Liczby e i π są przestępne

Zaczniemy od twierdzenia pochodzącego od J.Liouville'a — pierwszego, które pozwoliło na wykazanie, że niektóre liczby nie są pierwiastkami wielomianów o współczynnikach całkowitych.

Twierdzenie Liouville'a

Jeśli liczba niewymierna d jest pierwiastkiem wielomianu $a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, $n \geq 1$, to istnieje stała $C > 0$ taka, że dla dowolnej pary liczb całkowitych p, q, $q > 0$ zachodzi nierówność $\left|x_0 - \frac{p}{q}\right| \geq \frac{C}{q^n}$.

Dowód.

Niech $h(x) = a_0 + a_1 x + \cdots + a_n x^n$. Niech $\delta > 0$ będzie taką liczbą, że jeśli $0 < |x - x_0| \leq \delta$, to $h(x) \neq 0$. Taka liczba δ istniej, bo wielomian h ma skończoną liczbę pierwiastków — zakładamy, że jedynym pierwiastkiem h w przedziale $[x_0 - \delta, x_0 + \delta]$ jest x_0. Załóżmy, że $\left|\frac{p}{q} - x_0\right| \leq \delta$. Niech $\hat{C} = \sup\{|h'(x)|: \quad |x - x_0| \leq \delta\}$. Z określenia x_0, δ i twierdzenia o wartości średniej wynika, że

$$0 < \left|h(\tfrac{p}{q})\right| = \left|h(\tfrac{p}{q}) - h(x_0)\right| \leq \hat{C}\left|\tfrac{p}{q} - x_0\right|.$$

Jasne jest też, że $h(\frac{p}{q}) = \frac{\ell}{q^n}$ dla $\ell = a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n \in \mathbb{Z}$. Ponieważ $h(\frac{p}{q}) \neq 0$, więc $\ell \neq 0$, zatem $|\ell| \geq 1$. Wynika stąd, że $\left|\frac{p}{q} - x_0\right| \geq \frac{1}{\hat{C} q^n}$. Przyjmujemy $C = \min\{\frac{1}{\delta}, \frac{1}{\hat{C}}\}$. Jest jasne, że dla tak zdefiniowanej liczby C teza twierdzenia jest spełniona. ■

Zadanie

Udowodnić, że liczba $\sum\limits_{n=1}^{\infty} \frac{1}{10^{n!}}$ jest przestępna, tzn. nie jest pierwiastkiem żadnego niezerowego wielomianu o współczynnikach całkowitych. ■

A teraz cytat z miesięcznika Δ sprzed kilkunastu a może i dwudziestu lat (tu nie ma naruszenia praw autorskich, bo sam to pisałem).

◀ W 1761 roku niemieckiemu matematykowi, J.H.Lambertowi udało się udowodnić, że liczba π jest niewymierna. Jego dowód wykorzystywał tzw. ułamki łańcuchowe. Podobny dowód znalazł nieco później Francuz A.Legendre. Około stu lat później Liouville sformułował i udowodnił twierdzenie, które pozwoliło wskazać konkretne liczby przestępne, tj. takie, które nie są pierwiastkami żadnego niezerowego wielomianu o współczynnikach całkowitych. Po upływie niewielu lat Hermite udowodnił, że jedna z najważniejszych liczb w matematyce, liczba e jest przestępna, a wkrótce Lindemann wykazał, że znana od starożytności liczba π również jest przestępna.Tym samym, okazało się, że kwadratura koła nie jest wykonalna. O ile mi wiadomo, około 1956 roku I.Niven wzorując się na wspomnianym wyżej dowodzie Hermite'a, podał dowód niewymierności π wykorzystujący jedynie najprostsze własności całek, znane obecnie uczniom szkół średnich. Jego rozumowanie przytoczymy poniżej.

Załóżmy, że $\pi = \dfrac{p}{q}$, gdzie p oraz q oznaczają liczby naturalne. Zdefiniujmy ciąg (c_n) wzorem $c_n = \dfrac{q^n}{n!} \displaystyle\int_0^\pi [x(\pi - x)]^n \sin x \, dx$. Wykażemy, że

1° $\lim_{n\to\infty} c_n = 0$;

2° $c_n > 0$ dla każdej liczby naturalnej n;

3° c_n jest liczbą całkowitą dla każdej liczby naturalnej n.

