Liczby p-adyczne, czyli świat prawie dyskretny

Witold WIĘSŁAW, Wrocław

Jeżeli sięgnąć do jakiegokolwiek współczesnego podręcznika teorii liczb, np. do polsko-rosyjskiej koprodukcji: Z.I. Borewicz, I.R. Szafarewicz [2], to można tam znaleźć następującą definicję:

Niech p będzie ustaloną liczbą pierwszą. Rozważmy zbiór wszystkich ciągów $(x_1, x_2, x_3, \ldots)$ o wyrazach całkowitych, takich że

$$x_n \equiv x_{n-1} \pmod{p^{n-1}} \quad \text{dla każdego} \quad n \geq 2.$$

Dwa ciągi $x = (x_n)$ i $x' = (x'_n)$ uważamy za równe zgodnie z następującym określeniem

$$x = x' \;\Leftrightarrow\; x_n \equiv x'_n \pmod{p^n} \quad \text{dla każdego} \quad n \geq 1.$$

Klasę równoważności ciągu względem tak określonej równości nazywamy *liczbą p-adyczną całkowitą* i oznaczamy $\langle x_n \rangle$.

Z podanej wyżej definicji wynika, że za x_1 można przyjąć liczbę $0 \leq x_1 < p$, oraz

$$x_2 = x_1 + a_1 p, \quad 0 \leq a_1 < p$$
$$x_3 = x_2 + a_2 p^2 = x_1 + a_1 p + a_2 p^2, \; 0 \leq a_2 < p$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_n = x_1 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}, \; 0 \leq a_{n-1} < p.$$

Jeżeli przyjąć dla elegancji $a_0 = x_1 \; (0 \leq a_0 < p)$, to liczba p-adyczna całkowita $\langle x_1, x_2, \ldots \rangle$ reprezentowana jest przez ciąg

$$\langle a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots \rangle,$$

gdzie wszystkie a_j spełniają warunek: $0 \leq a_j < p$. Możemy więc liczbę $\langle x_n \rangle$ traktować formalnie jako wyrażenie

$$a_0 + a_1 p + a_2 p^2 + \ldots.$$

W zbiorze liczb p-adycznych całkowitych $\langle x_n \rangle$ definiujemy działania, określając je na reprezentantach:

$$\text{dodawanie:} \quad \langle x_n \rangle + \langle y_n \rangle = \langle x_n + y_n \rangle$$
$$\text{mnożenie:} \quad \langle x_n \rangle \cdot \langle y_n \rangle = \langle x_n y_n \rangle.$$

Nie wymaga dużej rutyny sprawdzenie, że tak określone działania są poprawne, tzn. nie zależą od wyboru reprezentantów x_n i y_n. Ponadto

zbiór liczb p-adycznych całkowitych jest pierścieniem całkowitym względem powyższych działań

(tzn. jest to pierścień przemienny, z jednością, bez dzielników zera). Pierścień ten tradycyjnie oznacza się przez $\mathbf{Z}_p$ i nazywa *pierścieniem całkowitych liczb p-adycznych*. Taką definicję podał Kurt Hensel w 1907 w książce *Zahlentheorie* [5]. O pierwszej definicji Hensela z 1897 powiemy później.

Ponieważ pierścień $\mathbf{Z}_p$ jest przemienny i nie ma dzielników zera, więc z jego elementów można w zwykły sposób tworzyć ułamki. Nazywamy je *liczbami p-adycznymi*, a ich zbiór oznaczamy przez $\mathbf{Q}_p$.

Jeśli np. $x = p^N(b_0 + b_1 p + b_2 p^2 + \ldots)$, $0 < b_0 < p$, $0 \leq b_j < p$ dla $j = 1, 2, \ldots$, to $x^{-1} = p^{-N}(b_0 + b_1 p + b_2 p^2 + \ldots)^{-1}$. Okazuje się, że ciąg odpowiadający mianownikowi daje się zapisać w postaci $c_0 + c_1 p + c_2 p^2 + \ldots$, $0 \leq c_j < p$, $c_0 \neq 0$, (bo jest elementem odwracalnym pierścienia $\mathbf{Z}_p$), co oznacza, że

każda liczba p-adyczna $a \in \mathbf{Q}_p$ ma postać

$$a = p^{\alpha}(c_0 + c_1 p + c_2 p^2 + \ldots), \tag{1}$$

gdzie $\alpha \in \mathbf{Z}$, $0 \leq c_j < p$ dla $j \geq 0$; $c_0 \neq 0$ dla $a \neq 0$.

