Osječki matematički list 23 (2023), 133–145

Zsigmondyjev teorem

Ivan Matić*

Sažetak

U radu ćemo predstaviti interesantan rezultat iz elementarne teorije brojeva, koji je poznat pod nazivom Zsigmondyjev teorem. Navest ćemo neke posljedice tog rezultata te prikazati njegovu primjenu na nizu problema.

Ključne riječi: *prosti brojevi, djeljivost, diofantske jednadžbe*

Zsigmondy's theorem

Abstract

In this paper we present an interesting result in elementary number theory, known as Zsigmondy's theorem. We discuss some of its consequences and show its applications on the series of examples.

Keywords: *prime numbers, divisibility, Diophantine equations*

1 Uvod

Problemi vezani uz djeljivost s punim pravom zauzimaju istaknuto mjesto kako u rekreativnoj matematici za entuzijaste i radoznalce, tako i u zadatcima koji se pojavljuju na natjecanjima iz matematike za sve dobne skupine i na svim jakosnim razinama. Jedan od razloga tome leži u činjenici da za

*Fakultet primijenjene matematike i informatike, Sveučilište J. J. Strossmayera u Osijeku, email: imatic@mathos.hr

razumijevanje iskaza takvih problema nije potrebno posebno široko matematičko predznanje te se radi o vrlo konkretnim objektima. No, to ne znači da je i rješavanje problema takvog tipa jednostavno.

Dapače, upravo su se pojedini problemi vezani uz djeljivost, ili općenitije uz teoriju brojeva, pokazali prilično tvrdim orahom i brojnim vrhunskim stručnjacima te su pokušaji njihova rješavanja bili zaslužni i za razvoj pojedinih grana matematike. Posvetimo se ipak nešto jednostavnijim problemima, koji su primjereniji za razmatranje i studentima početnih godina i srednjoškolcima.

Obično u matematici postoji više pristupa nekom problemu i više načina za njegovo rješavanje, svaki od kojih može na problem baciti drugačije svjetlo. Primjera radi, danas je poznato otprilike 400 dokaza Pitagorina teorema. Što se tiče problema vezanih uz djeljivost, oni često zahtijevaju preciznu analizu ostataka pri dijeljenju s pojedinim spretno odabranim prirodnim brojevima, prepoznavanje odgovarajućih gornjih ili donjih ograda promatranih izraza te primjenu poznatih općenitijih rezultata u danoj situaciji.

U ovom ćemo se radu posvetiti upravo posljednjoj opciji te opisati jedan rezultat koji nije previše razvikan, ali u pojedinim situacijama može biti vrlo koristan. Radi se o rezultatu iz elementarne teorije brojeva koji govori o prostim djeliteljima sume i razlike potencija relativno prostih prirodnih brojeva s jednakim eksponentima, a svoj naziv duguje matematičaru Karlu Zsigmondyju iz 19. stoljeća, autoru prve poznate varijante rezultata kojem ćemo se posvetiti.

U idućem ćemo poglavlju najprije navesti temeljni rezultat, Zsigmondyjev teorem za razlike, iz kojeg ćemo zatim izvesti analogan rezultat za sume te ga popratiti s osnovnim primjerima i s par općenitih posljedica. Zatim ćemo, u novom poglavlju, navesti i riješiti niz primjera iz elementarne teorije brojeva pri čijem se postupku rješavanja iskazani rezultati pokazuju izuzetno korisnima. Pri tome ćemo ciljano izbjegavati korištenje metoda koje nadilaze standardno gradivo srednjoškolske matematike.

2 Zsigmondyjev teorem

Ponovimo najprije jedan od temeljnih pojmova koji će nam biti potreban.

Kažemo da su prirodni brojevi a i b *relativno prosti* ukoliko je 1 njihov najveći zajednički djelitelj, odnosno ako ne postoji niti jedan prirodan broj veći od 1 koji dijeli i a i b. Na primjer, brojevi 14 i 27 su relativno prosti, dok brojevi 14 i 35 nisu, jer su oba djeljivi sa 7. Ukoliko je p prost broj i n prirodan broj manji od p, tada su p i n relativno prosti.