Oznaczać to będzie, że przyjęte założenie, że $\pi = \frac{p}{q}$ prowadzi do sprzeczności, bo ciąg dodatnich liczb całkowitych nie może być zbieżny do liczby 0.

Udowodnimy własności 1°, 2° i 3° ciągu (c_n).

Jeśli $0 \le x \le \pi$, to $x(\pi - x) \le \frac{\pi^2}{4}$ i $\sin x \ge 0$, zatem zachodzi nierówność: $\pi\left(\frac{\pi}{2}\right)^{2n} \ge \int_0^\pi [x(\pi-x)]^n \sin x dx \ge 0$. Stąd mamy $0 \le c_n \le \frac{\pi}{n!}\left(\frac{q\pi^2}{4}\right)^n$. Ponieważ $\lim_{n\to\infty} \frac{a^n}{n!} = 0$ dla każdej liczby rzeczywistej a, np. dla $a = \frac{q\pi^2}{n!}$, więc $\lim_{n\to\infty} c_n = 0$, co kończy dowód własności 1°.

Całkowana funkcja jest dodatnia wewnątrz przedziału $[0,\pi]$, więc całka z niej na tym przedziale jest dodatnia, zatem $c_n > 0$, co dowodzi, że własność 2° również ma miejsce.

Wykażemy, że własność 3° również przysługuje ciągowi (c_n). Ten fragment rozumowania jest najdłuższy. Niech w oznacza wielomian stopnia k. Pochodne funkcji w są więc równe 0 począwszy od $k+1$–ej, czyli $w^{(j)}(x) = 0$ dla $j \ge k+1$ i dowolnej liczby x. Zaczniemy od obliczenia całki nieoznaczonej $\int w(x)\sin x\,dx$. Całkując dwukrotnie przez części otrzymujemy: $\int w(x)\sin x\,dx = -w(x)\cos x + \int w'(x)\cos x\,dx = -w(x)\cos x + w'(x)\sin x - \int w''(x)\sin x\,dx$. Sprowadziliśmy zatem problem do obliczenia całki $\int w''(x)\sin x\,dx$, a więc do tego samego zadania z tym jednak, że udało się nam zmniejszyć o 2 stopień wielomianu, przez który wymnażamy sinus. Powtarzając to rozumowanie wielokrotnie i biorąc pod uwagę to, że pochodne wielomianu w począwszy od pochodnej $k+1$-ego rzędu zerują się otrzymujemy wzór:

$$\int w(x)\sin x\,dx = \cos x[-w(x) + w''(x) - w^{(4)}(x) + \ldots] + \sin x[w'(x) - w^{(3)}(x) + \ldots],$$

przy czym sumy w nawiasach kwadratowych są skończone, bo od pewnego momentu ich wszystkie składniki są zerami. Niech $w(x) = [x(\pi - x)]^n$. Oczywiście $w(x) = w(\pi - x)$. Wobec tego $w^{(j)}(x) = (-1)^j w^{(j)}(\pi - x)$ dla $j = 0, 1, 2, \ldots$. Jest również $\sin 0 = \sin\pi = 0$ oraz $\cos 0 = 1$, $\cos\pi = -1$. Do stwierdzenia całkowitości liczb c_n wystarczy więc, by liczby $\frac{q^n}{n!}w(0)$, $\frac{q^n}{n!}w''(0)$, $\frac{q^n}{n!}w^{(4)}(0), \ldots$ były całkowite. Zachodzi równość:

$$w^{(j)}(x) = \left(\pi^n x^n - \binom{n}{1}\pi^{n-1}x^{n+1} + \binom{n}{2}\pi^{n-2}x^{n+2} - \binom{n}{3}\pi^{n-3}x^{n+3} + \cdots + (-1)^n x^{2n}\right)^{(j)}.$$

