Lifting The Exponent lemma

Anh Dung „Tonda“ Le

Abstrakt. 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.

Značení. Pro dělitelnost zavádíme symbol $a \mid b$, který čteme „a dělí b“.

Tvrzení. (Zásadní!) *Pro dělitelnost platí následující tvrzení:*

(i) *Pokud je p prvočíslo, pak $p \mid ab \Rightarrow p \mid a \vee p \mid b$.*
(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). 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. (Eulerova věta) *Nechť a, n jsou nesoudělná čísla. Pak platí $a^{\varphi(n)} \equiv 1 \pmod{n}$, kde $\varphi(n)$ je Eulerova funkce, která značí počet čísel nesoudělných 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) $v_2(x^n - y^n) = v_2(x - y)$, *pokud n je liché,*

(ii) $v_2(x^n - y^n) = v_2(x + y) + v_2(x - y) + v_2(n) - 1$, *pokud n je sudé.*

Důkaz LTE ukážeme na přednášce, ale můžete ho zkusit vymyslet 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. Nechť a, n jsou přirozená čísla a p liché prvočíslo takové, že $p^n \mid a^p - 1$. Dokažte, že $p^{n-1} \mid a - 1$.

Příklad 3. Dokažte, že jediné přirozené číslo a takové, že $4(a^n + 1)$ je krychle pro všechna přirozená n, je 1.

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

Příklad 5. Nechť p je prvočíslo a a, n přirozená čísla. Dokažte, že pokud platí $2^p + 3^p = a^n$, pak $n = 1$. (Irsko 1996)

Příklad 6. Najděte všechna přirozená n, pro která platí $2^n \mid 3^n - 1$.

Příklad 7. 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 8. Mějme čísla $a, n \geq 2$ taková, že existuje přirozené číslo $k \geq 2$, pro které platí $n \mid (a-1)^k$. Dokažte, že $n \mid a^{n-1} + a^{n-2} + \cdots + 1$. (Romania TST 2009)

Příklad 9. Najděte všechny dvojice přirozených čísel (a, b) takových, že $b^a \mid a^b - 1$.

Příklad 10. Nechť $k > 1$ je přirozené číslo. Ukažte, že existuje nekonečně mnoho přirozených čísel n, pro která platí $n \mid 1^n + 2^n + \cdots + k^n$.

Příklad 11. Najděte všechna přirozená x, y taková, že $p^x - y^p = 1$, kde p je prvočíslo. (Celostátko 1996)

Příklad 12. Najděte všechny dvojice prvočísel (p, q) takových, že

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

Příklad 13. Pro která přirozená n platí, že $2^{n+2}(2^n-1)-8\cdot 3^n+1$ je čtverec?
(Vietnam TST 2011)

Příklad 14. 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 15. Najděte všechna přirozená čísla n splňující $n^2 \mid 2^n+1$.
(IMO 1990)

Nápovědy

1. Přímé dosazování do vzorce.

2. Berte p jako společný exponent.

3. Porovnejte $4(a^{np}+1)$ a $4(a^n+1)$, kde p je liché prvočíslo dělící $4(a^n+1)$.

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

5. Berte p jako společený exponent.

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

7. 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.

8. Použijte LTE na výraz a^n-1.

9. Dokažte, že je-li p nejmenší prvočíslo dělící b, pak $p \mid a-1$.

10. Pokud k je liché, pak vyberte p^m pro liché prvočíslo p dělící k. Pokud k je sudé, pak vyberte p^m pro liché prvočíslo dělící $k+1$.

11. Použijte LTE, pak poslední lemma.

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

13. Předpokládejte, že číselný výraz se rovná a^2, a upravte rovnici tak, aby na jedné straně stálo $8\cdot 3^n$ a na druhé součin dvou závorek. Snažte se eliminovat a a použijte lemma na prvočíslo 3. Dále ukažte, že n nemůže být moc velké.

14. Převeďte na úlohu 9.

15. Zjistěte, jaké můžou být dva nejmenší prvočíselné dělitele čísla n.

Literatura a zdroje

[1] Amir Hossein Parvardi: *Lifting The Exponent Lemma (LTE)*