X Liceum Ogólnokształcące im. Komisji Edukacji Narodowej

Weronika Stypuła

Wykładniki p-adyczne i ich własności

Praca matematyczna
napisana pod opieką
mgr Daniela Danieluka

Kraków 2023

Spis treści

Wstęp

Niniejsza praca została poświęcona wykładnikowi p-adycznemu – wygodnemu narzędziu do rozwiązywania zadań związanych z podzielnością liczb.

W pierwszym rozdziale autorka przedstawiła definicję wykładnika p-adycznego i jego własności wraz z dowodami. Drugi rozdział został poświęcony wykorzystaniu wykładników p-adycznych w rozwiązywaniu zadań.

Rozdział 1

Definicja wykładnika p-adycznego i jego własności

Definicja 1. (wykładnik p-adyczny)
Niech $a \in \mathbb{Z}\backslash\{0\}$, $p \in \mathbb{P}$, przy czym $\mathbb{P}$ jest zbiorem liczb pierwszych. Wykładnikiem p-adycznym liczby a, oznaczanym $v_p(a)$, nazywamy największą liczbę naturalną m, która spełnia warunek $p^m|a$. Ponadto przyjmujemy, że $v_p(0) = +\infty$.

Wszystkie własności będą rozważone dla liczb całkowitych dodatnich.

Własność 1. (zapis liczby)
Dowolną liczbę naturalną dodatnią a można zapisać jako nieskończony iloczyn naturalnych potęg liczb pierwszych, czyli

$$a = \prod_{p \in \mathbb{P}} p^{v_p(a)}.$$

Dowód. Każdą liczbę naturalną dodatnią a można rozłożyć na czynniki pierwsze, czyli przedstawić a jako skończony iloczyn potęg liczb pierwszych p. Wykładniki tych potęg są z definicji wykładnikami p-adycznymi liczby a. Powyższy iloczyn jest nieskończony, jednak tylko skończona liczba wykładników $v_p(a)$ jest różna od zera. Zatem tylko skończona liczba potęg p daje wkład do iloczynu. Powyższy wzór można traktować jako zapis rozkładu liczby a na czynniki pierwsze. □

Dla przykładu, liczbę 100 można zapisać jako $100 = 2^2 \cdot 5^2$. Z powyższego wzoru otrzymamy $100 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot ...$, co sprowadza się do $100 = 2^2 \cdot 5^2$. Pozostałe czynniki nie zmieniają nieskończonego iloczynu.

Własność 2. (wykładnik p-adyczny iloczynu)
Wykładnik p-adyczny iloczynu liczb naturalnych dodatnich a, b jest równy sumie wykładników p-adycznych tych liczb, to znaczy

$$v_p(ab) = v_p(a) + v_p(b).$$

Dowód. Z własności 1. wynika, że liczby a i b można zapisać w postaci

$$a = \prod_{p\in\mathbb{P}} p^{v_p(a)}, b = \prod_{p\in\mathbb{P}} p^{v_p(b)}.$$

Iloczyn tych liczb można zapisać na dwa sposoby

$$a \cdot b = \prod_{p\in\mathbb{P}} p^{v_p(a)} \cdot \prod_{p\in\mathbb{P}} p^{v_p(b)} = \prod_{p\in\mathbb{P}} p^{v_p(a)} \cdot p^{v_p(b)} = \prod_{p\in\mathbb{P}} p^{v_p(a)+v_p(b)},$$

$$a \cdot b = \prod_{p\in\mathbb{P}} p^{v_p(a\cdot b)}.$$

Porównując wykładniki otrzymuje się $v_p(ab) = v_p(a) + v_p(b)$. □

Własność 3. (wykładnik p-adyczny ilorazu)
Wykładnik p-adyczny ilorazu takich liczb naturalnych dodatnich a, b, że $a|b$ jest równy różnicy wykładników p-adycznych tych liczb, to znaczy

$$v_p\Big(\frac{b}{a}\Big) = v_p(b) - v_p(a).$$

Dowód. Dowód przebiega analogicznie do dowodu własności 2. □

Własność 4. (wykładnik p-adyczny sumy liczb)
Dla liczb całkowitych dodatnich a, b prawdą jest, że
a) jeśli $v_p(a) = v_p(b)$, to $v_p(a + b) \geq v_p(a)$,
b) jeśli $v_p(a) < v_p(b)$, to $v_p(a + b) = v_p(a)$.

