikami liczby $q_j^{\beta_j}$ postaci $4m + 1$ są liczby $q_j^0, q_j^2, \ldots, q_j^{\beta_j - 1}$, więc jest ich $\frac{1+\beta_j}{2}$. Dzielnikami postaci $4m + 3$ są liczby $q_j, q_j^3, \ldots, q_j^{\beta_j}$, więc jest ich $\frac{1+\beta_j}{2}$.

Poprzednie dwa akapity uzasadniają tezę dowodzonego lematu dla $\ell = 1$.

Rozwiązanie zadania F 967.
Układ połączonych baterii stanowi źródło o pewnej wypadkowej sile elektromotorycznej $\mathcal{E}$ i oporze wewnętrznym R_w. W przypadku (a) $\mathcal{E} = n\mathcal{E}_0$, $R_w = nr_w$, a w przypadku (b) $\mathcal{E} = \mathcal{E}_0$, $R_w = r_w/n$. Moc P wydzielana na oporze R dołączonym do źródła o danych $\mathcal{E}$ i R_w wynosi:

$$P = \frac{\mathcal{E}^2 R}{(R + R_w)^2}.$$

Przy danym R_w moc P osiąga maksimum dla $R = R_w$. W przypadku (a) należy więc do układu baterii podłączyć opór $R = nr_w$, a w przypadku (b) $R = r_w/n$. Jak łatwo sprawdzić, moc wydzielana na optymalnie dobranym oporze R, w obu przypadkach wynosi tyle samo:

$$P = \frac{n\mathcal{E}_0^2}{4r_w}.$$

Także prąd płynący przez każdą z n baterii i moc wydzielana na oporze wewnętrznym każdej z nich są w obu przypadkach takie same.

Rozwiązanie zadania F 968.
W jednorodnym polu magnetycznym ruch naładowanej cząstki jest złożeniem ruchu jednostajnego wzdłuż kierunku pola i ruchu po okręgu ze stałą prędkością kątową $\omega = 2\pi f$. Siłą dośrodkową jest tu siła Lorentza. Mamy więc:

$$m\omega^2 r = q\omega r B,$$

gdzie r jest promieniem okręgu, $B = |\vec{B}|$, a ωr jest wartością składowej prędkości prostopadłej do wektora indukcji $\vec{B}$. Otrzymujemy więc $\omega = qB/m$, czyli:

$$f = \frac{qB}{2\pi m}.$$

Częstotliwość f nie zależy od kierunku i wartości prędkości cząstki. Fakt ten wykorzystywany jest do wyznaczania efektywnych mas nośników prądu (elektronów i dziur) w półprzewodnikach.

Rozwiązanie zadania M 1588.
Rozważmy funkcję $g(x) = f(x) - x^2$. Wówczas

$$g(x+1) - g(x) = \\ = f(x+1) - f(x) - (x+1)^2 + x^2 = 0,$$

wobec czego funkcja $g(x)$ jest okresowa z okresem 1. Skoro $|f(x)| \leqslant 1$ dla $x \in [0,1]$, to

$$|g(x)| = |f(x) - x^2| \leqslant |f(x)| + x^2 \leqslant 2$$

dla $x \in [0,1]$ i w konsekwencji, wobec okresowości $g(x)$, $|g(x)| \leqslant 2$ dla każdego $x \in \mathbb{R}$. Stąd ostatecznie

$$|f(x)| = |g(x) + x^2| \leqslant |g(x)| + x^2 \leqslant x^2 + 2,$$

co było do udowodnienia.

