Lema o podizanju eksponenata (1)

Julije Jakšetić[1], *Josip Lopatič*[2], *Marjan Praljak*[3], *Robert Soldo*[4]

U ovom članku ćemo analizirati jednu vrlo korisnu lemu i atraktivan rezultat iz teorije brojeva. Radi se o lemi o podizanju eksponenata (eng. *Lifting The Exponent Lemma*, LTE) i svoju primjenu nalazi pri rješavanju brojnih zadataka iz tzv. olimpijskog folklora, napose eksponencijalnih diofantskih jednadžbi. U drugom dijelu ćemo na raznim zadatcima ilustrirati primjenu ove leme.

Za dva cijela broja a i b reći ćemo da je a djeljiv s b ili da b dijeli a i pišemo $b \mid a$ ako i samo ako postoji neki cijeli broj q takav da je $a = qb$. Definiramo $v_p(x)$ kao najveću potenciju s kojom prosti broj p dijeli x, tj. ako je $v_p(x) = \alpha$ tada $p^\alpha \mid x$, ali $p^{\alpha+1} \nmid x$

$$v_p(xy) = v_p(x) + v_p(y) \tag{1}$$

$$v_p(x+y) \geq \min\{v_p(x), v_p(y)\} \tag{2}$$

$$v_p(x^n) = n v_p(x) \tag{3}$$

$$\text{ako } \ y|x \ \text{ tada je } v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y) \tag{4}$$

$$v_p(0) = \infty. \tag{5}$$

Primjer 1. Najveća potencija od 2 koja dijeli broj 72 je 3 jer $2^3 = 8|72$, ali $2^4 = 16 \nmid 72$, pa pišemo $v_2(72) = 3$ ili još $2^3 \parallel 72$.

Primjer 2. Ako su p i q dva različita prosta broja, tada je $v_p(p^\alpha q^\beta) = \alpha$ ili $p^\alpha \parallel p^\alpha q^\beta$.

Najprije ćemo navesti dvije korisne leme.

Lema 1. *Neka su x i y (ne nužno pozitivni) cijeli brojevi i neka je n prirodan broj. Dan je proizvoljan prosti broj p (može biti i $p = 2$) takav da je $m(n, p) = 1$, $p \mid x - y$, te niti jedan od brojeva x, y nije djeljiv s p. Tada vrijedi*

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

Dokaz. Koristimo sljedeći identitet

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}). \tag{D}$$

Da bismo dokazali tvrdnju leme zbog rastava (D), te činjenice (1), dovoljno je pokazati da $p \nmid x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}$. Koristit ćemo pretpostavku da $p \mid x - y$, tj. $x - y \equiv 0 \pmod{p}$ ili $x \equiv y \pmod{p}$. Imamo

$$\begin{aligned} x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1} &\equiv x^{n-1} + x^{n-2} \cdot x + \ldots + x \cdot x^{n-2} + x^{n-1} \\ &\equiv nx^{n-1} \not\equiv 0 \pmod{p}, \end{aligned}$$

čime je dokaz dovršen. $\square$

---

[1] Autor je izvanredni profesor na Prehrambeno-biotehnološkom fakultetu, Zagreb; e-pošta: `jjaksetic@pbf.hr`

[2] Autor je predavač na VVG, Velika Gorica; e-pošta: `josiplopatic@gmail.com`

[3] Autor je izvanredni profesor na Prehrambeno-biotehnološkom fakultetu, Zagreb; e-pošta: `mpraljak@pbf.hr`

[4] Autor je inženjer teorijske matematike, zaposlen u firmi Pružne građevine, Zagreb; e-pošta:`robert.soldo@prg.hr`

Lema 2. *Neka su x i y cijeli brojevi i neka je n neparan prirodan broj. Dan je proizvoljan prosti broj p (može biti i $p = 2$) takav da je $m(n,p) = 1$, $p \mid x+y$, te niti jedan od brojeva x, y nije djeljiv s p. Tada vrijedi*

