Aproksymacje diofantyczne

Kazimierz SZYMICZEK, Katowice

Aproksymacje – XIV Szkoła Matematyki Poglądowej, Miętne, 27.01.–31.01.1995

Aproksymacje diofantyczne otrzymały swoją nazwę zapewne poprzez skojarzenie z równaniami diofantycznymi. Wywodząca się od Diofantosa tradycja rozwiązywania równań wielomianowych (i innych) w liczbach wymiernych (a począwszy od Fermata – w liczbach całkowitych) została usankcjonowana nadaniem temu działowi teorii liczb nazwy *równania diofantyczne*. Przez analogię, dział teorii liczb, którego wiodącym problemem jest przybliżanie liczb rzeczywistych liczbami wymiernymi nosi nazwę *aproksymacji diofantycznych*. Nazwę tę zawdzięczamy prawdopodobnie H. Minkowskiemu [1864–1909].

Aproksymacje diofantyczne stanowią bardzo rozległy dział teorii liczb z licznymi zastosowaniami i powiązaniami z innymi działami matematyki. Nie jest więc możliwe przedstawienie w krótkim szkicu wszystkich najistotniejszych rezultatów. Skoncentrowaliśmy się tutaj przede wszystkim na wiodącym temacie jednowymiarowych aproksymacji jednorodnych, gdzie prawie wszystkie główne zagadnienia zostały rozwiązane. Ale nie pomijamy także takich tematów, jak równomierny rozkład ciągów, liczby przestępne i najsławniejsze zastosowania w teorii liczb. Zebrana w końcu szkicu literatura zawiera monografie przedmiotu (Baker, Cassels, Koksma, Schmidt), szczególnie przystępne wprowadzenia (Hardy-Wright, Niven) oraz kilka najważniejszych prac oryginalnych. Może ona stanowić pewną pomoc w dotarciu do prac oryginalnych i szczegółowego przedstawienia poruszanych tu tematów.
Będziemy stosować następujące oznaczenia:

θ – liczba rzeczywista

$\{\theta\}$ – mantysa liczby θ, tzn., $\{\theta\} := \theta - [\theta]$, gdzie $[\theta]$ oznacza część całkowitą liczby θ.

$\|\theta\|$ – odległość liczby θ od najbliższej liczby całkowitej, tzn., $\|\theta\| := \min\{\{\theta\}, 1 - \{\theta\}\}$.

1. Aproksymacje jednorodne

Rozpatrzmy skończony układ liczb rzeczywistych $\theta_1, \ldots, \theta_n$. Głównym zagadnieniem w teorii aproksymacji jednorodnych jest ustalenie optymalnych twierdzeń o równoczesnych przybliżeniach liczb $\theta_1, \ldots, \theta_n$ liczbami wymiernymi $p_1/q, \ldots, p_n/q$ o wspólnym mianowniku q. Gdy $n = 1$, mówimy o jednowymiarowych aproksymacjach jednorodnych. A więc problem polega na zbadaniu możliwości aproksymowania liczby rzeczywistej θ liczbami wymiernymi. Na pierwszy rzut oka problem jest trywialny, bo liczby wymierne leżą gęsto w zbiorze $\mathbf{R}$ liczb rzeczywistych, można więc liczby rzeczywiste aproksymować liczbami wymiernymi z dowolną dokładnością. Jest to pierwszy poziom trywialności obserwacji. Gdybyśmy chcieli nadać mu oficjalną formę twierdzenia, to powiedzielibyśmy, że dla każdej liczby rzeczywistej θ i dla każdej liczby naturalnej q istnieje liczba całkowita p taka, że $|\theta - p/q| < 1/q$, lub równoważnie,

$$|q\theta - p| < 1.$$

Wystarczy bowiem oś liczbową podzielić na przedziały $p/q \le x < (p+1)/q$, gdzie p jest dowolną liczbą całkowitą. Przedziały te mają długość $1/q$ i liczba θ należy do jednego z nich, stąd odległość θ od liczby p/q jest mniejsza niż $1/q$.

A więc aproksymowanie liczb rzeczywistych liczbami wymiernymi o mianowniku $q > 0$ z dokładnością $1/q$ jest możliwe, ale jest trywialne. Powstaje jednak natychmiast pytanie, czy jest możliwe aproksymowanie liczb rzeczywistych liczbami wymiernymi o mianowniku $q > 0$ z dokładnością lepszą niż $1/q$, powiedzmy z dokładnością $1/q^2$ lub $1/q^3$? Znalezienie wyczerpujących odpowiedzi na te pytania zajęło matematykom ponad 100 lat. Przedstawiamy je w §1 i §3.

1.1. Twierdzenie Dirichleta

Punktem wyjścia teorii aproksymacji diofantycznych jest następujące proste ale nietrywialne twierdzenie Dirichleta. Prawdopodobnie w dowodzie tego twierdzenia Dirichlet użył po raz pierwszy tak zwanej *zasady szufladkowej* Dirichleta.

TWIERDZENIE 1.1 (G. P. L. Dirichlet, 1842).
Niech θ będzie liczbą rzeczywistą. Dla każdej liczby całkowitej $Q > 1$ istnieją liczby całkowite p, q takie, że

$$|q\theta - p| < \frac{1}{Q} \quad \text{oraz} \quad 0 < q \leq Q. \tag{1}$$

Dowód. Rozpatrzmy $Q+1$ liczb rzeczywistych $0 = \{0\theta\}, \{\theta\} = \{1\theta\}, \{2\theta\}, \ldots, \{Q\theta\}$.

Wszystkie one leżą w przedziale domknięto-otwartym $[0,1)$ i wobec tego przynajmniej dwie leżą w tym samym podprzedziale $i/Q \leq x < (i+1)/Q$, $i = 0, 1, \ldots, Q-1$, o długości $1/Q$. Stąd, biorąc różnicę dwóch takich liczb $\{r\theta\}$ i $\{s\theta\}$, gdzie $r > s$, otrzymujemy

$$\{r\theta\} - \{s\theta\} = (r-s)\theta - ([r\theta] - [s\theta]) = q\theta - p,$$

gdzie $q = r - s > 0$ i $p = [r\theta] - [s\theta]$ są liczbami całkowitymi oraz $|q\theta - p| < 1/Q$. ∎

Zauważmy, że jeśli p i q spełniają nierówności (1), to także $\left|\theta - \frac{p}{q}\right| < \frac{1}{qQ} \leq \frac{1}{q^2}$.

Z twierdzenia Dirichleta wynika następujący charakterystyczny rezultat.

WNIOSEK 1. *Dla każdej liczby niewymiernej θ istnieje nieskończenie wiele par liczb całkowitych p, q spełniających nierówność*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{2}$$

Dowód. Weźmy bowiem jakiekolwiek rozwiązanie p, q nierówności (2). Obieramy liczbę naturalną Q_1 taką, że $1/Q_1 < |q\theta - p|$ i dla liczby Q_1 dobieramy na podstawie twierdzenia Dirichleta liczby całkowite p_1, q_1 spełniające nierówność $|q_1\theta - p_1| < 1/Q_1$. Wtedy mamy także $|\theta - p_1/q_1| < 1/q_1^2$, a więc p_1, q_1 jest rozwiązaniem nierówności (2), i jest to rozwiązanie różne od rozwiązania p, q, gdyż $|q_1\theta - p_1| < 1/Q_1 < |q\theta - p|$.

