

Lema o podizanju eksponenta

Lifting The Exponent Lemma (LTE)

Adrian Satja Kurdija
askurdija@gmail.com

IMO i MEMO pripreme

23. lipnja 2014.

- 1 Uvod
- 2 Dvije korisne leme
- 3 LTE za $p \geq 3$
- 4 LTE za $p = 2$
- 5 Sažetak
- 6 Jedna zanimljivost
- 7 Zadaci
- 8 Literatura

- U eksponencijalnim diofantским jednadžbama često se javljaju izrazi oblika $a^n \pm b^n$.
- Često je tada potrebno za neki prost broj p pronaći potenciju s kojom on "ulazi" u $a^n \pm b^n$; preciznije, najveću njegovu potenciju koja dijeli $a^n \pm b^n$.
- Upravo o toj potenciji govori Lifting The Exponent Lemma (LTE).
- Kao što ćemo vidjeti, LTE nije jedna tvrdnja nego više njih (za razne slučajeve).

- b dijeli a (tj. a je djeljiv sa b):

$$b \mid a \iff \exists q \in \mathbb{Z} : a = qb.$$

- b ne dijeli a (tj. a nije djeljiv sa b) pišemo kao $b \nmid a$.
- $v_p(x)$ definiramo kao najveću potenciju broja p koja dijeli x :

$$v_p(x) = \alpha \iff p^\alpha \mid x \wedge p^{\alpha+1} \nmid x.$$

- $v_p(x) = \alpha$ pišemo i kao $p^\alpha \parallel x$.

- Ako $p \nmid n$, onda je $v_p(n) = 0$.
- $v_3(63) = 2$, tj. $3^2 \parallel 63$.
- Ako su $p \neq q$ prosti brojevi, onda je $v_p(p^\alpha q^\beta) = \alpha$.
- $v_p(ab) = v_p(a) + v_p(b)$, $a, b \in \mathbb{Z}$.
- $v_p(0) = \infty$.

Lema 1

Neka su $x, y \in \mathbb{Z}$ i $n \in \mathbb{N}$. Za prost broj p (dozvoljavamo i $p = 2$) takav da je $\gcd(n, p) = 1$, $p \mid x - y$, $p \nmid x$ i $p \nmid y$ vrijedi

$$v_p(x^n - y^n) = v_p(x - y).$$

Dokaz.

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + y^{n-1}),$$

pa je dovoljno pokazati

$$p \nmid x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + y^{n-1}.$$

Iz $x \equiv y \pmod{p}$ lako slijedi

$$x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + y^{n-1} \equiv nx^{n-1} \not\equiv 0 \pmod{p}.$$



Lema 2

Neka su $x, y \in \mathbb{Z}$ i $n \in \mathbb{N}$ neparan. Za proizvoljan prost broj p (dozvoljavamo i $p = 2$) takav da je $\gcd(n, p) = 1$, $p \mid x + y$, $p \nmid x$ i $p \nmid y$ vrijedi

$$v_p(x^n + y^n) = v_p(x + y).$$

Dokaz.

Primjena prethodne leme na $(x, -y)$. □

Teorem 1 (Prvi oblik LTE)

Neka su $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$. Za proizvoljan prost broj $p \geq 3$ takav da $p \mid a - b$, $p \nmid a$ i $p \nmid b$ vrijedi

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

Dokaz.

Stavimo $v_p(n) = m$, odnosno $n = kp^m$, pri čemu $p \nmid k$.

Faktorizirajmo $a^n - b^n$.

Na sljedećoj slici konačni faktori označeni su bojama.

Dokaz (nastavak).

$$a^{kp^m} - b^{kp^m}$$

$$a^{p^m} - b^{p^m}$$

$$a^{(k-1)p^m} + a^{(k-2)p^m} b^{p^m} + a^{(k-3)p^m} b^{2p^m} + \dots + b^{(k-1)p^m}$$

$$a^{p^{m-1}} - b^{p^{m-1}}$$

$$a^{(p-1)p^{m-1}} + a^{(p-2)p^{m-1}} b^{p^{m-1}} + a^{(p-3)p^{m-1}} b^{2p^{m-1}} + \dots + b^{(p-1)p^{m-1}}$$

...

$$a^{(p-1)p^{m-2}} + a^{(p-2)p^{m-2}} b^{p^{m-2}} + a^{(p-3)p^{m-2}} b^{2p^{m-2}} + \dots + b^{(p-1)p^{m-2}}$$

$$a^p - b^p$$

...

$$a - b$$

$$a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \dots + b^{p-1}$$

Dokaz (nastavak).

Želimo dobiti

$$v_p(a^{kp^m} - b^{kp^m}) = v_p(a - b) + m.$$

Iz skicirane faktorizacije slijedi da je dovoljno dokazati sljedeće:

- žuti faktor nije djeljiv s p , tj. v_p od njega je 0
(sastoji se od k međusobno kongruentnih članova modulo p , pa je kongruentan $k \cdot a^{(k-1)p^m} \not\equiv 0 \pmod{p}$),
- svaki od zelenih faktora djeljiv je s p
(analogno, sastoji se od p međusobno kongruentnih članova...),
- nijedan zeleni faktor nije djeljiv s p^2
(dokaz slijedi).

j -ti zeleni faktor (brojeći tako da je nulti onaj pri dnu slike) zapišimo kao

$$\Gamma_j = x^{p-1} + x^{p-2}y + x^{p-3}y^2 + \dots + y^{p-1},$$

za $x = a^{p^j}$ i $y = b^{p^j}$.

Dokaz (nastavak).