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

Dokaz. Primijenimo li lemu 1 na cijele brojeve x i $-y$, te koristeći činjenicu da je n neparan prirodan broj, dobivamo

$$v_p(x^n + y^n) = v_p\big(x^n - (-y)^n\big) = v_p\big(x - (-y)\big) = v_p(x+y). \qquad \square$$

Teorem 1. (prvi LTE oblik) *Neka su x i y cijeli brojevi i neka je n prirodan broj. Neka je p neparan prosti broj takav da $p \mid x-y$, te niti jedan od brojeva x, y nije djeljiv s p. Tada vrijedi*

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n). \tag{LTE1}$$

Dokaz. Dokazujemo prvo

$$v_p(x^p - y^p) = v_p(x-y) + 1, \tag{6}$$

a za to je dovoljno pokazati da su ispunjene sljedeće dvije činjenice

$$p \mid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1}, \tag{7}$$

$$p^2 \nmid x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1} \tag*{(8.)}$$

Tvrdnja (7) direktno slijedi jer je

$$x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod{p}.$$

Neka je sada $y = x + kp$, gdje je k neki cijeli broj. Za proizvoljan cijeli broj t, takav da je $1 \le t < p$, imamo

$$\begin{aligned}
y^t x^{p-1-t} &\equiv (x+kp)^t \cdot x^{p-1-t} \\
&\equiv x^{p-1-t} \cdot \Big(x^t + t(kp) \cdot x^{t-1} + \frac{t(t-1)}{2}(kp)^2 \cdot x^{t-2} + \ldots + (kp)^t\Big) \\
&\equiv x^{p-1-t} \cdot \big(x^t + t(kp) \cdot x^{t-1}\big) \\
&\equiv x^{p-1} + tkp \cdot x^{p-2} \pmod{p^2}.
\end{aligned}$$

Ovo znači da je

$$y^t x^{p-1-t} \equiv x^{p-1} + tkp\, x^{p-2} \pmod{p^2}, \qquad t = 1, 2, \ldots, p-1,$$

odakle proizlazi

$$\begin{aligned}
&x^{p-1} + x^{p-2}y + \ldots + xy^{p-2} + y^{p-1} \\
&\equiv x^{p-1} + \big(x^{p-1} + kp\, x^{p-2}\big) + \big(x^{p-1} + 2kp\, x^{p-2}\big) + \ldots + \big(x^{p-1} + (p-1)kp\, x^{p-2}\big) \\
&\equiv px^{p-1} + \big(1 + 2 + \ldots + (p-1)\big) \cdot kp\, x^{p-2} \\
&\equiv px^{p-1} + \frac{p-1}{2}kp^2\, x^{p-2} \\
&\equiv px^{p-1} \not\equiv 0 \pmod{p^2}.
\end{aligned}$$

Ovime smo dokazali tvrdnju (8), a time i (7).

Sada dokazujemo (LTE1). Uočimo da prirodan broj n možemo zapisati u sljedećem obliku $n = p^\alpha b$, gdje je $m(p,b) = 1$, $\alpha \geq 0$. Tada, koristeći lemu 1 i tvrdnju (6), imamo

$$\begin{aligned}
v_p(x^n - y^n) &= v_p\Big(\big(x^{p^\alpha}\big)^b - \big(y^{p^\alpha}\big)^b\Big) \\
&= v_p\big(x^{p^\alpha} - y^{p^\alpha}\big) \\
&= v_p\Big(\big(x^{p^{\alpha-1}}\big)^p - \big(y^{p^{\alpha-1}}\big)^p\Big) \\
&= v_p\big(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}\big) + 1 \\
&= v_p\Big(\big(x^{p^{\alpha-2}}\big)^p - \big(y^{p^{\alpha-2}}\big)^p\Big) + 1 \\
&= v_p\big(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}\big) + 2 \\
&\;\;\vdots \\
&= v_p(x^p - y^p) + \alpha - 1 = v_p(x-y) + \alpha = v_p(x-y) + v_p(n). \qquad \square
\end{aligned}$$

Teorem 2. (drugi LTE oblik) *Neka su x i y cijeli brojevi i neka je n neparan prirodan broj i p neparan prosti broj takav da $p \mid x+y$, te niti jedan od brojeva x, y nije djeljiv s p. Tada vrijedi*

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n). \tag{LTE2}$$

Dokaz. Slijedi neposredno iz teorema 1. $\square$

U uvjetima prethodnih teorema pretpostavili smo da je p neparan prosti broj, tj. $p \neq 2$, u protivnom razlomak $\dfrac{p-1}{2}$ u dokazu teorema 1 ne bi bio cijeli broj. Slučaj $p = 2$ ističemo zasebno.