Teorem 2.1. *Neka su a i b relativno prosti prirodni brojevi takvi da je $a > b$. Neka je n prirodan broj veći od 1. Tada postoji prost broj p takav da p dijeli $a^n - b^n$ i p ne dijeli $a^k - b^k$, za $k \in \{1, 2, \ldots, n-1\}$, osim u idućim dvjema situacijama:*

(i) $(a, b, n) = (2, 1, 6)$,

(ii) $(a + b, n) = (2^m, 2)$ *za neki prirodan broj m.*

Pogledajmo prethodni rezultat na konkretnom primjeru.

Primjer 2.1. *Neka je $a = 4$, $b = 3$ i $n = 4$. Tada je redom*

$$a^4 - b^4 = 256 - 81 = 175 = 5 \cdot 5 \cdot 7$$
$$a^3 - b^3 = 64 - 27 = 37$$
$$a^2 - b^2 = 16 - 9 = 7$$
$$a^1 - b^1 = 4 - 3 = 1.$$

Prema tome, za prost broj $p = 5$ vrijedi da p dijeli $a^4 - b^4$ i p ne dijeli $a^k - b^k$ za $k \in \{1, 2, 3\}$, dok za prost broj $q = 37$ vrijedi da q dijeli $a^3 - b^3$ i q ne dijeli $a^k - b^k$ za $k \in \{1, 2\}$.

Rezultat iskazan teoremom 2.1 se obično naziva Zsigmondyjev teorem ili, preciznije, Zsigmondyjev teorem za razlike, po austrijskom matematičaru Karlu Zsigmondyju mađarskog porijekla, koji je krajem 19. stoljeća pokazao navedeni rezultat u slučaju $b = 1$. Općeniti rezultat, koji smo i iskazali teoremom 2.1, dokazali su početkom 20. stoljeća Birkhoff i Vandiver metodama elementarne teorije brojeva. Dokaz zbog njegove duljine na ovom mjestu nećemo iznositi, a može se pronaći u [1].

S vremenom su nastajali i drugi dokazi teorema 2.1, mahom temeljeni na naprednijim metodama. Jedan se takav dokaz slučaja $b = 1$ može pronaći u [4, Theorem 3].

Prokomentirajmo posebne slučajeve koji se pojavljuju u teoremu 2.1:

Primijetimo da u slučaju $a = 2$, $b = 1$, $n = 6$ vrijedi $a^n - b^n = 2^6 - 1^6 = 64 - 1 = 63 = 3 \cdot 3 \cdot 7$ te su 3 i 7 jedini prosti djelitelji od $a^n - b^n$. No, za $k = 3$ imamo $a^k - b^k = 2^3 - 1^3 = 7$ te 7 dijeli $a^3 - b^3$, dok za $k = 4$ imamo $a^k - b^k = 2^4 - 1^4 = 15$ pa 3 dijeli $a^4 - b^4$.

S druge strane, ako je $n = 2$ vrijedi $a^n - b^n = a^2 - b^2 = (a - b)(a + b)$. Ukoliko prost broj dijeli produkt, tada dijeli i neki od njegovih faktora ([3, Lema 1.4.1]) pa za prost broj p koji dijeli $a^2 - b^2$ vrijedi da p dijeli $a - b$ ili p dijeli $a + b$. Ako je $a + b$ oblika 2^m, tada je jedini prost djelitelj od $a + b$ upravo broj 2. No, iz činjenice da je $a + b$ paran slijedi da su brojevi a i b iste

parnosti te je tada i $a - b$ paran. Zato u ovom slučaju svaki prost djelitelj od $a^2 - b^2$ dijeli i $a - b$.

Jedna je od direktnih posljedica teorema 2.1 rezultat koji se naziva i Zsigmondyjev teorem za sume.