Rozwiązanie zadania M 1589.
Przypuśćmy, że każda osoba w danej grupie ma co najwyżej czterech znajomych. Wówczas łączna liczba relacji znajomości w tej grupie nie przekracza

$$\frac{8 \cdot 4}{2} = 16.$$

Tymczasem, w myśl warunków zadania, w każdej z $\binom{8}{5} = 56$ piątek osób są co najmniej trzy znajomości, a każda taka trójka znających się nawzajem osób należy do dokładnie $\binom{8-3}{2} = 10$ piątek osób. Wobec tego łączna liczba znajomości w grupie jest nie mniejsza od

$$\frac{3 \cdot 56}{10} = 16{,}8.$$

Uzyskana sprzeczność oznacza, że w danej grupie musi istnieć osoba, nazwijmy ją A, która ma co najmniej 5 znajomych. Aby zakończyć rozwiązanie, wystarczy stwierdzić, że wśród znajomych osoby A pewnych trzech zna się wzajemnie, więc dołączając do nich A, otrzymujemy czwórkę osób o postulowanej własności.

Rozwiązanie zadania M 1590.
Odpowiedź: Największa możliwa liczba elementów zbioru T jest równa $2n$.

Przyjmując

$$T = \{n+1, n+2, \ldots, 3n\},$$

mamy $|T| = 2n$ oraz suma każdych trzech elementów T jest większa od $3n$, a zatem nie należy do T.

Z drugiej strony, zbiory $S_0 = \{n, 2n, 3n\}$ oraz

$$S_k = \{k, 2n-k, 2n+k\}$$

(dla $k = 1, 2, \ldots, n-1$) stanowią rozbicie zbioru S, a w każdym z nich jeden z elementów jest sumą trzech innych, mianowicie

$$3n = n + n + n$$

oraz

$$2n + k = k + k + 2n - k.$$

Pozostaje zauważyć, że jeżeli $T \subseteq S$ oraz $|T| \geqslant 2n+1$, to $S_k \subseteq T$ dla pewnego k i w konsekwencji zbiór T nie ma danej w treści zadania własności.

Załóżmy, że liczba $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_{\ell-1}^{\beta_{\ell-1}}$ ma $a_{\ell-1}$ dzielników postaci $4m+1$ oraz $b_{\ell-1}$ dzielników postaci $4m+3$.

Jeśli $2 \mid \beta_\ell$, to liczba $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_\ell^{\beta_\ell}$ ma $a_\ell = a_{\ell-1} \cdot \left(1 + \frac{\beta_\ell}{2}\right) + b_{\ell-1} \cdot \frac{\beta_\ell}{2}$ dzielników postaci $4m+1$ oraz $b_\ell = a_{\ell-1} \cdot \frac{\beta_\ell}{2} + b_{\ell-1} \cdot \left(1 + \frac{\beta_\ell}{2}\right)$ dzielników postaci $4m+3$. Zachodzi równość $a_\ell - b_\ell = a_{\ell-1} \cdot \left(1 + \frac{\beta_\ell}{2}\right) + b_{\ell-1} \cdot \frac{\beta_\ell}{2} - a_{\ell-1} \cdot \frac{\beta_\ell}{2} - b_{\ell-1} \cdot \left(1 + \frac{\beta_\ell}{2}\right) = a_{\ell-1} - b_{\ell-1}$.

Jeśli $2 \nmid \beta_\ell$, to liczba $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_\ell^{\beta_\ell}$ ma $a_\ell = a_{\ell-1} \cdot \frac{1+\beta_\ell}{2} + b_{\ell-1} \cdot \frac{1+\beta_\ell}{2}$ dzielników postaci $4m+1$ oraz $b_\ell = a_{\ell-1} \cdot \frac{1+\beta_\ell}{2} + b_{\ell-1} \cdot \frac{1+\beta_\ell}{2}$ dzielników postaci $4m+3$. Zachodzi więc równość $a_\ell - b_\ell = 0$.