Teorem 3. *Neka su x i y dva neparna cijela broja takva da $4 \mid x - y$. Tada, za svaki prirodan broj n, vrijedi*

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

Dokaz. Pretpostavimo prvo da je n neparan broj. Tada, za $p = 2$ imamo $m(n,p) = 1$, odnosno $v_2(n) = 0$. Nadalje, zbog neparnosti brojeva x i y, vrijedi $p \nmid x$, te $p \nmid y$. Po pretpostavci teorema $4 \mid x-y$, no tada specijalno i $2 \mid x-y$. U uvjetima smo leme 1, iz koje sada, zbog činjenice $v_2(n) = 0$, slijedi tvrdnja ovog teorema.

Prije nego li krenemo na dokaz teorema u slučaju n je paran broj, dokazat ćemo, uz pretpostavke ovog teorema, sljedeću tvrdnju koja vrijedi za proizvoljan prirodan broj n:

$$v_2\big(x^{2^n} - y^{2^n}\big) = v_2(x-y) + n. \tag{9}$$

Primjenom n-puta formule za razliku kvadrata, dobivamo narednu faktorizaciju

$$x^{2^n} - y^{2^n} = \big(x^{2^{n-1}} + y^{2^{n-1}}\big)\big(x^{2^{n-2}} + y^{2^{n-2}}\big) \cdot \ldots \cdot \big(x^2 + y^2\big)(x+y)(x-y). \tag{10}$$

Sada zbog $x \equiv y \equiv \pm 1 \pmod 4$, slijedi $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$ za sve $k \in \mathbb{N}$. Stoga je $x^{2^k} + y^{2^k} \equiv 2 \pmod 4$ za sve $k \in \mathbb{N}$. No, kako su x i y neparni brojevi i $4 \mid x-y$, imamo $x + y \equiv 2 \pmod 4$. To znači da je potencija broja 2 u svim faktorima rastava (10) jednaka 1, osim u faktoru $x - y$ u kojemu je potencija broja 2 jednaka $v_2(x-y)$. Koristeći relaciju (1), tvrdnja (9) sada direktno slijedi.

Vratimo se na preostali slučaj u dokazu ovog teorema, tj. pretpostavimo da je sada n paran broj. Tada n možemo zapisati u obliku $n = m \cdot 2^k$, pri čemu su k, m prirodni brojevi, takvi da $2 \nmid m$. Uočimo $v_2(n) = k$. Zbog $x^n - y^n = \left(x^m\right)^{2^k} - \left(y^m\right)^{2^k}$, prema relaciji (9), dobivamo $v_2\left(x^n - y^n\right) = v_2\left(x^m - y^m\right) + k = v_2\left(x^m - y^m\right) + v_2(n)$. Zbog neparnosti prirodnog broja m u uvjetima smo leme 1, stoga je $v_2\left(x^m - y^m\right) = v_2(x - y)$, čime je dokaz kompletan. $\square$

Teorem 4. *Neka su x i y dva neparna cijela broja i neka je n paran prirodan broj. Tada vrijedi:*

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

Dokaz. Kako je n paran broj, možemo ga zapisati u obliku $n = m \cdot 2^k$, pri čemu su k, m prirodni brojevi, takvi da $2 \nmid m$. Brojevi x i y su neparni pa su i brojevi x^{2^k} i y^{2^k} isto neparni, te stoga za njih vrijedi: $2 \mid x^{2^k} - y^{2^k}$, $2 \nmid x^{2^k}$, $2 \nmid y^{2^k}$. Prema lemi 1 sada je

$$v_2(x^n - y^n) = v_2\Big(\big(x^{2^k}\big)^m - \big(y^{2^k}\big)^m\Big) = v_2\big(x^{2^k} - y^{2^k}\big) = v_2\Big(\big(x^2\big)^{2^{k-1}} - \big(y^2\big)^{2^{k-1}}\Big). \tag{11}$$

