Lemat o zwiększaniu wykładnika p-adycznego

Bartłomiej BZDĘGA

W poprzednim kąciku omówiłem wykładnik p-adyczny $\nu_p(n)$ i jego podstawowe własności – zachęcam Czytelnika, aby się z nimi zapoznał przed przystąpieniem do lektury.

Weźmy dwie liczby całkowite a i b. Niech $p > 2$ będzie liczbą pierwszą oraz $p \nmid a, b$, ale $p \mid a - b$. Możemy wówczas zapisać $a = b + kp$ dla pewnego całkowitego k. Zachodzi równość

$$a^p - b^p = (b+kp)^p - b^p = \binom{p}{1} b^{p-1}kp + \binom{p}{2} b^{p-2}k^2p^2 + \ldots + \binom{p}{p} k^p p^p.$$

Zauważmy, że $\nu_p\left(\binom{p}{1}b^{p-1}kp\right) = \nu_p(kp) + 1 = \nu_p(a-b) + 1$, natomiast pozostałe składniki ostatniej sumy mają większe wykładniki p-adyczne. Na mocy własności $(2')$ z poprzedniego kącika wynika z tego, że $\nu_p(a^p - b^p) = \nu_p(a-b) + 1$.

Niech teraz $p = 2$. Interesują nas liczby nieparzyste a i b. Zachodzi równość $\nu_2(a^2+b^2) = \nu_2(a-b) + \nu_2(a+b)$, ale równość $\nu_2(a+b) = 1$ ma miejsce tylko wtedy, gdy $4 \mid a - b$.

Trzymając się wciąż powyższych założeń, wybierzmy liczbę naturalną m, która nie jest podzielna przez p. Wtedy

$$\frac{a^m - b^m}{a-b} = a^{m-1} + a^{m-2}b + \ldots + ab^{m-2} + b^{m-1} \equiv ma^{m-1} \not\equiv 0 \pmod{p},$$

więc w tym przypadku $\nu_p(a^m - b^m) = \nu_p(a-b)$.

Stosując indukcję oraz powyższe rozważania, wykazujemy tytułowy lemat.

Lemat o zwiększaniu wykładnika p-adycznego (wersja z odejmowaniem). Niech a i b będą całkowite, n – naturalne, $p > 2$ – pierwsze. Wówczas:

(1) jeśli $p \nmid a, b$ oraz $p \mid a - b$, to $\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n)$;
(2) dla nieparzystych a i b:
  (a) jeśli $4 \mid a - b$, to $\nu_2(a^n - b^n) = \nu_2(a-b) + \nu_2(n)$;
  (b) $\nu_2(a^n - b^n) = \nu_2(a-b)$ dla n nieparzystych;
  (c) $\nu_2(a^n - b^n) = \nu_2(a^2 - b^2) + \nu_2(n) - 1$ dla n parzystych.

Dla nieparzystego n zachodzi równość $a^n - b^n = a^n + (-b)^n$. Pisząc $-b$ zamiast b, otrzymamy analogiczny lemat dla dodawania.

Lemat o zwiększaniu wykładnika p-adycznego (wersja z dodawaniem). Niech a i b będą całkowite, n – naturalne nieparzyste, p – pierwsze. Jeśli $p \nmid a, b$ oraz $p \mid a + b$, to $\nu_p(a^n + b^n) = \nu_p(a+b) + \nu_p(n)$.

W zadaniach dość powszechne jest stosowanie nierówności $\nu_p(n) \leqslant \log_p n$, która być może jest oczywista, ale warto tu o niej wspomnieć.