Teza lematu wynika z powyższych rozważań natychmiast – prosta indukcja. □

Twierdzenie (o liczbie dzielników nieparzystych)**.** *Niech* $n = 2^\gamma \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_\ell^{\beta_\ell}$*, gdzie* $p_1, p_2, \ldots, p_k$ *są liczbami pierwszymi postaci* $4m+1$*, liczby* $q_1, q_2, \ldots, q_\ell$ *są liczbami pierwszymi postaci* $4m+3$*,* $m \geqslant 0$*, a wykładniki* $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k$*,* $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ *są dodatnimi liczbami całkowitymi. Wtedy:*

- *jeśli co najmniej jeden z wykładników* $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ *jest nieparzysty, to* n *ma tyle samo dzielników postaci* $4m+1$*, co dzielników postaci* $4m+3$*;*
- *jeżeli wszystkie wykładniki* $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ *są podzielne przez 2, to liczba* n *ma o* $\alpha := (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\ldots(\alpha_k+1)$ *więcej dzielników postaci* $4m+1$ *niż dzielników postaci* $4m+3$*.*

Dowód. Nieparzyste dzielniki liczby n są iloczynami dzielników liczb $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k}$ i $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdot \ldots \cdot q_\ell^{\beta_\ell}$. W pierwszej grupie jest $\alpha = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\ldots(\alpha_k+1)$ liczb. Każda z nich jest postaci $4m+1$. W drugiej grupie jest ϱ_1 liczb postaci $4m+1$ i ϱ_3 liczb postaci $4m+3$. Z lematu poprzedzającego dowodzone twierdzenie wynika, że jeśli co najmniej jeden wykładnik spośród $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ jest nieparzysty, to $\varrho_1 = \varrho_3$, więc również $\alpha \cdot \varrho_1 = \alpha \cdot \varrho_3$, co dowodzi pierwszej części tezy. Jeśli wszystkie liczby $\beta_1, \beta_2, \beta_3, \ldots, \beta_\ell$ są parzyste, to $\varrho_1 = \varrho_3 + 1$, więc $\alpha \cdot \varrho_1 = \alpha \cdot \varrho_3 + \alpha$, a to oznacza, że druga część tezy też jest prawdziwa. □

Teraz przyjrzyjmy się dwu liczbom: 2100 i 74529000. Znajdziemy liczbę punktów kratowych na okręgach o promieniach $\sqrt{2100}$ i $\sqrt{74529000}$ oraz powiążemy ją z liczbą nieparzystych dzielników każdej z tych liczb. Po tych przykładach pojawi się twierdzenie ogólne, którego dowód jest w zasadzie powtórzeniem rozumowania w tych szczególnych przypadkach, więc go opuszczamy.

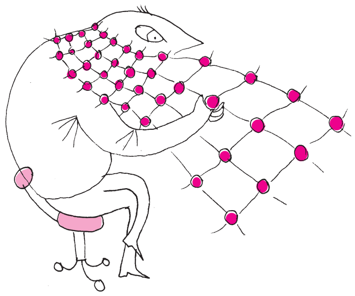
Liczba $2^2 \cdot 5^2 \cdot 3 \cdot 7 = 2100$ nie jest sumą kwadratów dwu liczb całkowitych, bo w jej rozkładzie na czynniki pierwsze występuje liczba postaci $4m+3$ z nieparzystym wykładnikiem (3 lub 7). W tej sytuacji na okręgu o promieniu $\sqrt{2100}$ nie ma punktów kratowych. Zwróćmy uwagę, że 2100 ma 6 dzielników postaci $4m+1$ (są to 1, 5, 5^2, $3 \cdot 7$, $3 \cdot 7 \cdot 5$, $3 \cdot 7 \cdot 5^2$) i tyle samo dzielników postaci $4m+3$ (są to 3, $3 \cdot 5$, $3 \cdot 5^2$, 7, $7 \cdot 5$, $7 \cdot 5^2$).