Jeżeli $j < n$, to każdy składnik sumy $w^{(j)}(x)$ zawiera zmienną x z dodatnim wykładnikiem, więc $w^{(j)}(0) = 0$. Dalej mamy $w^{(n)}(0) = n!\pi^n$, $w^{(n+1)}(0) = -(n+1)!\binom{n}{1}\pi^{n-1}$,

$$w^{(n+2)}(0) = (n+2)!\binom{n}{2}\pi^{n-2}, \ldots, w^{(2n)}(0) = (-1)^n(2n)!.$$

Jeśli więc $\pi = \frac{p}{q}$, to liczby $\frac{q^n}{n!}w^{(j)}(0)$ są całkowite dla każdej nieujemnej liczby całkowitej j. To stwierdzenie kończy dowód. ▶

Ten dowód niewymierności liczby π to naśladowanie dowodu przestępności e prezentowanego poniżej.

Niech $w(x) = ax^{p-1}(x-x_1)^p(x-x_2)^p \cdot \ldots \cdot (x-x_n)^p$, $x_1, x_2, \ldots, x_n \in \mathbb{C}$, $a \in \mathbb{Z} \setminus \{0\}$, $p > a$ jest liczbą pierwszą. Funkcja w jest wielomianem stopnia $m = p(n+1)-1$. Z wzoru Leibniza na k–tą pochodną iloczynu dwu lub większej liczby funkcji i z równości

$$\left((x-c)^\nu\right)^{(i)} = \nu(\nu-1)\cdot\ldots\cdot(\nu-i+1)(x-c)^{\nu-i} = i!\tbinom{\nu}{i}x^{\nu-i},$$

wynika, że

$$w^{(j)}(x) = \sum a\cdot j!\cdot\tbinom{p-1}{i_0}\cdot\tbinom{p}{i_1}\cdot\ldots\cdot\tbinom{p}{i_n}\cdot x^{p-i_0}\cdot(x-x_1)^{p-i_1}\cdot(x-x_1)^{p-i_1}\cdot\ldots\cdot(x-x_n)^{p-i_n} \qquad \textbf{(0)}$$

sumowanie rozciąga się na wszystkie ciągi $(i_0, i_1, \ldots, i_n)$, dla których

$$0 \le i_0 \le p-1,\ 0 \le i_1 \le p,\ \ldots,\ 0 \le i_n \le p,\ j = i_0 + i_1 + \cdots + i_n .$$

Bez trudu stwierdzić możemy, że

jeśli $j \ge p$, to $a\cdot j!\cdot\binom{p-1}{i_0}\cdot\binom{p}{i_1}\cdot\ldots\cdot\binom{p}{i_n}$ jest liczbą całkowitą podzielną przez p, **(0.1)**

jeśli $j = p-1$, to $a\cdot j!\cdot\binom{p-1}{i_0}\cdot\binom{p}{i_1}\cdot\ldots\cdot\binom{p}{i_n}$ są podzielne przez p z wyjątkiem:

$a\cdot j!\cdot\binom{p-1}{p-1}\cdot\binom{p}{0}\cdot\ldots\cdot\binom{p}{0} = a(p-1)!$ (przyp. $p > a$ i jest to liczba pierwsza), **(0.2)**

jeśli $j < p-1$, to dla $x \in \{0, x_1, x_2, \ldots, x_n\}$ zachodzi równość

$$a\cdot j!\cdot\tbinom{p-1}{i_0}\cdot\tbinom{p}{i_1}\cdot\ldots\cdot\tbinom{p}{i_n}\cdot x^{p-i_0}\cdot(x-x_1)^{p-i_1}\cdot(x-x_1)^{p-i_1}\cdot\ldots\cdot(x-x_n)^{p-i_n} = 0. \qquad \textbf{(0.3)}$$

Dowody przestępności liczb e oraz π wg. książki *A.Baker, „Transcendental Numbers Theory”*

Twierdzenie Hermite'a, 1873

Liczba e nie jest pierwiastkiem żadnego niezerowego wielomianu o współczynnikach całkowitych.

