Praca zbiorowa.
Redakcja: Jacek Dymel

1 Lifting The Exponent Lemma

Jan Kociniak

1.1 Teoria

Lifting The Exponent Lemma jest zbiorczą nazwą dla grupy twierdzeń pozwalających wyznaczyć potęgę, w jakiej liczba pierwsza p dzieli liczbę $x^n \pm y^n$ ($x, y \in \mathbb{Z}$, $n \in \mathbb{Z}_+$), w zależności od potęgi w jakiej p dzieli $x \pm y$ oraz n.

Definicja *Definiujemy $v_p(x)$ jako największą potęgę, w jakiej liczba pierwsza p dzieli liczbę całkowitą x, tj. $v_p(x) = \alpha \Leftrightarrow p^\alpha \mid x \wedge p^{\alpha+1} \nmid x$. Piszemy także $p^\alpha \mid\mid x$ wtedy i tylko wtedy gdy $v_p(x) = \alpha$. Kładziemy $v_p(0) = +\infty$. Liczbę $v_p(x)$ nazywamy wykładnikiem p-adycznym liczby x.*

Twierdzenie 1.1

- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

Definicja *Definiujemy rozszerzenie funkcji $v_p(x)$ określonej na zbiorze liczb całkowitych do funkcji $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$ poprzez następujące równości:*

$$v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y) \quad i \quad v_p(0) = +\infty.$$

*Równość i nierówność przedstawione w **Twierdzeniu 1.1** pozostają zachowane.*

1.1.1 Lifting The Exponent Lemma

Niech $x, y \in \mathbb{Z}$, $p, n \in \mathbb{Z}_+$ oraz p będzie liczbą pierwszą taką, że $p \mid x \pm y$, ale $p \nmid x$ ani $p \nmid y$. Wtedy zachodzi:

1. $v_p(x^n - y^n) = v_p(x - y)$ dla $\mathrm{NWD}(p, n) = 1$,
2. $v_p(x^n + y^n) = v_p(x + y)$ dla $2 \nmid n$, $\mathrm{NWD}(p, n) = 1$,
3. Kiedy $p \neq 2$:
   - $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$,
   - $v_p(x^n + y^n) = v_p(x + y) + v_p(n)$ dla $2 \nmid n$,
4. Kiedy $p = 2$:
   - $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$ dla $4 \mid x - y$,
   - $v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1$ dla $2 \mid x - y$, $2 \mid n$,
   - $v_2(x^n + y^n) = v_2(x + y) + v_2(n)$ dla $2 \nmid n$.

1.2 Zadania

Zadanie 1.1 Znaleźć sumę wszystkich dzielników d liczby $N = 19^{88} - 1$, które są postaci $d = 2^a 3^b$, gdzie $a, b \in \mathbb{Z}_+$.

Zadanie 1.2 Znaleźć wszystkie rozwiązania równania $x^{2009} + y^{2009} = 7^z$ w liczbach całkowitych dodatnich.

Zadanie 1.3 Niech a, n będą liczbami całkowitymi dodatnimi a p liczbą pierwszą taką, że

$$a^p \equiv 1 \pmod{p^n}.$$

Udowodnić, że

$$a \equiv 1 \pmod{p^{n-1}}.$$

Źródło: UNESCO Competition 1996

Zadanie 1.4 Niech x, y, p, k, n będą liczbami całkowitymi dodatnimi takimi, że n jest nieparzyste oraz p jest nieparzystą liczbą pierwszą. Udowodnić, że jeśli $x^n + y^n = p^k$, to n jest potęgą p.

Źródło: Rosja 1996

Zadanie 1.5 Wyznaczyć wszystkie liczby pierwsze p i liczby całkowite dodatnie x, y, dla których $p^x - y^3 = 1$.