A teraz przyjrzyjmy się liczbie $2^3 \cdot 5^3 \cdot 13^2 \cdot 3^2 \cdot 7^2 = 74529000$. Liczba $5^3 \cdot 13^2$ ma $4 \cdot 3 = 12$ dzielników, wszystkie postaci $4m+1$. Liczba $3^2 \cdot 7^2 = 441$ ma $3 \cdot 3 = 9$ dzielników, pięć z nich jest postaci $4m+1$ (są to: 1, 3^2, $3 \cdot 7$, 7^2 i $3^2 \cdot 7^2$), pozostałe cztery są postaci $4m+3$ (są to: 3, 7, $3^2 \cdot 7$ i $3 \cdot 7^2$). Liczba $2^3 \cdot 5^3 \cdot 13^2 \cdot 3^2 \cdot 7^2 = 74529000$ ma więc $12 \cdot 5 = 60$ dzielników postaci $4m+1$ oraz $12 \cdot 4 = 48$ dzielników postaci $4m+3$. Na okręgu o promieniu $2\sqrt{2} \cdot 5\sqrt{5} \cdot 13 \cdot 3 \cdot 7$ leży $4 \cdot (60-48) = 48$ punktów kratowych, co teraz udowodnimy. Z twierdzenia o podwajaniu sumy kwadratów wynika, że na tym okręgu leży tyle samo punktów kratowych, co na okręgu o promieniu $5\sqrt{5} \cdot 13 \cdot 3 \cdot 7$. Mamy

$$5^3 \cdot 13^2 \cdot 3^2 \cdot 7^2 = (2+i)^3 \cdot (2-i)^3 \cdot (2+3i)^2 \cdot (2-3i)^2 \cdot 3^2 \cdot 7^2.$$

Załóżmy, że $(x+yi)(x-yi) = x^2 + y^2 = 5^3 \cdot 13^2 \cdot 3^2 \cdot 7^2$ oraz $x, y \in \mathbb{Z}$.

Z twierdzenia o jednoznaczności rozkładu, równości $|x+yi| = |x-yi|$ i tego, że sprzężenie iloczynu to iloczyn sprzężeń, wynika, że liczba $x+yi$ jest iloczynem postaci $i^b (2+i)^{a_1} \cdot (2-i)^{3-a_1} \cdot (2+3i)^{a_2} \cdot (2-3i)^{2-a_2} \cdot 3 \cdot 7$, gdzie $b \in \{0,1,2,3\}$,



$a_1 \in \{0,1,2,3\}$ i $a_2 \in \{0,1,2\}$. Jest więc tych liczb 48. Okazuje się, że podobne rozumowanie można przeprowadzić dla każdej dodatniej liczby całkowitej n, otrzymując następujące:

Twierdzenie (o liczbie punktów kratowych na okręgu o promieniu $\sqrt{n}$)**.** *Liczba punktów kratowych leżących na okręgu o promieniu $\sqrt{n}$ jest równa pomnożonej przez 4 różnicy między liczbą dodatnich dzielników postaci $4m+1$ liczby całkowitej $n > 0$ i liczbą dodatnich dzielników postaci $4m+3$ liczby n.*

Niech $N(r)$ oznacza liczbę punktów kratowych w kole $K(r)$ o środku $(0,0)$ i promieniu $r > 0$, więc o polu πr^2. Kwadraty, dla których te punkty są wierzchołkami lewymi dolnymi nieomal pokrywają koło, choć tu i ówdzie za nie wystają. Sumą ich pól jest oczywiście $N(r)$. Kwadrat, który ma punkty wspólne z kołem $K(r)$, ale w tym kole nie jest zawarty, mieści się w różnicy kół $K(r+\sqrt{2})$ i $K(r-\sqrt{2})$, więc w pierścieniu o polu $\pi(r+\sqrt{2})^2 - \pi(r-\sqrt{2})^2 = 4\pi r\sqrt{2}$. Wobec tego $|N(r) - \pi r^2| \leqslant 4\pi r\sqrt{2}$, więc $\left|\frac{N(r)}{r^2} - \pi\right| \leqslant \frac{4\pi\sqrt{2}}{r}$. Z otrzymanej nierówności i z twierdzenia o trzech ciągach wynika natychmiast, że

