VAŽNI TEOREMI I TRIKOVI U TEORIJI BROJEVA

Dijana Kreso

1. Pellova jednadžba

Diofantska jednadžba oblika

$$x^2 - dy^2 = 1,$$

gdje je d prirodan broj koji nije potpun kvadrat, naziva se Pellova jednadžba. Slučaj kada je d potpun kvadrat isključujemo jer tada jednadžba ima samo trivijalna rješenja $x = \pm 1, y = 0$. Pellova jednadžba ima beskonačno mnogo rješenja u prirodnim brojevima. Za odrediti sva rješenja dovoljno je poznavati najmanje rješenje u prirodnim brojevima, njega zovemo fundamentalnim rješenjem i označavamo sa (x_1, y_1) ili sa $x_1 + y_1\sqrt{d}$, objašnjenje za drugi zapis slijedi iz sljedećeg teorema kojim su dana sva rješenja Pellove jednadžbe.

Theorem 1.1. *Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja u prirodnim brojevima. Ako je (x_1, y_1) fundamentalno rješenje, onda su sva rješenja u prirodnim brojevima dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}.$$

Dakle, primijenimo li binomni teorem na $(x_1 + y_1\sqrt{d})^n$ imamo da je

$$x_n + y_n\sqrt{d} = \sum_{i=0}^{n} \binom{n}{i} x_1^i (y_1\sqrt{d})^{n-i},$$

odakle se pak lako izdvoji x_n odnosno y_n.

Binomni teorem je svakako potrebno znati, fundamentalno rješenje Pellove jednadžbe se odredi "na prste". Postoje algoritmi za nalaženje fundamentalnog rješenja Pellove jednadžbe, no za potrebe natjecatelja oni nisu važni. Formulu iz teorema je jednostavno zapamtiti. I tu je kraj teoriji! Dakle, ovo se ne smije ne znati.

Svakako je dobro imati na umu da nizovi (x_n) i (y_n) koji zadovoljavaju $x_n + y_n\sqrt{d} = (x_1+y_1\sqrt{d})^n = \sum_{i=0}^{n} \binom{n}{i} x_1^i (y_1\sqrt{d})^{n-i}$ zadovoljavaju rekurzivne formule $x_{n+2} = 2x_1x_{n+1} - x_n$ i $y_{n+2} = 2x_1y_{n+1} - y_n$, $n \geq 0$, gdje je $(x_0, y_0) = (1, 0)$ i (x_1, y_1) fundamentalno rješenje, no njih nije potrebne pamtiti nego je važno imati na umu da nizovi zadovoljavaju jednostavne binarno-rekurzivne formule (binarnost kao ovisnost o prethodna dva člana niza) kako bi ih sami izveli u konkretnom zadataku ukoliko se pokaže potreba.

Promotrimo sada jedan jednostavni primjer, ne natjecateljski zadatak nego najjednostavniji primjer za vježbu.

Zadatak 1 Nađi sva rješenja u prirodnim brojevima (x, y) jednadžbe $x^2 - 6y^2 = 1$.

Rješenje: Fundamentalno rješenje je očito $(x_1, y_1) = (5, 2)$. Dakle, sva rješenja su dana

sa

$$x_n + y_n\sqrt{6} = (5 + 2\sqrt{6})^n.$$

Ako za x_n, y_n vrijedi navedeno onda je $x_n - y_n\sqrt{6} = (5 - 2\sqrt{6})^n$, što se lako pokaže. Zbrajanjem dobivamo da je

$$x_n = \frac{1}{2}((5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n),$$

a oduzimanjem jednadžbi da je

$$y_n = \frac{1}{2\sqrt{6}}((5 + 2\sqrt{6})^n - (5 - 2\sqrt{6})^n).$$

Dakle, sva rješenja (x, y) u prirodnim brojevima su

$$(\frac{1}{2}(5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n), \frac{1}{2\sqrt{6}}((5 + 2\sqrt{6})^n - (5 - 2\sqrt{6})^n)), \quad n \in \mathbb{N}$$

■

Slijedi jedan natjecateljski zadatak.