Źródło: XXXVIII OM - II - Zadanie 5

Zadanie 1.6 Niech $k > 1$ będzie liczbą całkowitą. Pokazać, że istnieje nieskończenie wiele dodatnich liczb całkowitych n takich, że

$$n | 1^n + 2^n + 3^n + \cdots + k^n.$$

Zadanie 1.7 Niech q będzie liczbą parzystą dodatnią. Dowieść, że dla każdej liczby całkowitej dodatniej n liczba

$$q^{(q+1)^n} + 1$$

dzieli się przez $(q+1)^{n+1}$ ale nie dzieli się przez $(q+1)^{n+2}$.

Źródło: XXXIII OM - II - Zadanie 5

Zadanie 1.8 Znaleźć największe $k \in \mathbb{Z}_+$ takie, że 1991^k dzieli liczbę

$$1990^{1991^{1992}} + 1992^{1991^{1990}}$$

.

Źródło: IMO Shortlist 1991

Zadanie 1.9 Wyznaczyć wszystkie liczby całkowite dodatnie n, dla których

$$n^n + 1 \quad \text{oraz} \quad (2n)^{2n} + 1$$

są liczbami pierwszymi.

Źródło: LVI OM - II - Zadanie 1

Zadanie 1.10 Niech $a, n \geq 2$ będą liczbami całkowitymi, które spełniają następujący warunek: istnieje taka liczba całkowita $k \geq 2$, że n dzieli $(a-1)^k$. Udowodnić, że n dzieli $a^{n-1} + a^{n-2} + \cdots + a + 1$.

Źródło: Rumunia TST 2009

Zadanie 1.11 Niech $a > b > 1$ będą liczbami całkowitymi, gdzie b jest nieparzysta. Niech n będzie liczbą całkowitą dodatnią. Udowodnić, że jeśli $b^n \mid a^n - 1$, to $a^b > \frac{3^n}{n}$.

Źródło: Chiny TST 2009

1.3 Rozwiązania

1.1 Zauważmy, że $3 \mid 19 - 1$ oraz $4 \mid 19^2 - 1$. Wtedy z lematu LTE:

$$v_3(19^{88} - 1) = v_3(19 - 1) + v_3(88) = v_3(18) + 0 = 2,$$

$$v_2(19^{88} - 1) = v_2((19^2)^{44} - 1) = v_2(19^2 - 1) + v_2(44) = 3 + 2 = 5.$$

Stąd szukana suma dzielników wynosi:

$$\sum_{\substack{1 \leq a \leq 5 \\ 1 \leq b \leq 2}} 2^a 3^b = (2 + 2^2 + 2^3 + 2^4 + 2^5)(3 + 3^2) = 2\frac{2^5 - 1}{2 - 1} \cdot 12 = 24 \cdot 31 = 744.$$

1.2 Załóżmy najpierw, że $v_7(x) \neq v_7(y)$. Bez straty ogólności możemy przyjąć, że $v_7(x) < v_7(y)$. Wtedy

$$k = v_7(7^k) = v_7(x^{2009} + y^{2009}) = \min\{v_7(x^{2009}), v_7(y^{2009})\} = v_7(x^{2009}).$$

Zatem możemy podzielić obie strony równania przez 7^k, co daje $1 = \frac{x^{2009}+y^{2009}}{7^k} \geq 1 + 7$, gdzie nierówność zachodzi, bo $v_7(x^{2009}) = k$ oraz $v_7(y^{2009}) > v_7(x^{2009}) = k$. Jest to oczywista sprzeczność, która dowodzi, że $v_7(x) = v_7(y)$. Oznaczmy teraz $x = 7^n a$ i $y = 7^n b$ $(a, b \in \mathbb{Z}_+, p \nmid a, p \nmid b)$. Wtedy $x^{2009} + y^{2009} = 7^k \Leftrightarrow a^{2009} + b^{2009} = 7^m$, gdzie $m = k - 2009n$. Oczywiście $2 \nmid 2009 \implies a + b \mid a^{2009} + b^{2009} \implies 7 \mid a + b$. Z lematu LTE

$$v_7(a^{2009} + b^{2009}) = v_7(a + b) + v_7(2009) = v_7(a + b) + 2$$

co implikuje $a^{2009} + b^{2009} = 7^2(a + b)k$. Ale lewa strona tej równości jest też potęgą siódemki, skąd $k = 1$. Zatem $a^{2009} + b^{2009} = 49(a + b)$, a to równanie nie ma rozwiązań w liczbach całkowitych dodatnich (lewa strona rośnie o wiele szybciej niż prawa).