$$\text{(L)} \qquad \lim_{r\to\infty} \frac{N(r)}{r^2} = \pi.$$

Załóżmy, że $r > 10$. Wtedy liczba punktów kratowych w kole $K(r)$ jest równa sumie liczb punktów kratowych na okręgach o promieniach $\sqrt{n}$, gdzie $n \in [0, r^2]$ oznacza liczbę całkowitą. Przypomnijmy, że liczba punktów na tym okręgu jest równa różnicy liczb dzielników n postaci $4m+1$ i $4m+3$ pomnożonej przez 4. Dodajmy te liczby dla wszystkich n. Liczba 1 jest dzielnikiem $\left\lfloor \frac{r^2}{1} \right\rfloor$ liczb n, liczba 3 dzielnikiem $\left\lfloor \frac{r^2}{3} \right\rfloor$ liczb n, liczba 5 dzielnikiem $\left\lfloor \frac{r^2}{5} \right\rfloor$ liczb n, liczba 7 dzielnikiem $\left\lfloor \frac{r^2}{7} \right\rfloor$ liczb n itd. Oznacza to, że na tych wszystkich okręgach znajduje się łącznie

Przypominamy, że $\lfloor x \rfloor$ to największa liczba całkowita z półprostej $(-\infty, x]$.

$$1 + 4\left(\left\lfloor \frac{r^2}{1} \right\rfloor - \left\lfloor \frac{r^2}{3} \right\rfloor + \left\lfloor \frac{r^2}{5} \right\rfloor - \left\lfloor \frac{r^2}{7} \right\rfloor + \ldots\right) = N(r)$$

punktów kratowych (dodajemy 1, bo trzeba też uwzględnić punkt $(0,0)$). Ta suma w rzeczywistości jest skończona, bo od pewnego miejsca kolejne składniki są zerami. Wykażemy, że

$$\lim_{r\to\infty} \frac{1}{r^2}\left(\left\lfloor \frac{r^2}{1} \right\rfloor - \left\lfloor \frac{r^2}{3} \right\rfloor + \left\lfloor \frac{r^2}{5} \right\rfloor - \left\lfloor \frac{r^2}{7} \right\rfloor + \ldots\right) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$$

Niech $a_1 \geqslant a_2 \geqslant a_3 \geqslant \ldots \geqslant 0$ i $k < \ell$. Niech $s_k = a_1 - a_2 + a_3 - a_4 + \ldots + (-1)^{k-1}a_k$. Wtedy zachodzi nierówność

$$(*) \quad |s_k - s_n| = |a_1 - a_2 + a_3 - \ldots + (-1)^{k-1}a_k - \bigl(a_1 - a_2 + a_3 - \ldots + (-1)^{n-1}a_n\bigr)| \leqslant \leqslant a_{k+1}.$$

Wynika ona z nierówności

$$s_{2j} \leqslant s_{2j} + a_{2j+1} - a_{2j+2} = s_{2j+2}, \quad s_{2j+1} \geqslant s_{2j+1} - a_{2j+2} + a_{2j+3} = s_{2j+3}$$
$$s_{2j} \leqslant s_{2j} + a_{2j+1} = s_{2j+1},$$

więc $s_{2j} \leqslant s_{2j+2} \leqslant s_{2j+3} \leqslant s_{2j+1}$ dla każdego naturalnego j. Stąd w szczególności wynika, że jeśli $\lim a_n = 0$, to ciągi monotoniczne (s_{2n}) i (s_{2n+1}) mają granice, te granice są równe i wobec tego skończone.

