Wykładniki p-adyczne i LTE

Teoria

Oznaczenia. $\mathbb{Z}_+$ oznacza zbiór liczb całkowitych dodatnich,

(a, b) - NWD liczb a i b, a $[a, b]$ będzie oznaczać ich NWW.

Definicja 1. Niech p będzie liczbą pierwszą oraz $c \neq 0$ liczbą całkowitą. Wówczas liczba $\nu_p(c)$ będzie oznaczać największą liczbę całkowitą k, dla którego $p^k | c$. Ponadto definiujemy $v(0) = +\infty$. Liczbę $\nu_p(c)$ nazywamy **wykładnikiem p-adycznym** liczby c.

Powyższa definicja może być rozszerzona dla liczb wymiernych, tzn. dla liczb całkowitych $a, b \neq 0$ mamy

$$\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$$

Twierdzenie 1. *Dana jest liczba pierwsza p oraz $a, b \in \mathbb{Z}$.*

1. $\nu_p(ab) = \nu_p(a) + \nu_p(b) \implies \nu_p(a^n) = n\nu_p(a)$,
2. *$a|b$ wtedy i tylko wtedy, gdy dla każdego p pierwszego zachodzi $\nu_p(a) \leqslant \nu_p(b) \implies a = b$ wtedy i tylko wtedy, gdy $\nu_p(a) = \nu_p(b)$,*
3. *$\nu_p(a \pm b) \geqslant min\{\nu_p(a), \nu_p(b)\}$, przy czym jeśli $\nu_p(a) \neq \nu_p(b)$ to zachodzi równość,*
4. $\nu_p(NWD(a, b)) = min\{\nu_p(a), \nu_p(b)\}, \quad \nu_p(NWW(a, b)) = max\{\nu_p(a), \nu_p(b)\}$,
5. *Liczba wymierna x jest całkowita wtedy i tylko wtedy, gdy $\nu_p(x) \geqslant 0$ dla każdej liczby pierwszej p.*

Twierdzenie 2 (Wzór Legendre'a)**.** *Jeżeli p jest liczbą pierwszą i $n \in \mathbb{Z}_+$ to*

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots = \frac{n - s_p(n)}{p - 1},$$

gdzie $s_p(n)$ to suma cyfr liczby n w zapisie przy podstawie p.

Twierdzenie 3 (LTE - Lifting the Exponent Lemma)**.** *Niech p będzie liczbą pierwszą, $n \in \mathbb{Z}_+$ oraz $x, y \in \mathbb{Z}$ takie, że $p \nmid x$ i $p \nmid y$. Wówczas*

1. *gdy $p \neq 2$ oraz $p|x - y$ to:* $\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)$,
2. *gdy $p = 2$ oraz $2|x - y$ i $2|n$ to:* $\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1$,
3. *gdy $p = 2$ oraz $2|x - y$ i $2 \nmid n$ to:* $\nu_2(x^n - y^n) = \nu_2(x - y)$,
4. *gdy $p|x + y$ oraz $2 \nmid n$ to:* $\nu_p(x^n + y^n) = \nu_p(x + y) + \nu_p(n)$.

Dowód tego twierdzenia będzie na końcu skryptu.

Twierdzenie 4 (Trik)**.** *Jeżeli liczby całkowite dodatnie a i b są względnie pierwsze i spełniają równość $ab = c^k$ dla pewnych $c, k \in \mathbb{Z}_+$, to a i b są k-tymi potęgami liczb całkowitych.*

Przykłady

1. Udowodnij, że dla każdej pary dodatnich liczb całkowitych a i b zachodzi równość: $(a,b)\cdot[a,b]=ab$.
2. Dane są niezerowe liczby całkowite x i y takie, że $\frac{x^2}{y}+\frac{y^2}{x}\in\mathbb{Z}$. Wykazać, że $\frac{x^2}{y}$ jest liczbą całkowitą.
3. Liczby dodatnie całkowite a i b są takie, że $a^n \mid b^{n+1}$ dla każdej liczby $n\in\mathbb{Z}_+$. Dowieść, że $a \mid b$.
4. Udowodnić, że $2^n \nmid n!$ dla każdej dodatniej liczby całkowitej n. Znajdź wszystkie $n\in\mathbb{Z}_+$ takie, że $2^{n-1}|n!$.
5. Niech k będzie dodatnią liczbą całkowitą. Znajdź wszystkie $n\in\mathbb{Z}_+$, dla których $3^k \mid 2^n-1$.
6. Niech p będzie liczbą pierwszą większą niż 3. Wyznaczyć $\nu_p((p-2)^{2(p-1)}-(p+4)^{p-1})$.