Kvadrat neparnog broja je oblika $4k+1$, pa je razlika kvadrata dva neparna cijela broja uvijek djeljiva s 4, dakle $4 \mid x^2 - y^2$. Sada smo u uvjetima teorema 3, odakle za $n = 2^{k-1}$, imamo

$$v_2\Big(\big(x^2\big)^{2^{k-1}} - \big(y^2\big)^{2^{k-1}}\Big) = v_2\big(x^2 - y^2\big) + v_2\big(2^{k-1}\big). \tag{12}$$

Primjenom (1), te koristeći činjenicu $v_2\left(2^{k-1}\right) = k - 1 = v_2(n) - 1$, slijedi tvrdnja teorema. $\square$

U nastavku ćemo dati primjene gornjih teorema na probleme, većinom s natjecanja. Neki od njih se mogu riješiti i bez primjene LTE rezultata, no mnogima dodaju elegantnije i kraće rješenje, a u nekima su i neophodni. Također, vjerujemo da će sljedeći primjeri dočarati koliko je širok raspon primjene LTE rezultata u problemima iz teorije brojeva.

Zadatak 1. (Slovenija 1977.) *Odredite sve prirodne brojeve n za koje je broj $2^n + 1$ djeljiv s 3.*

Rješenje. Moguća su dva slučaja, u ovisnosti o parnosti broja n. Pretpostavimo da je n paran prirodan broj, tj. $n = 2k$, za neki prirodan broj k. Tada je $2^n + 1 = 4^k + 1$. No, jer je $4 \equiv 1 \pmod 3$, to je $4^k \equiv 1 \pmod 3$, odnosno $4^k + 1 \equiv 2 \pmod 3$. Stoga, ako je n paran prirodan broj, 3 ne dijeli $2^n + 1$.

Pretpostavimo da je n je neparan prirodan broj. Stavimo li $x = 2$, te $y = 1$, $p = 3$, u uvjetima smo teorema 2, pa imamo $v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = 1 + v_3(n) \geq 1$, tj. potencija broja 3 koja se javlja u kanonskom rastavu broja $2^n + 1$ je barem 1.

Dakle, uvjet zadatka zadovoljavaju svi neparni prirodni brojevi.

Zadatak 2. (Hrvatska 1991.) *Dokažite da je broj $3^{6n} - 2^{6n}$ djeljiv s 35, za svaki prirodan broj n.*

Rješenje. Primijenimo teorem 1 prvo za $x = 3^2 = 9$, $y = 2^2 = 4$, jer $5 \mid x - y$ i onda $v_5\left(3^{6n} - 2^{6n}\right) = v_5\left((3^2)^{3n} - (2^2)^{3n}\right) = v_5(3^2 - 2^2) + v_5(3n) \geq 1$, za sve $n \in \mathbb{N}$.

Slično $3^6 - 2^6 = (3^3)^2 - (2^3)^2 \equiv (-1)^2 - 1^2 \equiv 0 \pmod 7$. Dakle, ponovnom primjenom teorema 1 za $x = 3^6$, $y = 2^6$, slijedi $v_7\left(3^{6n} - 2^{6n}\right) = v_7\left((3^6)^n - (2^6)^n\right) =$

$\nu_7(3^6 - 2^6) + \nu_7(n) \geq 1$. Ovime smo dokazali da $35 \mid 3^{6n} - 2^{6n}$ za svaki prirodan broj n.

Zadatak 3. *Neka je k pozitivan cijeli broj. Nađite sve prirodne brojeve n takve da $3^k | 2^n - 1$.*

Rješenje. Pretpostavimo, prvo, da je n neparan prirodan broj, $n = 2l+1$, $l \in \mathbb{N}$. Sada iz $4 \equiv 1 \pmod 3$ slijedi $4^l \equiv 1 \pmod 3$, odnosno $2^n - 1 = 2 \cdot 4^l - 1 \equiv 1 \pmod 3$. Dakle, u ovom slučaju $3 \nmid 2^n - 1$, a onda i $3^k \nmid 2^n - 1$.