Podobnie, jak w przypadku zwykłych ułamków utworzonych z liczb całkowitych,

zbiór $\mathbf{Q}_p$ *liczb p-adycznych jest ciałem,*

jeśli tylko na utworzonych ułamkach wykonywać zwykłe działania.

We wspomnianej książce [5] Hensel używał zapisu topologicznego. Liczbę (1) zapisywał jako

$$a = p - \lim \gamma_n,$$

gdzie $\gamma_n = p^{\alpha}(c_0 + c_1 p + \ldots + c_n p^n)$. Jednak był to tylko formalny zapis.

Inną definicję podał matematyk węgierski Kürschak, bardzo zasłużony dla węgierskich olimpiad matematycznych. Kürschak po raz pierwszy zdefiniował *ciało z wartością bezwzględną*. Funkcję $|\ | : K \to \mathbf{R}_+$ z ciała K w zbiór $\mathbf{R}_+$ nieujemnych liczb rzeczywistych nazwał *wartością bezwzględną*, gdy

1. $|x| > 0$ dla $x \neq 0$; $|0| = 0$,
2. $|xy| = |x|\,|y|$,
3. $|1 + x| \leq 1 + |x|$,

dla dowolnych elementów $x, y \in K$.

Każda wartość bezwzględna $|\ |$ w ciele K definiuje metrykę wzorem

$$d(x, y) = |x - y|.$$

O przykłady nietrudno. Oczywiście $\mathbf{R}$ i $\mathbf{C}$ ze zwykłą wartością bezwzględną są ciałami z wartością bezwzględną. Bardziej wyrafinowany przykład to funkcja $|\ |_g$ zdefiniowana jako

$$|x|_g = |g(x)|,$$

gdzie $|\ |$ jest zwykłą wartością bezwzględną w $\mathbf{C}$, a g automorfizmem ciała $\mathbf{C}$, różnym od identyczności i sprzężenia. Takie automorfizmy istnieją i jest ich tyle, ile wszystkich funkcji z $\mathbf{C}$ w $\mathbf{C}$, tzn. $2^{\mathfrak{c}}$. Ciało $\mathbf{C} = \mathbf{Q}(\mathcal{B})(\mathcal{A})$, gdzie $\mathcal{B}$ jest *bazą przestępną* $\mathbf{C}$ nad $\mathbf{Q}$, (tzn. maksymalnym zbiorem elementów algebraicznie niezależnych nad $\mathbf{Q}$, a więc takich, między którymi nie zachodzi żadna relacja algebraiczna ze współczynnikami z $\mathbf{Q}$), a $\mathcal{A}$ zbiorem elementów algebraicznych nad ciałem $\mathbf{Q}(\mathcal{B})$. Dowolną permutację (tzn. bijekcję) zbioru $\mathcal{B}$ przedłuża się do automorfizmu ciała $\mathbf{C}$, co wymaga trochę technik algebry, ale sam pomysł jest prosty. Automorfizm g przekształca $\mathbf{R}$ w gęsty podzbiór $\mathbf{C}$ – trzeba wiedzieć, że jeżeli $g(\mathbf{R}) = \mathbf{R}$, to g jest identycznością na $\mathbf{R}$ (udowodnił to Darboux [3] w 1880). A więc $g(x + iy) = g(x) + g(i)g(y) = x \pm iy$, bo $g(i) = \pm i$. Jeśli więc g nie jest identycznością ani sprzężeniem, to $g(\mathbf{R})$ nie jest podzbiorem $\mathbf{R}$, a więc istnieje $r_0 \in \mathbf{R}$, takie że $g(r_0) \notin \mathbf{R}$. Zbiór $\{a + br_0 : a, b \in \mathbf{Q}\}$ leży gęsto w $\mathbf{C}$, a więc tym bardziej $g(\mathbf{R})$ leży tam gęsto.