Postępując tak samo z parą p_1, q_1 znajdziemy rozwiązanie p_2, q_2 nierówności (2) spełniające

$$|q_2\theta - p_2| < |q_1\theta - p_1| < |q\theta - p|.$$

Kontynuując to postępowanie znajdziemy dowolnie długi ciąg rozwiązań nierówności (2). ∎

Natomiast jeśli liczba θ jest wymierna, $\theta = a/b$, gdzie a i b są liczbami całkowitymi oraz $b > 0$, to dla każdych liczb całkowitych p, q takich, że $\theta \neq p/q$ oraz $q > 0$, mamy

$$|\theta - p/q| = \left|\frac{aq - bp}{bq}\right| \geq \frac{1}{bq}.$$

Jeśli więc spełniona jest nierówność (2), to otrzymujemy $1/bq \leq |\theta - p/q| < 1/q^2$, skąd $q < b$. Stąd wynika, że nierówność (2) ma tylko skończoną liczbę rozwiązań w liczbach całkowitych p, q takich, że $\theta \neq p/q$.

Wprowadzimy teraz nieco oszczędniejszą symbolikę dla nierówności (2). Przede wszystkim interesujące są tylko te rozwiązania nierówności (2), w których q jest dużą liczbą naturalną, można więc zakładać, że $q > 2$. Jeśli p i $q > 2$ spełniają nierówność (2), to $|q\theta - p| < 1/q < 1/2$, a to oznacza, że $|q\theta - p| = ||q\theta||$. Zatem nierówność (2) jest równoważna nierówności

$$q||q\theta|| < 1. \tag{3}$$

Z twierdzenia Dirichleta wynika więc, że dla każdej liczby niewymiernej θ nierówność (3) ma nieskończenie wiele rozwiązań w liczbach naturalnych q. To sformułowanie ma tę przewagę nad poprzednimi, że nie występuje w nim

liczba p, która gra tu rolę drugorzędną i jest zawsze zdeterminowana przez liczbę q. Dla rozwiązania p, q nierówności (2) mamy bowiem zawsze $p = [q\theta]$ lub $p = [q\theta] + 1$.

1.2. Spektrum Lagrange'a

Za pomocą aparatu ułamków łańcuchowych można udowodnić, że każdą liczbę niewymierną θ można aproksymować liczbami wymiernymi z jeszcze nieco większą dokładnością, niż dają rozwiązania nierówności (3). Mamy bowiem następujące twierdzenie.

TWIERDZENIE* 1.1 (A. Hurwitz, 1891).
Jeśli θ jest liczbą niewymierną, to nierówność

$$q\|q\theta\| < \frac{1}{\sqrt{5}}$$

ma nieskończenie wiele rozwiązań w liczbach naturalnych q.

Ale zastąpienie stałej $\sqrt{5}$ przez jakąkolwiek większą liczbę rzeczywistą sprawia, że twierdzenie przestaje być prawdziwe: istnieją liczby niewymierne θ, dla których ta nierówność ma tylko skończoną liczbę rozwiązań. Okazuje się, że liczby θ, których nie można aproksymować z tak dużą dokładnością stanowią klasę liczb "równoważnych" z niewymiernością kwadratową $\theta_1 = (\sqrt{5}+1)/2$.

Tutaj liczbę θ uważamy za *równoważną* z liczbą α, jeśli

$$\theta = \frac{a\alpha + b}{c\alpha + d}, \quad \text{gdzie} \quad a, b, c, d \in \mathbf{Z} \quad \text{oraz} \quad ad - bc = \pm 1.$$

Bardziej uczenie można powiedzieć, że liczba θ jest równoważna z α, jeśli θ leży w orbicie liczby α w naturalnym działaniu grupy $PGL(2, \mathbf{Z})$ na zbiorze liczb rzeczywistych.

Można udowodnić, że dla wszystkich liczb niewymiernych nierównoważnych z liczbą θ_1 istnieje nieskończenie wiele rozwiązań nierówności

$$q\|q\theta\| < \frac{1}{\sqrt{8}}.$$

Tutaj historia się powtarza: dla niewymierności kwadratowej $\theta_2 = \sqrt{2}$ i liczb z nią równoważnych nie można zastąpić stałej $1/\sqrt{8}$ przez żadną liczbę mniejszą, natomiast po usunięciu wszystkich liczb równoważnych z θ_1 i θ_2, dla wszystkich pozostałych liczb niewymiernych θ nierówność

$$q\|q\theta\| < c \tag{4}$$

ma nieskończenie wiele rozwiązań ze stałą $c = 5/\sqrt{221}$.

Dla liczby niewymiernej θ połóżmy

$$\nu(\theta) := \liminf_{q\to\infty} q\|q\theta\|.$$

A więc jeśli $c > \nu(\theta)$, to nierówność (4) ma nieskończenie wiele rozwiązań, jeśli zaś $c < \nu(\theta)$, to nierówność (4) ma tylko skończoną liczbę rozwiązań. Jeśli $\nu(\theta) > 0$, oznacza to, że liczba θ nie daje się dobrze aproksymować liczbami wymiernymi, gdyż dla każdej dodatniej liczby $c < \nu(\theta)$ nierówność (4) ma tylko skończoną liczbę rozwiązań. Twierdzenie Hurwitza orzeka, że $\nu(\theta) \le 1/\sqrt{5}$ dla każdej liczby niewymiernej θ. Jest rzeczą interesującą zbadać zbiór tych wszystkich liczb rzeczywistych, które są wartościami funkcji ν.

Zbiór $\mathbf{L} := \{\nu(\theta) : \theta \in \mathbf{R}\}$ nazywa się *spektrum Lagrange'a*. Zauważmy, że $\mathbf{L} \subseteq [0, 1/\sqrt{5}]$. Jego główne własności opisane są w następującym twierdzeniu.

TWIERDZENIE* 1.2 (A.A. Markow, 1879).
Istnieje ciąg niewymierności kwadratowych

$$\mu_1 = 1/\sqrt{5} > \mu_2 = 1/\sqrt{8} > \mu_3 = 5/\sqrt{221} > \mu_4 = 13/\sqrt{1517} > \cdots$$

zbieżny do $1/3$ taki, że

(a) *dla każdej liczby μ_i istnieje skończona liczba klas równoważnych liczb niewymiernych (niewymierności kwadratowych) takich, że $\nu(\theta) = \mu_i$ wtedy i tylko wtedy, gdy θ należy do jednej z tych klas liczb równoważnych;*

(b) *jeśli c jest liczbą rzeczywistą taką, że $c > 1/3$ oraz $c \neq \mu_i$ dla każdego i, to nie istnieje liczba niewymierna θ taka, że $\nu(\theta) = c$; inaczej mówiąc,*

$$\mathbf{L} \cap (1/3, \infty) = \mathbf{L} \cap (1/3, 1/\sqrt{5}) = \{\mu_1, \mu_2, \ldots\};$$

(c) *istnieje continuum liczb θ takich, że $\nu(\theta) = 1/3$.*

Warto zwrócić uwagę, że z części (c) tego twierdzenia wynika istnienie liczb przestępnych θ takich, że $\nu(\theta) = 1/3$. A więc istnieją liczby przestępne, które nie dają się dobrze aproksymować liczbami wymiernymi (zob. Przykład 1 w §3, gdzie rozważa się sytuację przeciwstawną).

