Analiza 1, część druga

Definicja

Granicą górną ciągu (a_n) nazywamy kres górny zbioru złożonego z granic wszystkich tych podciągów ciągu (a_n), które mają granice (skończone lub nie). Oznaczamy ją przez $\limsup_{n\to\infty} a_n$ lub $\limsup_{n\to\infty} a_n$.
Granicą dolną ciągu (a_n) nazywamy kres dolny zbioru złożonego z granic wszystkich tych podciągów ciągu (a_n), które mają granice (skończone lub nie). Oznaczamy ją przez $\liminf_{n\to\infty} a_n$ lub $\liminf a_n$. ■

Całkowicie oczywiste jest stwierdzenie, że $\limsup_{n\to\infty} a_n = \liminf_{n\to\infty} a_n$ wtedy i tylko wtedy, gdy ciąg (a_n) ma granicę.

Do tej pory wyrazy ciągu musiały być liczbami rzeczywistymi. Teraz dopuścimy wśród wyrazów symbole $+\infty$ i $-\infty$. Definicje granic pozostają bez zmian np. $\lim a_n = +\infty$ wtedy i tylko wtedy, gdy dla każdej **liczby** $M \in \mathbb{R}$ istnieje **liczba** $n_M \in \mathbb{N}$ taka, że jeśli $n > n_m$, to $a_n > M$. Chodzi o to, by nie komplikować nadmiernie zdań, które i tak zbyt krótkie nie są.

Stwierdzenie 1.

Jeśli dla każdego $n \in \mathbb{N}$ istnieje podciąg ciągu (a_n), którego granicą jest g_n i $g = \lim_{n\to\infty} g_n$, to istnieje też podciąg ciągu (a_n), którego granicą jest g.

Dowód.

Niech $g_m = \lim_{n\to\infty} a_{\nu(m,n)}$ i $\nu(m,1) < \nu(m,2) < \nu(m,3) < \dots$ ($\nu(m,n)$ jest n–tym wyrazem podciągu zbieżnego do g_m). Załóżmy na razie, że dla wszystkich numerów m granica g_m jest liczbą rzeczywistą. Istnieje więc taki numer $\nu(1,k_1)$, że $|a_{\nu(1,k_1)} - g_1| < 1$. Istnieje numer $\nu(2,k_2) > \nu(1,k_1)$ taki, że zachodzi nierówność $|a_{\nu(2,k_2)} - g_2| < \frac{1}{2}$. Kontynuując (definicja indukcyjna) otrzymujemy ciąg liczb naturalnych $\nu(1,k_1) < \nu(2,k_2) < \nu(3,k_3) < \dots$ taki, że dla każdego n spełniona jest nierówność $|g_n - a_{\nu(n,k_n)}| < \frac{1}{n}$. Z twierdzenia o trzech ciągach wynika, że $\lim_{n\to\infty} a_{\nu(n,k_n)} = \lim_{n\to\infty}(g_n + \frac{1}{n}) = \lim_{n\to\infty}(g_n - \frac{1}{n}) = g$. Jeśli dla nieskończenie wielu n zachodzi $g_n = +\infty$, to $g = +\infty$ i oczywiście g jest granicą podciągu ciągu (a_n), to samo dotyczy przypadku $g_n = -\infty$ dla nieskończenie wielu n. ■

Stwierdzenie 2.

Dla każdego ciągu (a_n) zachodzi równość

$$\limsup_{n\to\infty} a_n = \lim_{n\to\infty} \big(\sup_k\{a_k\colon \quad k \geq n\}\big).$$

Dla każdego ciągu (a_n) zachodzi równość

$$\liminf_{n\to\infty} a_n = \lim_{n\to\infty} \big(\inf_k\{a_k\colon \quad k \geq n\}\big).$$

Dowód.