Zadatak 2 Ako je razlika dva uzastopna kuba u prirodnim brojevima n^2, $n \in \mathbb{N}$, onda je $2n - 1$ potpun kvadrat.

Rješenje: Jer je $(m+1)^3 - m^3 = n^2$, to je $3m^2 + 3m + 1 = n^2$, što se može trasnformirati u $(2n)^2 = 3(2m + 1)^2 + 1$, dakle $(2n, 2m + 1)$ je rješenje Pellove jednadžbe $x^2 - 3y^2 = 1$, odakle je $2n + (2m + 1)\sqrt{3} = (2 + \sqrt{3})^l$ za neki prirodan broj l. Jer je cjelobrojni dio na lijevoj strani paran, to je l neparan, dakle $l = 2k + 1$ za neki $k \geq 0$. Nadalje, jer je $2n + (2m + 1)\sqrt{3} = (2 + \sqrt{3})^l$, jasno je da je $4n = (2 + \sqrt{3})^l + (2 - \sqrt{3})^l$, odakle je $2n - 1 = \frac{1}{2}((2 + \sqrt{3})^l + (2 - \sqrt{3})^l) - 1 = \frac{1}{2}((2 + \sqrt{3})^{2k+1} + (2 - \sqrt{3})^{2k+1}) - 1$. Preostaje pokazati da je ovo potpun kvadrat. Jer je

$$\frac{1}{2}((2 + \sqrt{3})^{2k+1} = \frac{1}{2}(2 + \sqrt{3})((2 + \sqrt{3})^k)^2 = (\frac{1}{2}(1 + \sqrt{3})(2 + \sqrt{3})^k)^2,$$

to se može zaključiti da je $2n - 1 = N^2$ gdje je

$$N = \frac{1}{2}((1 + \sqrt{3})(2 + \sqrt{3})^k + (1 - \sqrt{3})(2 - \sqrt{3})^k).$$

Direktnim računom provjerimo da je zaista $2n - 1 = N^2$, a da je N prirodan broj se lako pokaže indukcijom i to je standardni natjecateljski zadačić. ■

Promotrimo i neke pellovske jednadžbe. To su Diofantske jednadžbe oblika

$$x^2 - dy^2 = N,$$

gdje je d prirodan broj koji nije potpun kvadrat i N cijeli broj različit od 0. Posebno su za teoriju zanimljive pellovske jednadžbe za $N \in \{\pm 1, \pm 4\}$. Njih ćemo i mi obraditi jer su one posebno zanimljive i za natjecatelje. Uočimo za početak da, za razliku od obične Pellove jednadžbe, jednadžba $x^2 - dy^2 = -1$ ne mora imati rješenja u prirodnim brojevima. Primjerice, jasno je da jednadžba $x^2 - 3y^2 = -1$ nema rješenja u prirodnim

brojevima, u suprotnom $x^2 \equiv -1 \equiv 2 \mod 3$, što znamo da nije moguće. Ukoliko ova jednadžba ima rješenje u prirodnim brojevima, najmanje rješenje zovemo fundamenatalnim rješenjem. Vrijedi sljedeći teorem.

Theorem 1.2. *Pretpostavimo da jednadžba $x^2 - dy^2 = -1$ ima rješenja u prirodnim brojevima, te da je (x_1, y_1) fundamentalno rješenje. Ako definiramo nizove (x_n) i (y_n) sa $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, n \in \mathbb{N}$, onda su $x_{2n} + y_{2n}\sqrt{d}$ sva rješenja u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, a $x_{2n+1} + y_{2n+1}\sqrt{d}$ sva rješenja u prirodnim brojevima jednadžbe $x^2 - dy^2 = -1$.*

Nadalje, jasno je da jednadžba $x^2 - dy^2 = 4$ uvijek ima rješenja u prirodnim brojevima. Naime, ako je (u, v) rješenje jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima, onda je $(2u, 2v)$ rješenje jednadžbe $x^2 - dy^2 = 4$ u prirodnim brojevima. Sljedećim teoremom dana su sva rješenja ove pellovske jednadžbe.