Inny przykład to *p-adyczna wartość bezwzględna* w $\mathbf{Q}$. Ustalmy liczbę pierwszą p. Dowolną niezerową liczbę wymierną x można jednoznacznie zapisać w postaci

$$x = p^{\alpha}\frac{a}{b}, \tag{2}$$

gdzie $\alpha, a, b \in \mathbf{Z}$ i ab jest względnie pierwsze z p. Teraz już można określić p-adyczną wartość bezwzględną w $\mathbf{Q}$:

$$|0|_p = 0 \ ; \quad |x|_p = p^{-\alpha} \quad \text{dla} \quad x \text{ postaci (2).} \tag{3}$$

Okazuje się, że $|\ |_p$ nie tylko jest wartością bezwzględną, ale nawet spełnia warunek mocniejszy niż 3:

$$|x + y|_p \leq \max(|x|_p, |y|_p). \tag{4}$$

Jest to tzw. *nierówność ultrametryczna.*

Trywialną wartość bezwzględną w ciele definiują warunki: $|0| = 0$, $|a| = 1$ dla $a \neq 0$. Wyznacza ona topologię dyskretną.

Już G. Cantor (1872), E. Heine (1872) i Ch. Méray (1869) nauczyli matematyków, jak definiować liczby rzeczywiste poprzez uzupełnienie przestrzeni metrycznej liczb wymiernych względem zwykłej topologii (por. [13]-[15]). Hausdorff na początku XX wieku nauczył tego dla dowolnych przestrzeni

metrycznych. W tej sytuacji Kürschak mógł już swobodnie zastosować znaną konstrukcję do ciała z wartością bezwzględną. Używając współczesnego języka, konstrukcję Kürschaka można określić następująco:

uzupełnieniem $(K, |\ |\widehat{\ })$ *ciała* K z wartością bezwzględną $|\ |$ nazywamy pierścień ilorazowy C/I, gdzie C jest pierścieniem ciągów Cauchy'ego z K względem $|\ |$, a I ideałem w C złożonym z ciągów zbieżnych do zera. Ciało K zanurza się izomorficznie w ciało $\widehat{K}$:

$$x \mapsto (x, x, x, \ldots), \quad x \in K.$$

Wartość bezwzględną $|\ |$ przedłuża się z K na $\widehat{K}$: jeżeli $x \in \widehat{K}$, $x = (x_1, x_2, \ldots) + I \in C/I$, to definiujemy

$$|x|\widehat{\ } = \lim_{n\to\infty} |x_n|. \tag{5}$$

Definicja wartości bezwzględnej w $\widehat{K}$ jest poprawna – nie zależy od wyboru reprezentanta (x_n). Jeżeli bowiem (y_n) jest dowolnym reprezentantem x, to $z_n = x_n - y_n$ dąży do zera: $|z_n| \to 0$. Zatem

$$|x_n| = |y_n + z_n| \leq |y_n| + |z_n|,$$
$$|y_n| = |x_n - z_n| \leq |x_n| + |z_n|,$$

skąd wynika, że $\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|$, o ile te granice istnieją. Ponieważ jednak

$$\Big||x_n| - |x_m|\Big| \leq |x_n - x_m|, \tag{6}$$

więc ciąg liczb rzeczywistych $|x_n|$ spełnia warunek Cauchy'ego w $\mathbf{R}$, zatem jest zbieżny, skąd wynika poprawność definicji (5). (Zewnętrzne kreski po lewej stronie nierówności (6) oznaczają zwykłą wartość bezwzględną w $\mathbf{R}$).

Okazuje się, że

1° K leży gęsto w $\widehat{K}$,
2° $(\widehat{K}, |\ |\widehat{\ })$ *jest zupełną przestrzenią metryczną.*

Kürschak [6] zauważył, że

ciało $\mathbf{Q}_p$ *liczb p-adycznych jest uzupełnieniem* $\mathbf{Q}$ *względem p-adycznej wartości bezwzględnej* $|\ |_p$.

Ostrowski dowiódł, że

zwykła wartość bezwzględna $|\ |$ *i p-adyczne wartości bezwzględne są jedynymi nietrywialnymi i nierównoważnymi wartościami bezwzględnymi w* $\mathbf{Q}$.

(Dwie wartości bezwzględne są *równoważne*, jeżeli definiują tą samą topologię).

Można więc liczby rzeczywiste i p-adyczne uważać za równoprawne obiekty skonstruowane z tego samego zbioru $\mathbf{Q}$ liczb wymiernych, tylko przy pomocy innej wartości bezwzględnej.