Dowód. Niech m, n, q będą liczbami całkowitymi dodatnimi. Wówczas z definicji wykładnika p-adycznego liczby naturalne a i b możemy zapisać jako $a = mp^{v_p(a)}$, $b = np^{v_p(b)}$, $a + b = qp^{v_p(a+b)}$ przy czym p nie dzieli m, n i q. Zatem

$$a + b = mp^{v_p(a)} + np^{v_p(b)} = p^{v_p(a)} \cdot \big[m + np^{v_p(b)-v_p(a)}\big].$$

Z tego otrzymujemy, że
a) jeśli $v_p(a) = v_p(b)$, to

$$a + b = p^{v_p(a)} \cdot (m + n).$$

Liczby m i n nie dzielą się przez p, ale ich suma może się dzielić przez p. Z równości

$$qp^{v_p(a+b)} = p^{v_p(a)} \cdot (m + n)$$

wynika, że $v_p(a + b) \geq v_p(a)$, przy czym równość zachodzi, jeśli p nie dzieli $(m + n)$.

b) dla $v_p(a) < v_p(b)$ wyrażenie $m + np^{v_p(b)-v_p(a)}$ nie dzieli się przez p, ponieważ jest sumą liczby podzielnej przez p i liczby niepodzielnej przez p. Zatem

$$qp^{v_p(a+b)} = \big[m + np^{v_p(b)-v_p(a)}\big]p^{v_p(a)}.$$

Porównując wykładniki, otrzymujemy

$$v_p(a+b) = v_p(a).$$

□

Własność 5. (równość liczb)
Liczby naturalne a i b są równe, wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p mają równe wykładniki p-adyczne

$$a = b \iff \forall_{p\in\mathbb{P}} v_p(a) = v_p(b).$$

Dowód. Z własności 1. możemy przedstawić iloraz liczb a, b w postaci

$$\frac{a}{b} = \frac{\prod_{p\in\mathbb{P}} p^{v_p(a)}}{\prod_{p\in\mathbb{P}} p^{v_p(b)}} = \prod_{p\in\mathbb{P}} p^{v_p(a)-v_p(b)}.$$

Dla $a = b$ mamy $\frac{a}{b} = 1$. Z drugiej strony $\prod_{p\in\mathbb{P}} p^{v_p(a)-v_p(b)} = 1$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p prawdziwa jest równość $v_p(b) - v_p(a) = 0$. Zatem $v_p(b) = v_p(a)$. □

Własność 6. (podzielność liczb)
Liczba naturalna a dzieli liczbę naturalną b, wtedy i tylko wtedy, gdy dla każdej liczby $p \in \mathbb{P}$ $v_p(a)$ jest mniejsze lub równe $v_p(b)$

$$a|b \iff \forall_{p\in\mathbb{P}} v_p(a) \leq v_p(b).$$

Dowód. Jeśli $a|b$, to $\frac{b}{a} = y$, $y \in \mathbb{Z}$.
Wtedy, korzystając z własności 1. otrzymujemy

$$y = \frac{\prod_{p\in\mathbb{P}} p^{v_p(b)}}{\prod_{p\in\mathbb{P}} p^{v_p(a)}} = \prod_{p\in\mathbb{P}} p^{v_p(b)-v_p(a)}.$$

Liczba y jest całkowita wtedy i tylko wtedy, gdy dla każdego $p \in \mathbb{P}$ $v_p(b) - v_p(a) \geq 0$.
□