Theorem 1.3. *Ako je (x_1, y_1) fundamentalno rješenje jednadzbe $x^2 - dy^2 = 4$, onda su sva rješenja u prirodnim brojevima dana formulom*

$$\frac{x_n + y_n\sqrt{d}}{2} = \Big(\frac{x_1 + y_1\sqrt{d}}{2}\Big)^n, \quad n \in \mathbb{N}.$$

Slično vrijedi za pellovsku jednadžbu $x^2 - dy^2 = -4$.

Theorem 1.4. *Pretpostavimo da jednadžba $x^2 - dy^2 = -4$ ima rješenja u prirodnim brojevima, te da je (x_1, y_1) fundamentalno rješenje. Tada su sva rješenja u prirodnim brojevima dana formulom*

$$\frac{x_n + y_n\sqrt{d}}{2} = \Big(\frac{x_1 + y_1\sqrt{d}}{2}\Big)^n, \quad n \quad \text{neparan.}$$

Pogledajmo još neke zadatke natjecateljskog tipa kod kojih je korisno poznavati rješenja Pellovih i pellovskih jednadžbi.

Zadatak 3 Nađite sve prirodne brojeve x, y za koje vrijedi $x(x + y) = y^2 + 1$.

Rješenje: Jednadžbu množimo s 4 i transformiramo u oblik $(2x + y)^2 = 5y^2 + 4$. Dakle, $(2x + y, y)$ je rješenje pellovske jednadžbe $p^2 - 5q^2 = 4$. Odmah vidimo da početna jednadžba ima beskonačno mnogo rješenja. Njeno fundamentalno rješenje je $(3, 1)$, odakle slijedi da je

$$\frac{(2x + y) + y\sqrt{5}}{2} = \Big(\frac{3 + \sqrt{5}}{2}\Big)^n$$

za neki $n \in \mathbb{N}$. Dakle,

$$\frac{(2x + y) - y\sqrt{5}}{2} = \Big(\frac{3 - \sqrt{5}}{2}\Big)^n,$$

odakle je

$$y = \frac{1}{\sqrt{5}}\Big(\Big(\frac{3 + \sqrt{5}}{2}\Big)^n - \Big(\frac{3 - \sqrt{5}}{2}\Big)^n\Big),$$

odnosno

$$y = \frac{1}{\sqrt{5}}\Big(\Big(\frac{1 + \sqrt{5}}{2}\Big)^{2n} - \Big(\frac{1 - \sqrt{5}}{2}\Big)^{2n}\Big).$$

Prepoznajemo formulu za $2n$-ti član Fibonaccijevog niza, ukoliko je ne prepoznajemo računamo vrijednost od y za nekoliko početnih vrijednosti od n i tako prepoznajemo Fibonaccijev niz. Dakle, $y \in \{F_{2n} : n \in \mathbb{N}\}$. Slično nađemo eksplicitnu formulu za x i uočimo da je $x = F_{2n-1}$. Dakle, sva rješenja jednadžbe (x, y) u prirodnim brojevima su u skupu $\{(F_{2n-1}, F_{2n}) : n \in \mathbb{N}\}$. ■

Usporedbe radi prikazat ćemo i službeno rješenje koje ne koristi pellovske jednadžbe. Zadatak je postavljen na Maloj Olimpijadi 2004. godine.

