Wykładniki p-adyczne

Bartłomiej BZDĘGA

Niech $n \neq 0$ będzie liczbą całkowitą, zaś p liczbą pierwszą. Wówczas największą taką liczbę całkowitą nieujemną α, dla której $p^\alpha \mid n$, nazywamy *wykładnikiem p-adycznym* liczby n i oznaczamy $\nu_p(n)$. Dodatkowo przyjmujemy, że $\nu_p(0) = +\infty$.

Dla $n \neq 0$ stwierdzenie $\nu_p(n) = \alpha$ jest równoważne stwierdzeniu, że $p^\alpha \mid n$ i $p^{\alpha+1} \nmid n$. Stosuje się również notację $p^\alpha \parallel n$, którą odczytujemy: p^α *dzieli dokładnie* n. Możemy też zapisać $n = p^\alpha m$, przy czym $p \nmid m$. Warto jeszcze zauważyć, że $\nu_p(n) = 0$ wtedy i tylko wtedy, gdy $p \nmid n$.

Wykładniki p-adyczne mają następujące własności dla całkowitych a, b i dowolnej liczby pierwszej p:

(1) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$; dla $a \mid b$ mamy $\nu_p(b/a) = \nu_p(b) - \nu_p(a)$;
(2) jeśli $\nu_p(a) < \nu_p(b)$, to $\nu_p(a+b) = \nu_p(a)$;
(3) jeśli $\nu_p(a) = \nu_p(b)$, to $\nu_p(a+b) \geqslant \nu_p(a)$.

Dowód. Przypadek $a = 0$ lub $b = 0$ jest trywialny, więc go pominiemy. Niech $a = p^\alpha n$ i $b = p^\beta m$, przy czym $p \nmid m, n$. Równość $ab = p^{\alpha+\beta}mn$ i niepodzielność $p \nmid mn$ dowodzą pierwszej części własności (1). Druga część jasno wynika z pierwszej. Aby wykazać (2) i (3), zapiszmy $a + b = p^\alpha(m + np^{\beta-\alpha})$. Korzystając z (1) mamy $\nu_p(a+b) = \alpha + \nu_p(m + np^{\beta-\alpha})$. Jeśli $\alpha < \beta$, to $p \nmid m + np^{\beta-\alpha}$, a jeśli $\alpha = \beta$, to liczba $m + np^{\beta-\alpha} = m + n$ może, choć nie musi, być podzielna przez p.

We własnościach (2) i (3) dodawanie można zastąpić odejmowaniem, dowód jest praktycznie taki sam. Indukcyjnie otrzymamy następujące uogólnienie na liczby całkowite $a, b, c, \ldots$:

(2′) jeśli w ciągu $(\nu_p(a), \nu_p(b), \nu_p(c), \ldots)$ istnieje dokładnie jeden wyraz najmniejszy, to $\nu_p(a+b+c+\ldots) = \min\{\nu_p(a), \nu_p(b), \nu_p(c), \ldots\}$;
(3′) w każdym przypadku $\nu_p(a+b+c+\ldots) \geqslant \min\{\nu_p(a), \nu_p(b), \nu_p(c), \ldots\}$.

Posługując się twierdzeniem o jednoznaczności rozkładu na czynniki pierwsze, można wykazać, że dla liczb całkowitych dodatnich $a, b, c, \ldots$:

(4) $a = b$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p zachodzi równość $\nu_p(a) = \nu_p(b)$;
(5) $a \mid b$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p zachodzi nierówność $\nu_p(a) \leqslant \nu_p(b)$;
(6) $\nu_p\big(\mathtt{NWD}(a,b,c,\ldots)\big) = \min\{\nu_p(a), \nu_p(b), \nu_p(c), \ldots\}$;
(7) $\nu_p\big(\mathtt{NWW}[a,b,c,\ldots]\big) = \max\{\nu_p(a), \nu_p(b), \nu_p(c), \ldots\}$;
(8) liczba a jest k-tą potęgą liczby naturalnej wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p zachodzi podzielność $k \mid \nu_p(a)$.

Dowód pozostawiamy Czytelnikowi.