Załóżmy, że jest ona pierwiastkiem wielomianu stopnia $n \ge 1$ o współczynnikach całkowitych. Istnieją więc liczby całkowite $a_0, a_1, \ldots, a_n$ takie, że $a_0 \ne 0 \ne a_n$ oraz

$$a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0. \qquad (1)$$

Niech $p > \max(n, |a_0|)$ oznacza liczbę pierwszą. Niech

$$w(x) = x^{p-1}(x-1)^p(x-2)^p\cdot\ldots\cdot(x-n)^p .$$

Funkcja w jest wielomianem stopnia $m = p(n+1)-1$. Z własności **(0.3), (0.2), (0,1)** wynika, że

$w^{(j)}(0) = 0$, jeśli $0 \le j < p-1$,

$w^{(p-1)}(0)$ jest liczbą podzielną przez $(p-1)!$, ale niepodzielną przez p (przyp. $p > a$),

$w^{(j)}(0)$ jest liczbą całkowitą podzielną przez $p!$ dla $j > p$.

Z własności **(0.3), (0.2), (0,1)** wynika również, że dla $i = 1, 2, \ldots, n$

$w^{(j)}(i) = 0$, jeśli $0 \le j < p$,

$w^{(j)}(i)$ jest liczbą całkowitą podzielną przez $p!$ dla $j > p$.

Wynika stąd, że liczba $a_0\big[w(0) + w'(0) + \cdots + w^{(m)}(0)\big]$ jest niepodzielna przez p i podzielna przez $(p-1)!$. Liczby $a_k\big[w(k) + w'(k) + \cdots + w^{(m)}(k)\big]$ są podzielne przez $p!$ dla $k = 1, 2, \ldots, n$.

Wobec tego liczba $a_0\big[w(0)+w'(0)+\cdots+w^{(m)}(0)\big]+\sum_{k=1}^{n}a_k\big[w(k)+w'(k)+\cdots+w^{(m)}(k)\big]$ jest niepodzielna przez p, ale jest podzielna przez $(p-1)!$. Jest zatem różna od 0. Wobec tego

$$\Big|a_0\big[w(0)+w'(0)+\cdots+w^{(m)}(0)\big]+\sum_{k=1}^{n}a_k\big[w(k)+w'(k)+\cdots+w^{(m)}(k)\big]\Big|\geq (p-1)! \qquad \mathbf{(2)}$$

Całkujemy przez części $m+1$ razy nie zapominając o tym, że $\deg w=m$, więc $w^{(m+1)}\equiv 0$:

$$I_w(x):=\int_0^x e^{x-t}w(t)\,dt=-e^{x-t}w(t)\Big|_0^x+\int_0^x e^{x-t}w'(t)\,dt=e^xw(0)-w(x)+\int_0^x e^{x-t}w'(t)\,dt=$$
$$=e^xw(0)-w(x)+e^xw'(0)-w'(x)+\int_0^x e^{x-t}w''(t)\,dt=$$
$$=e^x[w(0)+w'(0)]-[w(x)+w'(x)]+\int_0^x e^{x-t}w''(t)\,dt=$$
$$=\ldots=e^x[w(0)+w'(0)+\cdots+w^{(m)}(0)]-[w(x)+w'(x)+\cdots+w^{(m)}(x)]+\int_0^x e^{x-t}w^{(m+1)}(t)\,dt=$$
$$=e^x[w(0)+w'(0)+\cdots+w^{(m)}(0)]-[w(x)+w'(x)+\cdots+w^{(m)}(x)]. \qquad \mathbf{(3)}$$

Podstawiamy teraz kolejno $x=0$, $x=1$, ..., $x=n$, mnożymy kolejne równości przez $a_0,a_1,\ldots a_n$, dodajemy stronami i korzystamy z (1):

$$a_0I_w(0)+a_1I_w(1)+\cdots+a_nI_w(n)=$$
$$=a_0e^0[w(0)+w'(0)+\cdots+w^{(m)}(0)]+a_1e^1[w(0)+w'(0)+\cdots+w^{(m)}(0)]+\cdots+$$
$$+a_ne^n[w(0)+w'(0)+\cdots+w^{(m)}(0)]-a_0[w(0)+w'(0)+\cdots+w^{(m)}(0)]-$$
$$-a_1[w(1)+w'(1)+\cdots+w^{(m)}(1)]-\ldots-a_n[w(n)+w'(n)+\cdots+w^{(m)}(n)]=$$
$$=-a_0[w(0)+w'(0)+\cdots+w^{(m)}(0)]-\sum_{k=1}^{n}a_k\big[w(k)+w'(k)+\cdots+w^{(m)}(k)\big]. \qquad (4)$$