Udowodnimy to stwierdzenie tylko w przypadku granicy górnej, bowiem $\liminf_{n\to\infty} a_n = -\limsup_{n\to\infty}(-a_n)$. Niech $g = \lim_{n\to\infty} a_{k_n}$ i niech m będzie **ustaloną** liczbą naturalną. Dla dostatecznie dużych n zachodzi nierówność $k_n > m$, zatem $a_{k_n} \leq \sup\{a_j\colon \quad j \geq m\}$. Ponieważ dla prawie wszystkie wyrazy ciągu (a_{k_n}) zachodzi nierówność $a_{k_n} \leq \sup\{a_j\colon \quad j \geq m\}$, więc również $\lim_{n\to\infty} a_{k_n} \leq \sup\{a_j\colon \quad j \geq m\}$. Ta ostatnia nierówność ma miejsce dla każdej liczby naturalnej m. Mamy również

$$\sup\{a_j\colon \quad j\geq 1\}\geq \sup\{a_j\colon \quad j\geq 2\}\geq \sup\{a_j\colon \quad j\geq 3\}\geq\ldots,$$

zatem można mówić o granicy $\lim\limits_{n\to\infty}\big(\sup\limits_k\{a_k\colon \quad k\geq n\}\big)$ i — co więcej — napisać

$$\lim_{n\to\infty} a_{k_n}\leq \lim_{n\to\infty}\big(\sup_k\{a_k\colon \quad k\geq n\}\big).$$

Wynika stąd, że kres górny wszystkich możliwych lewych stron tej nierówności, czyli granica górna ciągu (a_n) spełnia nierówność

$$\limsup_{n\to\infty} a_n\leq \lim_{n\to\infty}\big(\sup_k\{a_k\colon \quad k\geq n\}\big).$$

Trzeba jeszcze wykazać nierówność przeciwną. Wykażemy dowodząc, że $\lim\limits_{n\to\infty}\big(\sup\limits_k\{a_k\colon \quad k\geq n\}\big)$ jest granicą pewnego podciągu ciągu (a_n). Jest tak oczywiście wtedy, gdy dla nieskończenie wielu n zachodzi równość $\sup\limits_k\{a_k\colon \quad k\geq n\}=\max\{a_k\colon \quad n\geq k\}$ — wybieramy wtedy te numery n_j, dla których $\sup\limits_k\{a_k\colon \quad k\geq n\}=a_{k_j}$ dla pewnego $k_j\geq n_j$, a następnie z ciągu (k_j) wybieramy podciąg ściśle rosnący (sam ciąg (k_j) jest niemalejący, jego granicą jest ∞). Jasne jest, że $\lim\limits_{j\to\infty} a_{k_j}=\lim\limits_{n\to\infty}\big(\sup\limits_k\{a_k\colon \quad k\geq n\}\big)$.

Teraz załóżmy, że dla dostatecznie dużych n w zbiorze $\{a_k\colon \quad k\geq n\}$ nie ma liczby największej. By nie komplikować oznaczeń założymy, że w żadnym zbiorze $\{a_k\colon \quad k\geq n\}$ nie ma liczby największej. Ponieważ w zbiorze $\{a_k\colon \quad k\geq n\}$ nie ma liczby największej, więc $b_n:=\sup\limits_k\{a_k\colon \quad k\geq n\}$ jest granicą pewnego podciągu ciągu (a_n). Na mocy stwierdzenia pierwszego również $\lim\limits_{n\to\infty} b_n$ jest granicą pewnego podciągu ciągu (a_n), a to właśnie mieliśmy wykazać. ■

Stwierdzenie 3.

Niech $I=[\liminf a_n,\limsup a_n]$. Jeśli $J\supseteq I$ jest przedziałem otwartym, to istnieje liczba n_J taka, że jeśli $n>n_J$, to $a_n\in J$ przy czym żaden mniejszy niż I przedział domknięty tej własności nie ma. ■

Prosty dowód tego stwierdzenia opuszczam, bo każdy powinien go przeprowadzić samodzielnie, by sprawdzić czy zrozumiał pojęcie granicy górnej.

Ćwiczenie (obowiązkowe!)

Wykazać, że $\limsup(a_n+b_n)\leq\limsup a_n+\limsup b_n$ i podać przykłady świadczące o tym, że nierówność może być ostra.