Zadania

1. Udowodnij, że dla liczb całkowitych dodatnich a, b i c zachodzą równości:
   - $[a,b,c]\cdot(a,b)\cdot(b,c)\cdot(c,a)=abc\cdot(a,b,c)$,
   - $(ab,bc,ca)\cdot[a,b,c]=abc=(a,b,c)\cdot[ab,bc,ca]$,
   - $(a,b,c)^2\cdot[a,b]\cdot[b,c]\cdot[c,a]=[a,b,c]^2\cdot(a,b)\cdot(b,c)\cdot(c,a)$.
2. Znajdź wszystkie dodatnie liczby całkowite n takie, że $7^n \mid 9^n-1$.
3. Dane są dodatnie liczby całkowite $a,b\leqslant 2^{2021}$. Załóżmy, że dla pewnej liczby całkowitej $m\geqslant 2021$ liczba a^{m+1} jest podzielna przez b^m, a liczba b^{m+1} jest podzielna przez a^m. Dowieść, że $a=b$.
4. Liczby $a,b,c\neq 0$ oraz $\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$ są całkowite. Wykaż, że abc jest sześcianem liczby całkowitej.
5. Udowdonić, że jeżeli $a^2+a=3b^2$ dla $a,b\in\mathbb{Z}_+$, to $a+1$ jest kwadratem liczby całkowitej.
6. Niech p będzie liczbą pierwszą oraz $a,n\in\mathbb{Z}_+$. Udowodnij, że jeżeli $2^p+3^p=a^n$, to $n=1$.
7. Dane są $a,b\in\mathbb{Z}_+$ spełniają podzielność $ab \mid a^2+b^2+a$. Wykazać, że a jest kwadratem liczby całkowitej.
8. Znajdź wszystkie takie trójki liczb całkowitych n, x, y, że $(x-y)^n=xy$.
9. Niech $x,y\in\mathbb{Z}_+$. Dowieść, że istnieje tylko skończenie wiele liczb $n\in\mathbb{Z}_+$ takich, że $\left(x+\frac{1}{2}\right)^n+\left(y+\frac{1}{2}\right)^n\in\mathbb{Z}$.
10. Niech $a\in\mathbb{Z}_+$ takie, że $4(a^n+1)$ jest sześcianem liczby całkowitej dla każdego $n\in\mathbb{Z}_+$. Wykaż, że $a=1$.
11. Niech $m,n\in\mathbb{Z}$ takie, że $7n^2-n=8m^2-m$. Dowieść, że $|n-m|$ jest kwadratem liczby całkowitej.
12. Udowodnić, że istnieje nieskończenie wiele dodatnich liczb całkowitych n takich, że
$$n|1^n+2^n+\ldots+10^n.$$
Spróbuj uogólnić zadanie dla $k>1$ liczb.
13. Znajdź największą liczbę k, która liczba 1991^k dzieli liczbę
$$1990^{1991^{1992}}+1992^{1991^{1990}},\qquad 1991=11\cdot 181.$$
14. Niech $n=16^{3^r}-4^{3^r}+1$. Udowodnić, że $n \mid 2^{n-1}-1$

Dowód LTE

Dowód.. Dowód będzie opierał się na indukcji przy $\nu_p(n)$. Udowodnimy bazę indukcyjną (która działa dla każdej liczby pierwszej!).

Lemat 1. Niech $x, y \in \mathbb{Z}$ i $n \in \mathbb{Z}_+$ oraz p będzie liczbą pierwszą taka, że $p \nmid n, x, y$ oraz $p \mid x - y$. Wówczas

$$\nu_p(x^n - y^n) = \nu_p(x - y).$$

Do dowodu tego lematu zużyjemy znany nam wzór $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$. Wykorzystamy założenie $p \mid x - y$, czyli $x \equiv y \pmod p$ co oznacza, że

$$x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1} \equiv x^{n-1} + x^{n-2} \cdot x + \ldots x \cdot x^{n-2} + x^{x-1} = nx^{n-1} \not\equiv 0 \pmod p$$

Udowodnimy najpierw dla $p \neq 2$: Zakładając już, że $p \nmid x, y$ oraz $p \mid x - y$. Wykażemy, że

$$(a) \quad \nu_p(x^p - y^p) = \nu_p(x - y) + 1.$$

Udowodnimy, że: $\quad p \mid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}$ oraz $p^2 \nmid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}$.