Korolar 2.1. *Neka su a i b relativno prosti prirodni brojevi takvi da je $a > b$. Neka je n prirodan broj veći od 1. Tada postoji prost broj p takav da p dijeli $a^n + b^n$ i p ne dijeli $a^k + b^k$, za $k \in \{1, 2, \ldots, n-1\}$, osim u slučaju $(a, b, n) = (2, 1, 3)$.*

Dokaz. Pogledajmo broj $a^{2n} - b^{2n}$. Kako je $2n > 2$, ukoliko je $(a, b, 2n) \neq (2, 1, 6)$, odnosno $(a, b, n) \neq (2, 1, 3)$, prema teoremu 2.1 postoji prost broj p koji dijeli $a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n)$, ali ne dijeli $a^k - b^k$ za $k \in \{1, 2, \ldots, 2n-1\}$. Prema tome, p je prost broj koji dijeli $(a^n - b^n)(a^n + b^n)$, ali ne dijeli $a^n - b^n$ te zato p dijeli $a^n + b^n$. Ako bi p dijelio $a^m + b^m$ za neki $m \in \{1, 2, \ldots, n-1\}$, tada bi p dijelio i $(a^m + b^m)(a^m - b^m) = a^{2m} - b^{2m}$, što nije moguće zbog $2m < 2n$.

Dakle, za $(a, b, n) \neq (2, 1, 3)$ postoji prost broj p koji dijeli $a^n + b^n$, ali ne dijeli $a^k + b^k$, za $k \in \{1, 2, \ldots, n-1\}$. □

Primijetimo kako je $2^3 + 1^3 = 9$ i $2^1 + 1^1 = 3$ te je 3 jedini prost djelitelj od $2^3 + 1^3$, a dijeli i $2^1 + 1^1$.

Pogledajmo neke općenite rezultate koje možemo pokazati primjenom korolara 2.1.

Propozicija 2.1. *Neka je n prirodan broj veći od 3 te neka su a i b relativno prosti prirodni brojevi takvi da je $a > b$. Tada postoji prost broj p koji dijeli $a^n + b^n$, ali ne dijeli $a^k + b^k$ za $k \in \{n+1, n+2, \ldots, 2n\}$.*

Dokaz. Kako je n veći do 3, prema prethodnom korolaru postoji prost broj p takav da p dijeli $a^n + b^n$ i p ne dijeli $a^k + b^k$ za $k \in \{1, 2, \ldots, n-1\}$. Dokažimo najprije da je $p \neq 2$. Ako je $p = 2$, tada su a^n i b^n iste parnosti jer p dijeli njihovu sumu. Kako su prirodan broj i svaka njegova potencija iste parnosti, slijedi da su a i b također iste parnosti pa je i $a + b$ paran, odnosno $p = 2$ dijeli i $a + b$, što nije moguće. Prema tome, $p \geq 3$.

Pokažimo sada da p ne dijeli niti umnožak ab. U suprotnom je neki od brojeva a i b djeljiv s p te možemo uzeti da je a djeljiv s p. Tada je i a^n djeljiv s p pa je s p djeljiv i $(a^n + b^n) - a^n = b^n$, što znači da je i b djeljiv s p, ali tada a i b nisu relativno prosti, suprotno pretpostavci.

Neka je $k \in \{n+1, n+2, \ldots, 2n-1\}$. Tada je $k = n + i$ za neki $i \in \{1, 2, \ldots, n-1\}$. Kako p dijeli $a^n + b^n$ slijedi da p dijeli i

$$(a^n + b^n)(a^i + b^i) = a^{n+i} + b^{n+i} + a^n b^i + a^i b^n$$
$$= a^k + b^k + a^i b^i (a^{n-i} + b^{n-i}) = a^k + b^k + (ab)^i (a^{n-i} + b^{n-i}).$$

Ako bi p dijelio $a^k + b^k$, tada bi morao dijeliti i $(ab)^i(a^{n-i} + b^{n-i})$, što nije moguće jer p ne dijeli niti ab niti $a^{n-i} + b^{n-i}$.