1.3 Przypadek $a = 1$ jest trywialny. Zauważmy, że dla $a > 1$ zachodzi $\mathrm{NWD}(a, p) = 1$, bo $p^n \mid a^p - 1 \implies p \mid a^p - 1$, co w przypadku $p \mid a$ jest oczywistą sprzecznością. Korzystając z małego twierdzenia Fermat'a otrzymujemy $a^p \equiv a \pmod{p}$. Z lematu LTE wynika, że $v_p(a^p-1) = v_p(a-1)+v_p(p) = v_p(a-1)+1$, ale $p^n \mid a^p - 1 \Leftrightarrow v_p(a^p - 1) \geq n$, skąd $v_p(a - 1) = v_p(a^p - 1) - 1 \geq n - 1 \Leftrightarrow p^{n-1} \mid a - 1$, co należało dowieść.

1.4 Analogicznie jak w zadaniu 1.2 dowodzimy, że $v_p(x) = v_p(y)$. Podstawiając $x = ap^\alpha, y = bp^\alpha$, gdzie $a, b \in \mathbb{Z}_+, p \nmid a, p \nmid b, \alpha \in \mathbb{Z}_{\geq 0}$, otrzymujemy $x^n + y^n = p^k \Leftrightarrow a^n + b^n = p^m$, gdzie $m = k - n\alpha$. Z lematu LTE (możemy skorzystać, bo $2 \nmid n$ oraz $p \mid a + b$ analogicznie jak w zadaniu 1.2) wynika, że $m = v_p(a^n + b^n) = v_p(a + b) + v_p(n)$. Oznaczmy $m_1 = m - v_p(a + b)$, wtedy $v_p(n) = m_1$. Niech $n = p^{m_1} z$. Zachodzi wtedy

$$p^{m_1} = \frac{a^n + b^n}{a + b} = \frac{a^{p^{m_1} z} + b^{p^{m_1} z}}{a + b} \geq \frac{a^{p^{m_1}} + b^{p^{m_1}}}{a + b} \geq p^{m_1},$$

gdzie ostatnia nierówność zachodzi, bo z lematu LTE $v_p\left(\frac{a^{p^{m_1}}+b^{p^{m_1}}}{a+b}\right) = v_p(a^{p^{m_1}} + b^{p^{m_1}}) - v_p(a + b) = v_p(p^{m_1}) = m_1$. Wynika stąd, że we wszystkich miejscach tej nierówności muszą zachodzić równości, co implikuje $z = 1$, czyli $n = p^{m_1}$, co należało dowieść.

1.5 Na początku rozpatrujemy możliwość $p = 2$:

$$2^x - y^3 = 1 \Leftrightarrow 2^x = y^3 + 1 = (y+1)(y^2 - y + 1) = (y+1)(y(y-1)+1).$$

Zauważmy, że y i $y-1$ to dwie kolejne liczby całkowite, więc jedna z nich jest parzysta, zatem liczba $y(y-1)+1$ jest nieparzysta. Gdyby $y(y-1)+1 > 1$, to 2^x miałoby nieparzysty dzielnik większy od 1, co jest oczywistą sprzecznością. Zatem $y(y-1)+1 = 1 \Leftrightarrow y = 1$, co prowadzi do trójki $(p, x, y) = (2, 1, 1)$ spełniającej warunki zadania. Załóżmy teraz, że $p \neq 2$ oraz $y \neq 1$. Korzystając z tezy zadania 1.4 otrzymujemy, że jeśli $p^x = y^3 + 1$, to 3 jest potęgą p, zatem $p = 3$. Z rozkładu $3^x = y^3 + 1 = (y+1)(y^2 - y + 1)$ wynika, że $y + 1 = 1$ albo $y + 1 = 3^{x_1}$, gdzie $1 \leq x_1 \leq x$. $y + 1 = 1$ implikuje $y = 0$ co stoi w sprzeczności z $y \in \mathbb{Z}_+$. Zatem $y + 1 = 3^{x_1}$. Z lematu LTE otrzymujemy