Jakkolwiek twierdzenie* 1.2 wiąże się z nazwiskiem Markowa, w pracy Markowa nie było żadnej wzmianki o aproksymacjach liczb rzeczywistych liczbami wymiernymi ani o spektrum Lagrange'a. Markow rozpatrywał problem wyznaczenia minimalnych wartości binarnych form kwadratowych o współczynnikach rzeczywistych dla całkowitych wartości zmiennych. Jeśli forma $f = f(X, Y) = aX^2 + bXY + cY^2$ ma współczynniki rzeczywiste, to liczbę $d = d(f) = b^2 - 4ac$ nazywa się wyróżnikiem formy f. Jeśli $d(f) > 0$, to forma f przyjmuje zarówno wartości dodatnie jak i ujemne i nazywa się ją formą nieokreśloną. Liczbę

$$m(f) := \inf \{|f(x, y)| : x, y \in \mathbf{Z}, \quad (x, y) \neq (0, 0)\}$$

nazywa się minimum formy f, chociaż forma f niekonieczenie przyjmuje wartość $m(f)$ dla całkowitych wartości zmiennych. Markow udowodnił, że istnieje pewien ciąg nieokreślonych binarnych form kwadratowych $f_1, f_2, \ldots$, zwanych dzisiaj formami Markowa, o następujących własnościach:

(a) jeśli dla nieokreślonej formy binarnej f, zachodzi nierówność $m(f) > \frac{1}{3} d^{1/2}$, to forma f jest równoważna z pewną formą Markowa f_i, lub jej krotnością αf_i, gdzie $\alpha \in \mathbf{R}$;

(b) na odwrót, nierówność ta zachodzi dla każdej formy Markowa i dla każdej formy binarnej f, która jest równoważna z pewną krotnością formy Markowa;

(c) minima $m(f_i)$ form Markowa są wyznaczone następująco:

$$m(f_i) = \mu_i \, d(f_i)^{1/2}, \quad i = 1, 2, \ldots,$$

gdzie liczby μ_i tworzą ten sam ciąg, który występuje w twierdzeniu* 1.2;

(d) Istnieje zbiór nieokreślonych binarnych form kwadratowych mocy continuum taki, że żadne dwie formy w tym zbiorze, ani żadne ich wielokrotności nie są równoważne, natomiast minimum $m(f)$ każdej formy f tego zbioru jest równe $\frac{1}{3} d^{1/2}$.

Okazuje się, że te fakty o minimach form binarnych pozwalają uzyskać rezultaty o spektrum Lagrange'a sformułowane w twierdzeniu* 1.2, stąd twierdzenie to nazywa się twierdzeniem Markowa.

Nasuwają się tutaj jeszcze dwie uwagi. Przede wszystkim stwierdzamy, że minima nieokreślonych form binarnych zachowują się dość nieoczekiwanie. Pewien przeliczalny zbiór klas równoważności tych form (o ustalonym wyróżniku d) ma minima izolowane, zbieżne do liczby $\frac{1}{3} d^{1/2}$, która z kolei jest minimum continuum parami nierównoważnych form. Zbiór

$$\mathbf{M} := \{ m(f) d(f)^{-1/2} \},$$

gdzie f przebiega wszystkie nieokreślone formy binarne z minimum $m(f) > 0$, nazywa się *spektrum Markowa*. Można udowodnić, że $\mathbf{L} \neq \mathbf{M}$, natomiast porównując rezultaty o spektrach Lagrange'a i Markowa widzimy, że

$$\mathbf{L} \cap (1/3, \infty) = \mathbf{M} \cap (1/3, \infty) = \{ \mu_1, \mu_2, \ldots \}.$$

Druga uwaga dotyczy nieokreślonych form kwadratowych wielu zmiennych. Tutaj problem znalezienia minimum $m(f)$ formy f (tzn. kresu dolnego wartości formy f dla całkowitych wartości zmiennych) okazał się bardzo trudny. Od roku 1929 znana była hipoteza A. Oppenheima, mówiąca, że jeśli f jest nieokreśloną formą kwadratową n (≥ 3) zmiennych o współczynnikach rzeczywistych i forma f nie jest wielokrotnością formy o współczynnikach wymiernych (te ostatnie

mogą mieć minima dodatnie), to $m(f) = 0$. Hipoteza ta została w końcu udowodniona w 1987 roku przez G. A. Margulisa, medalistę Fieldsa z 1978 roku.

Struktura spektrum Lagrange'a i spektrum Markowa jest bardzo skomplikowana. Zagadnieniom tym poświęcona jest specjalna monografia T. W. Cusicka i M. E. Flahive.

2. Aproksymacje niejednorodne

2.1. Twierdzenie Kroneckera

Podstawowym faktem w teorii aproksymacji niejednorodnych jest następujące twierdzenie, które po raz pierwszy zostało zauważone przez Czebyszewa. Ogólna wielowymiarowa wersja twierdzenia należy do Kroneckera. Cytowana poniżej wersja jednowymiarowa ze stałą 1/4 pochodzi od Minkowskiego. Stała 1/4 jest najlepszą możliwą stałą dla wersji jednowymiarowej.

TWIERDZENIE 2.1 (L. Kronecker, 1884; P. L. Czebyszew, 1866; H. Minkowski, 1900).
Niech θ będzie niewymierną liczbą rzeczywistą i niech α będzie dowolną liczbą rzeczywistą. Wtedy dla dowolnej dodatniej liczby rzeczywistej ε istnieją liczby całkowite p, q takie, że

$$|q\theta - p - \alpha| < \varepsilon. \tag{5}$$

Dokładniej, jeśli α nie daje się przedstawić w postaci $m\theta + n$, gdzie m, n są liczbami całkowitymi, to istnieje nieskończenie wiele par liczb całkowitych p, q takich, że

$$|q\theta - p - \alpha| < \frac{1}{4|q|}.$$

Dowód. Udowodnimy pierwszą, słabszą wersję (5) twierdzenia Kroneckera. Na podstawie twierdzenia Dirichleta istnieje liczba naturalna n taka, że $\{n\theta\} < \varepsilon$. Rozpatrzmy całkowite wielokrotności liczby $\{n\theta\}$. Tworzą one ciąg, którego kolejne wyrazy różnią się o mniej niż ε. Zatem dla pewnej liczby całkowitej m mamy

$$|m\{n\theta\} - \alpha| < \varepsilon.$$

Zauważmy, że $m\{n\theta\} = m(n\theta - [n\theta]) = mn\theta - m[n\theta]$. Obierając więc $p = m[n\theta]$ oraz $q = mn$ mamy

$$|q\theta - p - \alpha| = |m\{n\theta\} - \alpha| < \varepsilon,$$

co dowodzi istnienia rozwiązania nierówności (5). ∎

2.2. Równomierny rozkład

Jeśli θ jest liczbą niewymierną, to z twierdzenia Kroneckera wynika, że zbiór mantys całkowitych wielokrotności liczby θ jest gęstym podzbiorem przedziału $(0, 1)$. Faktycznie jednak można jeszcze wzmocnić twierdzenie Kroneckera pokazując, że każdy podprzedział I przedziału $[0, 1]$ zawiera proporcjonalną do swojej długości liczbę elementów spośród początkowych wyrazów naszego ciągu. Najlepiej tę własność wyrazić przy pomocy pojęcia *równomiernego rozkładu* ciągu.