Jasne jest, że jeśli $|t|\leq n$, to $|w(t)|\leq n^{p(n+1)-1}$. Stąd wynika, że jeśli $0\leq x\leq n$, to

$$0\leq\int_0^x e^{x-t}w(t)\,dt\leq x\cdot e^x\cdot n^{p(n+1)-1}\leq e^n\cdot n^{p(n+1)}. \qquad \mathbf{(5)}$$

Z równości **(4)** po uwzględnieniu nierówności **(2)** i **(5)** otrzymujemy

$$e^n\cdot(n^{n+1})^p\geq(p-1)!\,.$$

Przeczy to temu, że $\lim\limits_{p\to\infty}\frac{(n^{n+1})^p}{(p-1)!}=0$. Uzyskana sprzeczność przekonuje nas, że założenie, że e jest pierwiastkiem wielomianu o współczynnikach całkowitych jest błędne. ■

Twierdzenie F.Lindemanna, 1882

Teraz zajmiemy się liczbą π. Jeśli jest ona pierwiastkiem niezerowego wielomianu o współczynnikach całkowitych, to również liczba πi jest pierwiastkiem wielomianu o współczynnikach całkowitych. Jeśli bowiem $a_0+a_1\pi+a_2\pi^2+\cdots+a_n\pi^n=0$ i $a_n\neq0$, $a_j\in\mathbb{Z}$ dla $j=0,1,\ldots,n$, to

$$a_0-ia_1(\pi i)-a_2(\pi i)^2+ia_3(\pi i)^3+\cdots+(-i)^na_n(\pi i)^n=a_0+a_1\pi+a_2\pi^2+\cdots+a_n\pi^n=0,$$

zatem

$$a_0-a_2(\pi i)^2+a_4(\pi i)^4+\cdots=i\big[a_1(\pi i)-a_3(\pi i)^3+a_5(\pi i)^5+\cdots\big],$$

i wobec tego

$$\big[a_0-a_2(\pi i)^2+a_4(\pi i)^4+\cdots\big]^2=-\big[a_1(\pi i)-a_3(\pi i)^3+a_5(\pi i)^5+\cdots\big]^2,$$

czyli

$$\big[a_0-a_2(\pi i)^2+a_4(\pi i)^4+\cdots\big]^2+\big[a_1(\pi i)-a_3(\pi i)^3+a_5(\pi i)^5+\cdots\big]^2=0.$$

Po lewej stronie, po otwarciu nawiasów i uporządkowaniu wyrażenia względem potęg liczby πi otrzymujemy kombinację liniową o współczynnikach całkowitych liczb 1, πi, ..., $(\pi i)^{2n}$, przy czym współczynnik przy $(\pi i)^{2n}$ jest równy $a_n^2 \neq 0$.

Niech f będzie wielomianem najniższego dodatniego stopnia, o współczynnikach całkowitych, którego jednym z pierwiastków jest liczba $\pi i = z_1$. Niech $z_2, z_3, \ldots, z_n$ oznaczają pozostałe pierwiastki tego wielomianu.*

Mamy

$$\left(e^{z_1}+1\right)\left(e^{z_2}+1\right)\cdot\ldots\cdot\left(e^{z_n}+1\right) = \left(e^{\pi i}+1\right)\left(e^{z_2}+1\right)\cdot\ldots\cdot\left(e^{z_n}+1\right) = 0\,.$$

Wymnażając wyrażenia w nawiasach po lewej stronie otrzymujemy sumę 2^n wyrażeń postaci e^{α}, gdzie $\alpha = \varepsilon_1 z_1 + \varepsilon_2 z_2 + \cdots + \varepsilon_n z_n$, $\varepsilon_j \in \{0,1\}$. Niech k oznacza liczbę niezerowych wykładników α i niech $\alpha_1, \alpha_2, \ldots, \alpha_k$ oznaczają te niezerowe wykładniki. Mamy więc

$$0 = \left(e^{z_1}+1\right)\left(e^{z_2}+1\right)\cdot\ldots\cdot\left(e^{z_n}+1\right) = e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_k} + 2^n - k\,.$$