Własność 7. (wykładnik p-adyczny NWD liczb naturalnych a, b)
Wykładnik p-adyczny największego wspólnego dzielnika liczb naturalnych dodatnich a, b jest równy mniejszemu z wykładników p-adycznych tych liczb

$$v_p(NWD(a,b)) = min\{v_p(a), v_p(b)\}.$$

Dowód. Oznaczmy

$$d = NWD(a,b).$$

Z definicji największego wspólnego dzielnika to oznacza, że $d|a$ i $d|b$.
Z własności 6. wynika, że $v_p(d) \leq v_p(a)$ i $v_p(d) \leq v_p(b)$. Przy założeniu, że $v_p(a) \leq v_p(b)$ otrzymujemy

$$v_p(d) \leq v_p(a)$$

oraz

$$p^{v_p(a)}|p^{v_p(b)},$$

z czego otrzymujemy

$$p^{v_p(b)} = p^n \cdot p^{v_p(a)},$$

przy czym $n = v_p(b) - v_p(a)$. Z tego wynika, że $NWD(p^{v_p(a)}, p^{v_p(b)}) = p^{v_p(a)}$. Zatem $v_p(d) = v_p(a)$, co oznacza, że

$$v_p(NWD(a,b)) = min\{v_p(a), v_p(b)\}.$$

□

Własność 8. (wykładnik p-adyczny NWW liczb naturalnych a, b)
Wykładnik p-adyczny najmniejszej wspólnej wielokrotności liczb naturalnych dodatnich a, b jest równy większemu z wykładników p-adycznych tych liczb

$$v_p(NWW(a,b)) = max\{v_p(a), v_p(b)\}.$$

Dowód. Oznaczmy

$$w = NWW(a,b).$$

Z definicji najmniejszej wspólnej wielokrotności wiemy, że $a|w$ i $b|w$
Z własności 6. wynika, że $v_p(a) \leq v_p(w)$ i $v_p(b) \leq v_p(w)$. Przy założeniu, że $v_p(a) \leq v_p(b)$ otrzymujemy

$$v_p(b) \leq v_p(w).$$

Analogicznie do własności 7., $NWW(p^{v_p(a)}, p^{v_p(b)}) = p^{v_p(b)}$. Stąd $v_p(w) = v_p(b)$, czyli

$$v_p(NWW(a,b)) = max\{v_p(a), v_p(b)\}.$$

□

Własność 9. (potęga liczby naturalnej)
Liczba naturalna dodatnia a jest k-tą potęgą liczby naturalnej b, jeżeli $k|v_p(a)$.

Dowód. Liczba $a = b^k$, $b \in \mathbb{N}$, to znaczy, że

$$b = \sqrt[k]{a}.$$

Korzystając z zapisu z własności 1.

$$b = \prod_{p \in \mathbb{P}} \sqrt[k]{p^{v_p(a)}} = \prod_{p \in \mathbb{P}} p^{\frac{v_p(a)}{k}}$$

Jeśli liczba b jest liczbą naturalną, to $\frac{v_p(a)}{k}$ też jest liczbą naturalną, co oznacza, że $k | v_p(a)$. $\square$

Rozdział 2

Przykładowe zadania

Zadanie 1. *Pokazać, że dla żadnej liczby całkowitej dodatniej n liczba 2^n nie jest dzielnikiem liczby $n!$.*

Rozwiązanie. Liczby z zadania możemy zapisać w postaci $n! = 1 \cdot 2 \cdot 3 \cdot \ ... \ \cdot n = \prod_{k=1}^{n} k$, $2^n = \prod_{k=1}^{n} 2$. Jeżeli $2^n | n!$, to z własności 6. wynika, że $v_p(2^n) \leq v_p(n!)$. Sprawdzimy, czy ta nierówność jest prawdziwa.