DEFINICJA 1. Niech $\alpha_0, \alpha_1, \ldots$ będzie ciągiem liczb rzeczywistych. Dla dowolnego podprzedziału I przedziału $[0, 1]$ i dowolnej liczby naturalnej N, niech $A(N, I)$ oznacza liczbę elementów skończonego ciągu mantys $\{\alpha_0\}, \{\alpha_1\}, \ldots, \{\alpha_{N-1}\}$ należących do przedziału I.

Mówimy, że ciąg $\alpha_0, \alpha_1, \ldots$ ma *równomierny rozkład modulo* 1, jeśli dla każdego podprzedziału I przedziału $[0, 1]$ mamy

$$\lim_{N\to\infty} \frac{A(N, I)}{N} = |I|,$$

gdzie $|I|$ oznacza długość przedziału I.

TWIERDZENIE* 2.1 (P. Bohl, 1910; W. Sierpiński, 1910; H. Weyl, 1916).
Dla każdej liczby niewymiernej θ ciąg $\theta, 2\theta, \ldots, n\theta, \ldots$ ma równomierny rozkład modulo 1.

Dowód podany przez Weyla oparty był na znalezionym przez niego kryterium równomiernego rozkładu dowolnego ciągu. Kryterium to uzależnia równomierność rozkładu ciągu od asymptotycznego zachowania się pewnych sum trygonometrycznych związanych z ciągiem. Dokładniej, ciąg $\alpha_0, \alpha_1, \ldots$ ma równomierny rozkład modulo 1, jeśli

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n} \exp(2\pi i h \alpha_k) = 0$$

dla każdej liczby całkowitej h.

Pokażemy tylko, że z kryterium Weyla wynika natychmiast twierdzenie* 2.1. Otóż jeśli $\alpha_k = k\theta$, to

$$S_n := \sum_{k=0}^{n} \exp(2\pi i h k\theta) = \frac{(\exp(2\pi i h\theta))^{n+1} - 1}{\exp(2\pi i h\theta) - 1}.$$

Zatem $|S_n| \leq 2$, gdzie $c = |\exp(2\pi i h\theta) - 1|$ jest stałą dodatnią, i wobec tego dla każdej liczby całkowitej h mamy

$$\frac{1}{n}|S_n| \leq \frac{2}{nc} \to 0 \quad \text{gdy} \quad n \to \infty.$$

Ciąg całkowitych wielokrotności liczby niewymiernej θ spełnia więc warunek występujący w kryterium Weyla, ma zatem równomierny rozkład modulo 1.

Multyplikatywnym odpowiednikiem ciągu liczb $\{n\theta\}$ jest ciąg $\{\theta^n\}$, $n = 1, 2, \ldots$ J. F. Koksma udowodnił w 1935 roku, że dla prawie wszystkich liczb rzeczywistych $\theta > 1$ ciąg ten ma równomierny rozkład. Jest rzeczą interesującą, że nie potrafimy jednak wskazać ani jednej liczby rzeczywistej $\theta > 1$, dla której ciąg ten ma równomierny rozkład! Znane są natomiast takie liczby $\theta > 1$, dla których ciąg mantys $\{\theta^n\}$ jest gęsty w przedziale $[0, 1]$ ale nie ma równomiernego rozkładu. Są to tak zwane liczby Salema, które określa się jako liczby algebraiczne $\theta > 1$, których wszystkie liczby sprzężone różne od θ leżą w kole jednostkowym $|z| \leq 1$, z tym, że przynajmniej jedna liczba sprzężona z θ leży na okręgu jednostkowym $|z| = 1$ (zob. najnowszą monografię M. J. Bertina et al. poświęconą liczbom Salema i Pisota).

3. Aproksymacje liczb algebraicznych

J. Liouville odkrył w 1844 roku, że aproksymowanie liczb algebraicznych liczbami wymiernymi ma pewną charakterystyczną osobliwość, która nie obciąża wszystkich liczb rzeczywistych. Te liczby rzeczywiste, które nie mają tej "wady", są więc liczbami przestępnymi. Osobliwość ta polega na tym, że liczby algebraicznej θ stopnia $n > 1$ nie można aproksymować liczbami wymiernymi o mianowniku q z dokładnością $1/q^n$. Ta obserwacja była punktem wyjścia jednego z centralnych nurtów badań w teorii liczb przez okres ponad 100 lat. Nurt ten symbolizują trzy nazwiska: Axel Thue, Carl L. Siegel i Klaus F. Roth.

3.1. Od Liouville'a do Rotha

TWIERDZENIE 3.1 (J. Liouville, 1844).
Niech θ będzie rzeczywistą liczbą algebraiczną stopnia $n > 1$. Wtedy istnieje stała $c > 0$ zależna od liczby θ, taka , że dla każdej liczby wymiernej p/q takiej, że $q > 0$ oraz $|\theta - p/q| < 1$, zachodzi nierówność

$$\left|\theta - \frac{p}{q}\right| > \frac{c}{q^n}.$$

Dowód. Niech $f \in \mathbf{Z}[X]$ będzie wielomianem stopnia n takim, że $f(\theta) = 0$. Wtedy wielomian f nie ma wymiernych pierwiastków, zatem dla dowolnych $p, q \in \mathbf{Z}$, $q > 0$, mamy $f(p/q) \neq 0$. Ponadto, $f(p/q)$ jest liczbą wymierną o mianowniku q^n, zatem $|f(p/q)| \geq 1/q^n$. Z drugiej strony, na podstawie twierdzenia o wartości

średniej, istnieje liczba rzeczywista a leżąca między p/q i θ, taka że

$$f(p/q) = f(p/q) - f(\theta) = (p/q - \theta) \cdot f'(a).$$

Liczba a leży więc w przedziale $(\theta - 1, \theta + 1)$. Pochodna f' wielomianu f jest funkcją ograniczoną w każdym przedziale skończonym, niech więc M będzie liczbą rzeczywistą taką, że $f'(x) < M$ dla każdego x w przedziale $(\theta - 1, \theta + 1)$. Mamy więc

$$\frac{1}{q^n} \leq |f(p/q)| < |p/q - \theta| \cdot M,$$

skąd dla $c = 1/M$ otrzymujemy nierówność $\left|\theta - \frac{p}{q}\right| > \frac{c}{q^n}$. ∎

PRZYKŁAD 1. Weźmy liczbę $\theta = \sum_i 10^{-i!}$. Wtedy mianownik n–tej sumy częściowej jest równy $q := q_n = 10^{n!}$, jeśli więc licznik tej sumy oznaczymy $p := p_n$, to mamy nierówność

$$0 < \theta - \frac{p}{q} < \frac{2}{q^{n+1}}.$$

Gdyby θ była liczbą algebraiczną stopnia N, to na podstawie twierdzenia Liouville'a mielibyśmy nierówność $\frac{c}{q^N} < \theta - \frac{p}{q}$, dla pewnej stałej $c > 0$.

Stąd $q^{n+1-N} < 2$. Ta nierówność ma zachodzić przy stałych c i N dla każdego naturalnego n oraz $q = 10^{n!}$, co jest sprzeczne. A więc θ nie jest liczbą algebraiczną. Tego typu przykłady były pierwszymi znanymi liczbami przestępnymi.

WNIOSEK 2. *Jeśli θ jest rzeczywistą liczbą algebraiczną stopnia $n > 1$, to dla każdej liczby $\mu > n$ nierówność*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^\mu} \tag{6}$$

ma tylko skończoną liczbę rozwiązań w liczbach całkowitych p, q, gdzie $q > 0$.