Niech p oznacza liczbę pierwszą, b niech będzie współczynnikiem kierującym wielomianu f i niech

$$w(x) = b^{kp}\cdot x^{p-1}\cdot(x-\alpha_1)^p\cdot(x-\alpha_2)^p\cdot\ldots\cdot(x-\alpha_k)^p\,.$$

Niech $m = \deg w = (k+1)p - 1$. Definiujemy I_w jak poprzednio (zob. **(3)**):

$$I_w(x) = e^x[w(0)+w'(0)+\cdots+w^{(m)}(0)] - [w(x)+w'(x)+\cdots+w^{(m)}(x)] = \int_0^1 xe^{x(1-t)}w(tx)\,dt\,.$$

Występuje tu całka z funkcji o wartościach zespolonych, jest ona sumą całki z części rzeczywistej oraz iloczynu i przez całkę z części urojonej. Niech

$$J = \sum_{\iota=1}^{k} I_w(\alpha_\iota) = \sum_{\iota=1}^{k}\Big[e^{\alpha_\iota}\sum_{j=0}^{m} w^{(j)}(0) - \sum_{j=0}^{m} w^{(j)}(\alpha_\iota)\Big] = -\sum_{j=0}^{m}\sum_{\iota=1}^{k} w^{(j)}(\alpha_\iota) - [2^n-k]\sum_{j=0}^{m} w^{(j)}(0)\,.$$

Niech $S(\alpha_1,\alpha_2,\ldots,\alpha_k) = \frac{1}{p!}\sum_{\iota=1}^{k} w^{(j)}(\alpha_\iota)$. Funkcja S zmiennych $\alpha_1,\alpha_2,\ldots,\alpha_k$ jest wielomianem symetrycznym tych zmiennych, tzn. dla każdej permutacji $\sigma\{1,2,\ldots,k\} \longrightarrow \{1,2,\ldots,k\}$ zachodzi równość $S(\alpha_{\sigma(1)},\alpha_{\sigma(2)},\ldots,\alpha_{\sigma(k)}) = S(\alpha_1,\alpha_2,\ldots,\alpha_k)$. Współczynniki wielomianu S są liczbami całkowitymi, zob. własności **(0.1)**, **(0.2)**, **(0.3)**.

Ponieważ $w^{(j)}(\alpha_\iota) = 0$ dla $j < p$, $\iota \in \{1,2,\ldots k\}$, więc możemy potraktować S jako wielomian symetryczny zmiennych $b\alpha_1, b\alpha_2, \ldots, b\alpha_k$. Można więc potraktować to wyrażenie jako wielomian symetryczny wszystkich 2^n zmiennych: $y_1, y_2, \ldots, y_{2^n}$, gdzie $y_\nu = b(\varepsilon_1 z_1 + \varepsilon_2 z_2 + \cdots + \varepsilon_n z_n)$, $\varepsilon_j \in \{0,1\}$, $\nu = 1 + \sum_{\iota=1}^{n}\varepsilon_\iota 2^\iota$ po prostu dopisujemy „brakujące" jednomiany z „opuszczonymi" zerami.

Niech $s_1 = \sum_{1\le\mu\le 2^n} y_\mu$, $s_2 = \sum_{1\le\mu<\nu\le 2^n} y_\mu y_\nu$, $\ldots$, $s_{2^n} = y_1 y_2 \ldots y_{2^n}$.

Z zasadniczego twierdzenia teorii wielomianów symetrycznych (na końcu tego tekstu) wynika, że wielomian S możemy potraktować jako wielomian o współczynnikach całkowitych zmiennych $s_1, s_2, \ldots, s_{2^n}$. Z wzorów Viète'a wynika, że sumy $s_1, s_2, \ldots, s_{2^n}$ są wielomianami symetrycznymi o współczynnikach całkowitych zmiennych $z_1, z_2, \ldots, z_n$ (po to był współczynnik w definicji

* f nie ma pierwiastków podwójnych, gdyby miał, to moglibyśmy zmniejszyć stopień f dzieląc go przez $nwd(f,f')$ i mnożąc przez wspólną wielokrotność mianowników otrzymanego wielomianu o współczynnikach wymiernych.