Drugo rješenje: Izračunamo nekoliko prvih rješenja i primijetimo pojavljivanje Fibonaccijevih brojeva. Koristeći relaciju za Fibonaccijeve brojeve

$$F_{n-1}F_{n+1} = F_n^2 + (-1)^n,$$

poznatu kao Cassinijev identitet, imamo da je $F_{2n-1}F_{2n+1} = F_{2n}^2+1$ što se može zapisati u obliku $F_{2n-1}(F_{2n-1} + F_{2n}) + 1 = F_{2n}^2 + 1$. Dakle za svaki prirodan broj n je (F_{2n-1}, F_{2n}) rješenje početne jednadžbe u prirodnim brojevima. Ukoliko s T označimo skup svih rješenja jednadžbe u prirodnim brojevima,

$$T = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x(x + y) = y^2 + 1\},$$

zasad imamo da je $\{(F_{2n-1}, F_{2n}) : n \in \mathbb{N}\} \subset T$. Pokažimo da osim navedenih jednadžba nema drugih rješenja, odnosno da je $T = \{(F_{2n-1}, F_{2n}) : n \in \mathbb{N}\}$.

Pretpostavimo suprotno, dakle da postoje druga rješenja. Neka je (x, y) takvo rješenje za koje je $x + y$ minimalno. Jasno je da je $x \neq y$ jer je jedino rješenje jednadžbe za koje je $x = y$ očito $(1, 1)$ i ono naravno pripada skupu $\{(F_{2n-1}, F_{2n}) : n \in \mathbb{N}\}$. Jednadžbu zapišemo u obliku $(y - x)(y + x) = xy - 1$. Jer je $xy - 1 \geq 0$, to je $y \geq x$, a onda i $y > x$ zbog $x \neq y$. Jer je $xy - 1 < x(x + y)$ imamo da je $y - x < x$ odnosno $y < 2x$. Dakle, i $y - x$ i $2x - y$ su prirodni brojevi. Označimo $x_1 = 2x - y$ i $y_1 = y - x$. Lako se provjeri da je $(x_1, y_1) \in T$, a jer je $x_1 + y_1 = x < x + y$ to je prema pretpostavci $x_1 = F_{2n-1}, y_1 = F_{2n}$ za neki $n \in \mathbb{N}$. Očito je onda $x = x_1 + y_1 = F_{2n-1} + F_{2n} = F_{2n+1}$ i $y = x_1 + 2y_1 = F_{2n+2}$, no to je u kontradikciji s pretpostavkom, zbog čega su već navedena rješenja jedina moguća. ■

Zadatak 4 Nađite sva rješenja jednadžbe $5^x - 3^y = 2$ u prirodnim brojevima x, y.

Rješenje: Jedno rješenje je očito $(1, 1)$. Pokazat ćemo da je to jedino rješenje. Očito $x = 1$ implicira $y = 1$ i obratno. Zato možemo pretpostaviti da su $x, y > 1$. Promotrimo jednadžbu modulo 4. Imamo da je $1 + (-1)^y \equiv 2 \mod 4$, odakle slijedi da je y neparan. Promotrimo li jednadžbu modulo 3 imamo da je $(-1)^x \equiv 2 \mod 3$, odakle slijedi da je x neparan. Množenjem s 3^b jednadžbu transformiramo u oblik $5^x 3^y - (3^y)^2 = 2 \cdot 3^y$, što koristeći neparnost od x, y možemo transformirati u