$$v_p(2^n) = nv_p(2),$$

co jest niezerowe tylko dla $p = 2$. Wtedy $nv_2(2) = n$.
Dla $p \neq 2$ zachodzi równość $v_p(2) = 0$, jednak rozważanie zerowych wykładników p-adycznych nie wnosi nic do zadania. Z tego powodu w dalszej części rozwiązania będą rozważone tylko wykładniki 2-adyczne.
Liczbę $v_2(n!)$ można przedstawić w postaci

$$v_2(n!) = v_2\Big(\prod_{k=1}^{n} k\Big) = \sum_{k=1}^{n} v_2(k).$$

Niezerowy wkład do tej sumy mamy tylko dla parzystych k, czyli $k = 2m$, przy czym m jest liczbą całkowitą dodatnią. Stąd, powyższą sumę można przedstawić jako

$$\sum_{k=1}^{n} v_2(k) = \sum_{2m=2}^{n} v_2(2m) = \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} v_2(2) + \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} v_2(m).$$

Ponieważ $v_2(2) = 1$, pierwszy składnik w wyniku daje $\lfloor \frac{n}{2} \rfloor$, czyli największą liczbę całkowitą nie większą niż $\frac{n}{2}$. Niezerowy wkład do drugiego składnika dają tylko wartości $m = 2s$, przy czym s jest liczbą całkowitą dodatnią.
Stąd drugi składnik sumy można zapisać jako

$$\sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} v_2(m) = \sum_{2s=2}^{\lfloor \frac{n}{2} \rfloor} v_2(2s) = \sum_{s=1}^{\lfloor \frac{n}{4} \rfloor} v_2(2) + \sum_{s=1}^{\lfloor \frac{n}{4} \rfloor} v_2(s).$$

Z pierwszego składnika otrzymujemy $\lfloor \frac{n}{4} \rfloor$, a w drugim ponownie niezerowy wkład dają tylko parzyste wartości s.
Postępując analogicznie aż do wyczerpania niezerowych składników sumy otrzymujemy

$$v_2(n!) = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{4} \rfloor + \lfloor \frac{n}{8} \rfloor + ... + \lfloor \frac{n}{2^r} \rfloor,$$

przy czym $\frac{n}{2^r}$ jest ostatnim niezerowym składnikiem $v_2(n!)$, a r jest liczbą całkowitą dodatnią. Nasze wyrażenie można ograniczyć z góry w następujący sposób

$$v_2(n!) \leq \frac{n}{2} + \frac{n}{4} + \frac{n}{8} + ... + \frac{n}{2^r}$$

Po wyciągnięciu $\frac{n}{2}$ przed nawias otrzymujemy

$$v_2(n!) \leq \frac{n}{2}\Big(1 + \frac{1}{2} + ... + \frac{1}{2^{r-1}}\Big),$$

Ze wzoru skróconego mnożenia

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + a + 1)$$

otrzymujemy

$$a^{n-1} + a^{n-2} + ... + a + 1 = \frac{a^n - 1}{a - 1} = \frac{1 - a^n}{1 - a},$$

stąd

$$1 + \frac{1}{2} + \frac{1}{4} + ... + \frac{1}{2^{r-1}} = \frac{1 - \frac{1}{2^r}}{1 - \frac{1}{2}} = 2(1 - \frac{1}{2^r}),$$

z czego wynika, że

$$v_2(n!) \leq \frac{n}{2} \cdot 2(1 - \frac{1}{2^r})$$

Po przekształceniu otrzymujemy

$$v_2(n!) \leq n(1 - \frac{1}{2^r})$$

$$v_2(n!) \leq n - \frac{n}{2^r}$$

Liczba $\frac{n}{2^r}$ jest dodatnia, więc $n - \frac{n}{2^r} < n$. Wiedząc, że $v_2(2^n) = n$ otrzymujemy $v_2(n!) < v_2(2^n)$, co oznacza, że założenie, że $2^n | n!$ na początku rozwiązania jest błędne.

Zadanie 2. *Dane są takie liczby całkowite x, y, że suma*

$$\frac{x^2}{y} + \frac{y^2}{x}$$

jest liczbą całkowitą. Udowodnij, że obydwa składniki powyższej sumy są liczbami całkowitymi.