Niech $x>0$ oznacza liczbę rzeczywistą. Niech (c_n) oznacza ciąg dwustronny cyfr układu dziesiętnego, tzn. $c_n\in\{0,1,2,3,4,5,6,7,8,9\}$ o tej własności, że istnieje liczba naturalna k taka, że jeśli $n>k$, to $c_n=0$. Mówimy, że ciąg (c_n) jest ciągiem cyfr liczby x wtedy i tylko wtedy, gdy dla każdego $m<k$ spełniona jest nierówność

$$c_k10^k+c_{k-1}10^{k-1}+\cdots+c_m10^m\leq x\leq c_k10^k+c_{k-1}10^{k-1}+\cdots+(c_m+1)10^m.$$

Niech $x_m=c_k10^k+c_{k-1}10^{k-1}+\cdots+c_m10^m$. Będziemy mówić, że x_m jest przybliżeniem dziesiętnym x z błędem nie przekraczającym 10^m. Z definicji przybliżenie dziesiętnego wynika od razu, że $\lim\limits_{n\to\infty} x_{-n}=x$. Podamy trzy przykłady. Niech $c_j=3$ dla $j=0,-1,-2,\ldots$ i $c_j=0$ dla $j=1,2,3,\ldots$ Niech $x=\frac{10}{3}$. Dla $j>0$ mamy

$0\leq\frac{10}{3}-(3+3\cdot10^{-1}+3\cdot10^{-2}+\cdots+3\cdot10^{-j})=\frac{1}{3}(10-9-9\cdot10^{-1}-9\cdot10^{-2}-\cdots-9\cdot10^{-j})=\frac{1}{3}\cdot10^{-j}<10^{-j}$. Wobec

tego ciąg dwustronny $\ldots 0003{,}3333\ldots$ odpowiada liczbie $\frac{4}{3}$. Ciąg dwustronny $\ldots 0001{,}0000\ldots$ odpowiada, jak łatwo można sprawdzić, liczbie 1. Ciąg dwustronny $\ldots 0000{,}9999\ldots$ również odpowiada liczbie 1. Proszę sprawdzić szczegółowo, że te stwierdzenia są prawdziwe! Widzimy więc, że w niektórych przypadkach jednej liczbie mogą odpowiadać dwa ciągi. Przekonamy się zaraz, że więcej już nie, a każdej co najmniej jeden.

Twierdzenie o przybliżeniach dziesiętnych

Dla każdej liczby $x > 0$ istnieje ciąg (x_m) przybliżeń dziesiętnych. Jeśli istnieje liczba naturalna j taka, że $10^j \cdot x \in \mathbb{N}$, to istnieją dokładnie dwa różne ciągi przybliżeń dziesiętnych (x_m) i $(\tilde{x}_m)$ oraz liczba całkowita i taka, że $\tilde{x}_i = x_i + 1$ (lub odwrotnie) i dla każdego $m < i$ zachodzą równości $x_m = 9$, $\tilde{x}_m = 0$. Jeśli taka liczba j nie istnieje, to istnieje dokładnie jeden ciąg przybliżeń dziesiętnych.

Dowód.

Niech $k \in \mathbb{Z}$ będzie taką liczbą, że $10^k \leq x < 10^{k+1}$. Taka liczba całkowita k istnieje, bo $\lim\limits_{n\to\infty} 10^n = +\infty$ i $\lim\limits_{n\to\infty} 10^{-n} = -\infty$, zatem istnieją potęgi dziesiątki większe niż x, 10^{k+1} to najmniejsza z nich (w każdym ograniczonym z dołu zbiorze złożonym z liczb całkowitych znaleźć można najmniejszą). Niech $c_k \in \{1,2,3,4,5,6,7,8,9\}$ będzie największą cyfrą taką, że $c_k \cdot 10^k \leq x$. Zdefiniujemy cyfry $c_{k-1}, c_{k-2}, \ldots$ przez indukcję. Załóżmy, że zdefiniowaliśmy już cyfry $c_k, c_{k-1}, c_{k-2}, \ldots, c_i$ w taki sposób, że dla każdego $j \in \{i, i+1, i+2, \ldots, k\}$ zachodzi nierówność

$$c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_j \cdot 10^j \leq x < c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + (c_j + 1) \cdot 10^j .$$