Zadania

1. W zależności od n wyznaczyć $\nu_3\Big(\underbrace{111\ldots1}_{n}\Big)$ i $\nu_{11}\Big(\underbrace{111\ldots1}_{n}\Big)$.
2. Wyznaczyć wszystkie liczby naturalne n, dla których zachodzi podzielność:
   (a) $2^n \mid 3^n - 1$, (b) $5^n \mid 3^n + 7^n$.
3. Wyznaczyć wszystkie liczby pierwsze p, dla których $3^p + 4^p$ jest potęgą liczby naturalnej o wykładniku naturalnym większym niż 1.
4. Wyjaśnić, dlaczego nie istnieje lemat o zwiększaniu wykładnika p-adycznego w wersji z dodawaniem dla n parzystych.
5. Udowodnić, że dla naturalnych $n > 2$ liczba $n^{n-1} - 1$ jest podzielna przez kwadrat pewnej liczby pierwszej.
6. Liczby całkowite dodatnie a i b są różnej parzystości. Wykazać, że liczba $a^{a+b} + b^{a+b}$ jest podzielna przez kwadrat pewnej liczby pierwszej.
7. Niech a i b będą różnymi liczbami całkowitymi oraz niech $k > 1$ będzie liczbą naturalną. Wykazać, że liczba $\left(a + \frac{1}{k}\right)^n - \left(b + \frac{1}{k}\right)^n$ jest całkowita tylko dla skończenie wielu naturalnych n.
8. Ustalmy nieparzyste $a > 0$. Dla każdego naturalnego n liczba $\frac{a^n+1}{2}$ jest sześcianem liczby naturalnej. Wykazać, że $a = 1$.
9. Liczby a i b są całkowite i względnie pierwsze, a liczby $m, n \geqslant 1$ są naturalne. Dowieść, że
$$\mathtt{NWD}\big(a^n - b^n,\ a^m - b^m\big) = a^{\mathtt{NWD}(n,m)} - b^{\mathtt{NWD}(n,m)},$$
bez korzystania z algorytmu Euklidesa.

Wskazówki do zadań

1. Dzielić odpowiednim cechom podzielności dla $p = 3$ wystarczy rozważyć n podzielne przez 3, a dla $p = 11$ – rozważyć n parzyste. Dla $n = 3$ skorzystać z równości $111\ldots1 = (10^n - 1^n)/9$, a dla $p = 11$ i $n = 2m$ z równości $111\ldots1 = (100^m - 1^m)/9$.
2. (a) Dla takich n zachodzi nierówność $v_2(3^n - 1) \geqslant n$. Wartość $v_2(3^n - 1)$ można wyznaczyć dokładnie, w zależności od parzystości n. Skorzystać z nierówności $v_2(n) \leqslant \log_2 n$, aby wykazać, że $n \leqslant 4$.
   (b) Dla n parzystych $3^n + 7^n \equiv \pm 2 \pmod 5$. Dla n nieparzystych skorzystać z lematu w wersji z dodawaniem i postępować podobnie jak w podpunkcie (a).
3. Jeśli $p \neq 2, 7$, to $\nu_7(3^p + 4^p) = 1$.
4. Niech $p \mid a + b$ i $p \nmid a, b$. W przypadku $p = 2$ mamy $\nu_2(a^2 + b^2) = 1$, natomiast dla $p > 2$ mamy $\nu_p(a^2 + b^2) = 0$.
5. Można wziąć dowolny dzielnik pierwszy liczby $n - 1$ i stwierdzić, że $\nu_p(n^{n-1} - 1^{n-1}) > 1$.
6. Jeśli a i b mają wspólny dzielnik pierwszy p, to $p^2 \mid a^{a+b} + b^{a+b}$. W przeciwnym razie istnieje liczba pierwsza p spełniająca warunki $p \mid a + b$ i $p \nmid a, b$. Wystarczy skorzystać z lematu w wersji z dodawaniem, rozumując podobnie jak w poprzednim zadaniu.
7. Niech p będzie dowolnym dzielnikiem pierwszym liczby k. Jeśli liczba z zadania jest całkowita, to $p^n \mid (ak+1)^n - (bk+1)^n$ i można skorzystać z lematu, bo $p \mid (ak+1) - (bk+1)$ oraz $p \nmid ak+1, bk+1$.
8. Uzasadnić, że dla $a > 1$ liczba $a^2 + 1$ ma dzielnik pierwszy $p > 2$ i dla odpowiednio dobranego nieparzystego m liczba $\nu_p\left(\frac{a^{2m}-1}{2}\right)$ nie dzieli się przez 3.
9. Niech $d = \mathtt{NWD}(m, n)$. Stosując własności kongruencji, uzasadnić, że zbiór tych całkowitych $k > 0$, dla których $p \mid a^k - b^k$, jest postaci $\{r, 2r, 3r, \ldots\}$. Stąd jeśli $p \mid a^n - b^n$ i $p \mid a^m - b^m$, to $p \mid a^d - b^d$. Liczby n/d i m/d są względnie pierwsze, więc nie mogą obie dzielić się przez p. Wywnioskować z tego, że $\nu_p(a^d - b^d) = \nu_p(a^n - b^n)$ lub $\nu_p(a^d - b^d) = \nu_p(a^m - b^m)$. Wykorzystać własność (6) z poprzedniego kącika.