Prześledźmy jeszcze inną konstrukcję liczb p-adycznych. Niech $\mathbf{Z}/N\mathbf{Z}$ oznacza pierścień reszt modulo N ($N \geq 2$). Jeżeli M dzieli N, to odwzorowanie

$$\mathbf{Z}/N\mathbf{Z} \to \mathbf{Z}/M\mathbf{Z} \quad \text{dane przez} \quad x + N\mathbf{Z} \mapsto x + M\mathbf{Z}$$

jest homomorfizmem pierścieni. W szczególności, biorąc za N kolejne potęgi liczby pierwszej p, otrzymujemy nieskończony ciąg pierścieni i ich homomorfizmów

$$\ldots \xrightarrow{\varphi_{n+1}} \mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\varphi_n} \mathbf{Z}/p^{n-1}\mathbf{Z} \xrightarrow{\varphi_{n-1}} \ldots \xrightarrow{\varphi_3} \mathbf{Z}/p^2\mathbf{Z} \xrightarrow{\varphi_2} \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p. \tag{7}$$

Granicą odwrotną systemu (7) jest

$$\varprojlim(\mathbf{Z}/p^n\mathbf{Z}, \varphi_n) = \{x = (\ldots, x_n, \ldots, x_1) : x_n \in \mathbf{Z}/p^n\mathbf{Z}, \varphi_n(x_n) = x_{n-1} \forall n \geq 2\}.$$

Ale

$$\varphi_n(x_n) = x_n + p^{n-1}\mathbf{Z} = x_{n-1} + p^{n-1}\mathbf{Z},$$

czyli

$$x_n \equiv x_{n-1} (\mathrm{mod}\, p^{n-1}) \quad \text{dla każdego} \quad n \in \mathbf{N},\ n \geq 2. \tag{8}$$

Zatem

$$\mathbf{Z}_p = \varprojlim(\mathbf{Z}/p^n\mathbf{Z},\ \varphi_n), \quad \text{czyli} \quad \mathbf{Z}_p \subset \prod_{n\geq 1} \mathbf{Z}/p^n\mathbf{Z}.$$

Każda z przestrzeni (skończonych) $\mathbf{Z}/p^n\mathbf{Z}$ jest dyskretna, a więc zwarta, tzn. φ_n są funkcjami ciągłymi. Z twierdzenia Tichonowa wynika, że produkt $\prod \mathbf{Z}/p^n\mathbf{Z}$ jest przestrzenią zwartą. Zatem $\mathbf{Z}_p$ jest też zwarta, bo φ_n są funkcjami ciągłymi.

Na koniec jeszcze raz to samo, ale prościej.

Rozważmy pierścień $\mathbf{Z}$ liczb całkowitych i rodzinę ideałów $I_n = p^n\mathbf{Z}$, $n \geq 0$, gdzie p jest ustaloną liczbą pierwszą. Przyjmijmy $\mathcal{B} = \{I_n : n \geq 0\}$ za bazę otoczeń zera w pewnej topologii $\mathcal{T}_p$, definiując bazę $\mathcal{B}_a$ otoczeń punktu $a \in \mathbf{Z}$ przez przesunięcia zbiorów I_n:

$$\mathcal{B}_a = \{a + I_n :\ n \geq 0\} = a + \mathcal{B}.$$

Ponieważ I_n są ideałami w $\mathbf{Z}$, więc

1) $I_n + I_n \subset I_n$,
2) $I_nI_n \subset I_n$, a nawet $I_n\mathbf{Z} \subset I_n$.

Ponadto

3) $\bigcap_{n\geq 0} I_n = (0)$.

Z warunku 1) wynika ciągłość dodawania w zerze, z 2) – ciągłość mnożenia w zerze, a 3) oznacza, że $\mathcal{T}_p$ jest topologią Hausdorffa. Zatem $(\mathbf{Z}, \mathcal{T}_p)$ jest *pierścieniem topologicznym*, a rodzina zbiorów $\mathcal{B}$ określa *strukturę przestrzeni jednostajnej* w $\mathbf{Z}$. Liczby p-adyczne całkowite można teraz zdefiniować jako uzupełnienie tej struktury w sensie topologicznym:

$$\mathbf{Z}_p = (\mathbf{Z}, \mathcal{T}_p)\widehat{\ }.$$

W każdej sytuacji, kiedy buduje się, a potem bada jakiś obiekt matematyczny, powstaje pytanie, czy nie pojawia się on gdzieś indziej, w innym kontekście?

Podamy tu dwa przykłady, w których w naturalny sposób pojawiają się liczby p-adyczne całkowite.