Z tej nierówności wynika natychmiast, że $0 \leq x - (c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_j \cdot 10^j) < 10^j = 10 \cdot 10^{j-1}$, zatem $0 \leq x - (c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_j \cdot 10^j) \leq 9 \cdot 10^{j-1}$. Teraz możemy zdefiniować c_{i-1} jako największą liczbę ze zbioru $\{0,1,2,3,4,5,6,7,8,9\}$ (więc cyfrę) taką, że $0 \leq x - (c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_{i-1} \cdot 10^{i-1}) < 10^{i-1}$, czyli że

$$c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_i \cdot 10^i + c_{i-1} \cdot 10^{i-1} \leq x < \\ < c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_i \cdot 10^i + (c_{i-1} + 1) \cdot 10^{i-1} .$$

W ten sposób zdefiniowaliśmy dwustronny ciąg (c_n) spełniający żądane warunki.

Teraz zajmiemy się jednoznacznością. Załóżmy, że dwa ciągi (c_n) i $(\tilde{c}_n)$ związane są z liczbą x. Niech k będzie największą liczbą całkowitą, dla której $c_k \neq \tilde{c}_k$. Dla ustalenia uwagi załóżmy, że $\tilde{c}_k > c_k$. Niech ℓ będzie taką liczbą całkowitą, że dla $j > \ell$ zachodzi $c_j = \tilde{c}_j = 0$. Niech $m < k$ będzie liczbą całkowitą. Mamy więc

$$0 \leq x - (c_\ell \cdot 10^\ell + c_{\ell-1} \cdot 10^{\ell-1} + \cdots + c_{k+1} \cdot 10^{k+1} + c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_m \cdot 10^m) \leq 10^m \text{ oraz}$$
$$0 \leq x - (c_\ell \cdot 10^\ell + c_{\ell-1} \cdot 10^{\ell-1} + \cdots + c_{k+1} \cdot 10^{k+1} + \tilde{c}_k \cdot 10^k + \tilde{c}_{k-1} \cdot 10^{k-1} + \cdots + \tilde{c}_m \cdot 10^m) \leq 10^m .$$

Różnica liczb z przedziału o długości 10^m nie przekracza 10^m, więc

$$10^m \geq x - (c_\ell \cdot 10^\ell + c_{\ell-1} \cdot 10^{\ell-1} + \cdots + c_{k+1} \cdot 10^{k+1} + c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_m \cdot 10^m) - \\ - \left[x - (c_\ell \cdot 10^\ell + c_{\ell-1} \cdot 10^{\ell-1} + \cdots + c_{k+1} \cdot 10^{k+1} + \tilde{c}_k \cdot 10^k + \tilde{c}_{k-1} \cdot 10^{k-1} + \cdots + \tilde{c}_m \cdot 10^m)\right] = \\ = (\tilde{c}_k - c_k) \cdot 10^k + (\tilde{c}_{k-1} - c_{k-1}) \cdot 10^{k-1} + \cdots + (\tilde{c}_m - \tilde{c}_m) \cdot 10^m \geq 10^k - 9 \cdot 10^{k-1} - \ldots - 9 \cdot 10^m = 10^m .$$

Widać więc, że jeśli $\tilde{c}_k > c_k$, to muszą zachodzić równości. Wobec tego muszą być spełnione równości $\tilde{c}_k = c_k + 1$ i $\tilde{c}_{k-1} - c_{k-1} = \ldots = \tilde{c}_m - c_m = -9$, czyli $\tilde{c}_k = c_k + 1$ i $\tilde{c}_{k-1} = \ldots = \tilde{c}_m = 0$ i $c_{k-1} = \ldots = c_m = 9$.

Ponieważ m oznacza tu dowolną liczbę mniejszą niż k, więc wykazaliśmy, że „po" $\tilde{c}_k$ są już jedynie zera i jednocześnie „po" c_k są już tylko dziewiątki. Mamy więc $x = c_\ell \cdot 10^\ell + c_{\ell-1} \cdot 10^{\ell-1} + \cdots + c_{k+1} \cdot 10^{k+1} + \tilde{c}_k \cdot 10^k$, bo $0 \leq x - (c_\ell \cdot 10^\ell + c_{\ell-1} \cdot 10^{\ell-1} + \cdots + c_{k+1} \cdot 10^{k+1} + \tilde{c}_k \cdot 10^k) \leq 10^m$ dla każdej liczby całkowitej $m < k$. Jeśli $k \geq 0$, to przyjmujemy $j = 0$, jeśli zaś $k < 0$, to przyjmujemy $j = -k$. Dowód został zakończony. ■

Sformułowanie twierdzenia i jego dowód nieco (tylko nieco) się uproszczą, gdy wprowadzimy pojęcie sumy nieskończonej, czyli szeregu liczb rzeczywistych albo zespolonych.