Neka je sada n paran prirodan broj, tj. $n = 2l$, $l \in \mathbb{N}$. Tada je $2^n - 1 = 4^l - 1$ i ako $x = 4$, $y = 1$, $p = 3$, u uvjetima smo teorema 1, pa imamo $\nu_3(4^l - 1) = \nu_3(4-1) + \nu_3(l) = 1 + \nu_3(l)$. Da bi imali traženu djeljivost mora biti $\nu_3(4^l - 1) \geq k$, odnosno $\nu_3(l) \geq k-1$. Dakle, da bi posljednja nejednakost bila zadovoljena, l mora biti oblika $l = 3^{k-1} \cdot s$, gdje je s bilo koji prirodan broj. Zaključno $3^k \mid 2^n - 1$, ako je oblika $n = 2 \cdot 3^{k-1} \cdot s$ $(s \in \mathbb{N})$.

Zadatak 4. (Kazahstan 2001.) *Dokažite da postoji beskonačno mnogo prirodnih brojeva n, takvih da je $2^n + 3^n$ djeljiv s n.*

Rješenje. Uzmimo da je $n = 5^k$, za $k \in \mathbb{N}$. Prema teoremu 2 imamo $\nu_5(2^n + 3^n) = \nu_5(2+3) + \nu_5(5^k) = k+1$, što znači da $5^{k+1} \mid 2^n + 3^n$, a onda i $5^k \mid 2^n + 3^n$, za $n = 5^k$, $k \in \mathbb{N}$.

Zadatak 5. *Odredite najmanji prirodan broj n za koji je $2^n + 3^n$ djeljiv sa 625.*

Rješenje. Ako je n paran, tada je $2^n + 3^n \equiv 2^n + (-2)^n \equiv 2^{n+1} \not\equiv 0 \pmod 5$. Dakle traženi $n \in \mathbb{N}$ ne može biti paran.

Neka je sada n neparan prirodan broj. Stavimo li $x = 2$, $y = 3$, $p = 5$, u uvjetima smo teorema 2, prema kojemu imamo $\nu_5(2^n + 3^n) = \nu_5(2+3) + \nu_5(n) = 1 + \nu_5(n)$. Da bi $625 \mid 2^n + 3^n$, mora biti $\nu_5(2^n + 3^n) \geq 4$, stoga iz prethodne relacije, slijedi $1 + \nu_5(n) \geq 4$, odnosno $\nu_5(n) \geq 3$. Najmanji prirodan broj koji zadovoljava ovaj uvjet je $n = 5^3 = 125$.

Zadatak 6. (Irska 1996.) *Neka je p prost broj, te a i n prirodni brojevi. Dokažite, ako je $2^p + 3^p = a^n$, tada je $n = 1$.*

Rješenje. Za $p = 2$ je $a^n = 13$, te za $p = 5$ je $a^n = 275 = 5^2 \cdot 11$. U oba slučaja je očito $n = 1$. Ako je p prost broj različit od 2 i 5, specijalno p je neparan prirodan broj, pa prema teoremu 2 imamo $\nu_5(2^p + 3^p) = \nu_5(5) + \nu_5(p) = 1 + 0 = 1$, tj. $\nu_5(a^n) = 1$.

Zadatak 7. (Belgija 2001.) *Dokažite da je za svaki prirodan broj n, $n > 1$, broj $(n-1)^2$ djeljitelj broja $n^{n-1} - 1$.*

Rješenje. Ako je $n = 2$, tvrdnja zadatka je trivijalna. Uzmimo da je n proizvoljan prirodan broj, $n > 2$. Neka je s $n - 1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ dan kanonski rastav od $n-1$, pri čemu su $p_1, p_2, \ldots, p_k$ prosti brojevi takvi da je $p_1 < p_2 < \ldots < p_k$, te $\alpha_1, \alpha_2, \ldots, \alpha_k$ pripadne (pozitivne, cjelobrojne) potencije, odnosno $\alpha_j = \nu_{p_j}(n-1)$ za $j = 1, 2, \ldots, k$. Kanonski rastav od $(n-1)^2$ je tada $(n-1)^2 = p_1^{2\alpha_1} \cdot p_2^{2\alpha_2} \cdot \ldots \cdot p_k^{2\alpha_k}$.