Niech $G = \mathbf{C}_{p^\infty}$ oznacza zbiór wszystkich pierwiastków stopnia p^n z 1, gdzie p jest ustaloną liczbą pierwszą, a n przyjmuje nieujemne wartości całkowite. Zatem $\mathbf{C}_{p^\infty}$ jest sumą wstępującego ciągu grup cyklicznych

$$\mathbf{C}_p \subset \mathbf{C}_{p^2} \subset \mathbf{C}_{p^3} \subset \ldots \subset \mathbf{C}_{p^n} \subset \mathbf{C}_{p^{n+1}} \subset \ldots.$$

Możemy przyjąć, że $\mathbf{C}_{p^n}$ jest generowane przez $g_n = e^{2\pi i/p^n}$, tzn. $\mathbf{C}_{p^n} = \langle g_n \rangle$. Rozważmy zbiór $\mathrm{End}\,(G)$ endomorfizmów G, tzn. zbiór wszystkich homomorfizmów f G w G:

$$f :\ G \to G, \quad f(xy) = f(x)f(y) \quad \text{dla} \quad x, y \in G.$$

Jeżeli grupa G jest abelowa, to $\mathrm{End}\,(G)$ jest pierścieniem względem działań:

fg – mnożenie endomorfizmów, $(fg)(x) = f(x)g(x)$, jako dodawanie w pierścieniu,
$f \circ g$ – superpozycja endomorfizmów, $(f \circ g)(x) = f(g(x))$ jako mnożenie w pierścieniu $\mathrm{End}\,(G)$.

Niech $f \in \mathrm{End}\,(G)$. Ponieważ homomorfizm nie podwyższa rzędu elementu, więc $f(g_n) = g_n^{\alpha_n}$ dla jakiegoś $0 \leq \alpha_n < p^n$. Ponieważ $g_1^p = 1$ i ogólnie: $g_{n+1}^p = g_n$, więc $f(g_{n+1}^p) = f(g_n)$, skąd wynika, że

$$g_n^{\alpha_{n+1}} = (g_{n+1}^p)^{\alpha_{n+1}} = g_{n+1}^{p\alpha_{n+1}} = g_n^{\alpha_n}, \text{ tzn. } \alpha_{n+1} \equiv \alpha_n (\mathrm{mod}\, p^n).$$

Zatem, jeżeli $f, g \in \mathrm{End}(G)$, to można im przyporządkować ciągi

$$f \mapsto (\alpha_1, \alpha_2, \ldots), \quad \alpha_{n+1} \equiv \alpha_n (\mathrm{mod}\, p^n), \quad n \geq 1,$$
$$g \mapsto (\beta_1, \beta_2, \ldots), \quad \beta_{n+1} \equiv \beta_n (\mathrm{mod}\, p^n), \quad n \geq 1.$$

Jeżeli endomorfizmowi f przyporządkowany jest inny ciąg (α'_n), $f \mapsto (\alpha'_1, \alpha'_2, \ldots)$, to $\alpha_n \equiv \alpha'_n \pmod{p^n}$ dla $n \geq 1$. Ponieważ

$$(fg)(g_n) = f(g_n)g(g_n) = g_n^{\alpha_n} g_n^{\beta_n} = g_n^{\alpha_n + \beta_n},$$
$$(f \circ g)(g_n) = f(g(g_n)) = f(g_n^{\beta_n}) = (g_n^{\beta_n})^{\alpha_n} = g_n^{\alpha_n\beta_n},$$

więc

$$fg \mapsto (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots),$$
$$f \circ g \mapsto (\alpha_1\beta_1, \alpha_2\beta_2, \ldots),$$

tzn. endomorfizmy grupy $G = \mathbf{C}_{p^\infty}$ można uważać za całkowite liczby p-adyczne:

$$\mathrm{End}\,(\mathbf{C}_{p^\infty}) \simeq \mathbf{Z}_p.$$

Niech p i q będą dowolnymi liczbami pierwszymi, $\mathbf{F}_p$ – ciałem reszt modulo p, a $\overline{\mathbf{F}}_p$ jego algebraicznym domknięciem. Niech F_q będzie zbiorem tych elementów $x \in \overline{\mathbf{F}}_p$, których wielomian minimalny nad $\mathbf{F}_p$ jest stopnia q^n dla jakiegoś n, tzn. $[\mathbf{F}_p(x) : \mathbf{F}_p] = q^n$. Wiadomo, że grupą Galois $\mathbf{F}_p(x)$ nad $\mathbf{F}_p$ jest $\mathbf{C}_{q^n}$: $Gal\,(\mathbf{F}_p(x)/\mathbf{F}_p) = \mathbf{C}_{q^n}$.