Na razie jednak powiemy jeszcze kilka słów na temat liczb całkowitych.

Definicja

Liczba całkowita a jest dzielnikiem liczby całkowitej b wtedy i tylko wtedy, gdy istnieje liczba całkowita k taka, że $ak = b$. Piszemy wtedy $a|b$. ■

Stwierdzenie

Jeśli $a|b$ i $b|c$, to $a|c$.

Dowód.

Jeśli $b = ka$ i $c = b\ell$, to $c = k\ell a$. ■

Stwierdzenie

Każda liczba całkowita jest dzielnikiem 0.

Dowód.

Wynika to z tego, że $a \cdot 0 = 0$. ■

Definicja

Jeśli a i b są liczbami całkowitymi, $b \neq 0$ i istnieją liczby całkowite q, r takie, że $a = bq + r$ i $0 \leq q < |b|$, to mówimy, że q jest ilorazem z dzielenia a przez b zaś r — resztą z dzielenia a przez b. ■

Stwierdzenie

Dla dowolnych liczb całkowitych a, $b \neq 0$ istnieje dokładnie jedna para liczb całkowitych q, r taka, że $a = bq + r$ i $0 \leq r < |b|$.

Dowód.

Z równości $bq + r = (-b)(-q) + r$ wynika, że wystarczy udowodnić to stwierdzenie dla $b > 0$. W dalszym ciągu zakładamy, że $b > 0$. Niech $q = \sup\{n \in \mathbb{Z} : \ nb \leq a\}$. Zasada maksimum dla liczb całkowitych gwarantuje, że $q \in \mathbb{Z}$. Niech $r = a - qb$. Oczywiście $0 \leq r = a - qb < (q+1)b - qb = b$. Istnienie ilorazu i reszty zostało wykazane. Jeśli $bq + r = bq_1 + r_1$ i $0 \leq r, r_1 < b$, to $r - r_1 = b(q_1 - q)$. Oczywiście $|q_1 - q| < b$ (różnica dwu liczb nieujemnych mniejszych niż b ma wartość bezwzględną mniejszą niż b). Wobec tego $|b(q_1 - q1)| < b$, ale to wymusza nierówność $|q_1 - q| < 1$, czyli $|q_1 - q| = 0$, więc $q_1 = q$. Mamy więc $r - r_1 = b(q_1 - q) = 0$, co kończy dowód jednoznaczności ilorazu i reszty z dzielenia przez b. ■

Definicja

Liczba $p \in \mathbb{Z}$ nazywane jest pierwsza wtedy i tylko wtedy, gdy nie jest dzielnikiem liczby 1 i z tego, że $ab = p$ wynika, że jedna z liczb a, b jest dzielnikiem jedynki.

Największym wspólnym dzielnikiem liczb a, b nazywamy taka liczbę d, że $d|a$, $d|b$ i taką, że jeśli $d|d_1$,

$d_1|a$ i $d_1|b$, to liczba $\frac{d_1}{d}$ jest dzielnikiem jedynki. ■

Z tego, że $a|b$ i $b \neq 0$ wynika oczywiście, że $|a| \leq |b|$. Największym wspólnym dzielnikiem liczb 6 i 4 jest 2, ale również -2. Liczby $a = 0$ i $b = 0$ nie mają największego wspólnego dzielnika. Jedynymi dzielnikami jedynki są liczby ± 1. Studentów, którym te definicje wydają się nieco dziwaczne chciałbym uprzedzić, że w przyszłości zajmiemy się podzielnością w zbiorze wielomianów i wtedy przestaną być dziwaczne. Można też rozpatrywać podzielność w innych zbiorach, np. $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-5}]$ itp. Tym nie będziemy się zajmować, bo ta tematyka nie należy do analizy lecz do algebry oraz teorii liczb. Drobne wyjaśnienie tego o czym mowa znajduje się w jednym z dalszych ćwiczeń.