Pierwszą podzielność jest łatwo udowodnić z racji tego, że

$$x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod p.$$

Teraz niech $y = x + kp$, dla pewnej liczby całkowitej k. Dla liczby całkowitej $1 \leqslant r \leqslant p - 1$ mamy:

$$y^r x^{p-1-r} = (x + kp)^r x^{p-1-r} = x^{p-1-r}\left(x^r + r(kp)x^{r-1} + p^2 \cdot A\right) \equiv x^{p-1} + rkpx^{r-2} \pmod{p^2}.$$

Wówczas uzyskujemy

$$x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1} \equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + \ldots + (x^{p-1} + (p-1)kpx^{p-2})$$

$$\equiv px^{p-1} + (1 + 2 + \ldots + (p-1))kpx^{p-2} = px^{p-1} + \frac{p(p-1)}{2}kpx^{p-2} \equiv px^{p-1} \not\equiv 0 \pmod{p^2}.$$

Zatem udowodniliśmy (a). Teraz przejdźmy do ogólnego przypadku. Niech $n = p^a b$, gdzie $p \nmid b \quad (\nu_p(n) = a)$.

$$\nu_p(x^n - y^n) = \nu_p((x^{p^a})^b - (y^{p^a})^b) = \nu_p(x^{p^a} - y^{p^a}) \quad \text{z Lematu 1.}$$

$$= \nu_p((x^{p^{a-1}})^p - (y^{p^{a-1}})^p) = \nu_p(x^{p^{a-1}} - y^{p^{a-1}}) + 1 \quad \text{z (a)}$$

$$= \ldots = \nu_p(x^p - y^p) + a - 1 = \nu_p(x - y) + a = \nu_p(x - y) + \nu_p(n).$$

Przypadek $p = 2$ nie działa tak samo, gdyż w poprzednim przypadku zużyliśmy fakt, że $(p-1)/2$ jest liczbą całkowitą.

Wykażemy najpierw, że dla nieparzystych liczb całkowitych x i y takie, że $4 \mid x - y$ mamy

$$(b) \quad \nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(n).$$

Z lematu 1. wynika, że wystarczy udowodnić ten fakt dla potęg dwójki, czyli

$$\nu_2(x^{2^k} - y^{2^k}) = \nu_2(x-y) + k,$$

możemy to otrzymać poprzez użycie wiele razy wzoru na różnicę kwadratów

$$x^{2^k} - y^{2^k} = (x^{2^{k-1}} + y^{2^{k-1}})(x^{2^{k-1}} - y^{2^{k-1}}) = \ldots = (x^{2^{k-1}} + y^{2^{k-1}})(x^{2^{k-2}} + y^{2^{k-2}}) \ldots (x^2 + y^2)(x+y)(x-y).$$

Z racji tego, że $x \equiv y \equiv \pm 1 \pmod 4$ mamy, że $x^{2^m} \equiv y^{2^m} \equiv 1 \pmod 4$ dla każdej liczby całkowitej m, co daje $x^{2^m} + y^{2^m} \equiv 2 \pmod 4$ takich wyrażeń jest k, czyli wyszło to co chcieliśmy.

Wracając do ogólnego przypadku, tzn. dla x i y nieparzystych liczb całkowitych oraz parzystej liczb $n \in \mathbb{Z}_+$ mamy:

$$\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(x+y) + \nu_2(n) - 1.$$

Wobec tego, że mamy $2 \nmid x, y$ uzyskujemy $4 | x^2 - y^2$. Niech $n = 2^k \cdot m$, gdzie m jest nieparzyste ($k = \nu_2(n)$). Wówczas

$$\begin{aligned}
\nu_2(x^n - y^n) &= \nu_2((x^{2^k})^m - (y^{2^k})^m) = \nu_(x^{2^k} - y^{2^k}) \text{ z Lematu 1.} \\
&= \nu_2((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}) = \nu_2((x^2)^{2^{k-2}} - (y^2)^{2^{k-2}}) + 1 \text{ z (b)} \\
&= \ldots = \nu_2(x^2 - y^2) + k - 1 = \nu_2(x-y) + \nu_2(x+y) + \nu_2(n) - 1.
\end{aligned}$$

□