Wykorzystując różne fakty z algebry, jak również teorię Galois dla nieskończonych rozszerzeń algebraicznych ciał, pochodzącą od Wolfganga Krulla (1928), można dowieść, że *topologiczną grupą Galois* F_q nad $\mathbf{F}_p$ jest $\mathbf{Z}_q$:

$$Gal\,(F_q/\mathbf{F}_p) = \varprojlim \mathbf{C}_{q^n} \simeq \mathbf{Z}_q.$$

Niech w dalszym ciągu p będzie ustaloną liczbą pierwszą.

Twierdzenie. *Niech* $F \in \mathbf{Z}[X_1, \ldots, X_n]$. *Kongruencja*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^N} \tag{9}$$

jest rozwiązalna w $\mathbf{Z}^n$ *dla każdego* $N \geq 1$, *wtedy i tylko wtedy, gdy równanie*

$$F(x_1, \ldots, x_n) = 0 \tag{10}$$

ma rozwiązanie w $\mathbf{Z}_p^n$.

Dowód wykorzystuje zwartość pierścienia $\mathbf{Z}_p$ i postać liczb p-adycznych.

($\Leftarrow$) Załóżmy, że równanie (10) ma rozwiązanie w liczbach $A_1, \ldots, A_n \in \mathbf{Z}_p$:

$$A_j = a_0^{(j)} + a_1^{(j)}p + a_2^{(j)}p^2 + \ldots + a_k^{(j)}p^k + \ldots,$$

gdzie $0 \leq a_k^{(j)} < p$ dla każdego j, k. Jeżeli a_{jk} oznacza sumę $k+1$ początkowych składników napisanych powyżej, to

$$A_j \equiv a_{jk} \pmod{p^k} \quad \text{dla} \quad k \geq 1.$$

Stąd:

$$0 = F(A_1, \ldots, A_n) \equiv F(a_{1k}, \ldots a_{nk}) \pmod{p^k}, \quad k \geq 1.$$

($\Rightarrow$) Niech dla każdego $N \geq 1$, $(x_1^{(N)}, \ldots, x_n^{(N)}) \in \mathbf{Z}^n$ będzie rozwiązaniem kongruencji

$$F(x_1^{(N)}, \ldots, x_n^{(N)}) \equiv 0 \pmod{p^N}. \tag{11}$$

Ponieważ $x_1^{(N)} \in \mathbf{Z}_p$, a $\mathbf{Z}_p$ jest zwarte, więc istnieje podciąg N_k, dla którego ciąg $x_1^{(N_k)}$ jest zbieżny do jakiegoś $\alpha_1 \in \mathbf{Z}_p$. Z tych samych powodów ciąg $x_2^{(N_k)}$, $k \geq 1$, zawiera podciąg zbieżny do pewnego $\alpha_2 \in \mathbf{Z}_p$. W podobny sposób znajdziemy podciąg ciągu $x_n^{(N)}$ zbieżny do jakiegoś $\alpha_n \in \mathbf{Z}_p$. Przypuśćmy (dla uproszczenia zapisu), że ciągi $x_1^{(N)}, \ldots, x_n^{(N)}$ są zbieżne w $\mathbf{Z}_p$. Ponieważ wielomian jest funkcją ciągłą w topologii p-adycznej, a podzielność przez dowolnie duże potęgi p oznacza w tej topologii zbieżność do zera, więc z (11) wynika, że

$$F(\alpha_1, \ldots, \alpha_n) = \lim_{N \to \infty} F(x_1^{(N)}, \ldots, x_n^{(N)}) = 0.$$

Oryginalny pomysł Hensela [4] z 1897 sprowadzał się do udowodnionego twierdzenia. Hensel pisał:

Rozważmy teraz także równanie tylko jako kongruencję względem dowolnie dużej potęgi p^M *rzeczywistej liczby pierwszej* p *jako modułu (przynajmniej dla* $M = 10.000$*). Zachodzi wówczas twierdzenie:*
Kongruencja $F(X) \equiv 0 \pmod{p^M}$ *posiada dokładnie tyle pierwiastków, jaki jest jej stopień, bez względu na to, jak duży będzie wykładnik* M, *a każdy z* n *pierwiastków* $X_1, X_2, \ldots, X_n$ *tej kongruencji można rozwinąć w szereg potęgowy utworzony z rosnących potęg* p, *w którym co najwyżej skończenie wiele wyrazów*

początkowych posiada wykładniki ujemne. Ogólnie, wszystkie te rozwinięcia względem potęg p mają wykładniki całkowite, tzn. można je zapisać następująco:

$$X = \frac{A_{-n}}{p^n} + \ldots + \frac{A_{-1}}{p} + A_0 + A_1 p + \ldots ;$$

dla tych liczb otrzymuje się więc dokładnie takie same rozwinięcia, jak dla funkcji algebraicznych w otoczeniu punktu regularnego.

Dziś liczby p-adyczne używane są w wielu działach matematyki, m.in. w teorii liczb, algebrze, geometrii algebraicznej, geometrii diofantycznej etc.

Przed trzydziestu laty van der Blij i Monna [1] zaproponowali – motywując to odpowiednio – użycie przestrzeni $\mathbf{Q}_p^n$ w fizyce zamiast przestrzeni euklidesowej $\mathbf{R}^n$. Normę w $\mathbf{Q}_p^n$ określa się wzorem

$$\|x\| = \max(|x_1|_p, \ldots, |x_n|_p), \quad \text{gdzie } x = (x_1, \ldots, x_n) \in \mathbf{Q}_p^n.$$

Obecnie modele p-adyczne są często stosowane w fizyce; powstały na ten temat monografie, np. [8].

O roli liczb p-adycznych w matematyce może chociażby świadczyć fakt, że dowód Wielkiego Twierdzenia Fermata, podany przez Andrew Wilesa w 1995 roku, wykorzystuje w istotny sposób reprezentacje p-adyczne grup Galois.

Artykuł [9] zawiera informacje o analizie p-adycznej. Elementarny wykład ciał z wartością bezwzględną można znaleźć w [10]. Dalsze własności ciał liczb p-adycznych wraz z ich uogólnieniami opisane są w [11] i [12].

Bibliografia

[1] F. van der Blij, A.F. Monna, *Models of space and time in elementary physics*, Journal of Mathematical Analysis and Applications 22 (1968), 537-545.

[2] Z.I. Borewicz, I.R. Szafarewicz, *Teoria cziseł* (ros.), Moskwa, wyd. I (1964), wyd. II (1972), wyd. III (1985).

[3] G. Darboux, *Sur le théorème fondamental de la géométrie projective*, Mathematische Annalen 17 (1880), 55-61.

[4] K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresbericht der Deutschen Mathematiker–Vereinigung 6 (1897), 83-88.

[5] — , *Theorie der algebraischen Zahlen*, B.G. Teubner, Leipzig und Berlin, 1908.

[6] J. Kürschak, *Über Limesbildung und allgemeine Körpertheorie*, Journal für die reine und angewandte Mathematik 142 (1913), 211-253.

[7] A. Ostrowski, *Über einige Lösungen der Funktionalgleichung* $\varphi(x)\varphi(y) = \varphi(xy)$, Acta Mathematica 41 (1918), 271-284.

[8] V.S. Vladimirov, I.V. Volovich, E.I. Zelenov, *p-adic analysis and mathematical physics*, World Scientific, Singapore, Hong-Kong, 1984.

[9] W. Więsław, *Analiza niearchimedesowska i ciała liczb p-adycznych*, Wiadomości Matematyczne 11 (1970), 221-234.

[10] — , *Grupy, pierścienie, ciała*, Uniwersytet Wrocławski, wyd. I (1977), wyd. II (1979), wyd. III (1983).

[11] — , *Topological fields*, Acta Universitatis Wratislaviensis No 675. Matematyka, Fizyka, Astronomia XLIII, Wrocław 1982.

[12] — , *Topological fields*, Pure and Applied Mathematics. A Series of Monographs and Textbooks. No 119, Marcel Dekker, New York 1988.

[13] — , *Problemy z niewymiernością – stworzenie liczb rzeczywistych*, Matematyka, Społeczeństwo, Nauczanie, Numer 9 (VII 1992), 17-29.

[14] — , *Liczby niewymierne*, CODN – SNM, Warszawa 1992.

[15] — , *Powstanie liczb niewymiernych*, Zeszyty Naukowe Politechniki Śląskiej, seria: Matematyka-Fizyka, z. 76 (1995), 339-361.