Dowód. Przypuśćmy, że $\mu = n + \varepsilon$, gdzie $\varepsilon > 0$, i nasza nierówność ma nieskończnie wiele rozwiązań. Wtedy

$$\frac{c}{q^n} < \left|\theta - \frac{p}{q}\right| < \frac{1}{q^{n+\varepsilon}},$$

skąd $q^\varepsilon < 1$ dla nieskończenie wielu naturalnych q, sprzeczność. ∎

Ten rezultat był wielokrotnie poprawiany. Oto historia problemu polegającego na znalezieniu najmniejszej liczby μ gwarantującej skończoność liczby rozwiązań nierówności (6) dla liczby algebraicznej θ stopnia n :

Liouville (1844):	$\mu > n$
Thue (1909):	$\mu > \frac{1}{2}n + 1$
Siegel (1921):	$\mu > 2\sqrt{n}$
Dyson (1947), Gelfond (1952):	$\mu > \sqrt{2n}$
Roth (1955):	$\mu > 2$.

Twierdzenia Rotha brzmi więc następująco:

TWIERDZENIE* 3.1 (K. F. Roth, 1955).
Niech θ będzie rzeczywistą liczbą algebraiczną stopnia ≥ 2. Wtedy dla każdej liczby $\varepsilon > 0$ nierówność

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

ma tylko skończoną liczbę rozwiązań w liczbach całkowitych p, q.

Klaus F. Roth otrzymał medal Fieldsa na kongresie w Edynburgu w 1958 roku (drugim laureatem był R. Thom).

Twierdzenie Rotha orzeka, że dla liczby algebraicznej θ i dowolnej liczby $\varepsilon > 0$ nierówność

$$q\,\|q\theta\| < 1/q^\varepsilon$$

ma tylko skończoną liczbę rozwiązań w liczbach naturalnych q. Powstaje pytanie, czy zastępując tutaj $1/q^\varepsilon$ przez funkcję zmiennej q, która zmierza

wolniej do zera, można także twierdzić, że ta nowa nierówność ma tylko skończoną liczbę rozwiązań. Nierozstrzygnięta jest postawiona przez S. Langa w 1965 roku hipoteza, że jeśli θ jest liczbą algebraiczną stopnia ≥ 3, to dla dowolnej liczby $\alpha > 1$ nierówność

$$q\,\|q\theta\| < 1/(\log q)^{\alpha}$$

ma tylko skończoną liczbę rozwiązań w liczbach naturalnych q.

Istnieją także uogólnienia twierdzenia Rotha, w których rozpatruje się aproksymacje rzeczywistej liczby algebraicznej θ liczbami algebraicznymi α. Pierwszy wariant dopuszcza tylko liczby α z ustalonego ciała liczb algebraicznych $\mathbf{K}$ (skończonego rozszerzenia ciała $\mathbf{Q}$ liczb wymiernych).

TWIERDZENIE* 3.2 (W. J. LeVeque, 1956).
Niech θ będzie rzeczywistą liczbą algebraiczną i niech $\mathbf{K}$ będzie ciałem liczb algebraicznych. Dla każdej liczby rzeczywistej $\varepsilon > 0$ istnieje tylko skończenie wiele liczb $\alpha \in \mathbf{K}$ takich, że

$$|\theta - \alpha| < \frac{1}{H(\alpha)^{2+\varepsilon}}.$$

Tutaj $H(\alpha)$ oznacza *wysokość* liczby algebraicznej α. Określa się ją następująco. Obieramy wielomian o współczynnikach całkowitych względnie pierwszych, nierozkładalny nad ciałem liczb wymiernych i taki, że liczba α jest jego pierwiastkiem. *Wysokością* $H(\alpha)$ liczby α jest największy z modułów współczynników tego wielomianu.

Znacznie trudniejszy okazał się problem znalezienia uogólnienia twierdzenia Rotha, w którym aproksymuje się rzeczywistą liczbę algebraiczną θ dowolnymi liczbami algebraicznymi, których stopień nie przekracza danej liczby t. Ostateczny rezultat, który redukuje się do twierdzenia Rotha w przypadku $t = 1$ uzyskał W. M. Schmidt.

TWIERDZENIE* 3.3 (W. M. Schmidt, 1970).
Jeśli θ jest rzeczywistą liczbą algebraiczną, to dla każdej liczby rzeczywistej $\varepsilon > 0$ i dla każdej liczby naturalnej t istnieje tylko skończenie wiele liczb algebraicznych α stopnia $\leq t$ takich, że

$$|\theta - \alpha| < \frac{1}{H(\alpha)^{t+1+\varepsilon}}.$$

4. Aproksymacje wielowymiarowe

Zasada szufladkowa Dirichleta prowadzi także do ustalenia wzorca równoczesnej aproksymacji układu $n > 1$ liczb rzeczywistych liczbami wymiernymi o wspólnym mianowniku q.

TWIERDZENIE 4.1 (G. P. L. Dirichlet, 1842).
Niech $\theta_1, \ldots, \theta_n$ będą liczbami rzeczywistymi. Dla każdej liczby całkowitej $Q > 1$ istnieją liczby całkowite $p_1, \ldots, p_n, q$ takie, że

$$\|q\theta_i\| = |q\theta_i - p_i| < \frac{1}{Q}, \quad 0 < q \leq Q^n, \quad \text{dla } i = 1, \ldots, n.$$

Dowód. Na każdej osi układu współrzędnych przestrzeni $\mathbf{R}^n$ dzielimy przedział $[0,1)$ na podprzedziały $i/Q \leq x < (i+1)/Q$, $i = 0, 1, \ldots, Q-1$, każdy o długości $1/Q$. W ten sposób kostka jednostkowa podzielona zostanie na Q^n rozłącznych kostek o boku $1/Q$. Rozpatrzmy $Q^n + 1$ punktów przestrzeni $\mathbf{R}^n$:

$$P_k := (\{k\theta_1\}, \ldots, \{k\theta_n\}), \quad k = 0, 1, \ldots, Q^n.$$

Wszystkie one leżą w kostce jednostkowej przestrzeni $\mathbf{R}^n$ i wobec tego przynajmniej dwa leżą w tej samej kostce o boku $1/Q$. Jeśli są to punkty P_r i P_s, gdzie $r > s$, to różnice współrzędnych punktów P_r i P_s są mniejsze niż $1/Q$ oraz

$$P_r - P_s = P_{r-s} - P,$$

gdzie P jest punktem o współrzędnych całkowitych.

Jeśli więc $q := r - s$ oraz $P = (p_1, \ldots, p_n)$, to mamy $|q\theta_i - p_i| < 1/Q$ dla $i = 1, \ldots, n$. ■

Podobnie jak w przypadku $n = 1$ wyciągamy stąd wniosek, że jeśli przynajmniej jedna z liczb $\theta_1, \ldots, \theta_n$ jest niewymierna, to istnieje nieskończenie wiele liczb całkowitych $q > 0$ takich, że

$$q^{1/n}\|q\theta_i\| < 1, \quad \text{dla } i = 1, \ldots, n. \tag{7}$$

Zauważmy, że w przypadku $n = 1$ rezultat ten pokrywa się z (3).

Istnieją jeszcze inne warianty jednorodnych aproksymacji wielowymiarowych, których typowym przykładem jest następujący rezultat, wynikający z twierdzenia Dirichleta.

