Lifting The Exponent lemma

Anh Dung „Tonda“ Le

Abstrakt. Příspěvek se zabývá použitím „Lifting The Exponent lemmatu“ (dále jen LTE) při řešení exponenciálních Diofantických rovnic z olympiádní matematiky. Obsahuje také příklady k procvičování.

LTE je sice jednoduchý, ale mocný nástroj, který nám za určitých podmínek umožňuje najít největší mocninu prvočísla, která dělí součet nebo rozdíl dvou mocnin se stejným exponentem. Ve většině případů nám LTE ušetří hodně práce a času. Díky tomuto lemmatu můžeme odkrývat spoustu zajímavých, překvapujících a záhadných aspektů olympiádní teorie čísel.

Úmluva. Všechny proměnné v dalším textu jsou z oboru celých čísel, nebude-li řečeno jinak.

Tvrzení. (Zásadní!) *Pro dělitelnost zavádíme symbol $a \mid b$, který čteme „a dělí b“. Platí pro něj následující tvrzení.*

(i) *Pokud je p prvočíslo, pak platí implikace $p \mid ab \Rightarrow p \mid a \vee p \mid b$.*
(ii) *Pokud $d \mid a, d \mid b$, pak $d \mid ka + lb$.*
(iii) *Pokud $a \mid b$, pak $|a| \leq |b|$ (často dokonce $2|a| \leq |b|$ atd.).*

Tvrzení. *Nechť a, b jsou celá čísla. Jejich největší společný dělitel d značíme (a, b) a platí, že d je nejmenší nezáporné číslo, které lze zapsat ve tvaru $ka + lb$, kde k a l jsou celá čísla. Též platí $(a - b, b) = (a, b)$, díky čemuž lze (a, b) snadno vypočítat (tento postup se nazývá Euklidův algoritmus).*

Definice. Skutečnost, že $p \mid a - b$ budeme značit $a \equiv b \pmod{p}$ a říkat a je *kongruentní* s b modulo p.

Definice. Nejmenší společný násobek přirozených čísel a, b budeme značit $[a, b]$.

Definice. Čísla a, b nazveme *nesoudělná*, pokud $(a, b) = 1$.

Definice. Buď n přirozené číslo. Pak je pro každé prvočíslo p jednoznačně určený exponent v prvočíselném rozkladu čísla n. Tento exponent budeme označovat $v_p(n)$ a říkat mu *p-valuace* čísla n. Pokud $(p, n) = 1$, je $v_p(n) = 0$, a pokud $n = 0$, je $v_p(n) = \infty$.

Tvrzení. *Pro libovolná přirozená čísla a, b platí*

(i) $v_p(ab) = v_p(a) + v_p(b)$
(ii) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$
(iii) *Pokud* $v_p(a) \neq v_p(b)$, *pak dokonce* $v_p(a+b) = \min\{v_p(a), v_p(b)\}$.
(iv) $v_p((a,b)) = \min\{v_p(a), v_p(b)\}$
(v) $v_p([a,b]) = \max\{v_p(a), v_p(b)\}$

Tvrzení. *Nechť m, n jsou nesoudělná čísla. Pak platí $m^{\varphi(n)} \equiv 1 \pmod{n}$, kde $\varphi(n)$ je Eulerova funkce, která značí počet nesoudělných čísel s n a menších než n.*

Tvrzení. (LTE pro lichá prvočísla) *Nechť p je liché prvočíslo a n přirozené číslo. Pro celá čísla x, y, která nejsou dělitelná prvočíslem p, platí:*

(i) $v_p(x^n - y^n) = v_p(x-y) + v_p(n)$, *pokud* $x \equiv y \pmod{p}$,
(ii) $v_p(x^n + y^n) = v_p(x+y) + v_p(n)$, *pokud n je liché a* $x \equiv -y \pmod{p}$.