Twierdzenie o największym wspólnym dzielniku

Jeśli a, b są liczbami całkowitymi i co najmniej jedna z nich jest różna od 0, to mają one największy wspólny dzielnik, $\mathrm{nwd}(a, b)$ i istnieją liczby całkowite k, m takie, że liczba $ak + bm = \mathrm{nwd}(a, b)$.*

Dowód.

Rozważmy zbiór $D = \{ax+by: \quad x \in \mathbb{Z} \text{ i } y \in \mathbb{Z} \text{ i } ax+by > 0\}$. $D \neq \emptyset$, bo jeśli $a \neq 0$, to $|a| \in D$, gdyż $|a| = a \cdot 1 + b \cdot 0$, gdy $a > 0$ i $|a| = a \cdot (-1) + b \cdot 0$, gdy $a < 0$. Niech $d = ak + bm$ będzie najmniejszą liczbą w zbiorze D. Ponieważ zbiór D złożony jest z liczb dodatnich, więc $d > 0$. Wykażemy, że $d|a$. Jest tak, gdy $a = 0$. Załóżmy, że $a \neq 0$. Wtedy istnieją liczby całkowite q, r takie, że $a = qd + r$ i $0 \leq r < d$. Stąd $r = a - qd = a(1 - kq) + b(-m)$. Jeśli $r > 0$, to $r \in D$, co przeczy temu, że najmniejszą liczbą w zbiorze D jest d. Wobec tego $r = 0$, ale to oznacza, że $a = qd$, czyli że $d|a$. Analogicznie $d|b$. Wykazaliśmy, że d jest wspólnym dzielnikiem liczb a, b. Jeśli $\delta|a$ i $\delta|b$, to istnieją liczby $\lambda, \kappa \in \mathbb{Z}$ takie, że $a = \lambda\delta$ i $b = \kappa\delta$, zatem $d = ak + bl = \delta(k\lambda + m\kappa)$, zatem $\delta|d$. Stąd wynika, że jeśli również $d|\delta$, to $\delta = \pm d$, więc $\mathrm{nwd}(a, b) = d$. ■

Charakteryzacja liczb pierwszych

Liczba $p \neq 0$ jest pierwsza wtedy i tylko wtedy, gdy nie jest dzielnikiem 1 i z tego, że $p|ab$ wynika, że $p|a$ lub $p|b$.

Dowód.

Jeśli p **nie** jest liczbą pierwszą, to istnieją liczby całkowite a, b, które nie są dzielnikami jedynki i dla których zachodzi równość $p = ab$. Jeśli $p|a$, to $a = kp$ dla pewnej liczby całkowitej k i wobec tego $p = kpb$, więc $1 = pb$, co oznacza, że p i b są dzielnikami jedynki, wbrew założeniu. Załóżmy teraz, że $p|ab$ i że p jest liczbą pierwszą. Jeśli $p \not| a$, to $\mathrm{nwd}(a, p) = 1$, zatem istnieją liczby całkowite k, m takie, że $ak + pm = 1$. Wobec tego $b = abk + bpm$. Z założenia $p|abk$ i oczywiście $p|bpm$, więc $p|(abk + bpm) = b$.

Zasadnicze twierdzenie arytmetyki

czyli twierdzenie o jednoznaczności rozkładu na czynniki pierwsze

Niech $a \neq 0$ będzie liczbą całkowita, która nie jest dzielnikiem 1. Istnieją wtedy liczby pierwsze $p_1, p_2, \ldots, p_n$ takie, że $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Jeśli $a = \tilde{p}_1 \cdot \tilde{p}_2 \cdot \ldots \cdot \tilde{p}_m$ i liczby $\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_m$ są pierwsze, to $n = m$ i po ewentualnej zmianie kolejności (numeracji) zachodzą równości $p_1 = \eta_1\tilde{p}_1$, $p_2 = \eta_2\tilde{p}_2$, $\ldots$, $p_n = \eta_n\tilde{p}_n$, gdzie $\eta_1, \eta_2, \ldots, \eta_n$ są pewnymi dzielnikami jedynki.