Stavimo $y = x + kp$ za neki cijeli broj k (možemo zbog $x \equiv y \pmod{p}$).
U Γ_j javljaju se članovi oblika

$$x^{p-i}y^{i-1} = x^{p-i}(x + kp)^{i-1} = x^{p-i} \overbrace{(x + kp) \cdots (x + kp)}^{i-1}.$$

Možemo zanemariti članove djeljive s p^2 (jer nas zanima ostatak pri dijeljenju Γ_j s p^2) pa nam ostaju članovi oblika

$$x^{p-1} + (i-1)x^{p-2}kp.$$

Sumiranjem ovih izraza za $i = 1, 2, \dots, p$ dobivamo

$$\Gamma_j \equiv px^{p-1} + \frac{1}{2}(p-1)p^2kx^{p-2} \equiv px^{p-1} \not\equiv 0 \pmod{p^2}.$$

Odavde je $v_p(\Gamma_j) = 1$ za $j \in \{0, 1, \dots, m-1\}$ i dokaz je završen. □

Teorem 2 (Drugi oblik LTE)

Neka su $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$ neparan. Za proizvoljan prost broj $p \geq 3$ takav da $p \mid a + b$, $p \nmid a$ i $p \nmid b$ vrijedi

$$v_p(a^n + b^n) = v_p(a + b) + v_p(n).$$

Dokaz.

Primjena prethodnoga teorema na $(a, -b)$. □

Zašto ovi dokazi ne vrijede za $p = 2$?

Zato što $\frac{1}{2}(p-1)p^2 kx^{p-2}$ u tom slučaju nije djeljiv s p^2 .
($\frac{1}{2}(p-1)$ nije cijeli broj.)

A što ako je $p = 2$?

Teorem 3 (LTE za $p = 2$)

Neka su $x, y \in \mathbb{Z}$ neparni i takvi da $4 \mid x - y$. Tada za proizvoljan $n \in \mathbb{N}$ vrijedi

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

Dokaz.

Dokazujemo tvrdnju za proizvoljan eksponent $N = 2^n m$, gdje je m neparan. Imamo

$$\begin{aligned} v_2(x^N - y^N) &= v_2(x^{2^n m} - y^{2^n m}) \\ &= v_2((x^{2^n})^m - (y^{2^n})^m) \\ &= [\text{Lema 1}] \\ &= v_2(x^{2^n} - y^{2^n}). \end{aligned}$$

Dokaz (nastavak).

Preostaje pokazati

$$v_2(x^{2^n} - y^{2^n}) = v_2(x - y) + n. \quad (1)$$

Faktorizacija daje

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdots (x^2 + y^2)(x + y)(x - y). \quad (2)$$

Sada zbog $x \equiv y \equiv \pm 1 \pmod{4}$ imamo $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod{4}$ za sve $k \in \mathbb{N}$ pa slijedi

$$x^{2^k} + y^{2^k} \equiv 2 \pmod{4} \implies v_2(x^{2^k} + y^{2^k}) = 1, \quad k \in \mathbb{N}. \quad (3)$$

Budući da su x, y neparni i međusobno kongruentni modulo 4, slijedi i

$$x + y \equiv 2 \pmod{4} \implies v_2(x + y) = 1. \quad (4)$$

Primjenom funkcije v_2 na (2) i potom koristeći (3) i (4) izlazi (1). □

Korolar

Neka su $x, y \in \mathbb{Z}$ neparni i $n \in \mathbb{N}$ paran. Tada vrijedi

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

Dokaz.

Lako se pokaže da $4 \mid x^2 - y^2$.

Sada za $n = 2^k m$, pri čemu je $k \in \mathbb{N}$ i m neparan, vrijedi

$$\begin{aligned} v_2(x^{2^k m} - y^{2^k m}) &= v_2((x^2)^{2^{k-1} m} - (y^2)^{2^{k-1} m}) \\ &= [\text{prethodni teorem}] \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x - y) + v_2(x + y) + v_2(n) - 1. \end{aligned}$$



Neka je p prost broj i $x, y \in \mathbb{Z}$, $p \nmid x$, $p \nmid y$. Tada za $n \in \mathbb{N}$, uz uvjete s lijeve strane tablice, vrijedi jednakost na desnoj strani.

p	$x \pm y$	n	Jednakost
	$p \mid x - y$	$p \nmid n$	$v_p(x^n - y^n) = v_p(x - y)$
	$p \mid x + y$	$p \nmid n$, n neparan	$v_p(x^n + y^n) = v_p(x + y)$
$p = 2$	$4 \mid x - y$		$v_2(x^n - y^n) = v_2(x - y) + v_2(n)$
$p = 2$	$2 \mid x - y$	n paran	$v_2(x^n - y^n) =$ $v_2(x - y) + v_2(x + y) + v_2(n) - 1$
$p \geq 3$	$p \mid x - y$		$v_p(x^n - y^n) = v_p(x - y) + v_p(n)$
$p \geq 3$	$p \mid x + y$	n neparan	$v_p(x^n + y^n) = v_p(x + y) + v_p(n)$

Jedna zanimljivost:

ako je $a \in \mathbb{N}$, $a > 1$, onda je $v_q(a^{q-1} - 1) = 1$ za beskonačno mnogo prostih brojeva q .

Blog [2] navodi da je ovo otvoreni problem, tj. nije poznato je li navedena slutnja točna.

Na papiru i ploči.



A. H. Parvadi, "Lifting The Exponent Lemma (LTE)", *Art of Problem Solving*, <http://www.artofproblemsolving.com/Resources/Papers/LTE.pdf>



HroK, "Lifting the Exponent", *HroK's Blog*, <http://www.artofproblemsolving.com/blog/36408>



apgoucher, "Lifting the exponent", *Complex Projective 4-Space*, <http://cp4space.wordpress.com/2014/04/13/lifting-the-exponent/>



Zsigmondy's theorem, *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Zsigmondy's_theorem