$$15(5^{\frac{x-1}{2}} 3^{\frac{y-1}{2}})^2 - (3^y)^2 = 2 \cdot 3^y,$$

odnosno u

$$15(5^{\frac{x-1}{2}}3^{\frac{y-1}{2}})^2 - ((3^y)^2 + 2\cdot 3^y + 1) = -1,$$

dakle u

$$(3^y+1)^2 - 15(5^{\frac{x-1}{2}}3^{\frac{y-1}{2}})^2 = 1.$$

Dakle, $a = 3^y+1$ i $b = 5^{\frac{x-1}{2}}3^{\frac{y-1}{2}}$ su rješenja Pellove jednadžbe $x^2-15y^2=1$. Fundamentalno rješenje ove jednadžbe je $(4,1)$, dakle $a+b\sqrt{15} = (4+\sqrt{15})^n$ za neki $n\in\mathbb{N}$. Jer je b djeljiv s 3, promatramo djeljivost s 3 niza b_n gdje je $a_n+b_n\sqrt{15} = (4+\sqrt{15})^n$. Izračunamo prvih nekoliko vrijednosti i primijetimo da $3 \mid b_n$ akko $3 \mid n$. No, isto tako primijetimo i da u tom slučaju $7 \mid b_n$, što povlači da b_n ne može biti oblika $5^{\frac{x-1}{2}}3^{\frac{y-1}{2}}$. Preostaje to dokazati. Dokaz se može provesti na više načina, ali u principu su svi slični jer se svode na induktivne dokaze djeljivosti. Nađemo eksplicitnu formulu za b_n po istom principu kao u svakom zadataku do sad. Dakle, $b_n = \frac{1}{2\sqrt{15}}((4+\sqrt{15})^n - (4-\sqrt{15})^n)$. Nađemo rekurzivnu formulu za b_n, najjednostavnije računanjem prvih nekoliko članova niza, i dokažemo je indukcijom koristeći eksplicitnu formulu. Imamo da je $b_{n+2} = 8b_{n+1} - b_n$, a početni članovi su $b_1 = 1$, $b_2 = 8$. Promatramo djeljivost s 3 i lako indukcijom pokažemo ono sto smo htjeli, dakle da $3 \mid b_n$ akko $3 \mid n$, no i da $7 \mid b_{3n}$. Prema tome, početna jednadžba nema drugih rješenja osim već navedenog $(1,1)$. ■

2. Eisensteinov kriterij ireducibilnosti polinoma

Za polinom P kažemo da je reducibilan nad $\mathbb{C}$ ako postoje polinomi Q i R stupnja barem 1, s koeficijentima iz $\mathbb{C}$, takvi da je $P = Q\cdot R$, tj. $P(x) = Q(x)\cdot R(x)$ za sve x iz domene polinoma P. Ukoliko polinom nije reducibilan, kažemo da je ireducibilan. Posve analogno definiramo i reducibilnost i ireducibilnost polinoma nad $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ itd.

Natjecateljima je od posebnog interesa reducibilnost polinoma s cjelobrojnim koeficijentima nad $\mathbb{Z}$, odnosno reducibilnost polinoma s cjelobrojnim koeficijentima nad $\mathbb{Q}$ s obzirom da vrijedi sljedeća lema, u literaturi poznata kao Gaussova lema za polinome:

Lemma 2.1. *Polinom s cjelobrojnim koeficijentima je ireducibilan nad $\mathbb{Q}$ ako i samo ako je ireducibilan nad $\mathbb{Z}$.*

Zadaci u kojima je potrebno ustanoviti je li određeni polinom s cjelobrojnim koeficijentima reducibilan nad $\mathbb{Q}$ zahtijevaju individualan pristup, te ih se u skladu s time može naći i na najvišim razinama matematičkih natjecanja. Evo kako glasi jedan kriterij kojim su dani dovoljni uvjeti za utvrđivanje ireducibilnosti nad $\mathbb{Q}$ polinoma s cjelobrojnim koeficijentima, poznat kao Eisensteinov kriterij ireducibilnosti polinoma.

Theorem 2.2. *Neka je $P(x) = a_nx^n + \cdots + a_1x + a_0$ polinom s cjelobrojnim koeficijentima. Ako postoji prost broj p takav da $p \mid a_0,\ a_1, \ldots,\ a_{n-1}$, te $p \nmid a_n$ i $p^2 \nmid a_0$, tada je P ireducibilan nad $\mathbb{Q}$.*

Rijesimo par zadataka koristeci navedeni kriterij ireducibilnosti polinoma.

Zadatak 5. Dokažite da je polinom $P(x) = x^p + px + (p-1)$ ireducibilan nad $\mathbb{Z}$ za svaki prosti broj osim za 2.

