Liczby przestępne i twierdzenie Liouville'a

Pamięci Andrzeja Mąkowskiego

Michał KRYCH[*]

W 1744 roku w książce „Wprowadzenie do analizy” Leonhard Euler sformułował hipotezę, że jeśli liczby a, b są wymierne i nie istnieją takie liczby całkowite p, q, że $b = a^{p/q}$, to liczba $\log_a b$ nie jest pierwiastkiem żadnego wielomianu o współczynnikach całkowitych, czyli że $\log_a b$ jest *liczbą przestępną*. W tamtych czasach nikt nie potrafił udowodnić powyższej hipotezy ani nawet wykazać tego, że istnieją liczby przestępne. Minęło 100 lat i sytuacja uległa radykalnej zmianie. Joseph Liouville zdołał dowieść, że pewne liczby są przestępne. W roku 1851 opublikował pracę, dzięki której można np. pokazać, że liczba

$$\ell = 0{,}110\,001\,000\,000\,000\,000\,000\,001\,000\,000\,000\,000\,000\ldots =$$
$$= 10^{-1!} + 10^{-2!} + 10^{-3!} + 10^{-4!} + \cdots$$

jest przestępna. Nie zdołał jednak wykazać przestępności liczby e. Dopiero w 1873 roku dowiódł tego Charles Hermite, natomiast w 1882 r. Ferdinand Lindemann wykazał, że przestępna jest także liczba π. Przestępność logarytmów, o których pisał Euler, została udowodniona dopiero w pierwszej połowie dwudziestego wieku przez Aleksandra Gelfonda i Theodora Schneidera.

Sformułujemy teraz twierdzenie Liouville'a, dzięki któremu można wykazać przestępność liczby ℓ i które rozpoczęło bogatą i trudną teorię.

Twierdzenie Liouville'a. *Jeśli liczba niewymierna x_0 jest pierwiastkiem równania*

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

i liczby $a_0, a_1, a_2, \ldots, a_n$ są całkowite, przy czym $n \geqslant 1$ i $a_n \neq 0$, to istnieje taka liczba $C > 0$, że dla dowolnych liczb całkowitych p i $q > 0$ zachodzi nierówność

$$\left|x_0 - \frac{p}{q}\right| \geqslant \frac{C}{q^n}.$$

Dowód jest bardzo prosty. Niech

$$w(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

Równanie $w(x) = 0$ ma skończenie wiele rozwiązań. Istnieje więc taka liczba $\delta > 0$, że z nierówności $0 < |x_0 - r| \leqslant \delta$ i warunku $w(x_0) = 0$ wynika, iż $w(r) \neq 0$, tzn. w przedziale $[x_0 - \delta, x_0 + \delta]$ równanie $w(x) = 0$ ma tylko jeden pierwiastek x_0. Jeśli więc $r = \frac{p}{q} \in [x_0 - \delta, x_0 + \delta]$, a liczby p, q są całkowite i $|x_0 - r| \leqslant \delta$, to $w(r) \neq 0$. Oczywiście

$$w(r) = \frac{1}{q^n}(a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_np^n).$$

Wynika stąd, że liczba $q^nw(r)$ jest całkowita, a ponieważ jest różna od 0, więc $\left|q^nw(r)\right| \geqslant 1$.

W dalszym ciągu będziemy zakładać, że $\delta < 1$. Możemy, bo przedział o środku x_0, który nie zawiera pierwiastków wielomianu w, możemy tak skrócić, by jego długość była mniejsza niż 2. Ustalmy zatem $r = \frac{p}{q}$ takie, że $\left|x_0 - \frac{p}{q}\right| \leqslant \delta$. Niech A będzie największą z liczb całkowitych $|a_0|, |a_1|, |a_2|, \ldots, |a_n|$ i niech $M = 1 + |x_0|$. W szczególności wiemy, że $|r| \leqslant M$. Mamy

$$|w(r)| = |w(x_0) - w(r)| = |a_1(x_0 - r) + a_2(x_0^2 - r^2) + \cdots + a_n(x_0^n - r^n)| =$$
$$= |x_0 - r| \cdot |a_1 + a_2(x_0 + r) + \cdots + a_n(x_0^{n-1} + x_0^{n-2}r + x_0^{n-3}r^2 + \cdots + r^{n-1})| \leqslant$$
$$\leqslant |x_0 - r| \cdot (|a_1| + |2a_2M| + \cdots + |na_nM^{n-1}|) \leqslant$$
$$\leqslant A(1 + 2M + 3M^2 + \cdots + nM^{n-1})|x_0 - r|.$$

Wynika stąd, że

$$1 \leqslant |q^nw(r)| \leqslant q^nA(1 + 2M + 3M^2 + \cdots + nM^{n-1})|x_0 - r|.$$