$$v_3(y^3 + 1) = v_3(y + 1) + v_3(3) = v_3(y + 1) + 1$$

co wobec rozkładu $y^3 + 1 = (y + 1)(y^2 - y + 1)$ implikuje $y^2 - y + 1 = 3 \Leftrightarrow (y - 2)(y + 1) = 0$, skąd otrzymujemy $y = 2$ oraz dalej $x = 2$. Zatem drugim rozwiązaniem jest trójka $(p, x, y) = (3, 2, 2)$.

1.6 Jeśli $1+k$ nie jest potęgą 2, bierzemy nieparzystą liczbę pierwszą $p \mid 1+k$ oraz $n = p^m$. Wtedy z lematu LTE dla każdego j niepodzielnego przez p mamy $v_p(j^n + (k + 1 - j)^n) = v_p(k + 1) + v_p(n) \geq m + 1$. Oprócz tego jeśli $p \mid j$ (i co za tym idzie $p \mid k + 1 - j$), to $n \mid p^m \mid p^n \mid j^n$ więc suma dana w zadaniu jest podzielna przez $p^m = n$. Jeśli $1 + k$ jest potęgą 2, bierzemy nieparzysty dzielnik pierwszy p liczby k oraz powtarzamy poprzednie rozumowanie dla $k - 1$ zamiast k.

1.7 Niech p będzie liczbą pierwszą dzielącą $q+1$. Z parzystości q wynika, że $p \neq 2$ oraz $2 \nmid (q + 1)^n$. Stosując lemat LTE otrzymujemy $v_p(q^{(q+1)^n} + 1) = v_p(q + 1) + v_p((q + 1)^n)) = v_p(q + 1) + n \cdot v_p(q + 1) = (n + 1)v_p(q + 1)$, co kończy dowód.

1.8 Przekształćmy daną liczbę do postaci sumy dwóch potęg o równych wykładnikach:

$$1990^{1991^{1992}} + 1992^{1991^{1990}} = 1990^{1991^{1990} \cdot 1991^2} + 1992^{1991^{1990}} =$$

$$= (1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}.$$

Zbadajmy teraz, z jakim wykładnikiem do liczby $1990^{1991^2} + 1992$ wchodzi 1991:

$$1990^{1991^2} + 1992 = (1991 - 1)^{1991^2} + 1991 + 1 =$$

$$= \sum_{i=0}^{1991^2} \binom{1991}{i} 1991^i (-1)^{1991^2 - i} + 1991 + 1 =$$

$$= \sum_{i=1}^{1991^2} \binom{1991}{i} 1991^i (-1)^{1991^2-i} - 1 + 1991 + 1 =$$

$$= \sum_{i=1}^{1991^2} \binom{1991}{i} 1991^i (-1)^{1991^2-i} + 1991 = 1991(1991l + 1)$$

gdzie l jest pewną liczbą całkowitą. W połączeniu z tym, że $1991 = 11 \cdot 181$, gdzie 11 i 181 to liczby pierwsze otrzymujemy, że $v_{11}\left(1990^{1991^2} + 1992\right) = v_{181}\left(1990^{1991^2} + 1992\right) = 1$. Korzystając teraz z lematu LTE dostajemy:

$$v_{11}\left((1990^{1991^2})^{1991^{1990}} + 1992^{1991^{1990}}\right) =$$

$$= v_{11}\left(1990^{1991^2} + 1992\right) + v_{11}\left(1991^{1990}\right) = 1 + 1990 = 1991.$$

Analogicznie pokazujemy, że 181 też wchodzi w rozkład tej liczby z potęgą 1991. Zatem szukane k to 1991.