Rješenje: $P(x+1) = (x+1)^p + p(x+1) + (p-1)$, što se korištenjem binomnog teorema, te potom zbrajanjem monoma, može zapisati i ovako: $P(x+1) = x^p + px^{p-1} + \ldots 2px + 2p$. Sasvim je jasno da je $P(x+1)$ prema Eisensteinovom kriteriju ireducibilnosti polinoma ireducibilan ukoliko je $p \neq 2$, a onda je i $P(x)$ ireducibilan. Direktnom provjerom ustanovimo da za $p = 2$ vrijedi $P(x) = (x+1)^2$ tj. u ovom slučaju P je reducibilan. ■

Zadatak 6. Dokažite da je za svaki prosti broj p polinom $P(x) = x^{p-1} + \cdots + x + 1$ ireducibilan nad $\mathbb{Q}$

Rješenje: Jer je $P(x) = (x^p - 1)/(x-1)$, to je $P(x+1) = ((x+1)^p - 1)/x$, što koristeći binomni teorem možemo zapisati kao $P(x+1) = (x^p + px^{p-1} + \cdots + px + 1 - 1)/x = x^{p-1} + px^{p-2} + \cdots + p$. Vodeći koeficijent je 1, a ostali su $\binom{p}{k}$ gdje je k između 1 i $(p-1)$. Jer je $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ i jer su svi prosti faktori u nazivniku manji od p za $1 \leq k \leq p-1$, a p prost, to ne moze doći do kraćenja p-a iz brojnika. Dakle, cijeli broj $\binom{p}{k}$ je djeljiv s p za $1 \leq k \leq p-1$. Kako ni slobodni koeficijent nije djeljiv s p^2, to su zadovoljeni svi uvjeti Eisensteinovog kriterija, te možemo zaključiti da je $P(x+1)$ ireducibilan nad $\mathbb{Q}$, a onda je to i $P(x)$. ■

Na Međunarodnoj matematičkoj Olimpijadi 1993. godine u Turskoj pojavio se sljedeći zadatak.

Zadatak 7. Zadan je polinom $P(x) = x^n + 5x^{n-1} + 3$, gdje je $n > 1$. Dokažite da ne postoje polinomi Q i R s cjelobrojnim koeficijentima, stupnja barem 1, takvi da je $P(x) = Q(x) \cdot R(x)$.

Tu nam Eisensteinov kriterij ne može pomoći, no Eisensteinov kriterij može se i generalizirati. Jedna generalizacija, koju nazivamo proširenim Eisensteinovim kriterijem ireducibilnosti, izgleda ovako:

Theorem 2.3. *Neka $P(x) = a_n x^n + \cdots + a_1 x + a_0$ polinom s cjelobrojnim koeficijentima. Pretpostavimo da postoji prost broj p te prirodan broj $i \leq n$ takav da $p \mid a_0, a_1, \ldots, a_{i-1}$ i $p \nmid a_i$, te $p^2 \nmid a_0$. Tada P ima ireducibilan faktor stupnja barem i.*

Rješenje Zadatka 7: Očito je da prost broj 3 dijeli sve koeficijente a_i za $0 \leq i < n-1$, te $3^2 = 9$ ne dijeli $a_0 = 3$, i 3 ne dijeli keoficijent a_{n-1} tj. 5. Prema proširenom Eisensteinovom kriteriju ireducibilnosti polinoma, P ima ireducibilan faktor stupnja barem $n-1$. Dakle, ili je ireducibilan ili ima ireducibilni faktor stupnja $n-1$. U ovom drugom slučaju P ima i linearni faktor, jer je stupanj od P jednak n. Dakle, P se može zapisati u obliku $P(x) = (x-c)Q(x)$, gdje je Q ireducibilan stupnja $n-1$ i c element od $\mathbb{Z}$. Dakle, $P(c) = 0$, tj. $c^n + 5c^{n-1} + 3 = 0$. Preostaje pokazati da ovo nije moguće, tj. da ne postoji cijeli broj c koji zadovoljava ovu jednakost. No, to je zapravo sasvim očito.

Naime, izraz na lijevoj strani je neparan broj za sve cijele brojeve c, što je u kotradikciji s parnošću nule. ■