Pretpostavimo prvo da je n $(n > 2)$ paran prirodan broj. Tada je $n-1$ neparan broj, te su svi p_j $(j = 1, 2, \ldots, k)$ u njegovom kanonskom rastavu neparni prosti brojevi. Stavimo li $x = n$, $y = 1$, u uvjetima smo teorema 1, $p_j \mid x - y$ $(j = 1, 2, \ldots, k)$. Slijedi

$$\nu_{p_j}\left(n^{n-1} - 1\right) = \nu_{p_j}(n-1) + \nu_{p_j}(n-1) = 2\nu_{p_j}(n-1) = \nu_{p_j}\left((n-1)^2\right) = 2\alpha_j,$$

tj. $p_j^{2\alpha_j} \mid n^{n-1} - 1$, za sve $j = 1, 2, \ldots, k$, a čime je tvrdnja zadatka, u slučaju n $(n > 2)$ paran prirodan broj, dokazana.

Neka je sada n $(n > 2)$ neparan prirodan broj. Tada je $n-1$ paran broj, stoga je, u kanonskom rastavu od $n-1$, $p_1 = 2$. Kao u slučaju n $(n > 2)$ paran prirodan broj, dokazujemo da $p_j^{2\alpha_j} \mid n^{n-1} - 1$, za sve $j = 2, \ldots, k$. Da bismo i u ovom slučaju dokazali tvrdnju zadatka, preostaje nam pokazati da $2^{2\alpha_1} \mid n^{n-1} - 1$. Najprije, uočimo, jer je $n+1$ paran broj to je $v_2(n+1) \geq 1$. Stavimo li, kao i ranije, $x = n$, $y = 1$, uz činjenicu da je $n-1$ paran broj, u uvjetima smo teorema 4,

$$\begin{aligned} v_2\bigl(n^{n-1} - 1\bigr) &= v_2(n-1) + v_2(n+1) + v_2(n-1) - 1 \\ &= v_2\bigl((n-1)^2\bigr) + \bigl(v_2(n+1) - 1\bigr) \geq v_2\bigl((n-1)^2\bigr) = 2\alpha_1, \end{aligned}$$

čime smo pokazali $2^{2\alpha_1} \mid n^{n-1} - 1$.

Zadatak 8. (IMO, Shortlist 1991.) *Nađite najveći eksponent k s kojim potencija 1991^k dijeli broj*

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

Rješenje. Označimo zadani broj s N i uočimo da je $1991 = 11 \cdot 181$, (181 je prost broj). Zapišimo N u obliku

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

Stavimo $x = 1990^{1991^2}$, $y = 1992$ i $n = 1991^{1990}$ (koji je neparan broj).

Dalje, imamo $1990 \equiv -1 \pmod{11}$, odakle slijedi $1990^{1991^2} \equiv -1 \pmod{11}$. Kako je $1992 \equiv 1 \pmod{11}$, dobivamo $x + y \equiv 0 \pmod{11}$, tj. u uvjetima smo teorema 2, prema kojemu je

$$\begin{aligned} v_{11}(N) &= v_{11}\bigl(1990^{1991^2} + 1992\bigr) + v_{11}\bigl(1991^{1990}\bigr) \\ &= v_{11}\bigl(1990^{1991^2} + 1992\bigr) + 1990. \end{aligned} \tag{14}$$