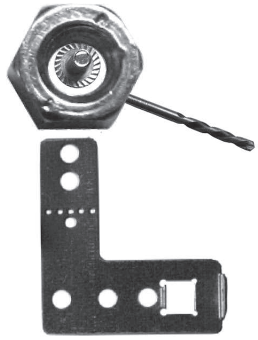
Wystarczy więc przyjąć, iż

$$C = \frac{1}{A(1 + 2M + 3M^2 + \cdots + nM^{n-1})},$$

by teza twierdzenia była spełniona dla $\frac{p}{q} = r \in [x_0 - \delta, x_0 + \delta]$. Jeśli $\left|x_0 - \frac{p}{q}\right| \geqslant \delta$,

[*]Instytut Matematyki, Uniwersytet Warszawski

to nierówność może nie zachodzić, ale wystarczy zastąpić C przez $\tilde{C} = C\delta < C$, by była ona spełniona dla wszystkich liczb wymiernych $\frac{p}{q}$. W ten sposób zakończyliśmy dowód twierdzenia.



Pokażemy teraz, że liczba ℓ nie spełnia warunku z twierdzenia Liouville'a niezależnie od wyboru n. Załóżmy, że ℓ jest pierwiastkiem wielomianu stopnia $n \geqslant 1$ o współczynnikach całkowitych. Istnieje wtedy taka liczba $C > 0$, że dla dowolnych liczb całkowitych p, q zachodzi nierówność

$$\left|\ell - \frac{p}{q}\right| \geqslant \frac{C}{q^n}.$$

Niech $q = 10^{k!}$ i $p = q \cdot \left(10^{-1!} + 10^{-2!} + 10^{-3!} + 10^{-4!} + \dots + 10^{-k!}\right)$. Wtedy

$$\frac{C}{10^{n\cdot k!}} \leqslant \left|\ell - \frac{p}{q}\right| = \ell - \frac{p}{q} = 10^{-(k+1)!} + 10^{-(k+2)!} + 10^{-(k+3)!} + \dots < \frac{2}{10^{(k+1)!}}.$$

Wynika stąd, że

$$10^{(k+1-n)\cdot k!} < \frac{2}{C},$$

co nie jest możliwe, bo liczbę $10^{(k+1-n)\cdot k!}$ możemy uczynić tak dużą, jak chcemy, wybierając odpowiednio dużą liczbę k. Przekonaliśmy się, że liczba ℓ nie jest pierwiastkiem żadnego wielomianu o współczynnikach całkowitych.

Twierdzenie Liouville'a mówi, że pierwiastków wielomianów o współczynnikach całkowitych nie można zbyt dobrze przybliżać liczbami wymiernymi: jeśli chcemy podejść bardzo blisko takiego pierwiastka, to musimy mocno zwiększyć mianownik. Oczywiście można powiedzieć, że dowolnie blisko liczby rzeczywistej znajdą się liczby wymierne, ale pomysł porównania tej odległości z odwrotnością potęgi mianownika okazał się niezwykle owocny.

Można udowodnić, że dla każdej liczby niewymiernej x_0 i każdej liczby naturalnej n istnieją takie liczby całkowite p_n i $q_n > n$, że

$$\left|x_0 - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Nie jest to wcale trudne, uzasadnienie można znaleźć np. w każdej książce, w której omawiane są tzw. ułamki łańcuchowe, którymi zresztą Liouville też się zajmował.

Jeśli x_0 jest pierwiastkiem wielomianu kwadratowego o współczynnikach całkowitych i $\varepsilon > 0$, to z twierdzenia Liouville'a wynika, że nierówność

$$\left|x_0 - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

jest spełniona jedynie dla skończenie wielu par liczb całkowitych p, q. Ta uwaga prowadzi do pytania:

Dana jest liczba niewymierna x_0. Dla jakich liczb $\varepsilon > 0$ istnieje jedynie skończenie wiele par liczb całkowitych p, q, dla których

$$\left|x_0 - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}} \ ?$$

Z twierdzenia Liouville'a wynika, że dla pierwiastków wielomianów stopnia n o współczynnikach całkowitych jest tak, gdy $2 + \varepsilon > n$. W 1909 r pojawiła się praca Axela Thue, w której autor wykazał, że wystarczy, by $2 + \varepsilon > \frac{n}{2} + 1$. W roku 1921 Carl Siegel wykazał, że wystarczy, by $2 + \varepsilon > 2\sqrt{n}$. W końcu w roku 1955 Klaus Roth wykazał, że wystarczy, by $2 + \varepsilon > 2$, czyli że $\varepsilon > 0$ może być dowolny. Za ten wynik został w 1958 r. nagrodzony medalem Fieldsa. Z twierdzenia Thue–Siegela–Rotha wynika, że jeśli $\varepsilon > 0$ i dla każdej liczby naturalnej n istnieją takie liczby całkowite p_n i $q_n > n$, że

$$\left|x_0 - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{2+\varepsilon}},$$

to liczba niewymierna x_0 nie jest pierwiastkiem wielomianu o współczynnikach całkowitych.