Zadania

1. Udowodnić następujące równości dla liczb całkowitych dodatnich a, b i c:
   (a) $\frac{\mathtt{NWW}[a,b,c]\mathtt{NWD}(a,b)\mathtt{NWD}(b,c)\mathtt{NWD}(c,a)}{\mathtt{NWD}(a,b,c)} = abc$,
   (b) $\frac{\mathtt{NWW}[a,b]\mathtt{NWW}[b,c]\mathtt{NWW}[c,a]}{\mathtt{NWW}[a,b,c]^2} = \frac{\mathtt{NWD}(a,b)\mathtt{NWD}(b,c)\mathtt{NWD}(c,a)}{\mathtt{NWD}(a,b,c)^2}$.
2. Korzystając z *postulatu Bertranda* (dla każdego rzeczywistego $x \geqslant 1$ w przedziale $[x, 2x]$ znajduje się co najmniej jedna liczba pierwsza), udowodnić, że dla naturalnych $n > 1$:
   (a) liczba $n!$ nie jest potęgą liczby naturalnej o wykładniku naturalnym i większym niż 1,
   (b) liczba $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ nie jest naturalna.
3. Liczby $a, b \neq 0$ oraz $\frac{b^2}{a} + \frac{a^2}{b}$ są całkowite. Wykazać, że liczby $\frac{b^2}{a}$ i $\frac{a^2}{b}$ też są całkowite.
4. Liczby $a, b, c \neq 0$ oraz $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ są całkowite. Dowieść, że abc jest sześcianem liczby całkowitej.
5. Liczby całkowite $a, b > 0$ spełniają podzielność $ab \mid a^2 + b^2 + a$. Wykazać, że a jest kwadratem liczby naturalnej.
6. Liczby naturalne a i b są dzielnikami n. Wykazać, że jeśli liczba $\frac{n}{a} + \frac{n}{b}$ jest podzielna przez a i b, to liczba n jest podzielna przez liczbę $\frac{\mathtt{NWW}(a,b)^2}{\mathtt{NWD}(a,b)}$.

Wskazówki do zadań

Uwaga. O ile nie napisano inaczej, we wszystkich wskazówkach p jest pewną liczbą pierwszą oraz

$\alpha = \nu_p(a)$, $\beta = \nu_p(b)$, $\gamma = \nu_p(c)$.

1. Można bez straty ogólności przyjąć, że $\alpha \leqslant \beta \leqslant \gamma$, i skorzystać z własności (1), (6) i (7), a na koniec (4).
2. Weźmy liczbę pierwszą p, spełniającą nierówność $\frac{1}{2}n \leqslant p \leqslant n$.
   (a) $\nu_p(n!) = 1$,
   (b) zapisać tę sumę w postaci $a/n!$ i stosując własność (2′), wykazać, że $\alpha = 0$.
3. Zachodzi podzielność $ab \mid a^3 + b^3$, z której wnioskujemy, że $\alpha + \beta \leqslant \nu_p(a^3 + b^3)$. Rozważając osobno przypadki $\alpha = \beta$ i $\alpha \neq \beta$, korzystając z własności (2) i (3), wykazać nierówności $\alpha \leqslant 2\beta$ i $\beta \leqslant 2\alpha$. Dowód kończy zastosowanie (5).
4. Zachodzi podzielność $abc \mid a^2c + b^2a + c^2b$, którą należy przeliczyć na nierówności z udziałem α, β i γ. Rozważyć dwa przypadki: liczby $2\alpha + \gamma$, $2\beta + \alpha$, $2\gamma + \beta$ są różne, lub pewne dwie z nich są równe. Pierwszy przypadek w połączeniu z własnościami (2′) i (5) prowadzi do sprzeczności, drugi do równości $\alpha + \beta = 2\gamma$ lub analogicznej – wówczas $3 \mid \nu_p(abc)$.
5. Wystarczy rozważyć tylko te liczby pierwsze p, które dzielą a – zakładamy więc, że $\alpha > 0$. Zachodzi nierówność $\alpha + \beta \leqslant \nu_p(a^2 + b^2 + a)$. Zauważyć, że każda z nierówności: $\alpha < 2\beta$ i $\alpha > 2\beta$ prowadzi do sprzeczności, posługując się własnościami (2′) i (5).
6. Bez straty ogólności niech $\alpha \leqslant \beta$. Trzeba wykazać, że $\nu_p(n) \geqslant 2\beta - \alpha$. Jeśli $\alpha = \beta$, to wynika to z podzielności $b \mid n$. W przeciwnym razie wystarczy zastosować własności (5) i (2) dla podzielności $b \mid \frac{n}{a} + \frac{n}{b}$.