* W licznych książkach poświęconych teorii liczb największy wspólny dzielnik liczb a,b oznaczany jest symbolem (a,b).

Przed podaniem dowodu wypada powiedzieć, że to twierdzenie mówi, że każdą liczbę całkowitą, z wyjątkiem $0, -1, 1$ można przedstawić w postaci iloczynu liczb pierwszych na jeden tylko sposób, jeśli nie brać pod uwagę zmian kolejności czynników i zmian ich znaków: $6 = 2 \cdot 3 = (-2) \cdot (-3) = 3 \cdot 2 = (-3) \cdot (-2)$.

Dowód.

Wykażemy najpierw istnienie rozkładu na czynniki pierwsze. Zastosujemy indukcję względem wartości bezwzględnej liczby całkowitej, czyli udowodnimy twierdzenie dla liczb naturalnych. Jeśli $a = 2$, to twierdzenie jest prawdziwe, bo 2 jest liczbą pierwszą, przyjmujemy więc $n = 1$, $p_1 = 2$. Załóżmy, że twierdzenie jest prawdziwe dla wszystkich liczb naturalnych mniejszych niż k. Jeśli n jest liczbą pierwszą, to dla k teza też zachodzi. Jeśli k liczbą pierwszą nie jest, to dla pewnych liczb k_1, k_2, które nie są dzielnikami jedynki zachodzi równość $k = k_1 \cdot k_2$. Ponieważ liczby k_1, k_2 nie są dzielnikami jedynki są różne od 0, więc $k_1, k-2 > 1$ i wobec tego $k_1, k_2 < k$. Wobec tego każda z nich jest iloczynem liczb pierwszych, a stąd wynika od razu, że również k jest iloczynem liczb pierwszych. Zakończyliśmy rozumowanie indukcyjne.

Teraz zajmiemy się jednoznaczością rozkładu. Jeśli $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n = \tilde{p}_1 \cdot \tilde{p}_2 \cdot \ldots \cdot \tilde{p}_m = \tilde{p}_1 \cdot (\tilde{p}_2 \cdot \ldots \cdot \tilde{p}_m)$, to $p_1 | \tilde{p}_1$ lub $p_1 | (\tilde{p}_2 \cdot \tilde{p}_3 \cdot \ldots \cdot \tilde{p}_m)$. Jeśli $p_1 | \tilde{p}_1$, to $\tilde{p}_1 = \eta_1 \cdot p_1$, a ponieważ $\tilde{p}_1$ jest liczbą pierwszą i p_1 nie jest dzielnikiem jedynki (jako liczba pierwsza), więc η_1 jest dzielnikiem jedynki. Przyjmując, że $a > 0$ jest najmniejszą dodatnią liczbą naturalną stwierdzamy, że liczba $\tilde{p}_2 \cdot \tilde{p}_3 \cdot \ldots \cdot \tilde{p}_m < a$ rozkłada się na iloczyn czynników pierwszych tylko w jeden sposób (z wymienionymi przed dowodem zastrzeżeniami na temat kolejności czynników i mnożenia ich przez dzielniki jedynki). Liczba ta dzieli się przez p_1, zatem p_1 jest równa z dokładnością do pomnożenia przez dzielnik jedynki którejś z liczb $\tilde{p}_2$, $\tilde{p}_3$, $\ldots$, $\tilde{p}_m$. Bez straty ogólności rozważań można przyjąć, że $p_1 = \tilde{p}_2$. Stąd wynika równość $\frac{a}{p_1} = p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n = \tilde{p}_1 \cdot \tilde{p}_3 \cdot \tilde{p}_4 \cdot \ldots \cdot \tilde{p}_m$. Liczbę całkowitą $\frac{a}{p_1} < a$ można przedstawić w postaci iloczynu liczb pierwszych na jeden tylko sposób, bo jest mniejsza od a, a można przyjąć, że a jest najmniejszą liczbą, dla której rozkład na czynniki pierwsze jest niejednoznaczny. Dowód został zakończony. ■