wielomianu w, inaczej mogłyby być wymierne, niekoniecznie całkowite). Wynika stąd, że liczba $\sum_{j=0}^{m}\sum_{\iota=1}^{k} w^{(j)}(\alpha_\iota)$ jest całkowita i podzielna przez $p!$. Natomiast suma $\sum_{j=0}^{m} w^{(j)}(0)$ jest podzielna przez $(p-1)!$, ale **nie** jest podzielna przez $p!$, jeśli $p > |b|$. Stąd wynika, że liczba całkowita J nie jest równa 0 (jako niepodzielna przez p), a ponieważ jest podzielna przez $(p-1)!$, więc $|J| \geq (p-1)!$.

Niech $\beta = \max\{|\alpha_1|, |\alpha_2|, \ldots, |\alpha_n|, |b^k|\}$ i niech $|x| \leq \beta$. Wtedy

$$|w(x)| \leq |b^k|^p \cdot |x|^{p-1} \cdot |x-\alpha_1|^p \cdot |x-\alpha_2|^p \cdot \ldots \cdot |x-\alpha_n|^p \leq \beta^p \cdot \beta^{p-1} \cdot (2\beta)^{np} < (2\beta)^{(n+2)p-1}.$$

Wobec tego, jeśli $|x| \leq \beta$, to

$$|I_w(x)| \leq |x| \cdot e^{|x|}(2\beta)^{(n+2)p-1} < e^\beta \cdot (2\beta)^{(n+2)p}$$

Stąd wynika, że

$$|J| = \Big|\sum_{\iota=1}^{k} I_w(\alpha_\iota)\Big| \leq ke^\beta \cdot (2\beta)^{(n+2)p} \leq 2^n e^\beta \cdot (2\beta)^{(n+2)p}.$$

Uzyskana nierówność w połączeniu z poprzednią prowadzi do wniosku, że

$$(p-1)! \leq |J| \leq 2^n e^\beta \cdot (2\beta)^{(n+2)p},$$

co przeczy temu, że

$$\lim_{p\to\infty} 2^n \beta \frac{(2\beta)^p}{(p-1)!} = 0.$$

Dowód przestępności liczby π został zakończony.

Wielomiany symetryczne

Funkcję $f\colon \mathbb{R}^k \longrightarrow \mathbb{R}$ lub $f\colon \mathbb{C}^k \longrightarrow \mathbb{C}$ nazywamy wielomianem symetrycznych k zmiennych, jeśli istnieją liczby $a_{i_1,i_2,\ldots,i_k}$, $0 \leq i_1, i_2, \ldots, i_k \leq d$, takie, że dla każdego $\mathbf{x} \in \mathbb{R}^k$ zachodzi równość

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_k) = \textstyle\sum_{i_1,i_2,\ldots,i_k} a_{i_1,i_2,\ldots,i_k} x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}$$

i dla każdej permutacji $\sigma\colon \{1,2,\ldots,k\} \longrightarrow \{1,2,\ldots,k\}$ zachodzi równość

$$f(x_1, x_2, \ldots, x_k) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(k)}).$$

Algebraicy definiują wielomiany nieco inaczej, nazywają oni obiekt przez nas zdefiniowany funkcją wielomianową, ale w przypadku wielomianów o współczynnikach rzeczywistych, zespolonych, wymiernych różnica jest tylko formalna.

Funkcja f zdefiniowana wzorem $f(x_1,x_2) = x_1x_2^2$ nie jest wielomianem symetrycznym, bo $f(1,3) = 9 \neq 3 = f(3,1)$. Funkcja $x_1^2 + x_1x_2 + x_2^2 + x_3^2 + x_3(x_1+x_2)$ jest wielomianem symetrycznym. Uczniowie w szkołach spotykają się z wielomianami symetrycznymi dwu zmiennych przy okazji równań kwadratowych. Stosują wzory Viète'a, by wyrazić np. sumę $x_1^3 + x_2^3$ za pomocą współczynników wielomianu kwadratowego. Odbywa się to mniej więcej tak :

$$x_1^3 + x_2^3 = (x_1+x_2)^3 - 3x_1^2x_2 - 3x_1x_2^2 = (x_1+x_2)^3 - 3(x_1x_2)(x_1+x_2).$$