1.9 Niech $n = 2^\alpha \cdot n_1$, gdzie $\alpha, n_1 \in \mathbb{Z}_{\geq 0}$ oraz $2 \nmid n_1$. Załóżmy, że $n_1 > 1$. Jeśli $\alpha \geq 1$, to liczba $(2^\alpha n_1)^{2^\alpha} + 1$ jest nieparzysta i większa od 1, więc posiada nieparzysty dzielnik pierwszy p. Oczywiście $p \nmid n_1$. Z lematu LTE $v_p(((2^\alpha n_1)^{2^\alpha})^{n_1} + 1) = v_p((2^\alpha n_1)^{2^\alpha} + 1) + v_p(n_1) = v_p((2^\alpha n_1)^{2^\alpha} + 1)$. Z założeń zadania liczba $((2^\alpha n_1)^{2^\alpha})^{n_1} + 1$ jest pierwsza, zatem $((2^\alpha n_1)^{2^\alpha})^{n_1} + 1 = p$. Ale $p \mid (2^\alpha n_1)^{2^\alpha} + 1$, skąd $((2^\alpha n_1)^{2^\alpha})^{n_1} + 1 \leq (2^\alpha n_1)^{2^\alpha} + 1$ co jest sprzecznością przy $n_1 > 1$. Jeśli $\alpha = 0$, to przeprowadzamy analogiczne rozumowanie dla liczby $(2n)^{2n} + 1$. Zatem $n_1 = 1$ skąd $n = 2^\alpha$. Dla $\alpha = 0$ zachodzi $n^n + 1 = 2$ oraz $(2n)^{2n} + 1 = 5$, więc teza zadania jest spełniona. Zauważmy, że dla $\alpha \geq 2$ co najmniej jedna z liczb $k \cdot 2^\alpha$, $(\alpha + 1) \cdot 2^{\alpha+1}$ ma nieparzysty dzielnik większy od 1, wówczas stosując rozumowanie analogiczne do poprzedniego dostajemy $\alpha = 1$. Stąd $n = 2$ oraz po sprawdzeniu ta liczba w istocie spełnia warunki zadania.

1.10 Zauważmy, że $a^{n-1} + a^{n-2} + \cdots + a + 1 = \frac{a^n - 1}{a - 1}$. Z warunku zadania wnioskujemy, że zbiór dzielników pierwszych liczby n jest podzbiorem dzielników pierwszych liczby $a - 1$. Weźmy dowolny dzielnik pierwszy p ze zbioru dzielników pierwszych liczby n. Wtedy z lematu LTE

$$v_p\left(\frac{a^n - 1}{a - 1}\right) = v_p(a^n - 1) - v_p(a - 1) = v_p(a - 1) + v_p(n) - v_p(a - 1) = v_p(n)$$

co implikuje, że $n \mid a^{n-1} + a^{n-2} + \cdots + a + 1$.

1.11 Wystarczy udowodnić dla $b = p$, gdzie p jest liczbą pierwszą, ponieważ dla $p \mid b$ zachodzi $a^b \geq a^p$. Niech $d = \mathrm{ord}_p(a)$. Wtedy $n = dk$ dla pewnego $k \in \mathbb{Z}_+$. Z lematu LTE

$$n \leq v_p(a^n - 1) = v_p((a^d)^k - 1) = v_p(a^d - 1) + v_p(k) =$$

$$= v_p(a^d - 1) + v_p\left(\frac{n}{d}\right) \leq v_p(a^d - 1) + v_p(n) = v_p((a^d - 1)n)$$

co implikuje $p^n \leq (a^d - 1)n \Leftrightarrow a^d - 1 \geq \frac{p^n}{n} \geq \frac{3^n}{n}$. Jednakże $d \leq p - 1$, skąd $a^p > a^d - 1 \geq \frac{3^n}{n}$, co należało udowodnić.