



Wykładniki p -adyczne

Bartłomiej BZDEGA

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 $\nu_p(a+b) \geq \nu_p(a)$.

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, \dots :

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

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

- (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 $\nu_p(a) \leq \nu_p(b)$;
- (6) $\nu_p(\text{NWD}(a, b, c, \dots)) = \min\{\nu_p(a), \nu_p(b), \nu_p(c), \dots\}$;
- (7) $\nu_p(\text{NWW}[a, b, c, \dots]) = \max\{\nu_p(a), \nu_p(b), \nu_p(c), \dots\}$;
- (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) $\frac{\text{NWW}[a, b, c] \text{NWD}(a, b) \text{NWD}(b, c) \text{NWD}(c, a)}{\text{NWD}(a, b, c)} = abc$,
 - (b) $\frac{\text{NWW}[a, b] \text{NWW}[b, c] \text{NWW}[c, a]}{\text{NWW}[a, b, c]^2} = \frac{\text{NWD}(a, b) \text{NWD}(b, c) \text{NWD}(c, a)}{\text{NWD}(a, b, c)^2}$.
2. Korzystając z *postulatu Bertranda* (dla każdego rzeczywistego $x \geq 1$ 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 $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ 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 $\frac{\text{NWW}(a, b)^2}{\text{NWD}(a, b)}$.

Wskazówki do zadań
 Uwaga. O ile nie napisano inaczej, we wszystkich wskazówkach p jest pewną liczbą pierwszą oraz
 1. Można bez straty ogólności przyjąć, że $a \leq b \leq c$, i skorzystać z własności (1), (6) i (7), a na koniec (4).
 2. Weźmy liczbę pierwszą p , spełniającą nierówność $\frac{1}{2}n \leq p \leq n$.
 (a) $a = 1$,
 (b) zapisać tę sumę w postaci a/n i stosując własność (2'), wykazać, że $a = 0$.
 3. Zachodzi podzielność $ab \mid a^3 + b^3$, z której wnioskujemy, że $a + b \mid a^2 + b^2 + a^2 + b^2$. Rozważając osobno przypadki $a = b$ i $a \neq b$, korzystając z własności (2) i (3), wykazać nierówność $a \leq 2b$ i $b \leq 2a$. Dowód kończy zastosowanie (5).
 4. Zachodzi podzielność $abc \mid a^2c + b^2a + a^2b$, która należy przeliczyć na nierówność z udziałem a, b i c . Rozważyć dwa przypadki: liczby pewne dwie z nich są równe. Pierwszy przypadek w połączeniu z własnościami (2'), (5) i (6) prowadzi do sprzeczności, drugi do równości $a + b = 2c$ lub analogicznej.
 5. Wystarczy rozważyć tylko te liczby pierwsze p , które dzielą $a - b$. Zakładamy więc, że $a < b$.
 6. $\nu_p(\text{NWD}(a, b, c, \dots)) = \min\{\nu_p(a), \nu_p(b), \nu_p(c), \dots\}$;
 7. $\nu_p(\text{NWW}[a, b, c, \dots]) = \max\{\nu_p(a), \nu_p(b), \nu_p(c), \dots\}$;
 8. $a \mid b$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p zachodzi nierówność $\nu_p(a) \leq \nu_p(b)$;
 9. $a = b$ wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p zachodzi równość $\nu_p(a) = \nu_p(b)$;
 10. Bez straty ogólności niech $a \leq b$.
 11. Trzeba wykazać, że $\nu_p(n) \geq 2\nu_p(a) - \alpha$. Jeśli $\alpha = \beta$, to wynika to z podzielności $b \mid n$.
 12. W przeciwnym razie wystarczy zastosować własności (5) i (2) dla $\frac{b}{a}$ i $\frac{a}{b}$.