Tvrzení. (LTE pro 2) *Nechť n je přirozené číslo. Pro lichá celá čísla x, y platí:*

(i) $v_2(x^n - y^n) = v_2(x-y) + v_2(n)$ *pro* $4 \mid x - y$,
(ii) $v_2(x^n - y^n) = v_2(x+y) + v_2(x-y) + v_2(n) - 1$ *pro sudé n.*

Důkaz LTE ukážeme na přednášce, ale můžete to zkusit sami. Použijte matematickou indukci na $v_p(n)$.

Lemma. *Hodnota $n - v_p(n)$ roste nade všechny meze pro $n \to \infty$.*

Příklad 1. Dokažte, že pro přirozené n platí $3^{n+3} \mid 1997^{3^n} + 1$.

Příklad 2. Najděte $v_p((p-2)^{2(p-1)} - (p+4)^{p-1})$ pro prvočíslo p.

Příklad 3. Najděte $v_{1991}\big(1990^{1991^{1992}} + 1992^{1991^{1990}}\big)$. (IMO shortlist 1991)

Příklad 4. Najděte všechna přirozená n, pro která platí: $2^n \mid 3^n - 1$.

Příklad 5. Nechť a, b jsou racionální čísla. Dokažte, že je-li hodnota $a^n - b^n$ celá pro nekonečně mnoho přirozených n, pak jsou obě čísla a, b celá.

Příklad 6. Nechť $a, n \geq 2$ taková, že existuje přirozené číslo $k \geq 2$ takové, že $n \mid (a-1)^k$. Dokažte, že n dělí $a^{n-1} + a^{n-2} + \cdots + 1$. (Romania TST 2009)

Příklad 7. Najděte všechy dvojice přirozených čísel (a, b) takových, že $b^a \mid a^b - 1$.

Příklad 8. Najděte všechny dvojice prvočísel (p, q) takových, že

$$pq \mid (5^p - 2^p)(5^q - 2^q).$$

Příklad 9. Pro která přirozená n platí, že $2^{n+2}(2^n - 1) - 8 \cdot 3^n + 1$ je čtverec? (Vietnam TST 2011)

Příklad 10. Najděte všechny dvojice přirozených čísel (m, n), které splňují

$$m^2 + 2 \cdot 3^n = m\left(2^{n+1} - 1\right).$$

(IMO shortlist 2010)

Příklad 11. Najděte všechna přirozená čísla n splňující $n^2 \mid 2^n + 1$.

(IMO 1990)

Příklad 12. Najděte všechna přirozená čísla n taková, že $n \mid 2^{n-1} + 1$.

Hinty k příkladům

1. Přímé dosazování do vzorce.

2. Berte $(p - 1)$ jako společný exponent.

3. Berte 1991^{1990} jako společný exponent.

4. Použijte LTE na prvočíslo 2 a pak ukažte, že n nemůže být moc velké.

5. Je-li t nejmenší číslo, pro které platí, že $a^t - b^t$ je celé číslo, pak dokažte, že každý exponent s touto vlastností je násobek čísla t.

6. Použijte LTE na výraz $a^n - 1$.

7. Dokažte, že je-li p nejmenší prvočíslo dělící b, pak $p|a - 1$.

8. Předpokládejte, že p je menší pročíslo a ukažte, že p musí být 3.

9. Předpokládejte, že číselný výraz se rovná a^2, a upravte rovnici tak, aby na jedné straně stálo 8.3^n a na druhé součin dvou závorek. Snažte se eliminovat a a použijte lemma na prvočíslo 3. Dále ukažte, že n nemůže být moc velké.

10. Převeďte na úlohu 9.

11. Zjistěte, jaké můžou být 2 nejmenší prvočíselné dělitele čísla n.

12. Vyšetřujte největší mocniny 2, které dělí $n - 1$ a $p - 1$, kde p jsou prvočíselné dělitele čísla n.

Literatura a zdroje

[1] Amir Hossein Parvardi: článek *Lifting The Exponent Lemma*
[2] *www.mathlinks.ro*