Također p dijeli i

$$(a^n + b^n)^2 = a^{2n} + 2a^n b^n + b^{2n} = a^{2n} + b^{2n} + 2(ab)^n.$$

Ako bi p dijelio $a^{2n} + b^{2n}$, tada bi morao dijeliti i $2(ab)^n$, što nije moguće jer je $p > 2$ i p ne dijeli ab. Dakle, pokazali smo da p ne dijeli $a^k + b^k$ za $k \in \{n+1, n+2, \ldots, 2n\}$. □

Propozicija 2.2. *Neka je n prirodan broj veći od 1 te neka su a i b relativno prosti prirodni brojevi takvi da je $a > b$. Tada postoji prost broj p koji dijeli $a^{2n} + b^{2n}$, ali ne dijeli $a^k - b^k$ za $k \in \{1, 2, \ldots, n-1\}$.*

Dokaz. Kako je n veći od 1, slijedi da je $2n \geq 4$ te, prema korolaru 2.1, postoji prost broj p takav da p dijeli $a^{2n} + b^{2n}$, ali p ne dijeli $a^k + b^k$ za $k \in \{1, 2, \ldots, 2n-1\}$. Na isti način kao u dokazu prethodne propozicije možemo vidjeti da p ne dijeli umnožak ab.

Neka je $k \in \{1, 2, \ldots, n-1\}$. Kako p dijeli $a^{2n} + b^{2n}$, p dijeli i

$$(a^{2n} + b^{2n})(a^{2n-2k} + b^{2n-2k}) = a^{4n-2k} + b^{4n-2k} + a^{2n-2k}b^{2n-2k}(a^{2k} + b^{2k}).$$

Kako p ne dijeli $a^{2n-k} + b^{2n-k}$, p ne dijeli niti

$$(a^{2n-k} + b^{2n-k})^2 = a^{4n-2k} + 2a^{2n-k}b^{2n-k} + b^{4n-2k}.$$

Ukoliko p dijeli umanjenik, a ne dijeli umanjitelj, tada neće dijeliti niti razliku pa p ne dijeli

$$\begin{gathered}(a^{4n-2k} + b^{4n-2k} + a^{2n-2k}b^{2n-2k}(a^{2k} + b^{2k})) - \\ (a^{4n-2k} + 2a^{2n-k}b^{2n-k} + b^{4n-2k}) = \\ a^{2n-2k}b^{2n-2k}(a^{2k} + b^{2k}) - 2a^{2n-k}b^{2n-k} = \\ a^{2n-2k}b^{2n-2k}(a^{2k} + b^{2k} - 2a^k b^k) = \\ a^{2n-2k}b^{2n-2k}(a^k - b^k)^2,\end{gathered}$$

odakle slijedi da p ne dijeli niti $a^k - b^k$. □

3 Primjene Zsigmondyjeva teorema

U ovom ćemo poglavlju promotriti probleme u kojima se korištenjem Zsigmondyjevih teorema može izbjeći kompliciranija analiza i korištenje kompleksnijih metoda.

Najprije podsjetimo kako za prirodne brojeve a, b i n vrijede iduće jednakosti:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \tag{1}$$
$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - \cdots - ab^{2n-1} + b^{2n}).$$

Slijedi da $a-b$ dijeli $a^n - b^n$ dok $a+b$ dijeli $a^{2n+1} + b^{2n+1}$. Pogledajmo sada i jednu primjenu prethodnih rastava.

Propozicija 3.1. *Neka su a i b relativno prosti prirodni brojevi takvi da je $a > b$ te neka je n prirodan broj veći od 1.*

(*i*) *Ako je $a - b \geq 2$, $(a,b,n) \neq (2,1,6)$ i $(a+b,n) \neq (2^m,2)$ za prirodan broj m, tada $a^n - b^n$ nije potencija prostog broja.*

(*ii*) *Ako je n neparan i $(a,b,n) \neq (2,1,3)$, tada $a^n + b^n$ nije potencija prostog broja.*

Dokaz. Dokažimo prvi dio propozicije, drugi dio slijedi na isti način. Iz $a - b \geq 2$ slijedi da postoji prost broj koji dijeli $a-b$. Kako $a-b$ dijeli $a^n - b^n$, prost djelitelj od $a-b$ je prost djelitelj i od $a^n - b^n$.