TWIERDZENIE* 4.1.
Jeśli liczby $1, \theta_1, \ldots, \theta_n$ są liniowo niezależne nad ciałem liczb wymiernych, to istnieje nieskończenie wiele układów liczb całkowitych $q_1, \ldots, q_n, p$ takich, że

$$|q_1\theta_1 + \cdots + q_n\theta_n - p| < \frac{1}{q^n}, \quad \text{gdzie} \quad q := \max\{|q_1|, \ldots, |q_n|\}.$$

Bardzo trudnym zagadnieniem okazało się pytanie, czy wykładniki liczby q w tych dwóch ostatnich rezultatach są najlepsze możliwe. Już w przypadku $n = 1$ jest to pytanie, na które odpowiedzią było dopiero twierdzenie Rotha. W. M. Schmidt udowodnił w 1970 roku, że tak istotnie jest.

TWIERDZENIE* 4.2 (W. M. Schmidt, 1970).
Jeśli liczby $\theta_1, \ldots, \theta_n$ są algebraiczne oraz liczby $1, \theta_1, \ldots, \theta_n$ są liniowo niezależne nad ciałem liczb wymiernych, to dla każdej liczby $\varepsilon > 0$ istnieje tylko skończona liczba rozwiązań nierówności

$$q^{1+\varepsilon}\|q\theta_i\| < 1, \quad \text{dla} \quad i = 1, \ldots, n,$$

w liczbach całkowitych $p_1, \ldots, p_n, q$, a także tylko skończona liczba układów liczb $q_1, \ldots, q_n, p$ spełniających nierówność

$$|q_1\theta_1 + \cdots + q_n\theta_n - p| < \frac{1}{q^{n+\varepsilon}},$$

gdzie $q := \max\{|q_1|, \ldots, |q_n|\} > 0$.

Każde z tych stwierdzeń w przypadku $n = 1$ redukuje się do twierdzenia Rotha. Z tych rezultatów Schmidt otrzymał już łatwo uogólnienie twierdzenia Rotha na aproksymacje liczb algebraicznych liczbami algebraicznymi (zob. twierdzenie* 3.3).

Na podstawie twierdzenia Dirichleta wiemy, że jeśli wśród liczb rzeczywistych $\theta_1, \ldots, \theta_n$ jest przynajmniej jedna liczba niewymierna, to układ nierówności (7) ma nieskończenie wiele rozwiązań w liczbach całkowitych $q > 0$. Mnożąc te nierówności stronami otrzymujemy nierówność

$$q\|q\theta_1\| \cdots \|q\theta_n\| < 1,$$

która wobec tego także ma nieskończenie wiele rozwiązań w liczbach całkowitych $q > 0$. Można się spodziewać, że być może niektóre czynniki tego iloczynu są znacznie mniejsze od innych i wobec tego iloczyn jest zawsze znacznie mniejszy niż 1, powiedzmy mniejszy niż $1/q^{\varepsilon}$, gdzie $\varepsilon > 0$. Okazuje się, że tak nie jest.

TWIERDZENIE* 4.3 (W. M. Schmidt, 1970).
Jeśli liczby algebraiczne $1, \theta_1, \ldots, \theta_n$ są liniowo niezależne nad ciałem liczb wymiernych, to dla każdego $\varepsilon > 0$ istnieje tylko skończenie wiele liczb naturalnych q takich, że

$$q^{1+\varepsilon}\|q\theta_1\| \cdots \|q\theta_n\| < 1.$$

Wykładnik $1 + \varepsilon$ jest najlepszym możliwym wykładnikiem w tym sensie, że zastąpienie go wykładnikiem 1 sprawia, iż twierdzenie przestaje być prawdziwe. W ten sposób ustalony jest stopień dokładności równoczesnego aproksymowania układu liczb rzeczywistych liczbami wymiernymi o wspólnym mianowniku q. Jednakże dokładniejsze przyjrzenie się tej sytuacji prowadzi do wniosku, że twierdzenie* 4.3 nie mówi całej prawdy o najlepszym możliwym równoczesnym przybliżaniu liczb rzeczywistych liczbami wymiernymi o wspólnym mianowniku.

Wprawdzie wiemy, że dla każdego $\varepsilon > 0$ nierówność

$$q\|q\theta_1\| \cdots \|q\theta_n\| < \frac{1}{q^\varepsilon}$$

ma tylko skończoną liczbę rozwiązań w liczbach całkowitych $q > 0$, ale być może istnieje nieskończenie wiele rozwiązań nierówności

$$q\|q\theta_1\| \cdots \|q\theta_n\| < f(q), \tag{8}$$

gdzie f jest funkcją, która zmierza do zera wolniej niż $q^{-\varepsilon}$? Nie wiemy nawet czy nierówność (8) ma nieskończenie wiele rozwiązań, gdy f jest *jakąkolwiek* funkcją zmierzającą do zera, gdy $q \to \infty$. Pozytywna odpowiedź na to pytanie stanowiłaby rozstrzygnięcie otwartej od kilkudziesięciu lat hipotezy J. E. Littlewooda:

Niech $\theta_1, \ldots, \theta_n$ będą liczbami rzeczywistymi; dla każdego $\varepsilon > 0$ istnieje liczba naturalna q taka, że

$$q\,\|q\theta_1\| \cdots \|q\theta_n\| < \varepsilon.$$

Inaczej mówiąc, hipoteza Littlewoda przewiduje, że

$$\liminf_{q\to\infty} q\,\|q\theta_1\| \cdots \|q\theta_n\| = 0.$$

Hipotezę Littlewooda wystarczyłoby udowodnić dla $n = 2$, gdyż jest rzeczą oczywistą, że jeśli jest ona prawdziwa dla $n = n_0$, to jest także prawdziwa dla każdego $n > n_0$.

Nasze omówienie aproksymacji wielowymiarowych akcentuje aproksymacje jednorodne. Tymczasem zarówno twierdzenie Kroneckera jak i problematyka równomiernego rozkładu ciągów mają swoje wielowymiarowe odpowiedniki. Zainteresowanego Czytelnika odsyłamy do monografii Koksmy i Casselsa.

5. Liczby przestępne

5.1. Od Eulera do Gelfonda

Euler (1744) wyraził opinię, że dla dodatnich liczb wymiernych a, b, jeśli b nie jest potęgą liczby a o wykładniku wymiernym, to liczba $\log_a b = (\log b)/(\log a)$ jest nie tylko liczbą niewymierną, ale wykracza poza możliwości konstrukcji algebraicznych. Innymi słowy, liczba ta nie może być pierwiastkiem wielomianu o współczynnikach wymiernych, czyli jest *przestępna*. Dopiero jednak 100 lat później Liouville udowodnił, że liczby przestępne w ogóle istnieją, a przestępność takich liczb jak e lub π została udowodniona jeszcze po upływie kilkudziesięciu lat (Hermite, 1873, oraz Lindemann, 1882). Ciągle jednak problem postawiony przez Eulera pozostawał otwarty.

W roku 1900 na kongresie w Paryżu D. Hilbert przedstawił 23 otwarte problemy, które w jego opinii stanowiły najpoważniejsze wyzwanie dla matematyki wieku dwudziestego. Wśród nich znajdował się problem siódmy będący zmodyfikowaną wersją problemu Eulera: udowodnić, że jeśli α i β są liczbami algebraicznymi, $\alpha \neq 0, 1$, oraz β nie jest liczbą wymierną, to każda wartość potęgi α^β jest liczbą przestępną.