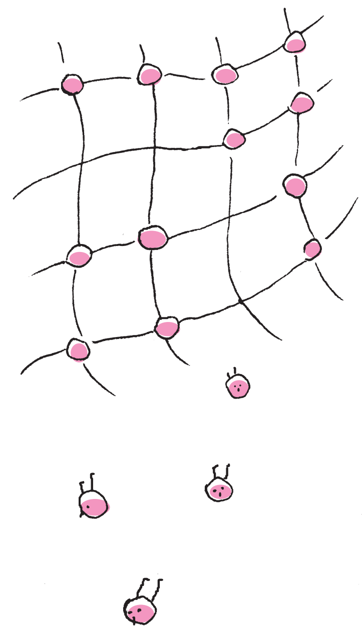
Wróćmy do wyjściowego problemu. Niech s będzie taką liczbą naturalną, że $2s+1 \leqslant r < 2s+3$, oczywiście dla różnych r otrzymujemy różne liczby s, w każdym razie niekoniecznie takie same. Liczba r wyznacza s jednoznacznie (s jest funkcją r). Mamy $\lim\limits_{r\to\infty} \frac{s}{r^2} = 0$, bo $0 < \frac{s}{r^2} < \frac{2s+1}{r^2} \leqslant \frac{1}{r}$.

Zachodzą oczywiste nierówności:

$$\left\lfloor \frac{r^2}{1} \right\rfloor \geqslant \left\lfloor \frac{r^2}{3} \right\rfloor \geqslant \left\lfloor \frac{r^2}{5} \right\rfloor \geqslant \left\lfloor \frac{r^2}{7} \right\rfloor \geqslant \ldots$$

Z nierówności $(*)$ wynika, że kończąc dodawanie na składniku $(-1)^s\left\lfloor \frac{r^2}{2s+1} \right\rfloor$ popełniamy błąd, którego moduł jest mniejszy od $\left\lfloor \frac{r^2}{2s+3} \right\rfloor < \frac{r^2}{r} = r$. Wobec tego

$$\text{(1)} \quad \left| \frac{1}{r^2}\left(\left\lfloor \frac{r^2}{1} \right\rfloor - \left\lfloor \frac{r^2}{3} \right\rfloor + \ldots\right) - \frac{1}{r^2}\left(\left\lfloor \frac{r^2}{1} \right\rfloor - \left\lfloor \frac{r^2}{3} \right\rfloor + \ldots + (-1)^s \left\lfloor \frac{r^2}{2s+1} \right\rfloor\right)\right| < \frac{1}{r}.$$



Mamy również

$$(2)\qquad \left|\left(1-\frac{1}{3}+\ldots\right)-\left(1-\frac{1}{3}+\ldots+(-1)^s\frac{1}{2s+1}\right)\right|<\frac{1}{2s+3}<\frac{1}{r}.$$

Zauważmy jeszcze, że $\left\lfloor\frac{r^2}{2j+1}\right\rfloor\leqslant\frac{r^2}{2j+1}<\left\lfloor\frac{r^2}{2j+1}\right\rfloor+1$, zatem

$$0\leqslant\frac{1}{2j+1}-\frac{1}{r^2}\left\lfloor\frac{r^2}{2j+1}\right\rfloor<\frac{1}{r^2}.$$

Liczb nieparzystych od 1 do $2s+1$ jest $s+1<r$, więc

$$(3)\qquad \left|\left(1-\frac{1}{3}+\ldots+(-1)^s\frac{1}{2s+1}\right)-\frac{1}{r^2}\left(\left\lfloor\frac{r^2}{1}\right\rfloor-\left\lfloor\frac{r^2}{3}\right\rfloor+\ldots+(-1)^s\left\lfloor\frac{r^2}{2s+1}\right\rfloor\right)\right|<$$
$$<r\cdot\frac{1}{r^2}=\frac{1}{r}.$$