W książce „The Higher Arithmetic, An Introduction to the Theory of numbers" Harolda Davenporta (przełożonej na rosyjski) można znaleźć prostszy dowód i kilka innych dowodów zasadniczego twierdzenia arytmetyki. Ten najprostszy przytoczymy. Tym razem nie skorzystamy z charakteryzacji liczb pierwszych.

drugi dowód zasadniczego twierdzenia arytmetyki

Istnienie rozkładu wykazujemy tak, jak poprzednio, więc tej części dowodu nie przepisujemy. Załóżmy, że $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n = \tilde{p}_1 \cdot \tilde{p}_2 \cdot \ldots \cdot \tilde{p}_m$ jest najmniejszą liczbą naturalną, która ma dwa różne rozkłady na czynniki pierwsze i że liczby naturalne $p_1, p_2, \ldots, p_n, \tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_m$ są pierwsze. Jeśli rozkłady są różne, to żadna z liczb $p_1, p_2, \ldots, p_n$ nie pojawia się wśród liczb $\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_m$. Możemy przyjąć, że $\tilde{p}_1 \leq \tilde{p}_2 \leq \ldots \leq \tilde{p}_m$ i $p_1 \leq p_2 \leq \ldots \leq p_n$. Ponieważ liczba a nie jest pierwsza, więc $n \geq 2$ i $m \geq 2$, zatem $a \geq p_1^2$ i $a \geq \tilde{p}_1^2$ i oczywiście $p_1 \neq \tilde{p}_1$. Wobec tego $a > p_1 \tilde{p}_1$, zatem liczba $a - p_1 \tilde{p}_1$ jest liczbą naturalną mniejszą od a, zatem mającą dokładnie jeden rozkład na iloczyn naturalnych czynników pierwszych. Wobec tego liczba $a - p_1 \tilde{p}_1$ jest podzielna przez p_1 oraz przez $\tilde{p}_1 \neq p_1$, zatem również przez $p_1 \tilde{p}_1$, bo ta ma tylko jeden rozkład na czynniki, a z tego wynika, że jeśli jest podzielna przez jakąś liczbę pierwszą, to ta liczba pierwsza występuje

w **jedynym** rozkładzie na czynniki pierwsze. Wobec tego $a - p_1\tilde{p}_1 = p_1\tilde{p}_1 q_1 q_2 \dots q_j$ dla pewnych liczb pierwszych $q_1, q_2, \dots, q_j$. Dzieląc tę równość stronami przez p_1 otrzymujemy $p_2 p_3 \dots p_n - \tilde{p}_1 = \tilde{p}_1 q_1 q_2 \dots q_j$, a stąd wynika, że liczba $\tilde{p}_1$ jest dzielnikiem liczby $p_2 p_3 \dots p_n < a$, więc przedstawialnej w postaci iloczynu liczb pierwszych w jeden tylko sposób. Stąd jednak wynika, że wśród liczb $p_2, p_3, \dots, p_n$ występuje liczba $\tilde{p}_1$, wbrew założeniu. ■

Po tym dowodzie H.Davenport napisał *czytelnik zgodzi się, że chociaż dowód ten ani nie jest długi ani trudny, to jednak jest dosyć delikatny (cienki).* Zachęcam do przemyślenia logiki tego rozumowania, choć nie zamierzam go przedstawiać na wykładzie (mogę po lub przed, np. w piątek.)

Zadanie (ale nie z analizy)

Wykazać, że w zbiorze $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\colon \quad a, b \in \mathbb{Z}\}$ jest jednoznaczność rozkładu na czynniki pierwsze, a w zbiorze $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5}\colon \quad a, b \in \mathbb{Z}\}$ jednoznaczności rozkładu na czynniki pierwsze nie ma. W obu przypadkach wykazać, że dzielników jedynki jest nieskończenie wiele. Opisać dzielniki jedynki!

To zadanie z pewnością nie powinno być robione na ćwiczeniach z analizy, tego typu zadania zapewne pojawią się kiedyś na na algebrze, ale nie na GAL–u. Zamieszczam, by osoby studiujące matematykę mogły ewentualnie pomysleć o twierdzeniu o jednoznaczności rozkładu i lepiej zrozumieć, jakie trudności są zwalczane.