Warto tutaj zwrócić uwagę na ogólność sformułowań. Liczby α i β są dowolnymi *zespolonymi* liczbami algebraicznymi, a założenie o liczbie β jest tylko takie, że $\beta \notin \mathbf{Q}$. Ponadto, zespolona funkcja potęgowa jest funkcją wieloznaczną, przewiduje się więc, że *każda* wartość potęgi α^β jest liczbą przestępną. Jako przykład, Hilbert wymienia liczby $2^{\sqrt{2}}$ oraz $i^{-2i} = e^\pi$, które powinny być przestępne.

Pierwszy istotny krok w kierunku rozwiązania problemu Hilberta uczynił A. O. Gelfond w 1929 roku. Udowodnił on, że przypuszczenie Hilberta jest prawdziwe, gdy β jest nierzeczywistą niewymiernością kwadratową. A więc, na przykład, $\beta = -2i$ jest nierzeczywistą niewymiernością kwadratową, i na podstawie twierdzenia Gelfonda liczba

$$i^{-2i} = e^{-2i\log i} = e^{(-2i)(-i\pi/2)} = e^\pi$$

jest przestępna. Metody użyte przez Gelfonda miały jednak ograniczony zasięg.

Do pełnego rozstrzygnięcia siódmego problemu Hilberta niezbędne okazało się nowe podejście, które znaleźli niezależnie Gelfond i Th. Schneider w roku 1934.

TWIERDZENIE* 5.1 (A. O. Gelfond, Th. Schneider, 1934).
Jeśli α i β są liczbami algebraicznymi oraz $\alpha \neq 0, 1$ i β nie jest liczbą wymierną, to liczba α^β jest liczbą przestępną.

5.2. Od Gelfonda do Bakera: kombinacje liniowe logarytmów

Twierdzenie Gelfonda-Schneidera można wypowiedzieć następująco:

TWIERDZENIE* 5.2.
Jeśli α, α_1 są niezerowymi liczbami algebraicznymi i liczby $\log\alpha$, $\log\alpha_1$ są liniowo niezależne nad ciałem $\mathbf{Q}$ liczb wymiernych, to $\log\alpha$, $\log\alpha_1$ są liniowo niezależne nad ciałem $\mathbf{A}$ wszystkich liczb algebraicznych.

Przede wszystkim zauważmy, że jeśli liczby $\log\alpha$, $\log\alpha_1$ są liniowo niezależne nad $\mathbf{Q}$ (nad $\mathbf{A}$), to $\alpha \neq 1$ oraz ich iloraz $\log\alpha_1/\log\alpha$ nie należy do $\mathbf{Q}$ (do $\mathbf{A}$).

Pokażemy najpierw, że 5.1 $\Rightarrow$ 5.2. Przypuśćmy, że iloraz $\beta := \log\alpha_1/\log\alpha$ nie jest liczbą wymierną, ale jest liczbą algebraiczną. Wtedy to na podstawie 5.1 liczba $\alpha_1 = \alpha^\beta$ jest przestępna, sprzeczność. A więc jeśli $\beta \notin \mathbf{Q}$, to także $\beta \notin \mathbf{A}$, co dowodzi 5.2.

A teraz dowód, że 5.2 $\Rightarrow$ 5.1. Załóżmy więc, że $\alpha \neq 0, 1$ oraz β są liczbami algebraicznymi oraz $\beta \notin \mathbf{Q}$. Połóżmy $\alpha_1 = \alpha^\beta$. Gdyby liczba α_1 była algebraiczna, to na podstawie 5.2 byłoby $\beta = \log\alpha_1/\log\alpha \notin \mathbf{A}$, sprzeczność. A więc liczba α_1 jest przestępna, co dowodzi 5.1.

Widzimy teraz, że twierdzenie Gelfonda-Schneidera w sformułowaniu 5.2 potwierdza opinię Eulera: jeśli a i b są dodatnimi liczbami wymiernymi oraz $(\log b)/(\log a)$ nie jest liczbą wymierną, to nie jest też liczbą algebraiczną.

Twierdzenie* 5.2 nasuwa natychmiast pytanie, czy podobny rezultat ma miejsce dla logarytmów dowolnej skończonej liczby liczb algebraicznych $\alpha_1, \ldots, \alpha_n$. Metody Gelfonda i Schneidera nie przenoszą się automatycznie na ten ogólniejszy przypadek i dopiero po 30 latach udało się udowodnić następującą ogólną wersję twierdzenia* 5.2.

TWIERDZENIE* 5.3 (A. Baker, 1966).
Jeśli $\alpha_1, \ldots, \alpha_n$ są niezerowymi liczbami algebraicznymi oraz $\log\alpha_1, \ldots, \log\alpha_n$ są liniowo niezależne nad ciałem $\mathbf{Q}$ liczb wymiernych, to liczby $1, \log\alpha_1, \ldots, \log\alpha_n$ są liniowo niezależne nad ciałem $\mathbf{A}$ wszystkich liczb algebraicznych.

Twierdzenie Bakera pozwala znacznie rozszerzyć klasę przykładów liczb przestępnych. Oto wnioski z twierdzenia Bakera.

(a) Każda niezerowa kombinacja liniowa $\beta_1\log\alpha_1 + \cdots + \beta_n\log\alpha_n$, logarytmów niezerowych liczb algebraicznych $\alpha_1, \ldots, \alpha_n$ z algebraicznymi współczynnikami $\beta_1, \ldots, \beta_n$, jest liczbą przestępną.

(b) Liczba $e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$, gdzie $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n$ są niezerowymi liczbami algebraicznymi, jest liczbą przestępną.

(c) Liczba $\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$, gdzie $\alpha_1, \ldots, \alpha_n$ są liczbami algebraicznymi różnymi od 0 i 1 oraz $1, \beta_1, \ldots, \beta_n$ są liczbami algebraicznymi liniowo niezależnymi nad ciałem liczb wymiernych, jest przestępna.

Alan Baker otrzymał medal Fieldsa w Nicei w 1970 roku (pozostali laureaci: Hironaka, Novikov, Thompson).

6. Zastosowania

Spośród licznych zastosowań aproksymacji diofantycznych wskażemy tylko trzy najsłynniejsze. Pierwszym jest twierdzenie Thuego o skończoności liczby rozwiązań pewnej klasy równań diofantycznych.

TWIERDZENIE* 6.1 (A. Thue, 1908).
Niech $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$ *będzie formą dwóch zmiennych stopnia* $n \geq 3$ *o współczynnikach całkowitych, nierozkładalną nad ciałem liczb wymiernych* $\mathbf{Q}$. *Wtedy dla każdej liczby całkowitej* m *równanie*

$$F(X,Y) = m \tag{9}$$

ma tylko skończoną liczbę rozwiązań w liczbach całkowitych.

Idea dowodu tego twierdzenia jest dość przejrzysta. Rozpatrujemy wielomian $f = f(X) = F(X,1)$ i dla uproszczenia zakładamy, że $a_0 = 1$. Niech $\theta_1, \ldots, \theta_n$ będą pierwiastkami wielomianu f w ciele liczb zespolonych. Zatem wobec tożsamości $F(X,Y) = Y^n f(X/Y)$ dla każdego rozwiązania x, y, $y \neq 0$ naszego równania mamy

$$|f(x/y)| = \left|\frac{x}{y} - \theta_1\right| \cdots \left|\frac{x}{y} - \theta_n\right| = \frac{|m|}{|y|^n}. \tag{10}$$

Zauważmy, że nierozkładalność formy F nad ciałem liczb wymiernych pociąga za sobą to, że pierwiastki wielomianu f są jednokrotne. Zatem liczba

$$c := \min_{i \neq j} \{ |\theta_i - \theta_j| \}$$

jest dodatnią liczbą rzeczywistą.