Rozwiązanie. Chcąc udowodnić, że składniki sumy $\frac{x^2}{y}+\frac{y^2}{x}$ są liczbami całkowitymi, wystarczy pokazać, że jeden z nich jest całkowity.
Jeżeli $\frac{y^2}{x}$ miałaby być liczbą całkowitą, to z własności 6. wynika, że $v_p(x) \leq v_p(y^2)$ dla dowolnego $p \in \mathbb{P}$. Zatem wystarczy wykazać, że ta nierówność zachodzi dla każdej liczby pierwszej p.
Sumę z zadania możemy zapisać w postaci

$$\frac{x^2}{y} + \frac{y^2}{x} = \frac{x^3 + y^3}{xy}.$$

Wtedy z własności 6. wynika, że

$$v_p(xy) \leq v_p(x^3 + y^3).$$

Z własności 2. i powyższej nierówności otrzymujemy

$$v_p(x) + v_p(y) \leq v_p(x^3 + y^3).$$

Rozważmy sytuację, w której liczby $v_p(x^3)$ i $v_p(y^3)$ są różne. Jeśli $v_p(x^3) > v_p(y^3)$, to z własności 4b) wiemy, że $v_p(x^3 + y^3) = v_p(y^3)$. Zatem nierówność

$$v_p(x) + v_p(y) \leq v_p(x^3 + y^3).$$

możemy zapisać jako

$$v_p(x) + v_p(y) \leq v_p(y^3).$$

$v_p(y^3) = 3v_p(y)$, więc

$$v_p(x) \leq 2v_p(y),$$

co oznacza, że

$$v_p(x) \leq v_p(y^2).$$

Natomiast jeśli jest odwrotnie, czyli $v_p(x^3) < v_p(y^3)$, to naszą nierówność możemy zapisać w postaci

$$v_p(x) + v_p(y) \leq v_p(x^3).$$

Stąd

$$v_p(y) \leq v_p(x^2).$$

Ostatnim przypadkiem jest równość $v_p(x^3) = v_p(y^3)$, która oznacza, że $v_p(x) = v_p(y)$. Podstawiając to do nierówności

$$v_p(x) + v_p(y) \leq v_p(x^3 + y^3)$$

otrzymujemy

$$2v_p(x) \leq v_p(x^3),$$

czyli

$$v_p(x) \geq 0,$$

co jest zawsze prawdziwe.

Zadanie 3. *Liczby naturalne a i b mają tę własność, że dla każdego n naturalnego liczba b^{n+1} jest podzielna przez liczbę a^n. Udowodnić, że a jest dzielnikiem b*

Rozwiązanie. Skoro $a^n | b^{n+1}$, to $\frac{b^{n+1}}{a^n} \in \mathbb{Z}$. Nasz ułamek można przedstawić w postaci

$$\frac{b^{n+1}}{a^n} = b \cdot \frac{b^n}{a^n} = b \cdot \left(\frac{b}{a}\right)^n$$

Z własności 2. wynika, że

$$v_p\left(\frac{b^{n+1}}{a^n}\right) = v_p(b) + v_p\left[\left(\frac{b}{a}\right)^n\right] = v_p(b) + nv_p\left(\frac{b}{a}\right)$$

Jeśli $\frac{b^{n+1}}{a^n}$ jest liczbą całkowitą, to $v_p(b) + nv_p\left(\frac{b}{a}\right)$ też musi być całkowite. Wiemy, że liczby $v_p(b)$ i n są liczbami całkowitymi, więc $v_p\left(\frac{b}{a}\right) \in \mathbb{Z}$. To oznacza, że $\frac{b}{a} \in \mathbb{Z}$, czyli $a|b$.

Bibliografia

[1] Wykładniki p-adyczne, http://www.deltami.edu.pl/temat/matematyka/teoria_liczb/2020/10/31/
p-adyczne/ , dostęp 26.02.2023

[2] Wykładniki p-adyczne, https://indekswkieszeni.pl/wykladniki-p-adyczne/ , dostęp 26.02.2023

[3] Lista zadań z warsztatów matematycznych w I LO w Koszalinie, https://www.mimuw.edu.pl/ amecel//liceum/ord_zadania.pdf , dostęp 26.02.2023