Udaje się więc wyrazić wielomian symetryczny za pomocą wyrażenia zależnego jedynie od x_1+x_2 i x_1x_2 (wielomianu zmiennych x_1+x_2 i x_1x_2), przy czym jeśli współczynniki wyjściowego wielomianu są liczbami całkowitymi, to również współczynniki drugiego wielomianu są liczbami całkowitymi. Nie jest to przypadek. Zaczniemy od definicji elementarnych wielomianów symetrycznych, która jest niezbędna do sformułowania twierdzenia. Niech

$$
\begin{aligned}
&s_1 = x_1 + x_2 + \cdots + x_k\,, \\
&s_2 = \textstyle\sum_{1\le i_1<i_2\le k} x_{i_1}x_{i_2} = x_1x_2 + x_1x_3 + \cdots + x_{k-1}x_k\,, \\
&s_3 = \textstyle\sum_{1\le i_1<i_2<i_3\le k} x_{i_1}x_{i_2}x_{i_3} = x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{k-2}x_{k-1}x_k\,, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&s_k = x_1x_2\ldots x_k\,.
\end{aligned}
$$

Można zdefiniować stopień wielomianu jako największą z liczb $i_1 + i_2 + \cdots + i_k$. Wtedy np. stopień wielomianu $x_1x_2^2$ jest równy 3. Można też udowodnić, że przedstawienia w postaci $\sum_{i_1,i_2,\ldots,i_k} a_{i_1,i_2,\ldots,i_k} x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}$ wielomianu k zmiennych jest jednoznaczne niezależnie od tego, czy jest on symetryczny, czy nie pod warunkiem, że każdy ciąg wykładników pojawia się jeden raz.

Zasadnicze twierdzenie twierdzenie teorii wielomianów symetrycznych
Jeśli f jest wielomianem symetrycznym zmiennych $x_1, x_2, \ldots, x_k$, to istnieje wielomian g taki, że dla każdego $\mathbf{x} \in \mathbb{R}^n$ zachodzi równość

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_k) = g(s_1, s_2, \ldots, s_k)\,.$$

Jeśli współczynniki wielomianu f są liczbami całkowitymi, to również współczynniki wielomianu g są całkowite.

Dowód *(wg. A. Mostowski, M.Stark „Elementy Algebry wyższej")*
Z jednoznaczności współczynników i symetrii wielomianu f wynika, że dla każdej permutacji σ zbioru $\{1, 2, \ldots, k\}$ zachodzi równość $a_{1,2,\ldots,k} = a_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(k)}$. Uporządkujmy wyrażenia $x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}$ leksykograficznie: najpierw wypisujemy te, w których wykładnik z jakim występuje x_1 jest najwyższy, jeśli jest ich wiele, to (przy równym wykładniku zmiennej x_1) najpierw wypisujemy te, w których wykładnik przy x_2 jest największy, potem interesuje nas x_3 itd. Załóżmy, że już wypisaliśmy składniki wielomianu f w podany sposób i że $a_{i_1,i_2,\ldots,i_k}x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}$ jest pierwszym wypisanym. Z symetrii wielomianu f wynika, że $i_1 \ge i_2 \ge \ldots \ge i_k$. Odejmujemy od wielomianu f wielomian $a_{i_1,i_2,\ldots,i_k}s_1^{i_1-i_2} \cdot s_2^{i_2-i_3} \cdot \ldots \cdot s_{k-1}^{i_{k-1}-i_k} \cdot s_k^{i_k}$. Łatwo można zauważyć, że w różnicy nie wystąpi składnik typu $cx_1^{i_1}x_2^{i_2}\ldots x_k^{i_k}$, $c \ne 0$. Otrzymana różnica jest wielomianem symetrycznym jako różnica dwóch wielomianów symetrycznych. Powtarzamy zastosowaną operację w odniesieniu do tej różnicy. W ten sposób likwidujemy kolejno składniki typu $cx_1^{j_1}x_2^{j_2}\ldots x_k^{j_k}$. ■