Przypuśćmy teraz, że równanie (9) ma nieskończenie wiele rozwiązań w liczbach całkowitych x, y. Wtedy z równości (10) wynika, że dla każdego rozwiązania x, y, gdzie $y \neq 0$, przynajmniej jeden z czynników $|x/y - \theta_i|$ jest bardzo małą liczbą rzeczywistą (gdyż $f(x/y) \to 0$, gdy $|y| \to \infty$). Weźmy rozwiązanie x, y równania (9) takie, że po ewentualnej zmianie numeracji pierwiastków $\theta_1, \ldots, \theta_n$ zachodzi nierówność

$$\left|\frac{x}{y} - \theta_1\right| < \frac{1}{2}c. \tag{11}$$

Wtedy dla $i > 1$ mamy

$$\left|\frac{x}{y} - \theta_i\right| = |\theta_i - \theta_1 - \left(\frac{x}{y} - \theta_1\right)| \geq |\theta_i - \theta_1| - \left|\frac{x}{y} - \theta_1\right| > c - \frac{1}{2}c = \frac{1}{2}c.$$

Ponieważ założyliśmy, że istnieje nieskończenie wiele rozwiązań x, y równania (9), więc z zasady szufladkowej Dirichleta wynika, że dla pewnego pierwiastka θ_1 wielomianu f nierówność (11) jest spełniona przez nieskończenie wiele rozwiązań x, y równania (9).

Dla x, y w tej serii rozwiązań mamy zatem

$$\left|\frac{x}{y} - \theta_1\right| \cdot \left(\frac{1}{2}c\right)^{n-1} < |f(x/y)| = \frac{|m|}{|y|^n}.$$

Istnieje więc stała $c_1 > 0$ taka, że nierówność

$$\left|\frac{x}{y} - \theta_1\right| < \frac{c_1}{|y|^n}$$

zachodzi dla nieskończenie wielu par liczb całkowitych x, y. Zauważmy, że liczba θ_1 musi być liczbą rzeczywistą, gdyż nierzeczywista liczba zespolona nie daje się aproksymować liczbami wymiernymi. Tymczasem jednak na podstawie twierdzenia Thuego o aproksymacji liczb algebraicznych liczbami wymiernymi istnieje taka stała c_2, że

$$\frac{c_2}{|y|^{n/2+1+1/4}} < \left|\frac{x}{y} - \theta_1\right|$$

dla każdych liczb całkowitych x, y. Stąd wynika, że

$$|y|^{n/2-5/4} < c_1/c_2. \tag{12}$$

Ponieważ $n \geq 3$, wykładnik $n/2 - 5/4$ jest liczbą dodatnią, zatem nierówność (12) nie może zachodzić dla dostatecznie dużych wartości $|y|$. Dowodzi to, że równanie $F(X,Y) = m$ nie może mieć nieskończenie wielu rozwiązań w liczbach całkowitych.

Jako drugi słynny przykład przytoczymy rozwiązanie tak zwanego problemu dziesiątego wyróżnika w teorii form kwadratowych i algebraicznej teorii

liczb. Problem ten pochodzi od samego Gaussa, który w 1801 roku w swoich znakomitych *Disquisitiones Arithmeticae* stworzył podstawy głębokiej arytmetycznej teorii form kwadratowych. Dla form binarnych z całkowitymi współczynnikami i wyróżnikiem ujemnym Gauss znalazł tylko dziewięć wyróżników d o tej własności, że każde dwie formy o wyróżniku d są równoważne. Wyraził też przekonanie, że więcej takich ujemnych wyróżników nie ma. Pod koniec wieku dziewiętnastego stwierdzono, że problem Gaussa ma równoważne sformułowanie w języku nierzeczywistych ciał kwadratowych $\mathbf{Q}(\sqrt{d})$. Okazuje się, że dla $d < 0$ każde dwie binarne formy kwadratowe o wyróżniku d są równoważne wtedy i tylko wtedy, gdy ciało kwadratowe $\mathbf{Q}(\sqrt{d})$ ma własność jednoznaczności rozkładu liczb na czynniki nierozkładalne. W języku ciał liczbowych przypuszczenie Gaussa oznacza więc, że istnieje tylko 9 nierzeczywistych ciał kwadratowych z własnością jednoznaczności rozkładu. W 1934 roku Heilbronn i Linfoot udowodnili, że hipoteza Gaussa jest niemal prawdziwa: istnieje co najwyżej 10 takich wyróżników.

Problem został w końcu rozstrzygnięty w 1966 roku przez A. Bakera przy pomocy znalezionych przez niego efektywnych oszacowań dla kombinacji liniowych logarytmów liczb algebraicznych. W tym samym roku inne rozwiązanie tego problemu znalazł także H. M. Stark. Rezultat jest więc następujący:

Jedynymi nierzeczywistymi ciałami kwadratowymi z własnością jednoznaczności rozkładu na czynniki nierozkładalne są następujące ciała:

$$\mathbf{Q}(\sqrt{d}), \quad \text{dla } d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Wreszcie wspomnijmy o ekspansji idei i technik aproksymacji diofantycznych na obszar geometrii algebraicznej. Wielkim sukcesem arytmetycznej geometrii algebraicznej ostatnich lat jest znalezienie nowych dowodów hipotezy Mordella o skończoności liczby punktów całkowitych na krzywych rodzaju ≥ 2 (Paul Vojta, Gerd Faltings i Enrico Bombieri). Bazują one w dużej mierze na technice aproksymacji diofantycznych (aproksymacje diofantyczne na rozmaitościach abelowych). Zainteresowanego Czytelnika odsyłamy do Mathematical Reviews 93d:11065, 11066, gdzie znajduje się świetne omówienie tej problematyki.

Literatura

A. Baker, *Transcendental Number Theory.* Cambridge University Press, Cambridge 1975.

M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J. P. Schreiber, *Pisot and Salem numbers.* Birkhäuser, Basel 1992.

J.W.S. Cassels, *An Introduction to Diophantine Approximation.* Cambridge University Press, Cambridge 1957. (Tłum. j. ros., Moskwa 1961).

T. W. Cusick and M. E. Flahive, *The Markoff and Lagrange Spectra.* Math. Surveys and Monographs, AMS, Providence, RI, 1989.

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* 4-th ed., Clarendon Press, Oxford 1960.

J. F. Koksma, *Diophantische Approximationen.* Ergebnisse der Math. und ihrer Grenzgebiete 4. Springer Verlag, Berlin und Leipzig 1936.

L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences.* Wiley, New York 1974.

I. Niven, *Irrational Numbers.* Carus Math. Monographs 11. MAA 1956.

K. F. Roth, *Rational approximation to algebraic numbers.* [w:] Mathematika **2** (1955), 1–20.

W. M. Schmidt, *Simultaneous approximation to algebraic numbers by rationals.* [w:] Acta Math. **125** (1970), 189–201.

W. M. Schmidt, *Diophantine Approximation.* Lecture Notes in Mathematics 785. Springer Verlag, 1980. (Tłum. j. ros., Moskwa 1983).