Z nierówności (2), (3) i (1) oraz z nierówności trójkąta ($|a+b|\leqslant|a|+|b|$) wynika, że

$$\left|\left(1-\frac{1}{3}+\ldots\right)-\frac{1}{r^2}\left(\left\lfloor\frac{r^2}{1}\right\rfloor-\left\lfloor\frac{r^2}{3}\right\rfloor+\ldots\right)\right|<\frac{3}{r},$$

a stąd wynika, że

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\ldots=\lim_{r\to\infty}\frac{1}{r^2}\left(\left\lfloor\frac{r^2}{1}\right\rfloor-\left\lfloor\frac{r^2}{3}\right\rfloor+\left\lfloor\frac{r^2}{5}\right\rfloor-\left\lfloor\frac{r^2}{7}\right\rfloor+\ldots\right)=$$
$$=\lim_{r\to\infty}\frac{N(r)}{4r^2}=\frac{\pi}{4}.$$

Różni ludzie, w tym bardzo wybitni, zajmowali się różnicą $N(r)-\pi r^2$ i uzyskiwali coraz dokładniejsze wyniki. Przytoczę niektóre z nich. Carl Friedrich Gauss (1798): $|N(r)-\pi r^2|\leqslant 2\sqrt{2}\pi r$; Wacław Sierpiński (1906) $|N(r)-\pi r^2|\leqslant r^{2/3}$ zmniejszając wykładnik przy r z 1 do $2/3$. Najlepszy wynik w tej dziedzinie, wedle tego co wiem, osiągnął w 2017 roku Jean Bourgain, laureat medalu Fieldsa z 1994 roku: $\frac{517}{824}\approx 0{,}627$. Godfrey Hardy (1915) wykazał, że nie istnieje taka stała $c>0$, że $|N(r)-\pi r^2|\leqslant cr^{1/2}$, podobny wynik niezależnie uzyskał Edmund Landau. Hipoteza: dla każdej liczby $d>\frac{1}{2}$ istnieje taka stała $c>0$, że $|N(r)-\pi r^2|\leqslant cr^d$. Do zbadania został już tylko przedział długości $\frac{517}{824}-\frac{1}{2}=\frac{105}{824}\approx 0{,}127$.

Zadania

Przygotował Łukasz BOŻYK

M 1588. Funkcja $f\colon\mathbb{R}\to\mathbb{R}$ spełnia dla każdego $x\in\mathbb{R}$ równość
$$f(x+1)-f(x)=2x+1$$
oraz $|f(x)|\leqslant 1$ dla $x\in[0,1]$. Wykazać, że $|f(x)|\leqslant x^2+2$ dla każdego $x\in\mathbb{R}$.
Rozwiązanie na str. 16

M 1589. Grupa ośmiu osób ma tę własność, że pośród dowolnych pięciu spośród nich można wskazać trzy osoby, które znają się wzajemnie. Wykazać, że w tej grupie są cztery osoby, które znają się wzajemnie.
Rozwiązanie na str. 16

M 1590. Dana jest dodatnia liczba całkowita n oraz zbiór $S=\{1,2,3\ldots,3n\}$. Wyznaczyć największą możliwą liczbę elementów podzbioru $T\subseteq S$ o następującej własności: Dla każdej trójki (niekoniecznie różnych) elementów T ich suma nie należy do T.
Rozwiązanie na str. 16

Przygotował Andrzej MAJHOFER

F 967. Mamy do dyspozycji n identycznych baterii o sile elektromotorycznej $\mathcal{E}_0$ i oporze wewnętrznym r_w każda. Chcemy uzyskać jak największą moc wydzieloną na oporniku podłączonym do źródła zbudowanego z tych baterii. Jaką moc możemy uzyskać, łącząc baterie (a) szeregowo i (b) równolegle? Ile powinien wynosić opór R dołączanego opornika w każdym z przypadków, by wydzielona moc była maksymalna?
Rozwiązanie na str. 15

F 968. Cząstka o ładunku q i masie m wpada w obszar jednorodnego pola magnetycznego. Prędkość cząstki tworzy różny od zera kąt z wektorem indukcji $\vec{B}$ pola. Ile wynosi częstotliwość f, z jaką cząstka obiega kierunek pola $\vec{B}$?
Rozwiązanie na str. 15