U nastavku računamo $v_{11}\bigl(1990^{1991^2} + 1992\bigr)$ i zato ćemo prvo odrediti $v_{11}\bigl(1990^{1991^2} + 1\bigr)$. Ponovno, jer $11 \mid 1990 + 1$, te jer je 1991^2 neparan broj, prema teoremu 2 slijedi $v_{11}\bigl(1990^{1991^2} + 1\bigr) = v_{11}(1990+1) + v_{11}(1991^2) = 3 \cdot v_{11}(1991) = 3$, tj. $1990^{1991^2} + 1 = 11^3 \cdot k$, za neki prirodan broj k takav da $11 \nmid k$. Dalje, imamo $1990^{1991^2} + 1992 = \bigl(1990^{1991^2} + 1\bigr) + 1991 = 11^3 \cdot k + 11 \cdot 181 = 11(11^2 \cdot k + 181)$, odakle dobivamo $v_{11}\bigl(1990^{1991^2} + 1992\bigr) = 1$.

Sada, iz (14) slijedi $v_{11}(N) = 1991$. Analogno se pokazuje $v_{181}(N) = 1991$, pa je potencija broja 1991 s kojom se javlja u kanonskom zapisu broja N jednaka 1991.

Zadatak 9. Neka su a i b različiti cijeli brojevi i $k > 1$ prirodan broj. Dokažite da

$$\left(a + \frac{1}{k}\right)^n - \left(b + \frac{1}{k}\right)^n$$

može biti cijeli broj za najviše konačno mnogo prirodnih brojeva n.

Rješenje. Neka je p prosti broj koji dijeli k. Ako je

$$\left(a+\frac{1}{k}\right)^n-\left(b+\frac{1}{k}\right)^n=\frac{(ak+1)^n-(bk+1)^n}{k^n}$$

cijeli broj, onda $p^n \mid (ak+1)^n-(bk+1)^n$. Zbog $p \mid (ak+1)-(bk+1)=k(a-b)$ i $p \nmid ak+1$, $p \nmid bk+1$ možemo primijeniti teorem 1:

$$v_p((ak+1)^n-(bk+1)^n)=v_p(k(a-b))+v_p(n).$$

Dakle uvjet $v_p((ak+1)^n-(bk+1)^n) \geq n$ je ekvivalentan $v_p(k(a-b)) \geq n-v_p(n)$ pa zbog $v_p(n) \leq n/2$ (vidi dolje zadatak 1) slijedi $n \leq 2v_p(k(a-b))$. Desna strana ove nejednakosti je neovisna o n i tvrdnja zadatka je time dokazana.

U sljedećem broju nastavit ćemo primjenjivati LTE rezultate na složenijim problemima.

Zadatci za vježbu

1. Dokažite da je za svaki prosti broj p i svaki prirodni broj n vrijedi $v_p(n) \leq n/2$.
2. Neka su x i y neparni prirodni brojevi i n paran prirodan broj. Dokažite da vrijedi
$$v_2(x^n-y^n)=v_2\left(\frac{x^2-y^2}{2}\right)+v_2(n).$$
3. Dokažite
$$v_3(\underbrace{11\cdots1}_{n})=\begin{cases} v_3(n) & \text{ako } 3 \mid n \\ 0 & \text{ako } 3 \nmid n; \end{cases}$$
$$v_{11}(\underbrace{11\cdots1}_{n})=\begin{cases} 1+v_{11}\left(\dfrac{n}{2}\right) & n \text{ paran} \\ 0 & n \text{ neparan.} \end{cases}$$
4. (Hrvatska, školsko natjecanje 2022.) Dokažite da je broj $6^{2022}-2^{2022}$ djeljiv s 2^{2025}.

Literatura

[1] A. H. Parvardi, *Lifting The Exponent Lemma (LTE)*, 2011.
`https://www.academia.edu/4034266/Lifting_The_Exponent_Lemma_LTE_`

[2] P. Koževnikov, V. Senderov, *Stepeni n i $n-e$ stepeni*, Kvant 2012, br. 1.

[3] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb 2019.

[4] N. Elezović, *Odabrani zadaci elementarne matematike*, Element, Zagreb 1992.

[5] B. Bzdega, *Lema o podizanju p-adskog exponenta*, Delta, časopis (Poljska), no. 12, 2020.
`https://www.deltami.edu.pl/temat/matematyka/teoria_liczb/2020/11/30/lemat-o-zwiekszaniu-wykladnika-p-adycznego/`