Ukoliko je $(a,b,n) \neq (2,1,6)$ i $(a+b,n) \neq (2^m,2)$ za prirodan broj m, prema teoremu 2.1 postoji prost djelitelj od $a^n - b^n$ koji nije djelitelj od $a-b$. Zato $a^n - b^n$ ima barem dva prosta djelitelja pa ne može biti jednako potenciji prostog broja, jer je jedini prost djelitelj broja oblika p^m, pri čemu je p prost i m prirodan broj, upravo broj p. □

Pogledajmo direktnu primjenu prethodne propozicije u rješavanju diofantskih jednadžbi.

Primjer 3.1. *Odredimo sva rješenja jednadžbe $x^{2023} + y^{2023} = 19^z$ u skupu prirodnih brojeva.*

Rješenje. Ako su x i y relativno prosti, tada prema drugom dijelu propozicije 3.1, $x^{2023} + y^{2023}$ ne može biti jednako potenciji prostog broja 19. Pretpostavimo zato da x i y nisu relativno prosti. Kako svaki zajednički djelitelj od x i y dijeli $x^{2023} + y^{2023}$, tada mora dijeliti i 19^z pa postoje relativno prosti prirodni brojevi x_1 i y_1 te prirodni brojevi k_1 i k_2 takvi da je $x = 19^{k_1}x_1$, $y = 19^{k_2}y_1$ te 19 ne dijeli niti x_1 niti y_1. Sada je

$$x^{2023} + y^{2023} = 19^{2023k_1}x_1^{2023} + 19^{2023k_2}y_1^{2023}.$$

Možemo pretpostaviti da je $k_1 \geq k_2$, u suprotnom možemo zamijeniti uloge od x i y, te dobivamo

$$19^{2023k_2}(19^{2023k_1-2023k_2}x_1^{2023} + y_1^{2023}) = 19^z,$$

odakle je $z \geq 2023k_2$. Slijedi

$$19^{2023k_1-2023k_2}x_1^{2023} + y_1^{2023} = 19^{z-2023k_2}.$$

Kako je $19^{2023k_1-2023k_2}x_1^{2023} + y_1^{2023} \geq 2$, slijedi $z > 2023k_2$.

Ako je $k_1 = k_2$, dobivamo jednadžbu

$$x_1^{2023} + y_1^{2023} = 19^{z-2023k_2},$$

koja nema rješenja u skupu prirodnih brojeva prema drugom dijelu propozicije 3.1 jer su x_1 i y_1 relativno prosti.

Ako je $k_1 > k_2$, slijedi da 19 dijeli y_1^{2023} pa 19 dijeli i y_1, što nije moguće. Zato polazna jednadžba nema rješenja u skupu prirodnih brojeva. ◀

Primjer 3.2. *Odredimo sve uređene trojke prirodnih brojeva (a, b, p) takve da je p prost i vrijedi $2^a + p^b = 31^a$.*

Rješenje. Iz $2^a + p^b = 31^a$ dobivamo $31^a - 2^a = p^b$. Ako je $a > 2$, iz prvog dijela Propozicije 3.1 slijedi da $31^a - 2^a$ nije potencija prostog broja. Za $a = 2$ dobivamo $p^b = 31^2 - 2^2 = 957$, što nije potencija prostog broja. Za $a = 1$ je $p^b = 31 - 2 = 29$ te je jedina tražena uređena trojka $(a, b, p) = (1, 1, 29)$.◀

Primjer 3.3. *Odredimo sve uređene četvorke prirodnih brojeva (a, b, c, p), pri čemu je p prost broj, a neparan broj, dok su b i c veći od 1, takve da je $a^b - 1 = p^c$.*

Rješenje. Primijetimo da je $a^b - 1 = a^b - 1^b$. Ako je $(a, b) \neq (2, 6)$ i $(a + 1, b) \neq (2^m, 2)$, za prirodan broj m, prema prvom dijelu propozicije 3.1 broj $a^b - 1$ ne može biti jednak potenciji prostog broja.

Kako je a neparan, preostaje provjeriti slučaj $(a + 1, b) = (2^m, 2)$. Tada je $a = 2^m - 1$ i $a^b - 1 = p^c$ mora biti paran broj, odakle je $p = 2$. Dobivamo $a^2 - 1 = 2^c$, odakle je

$$2^c = (a-1)(a+1) = (a-1)2^m = ((a+1)-2)2^m = (2^m-2)2^m.$$

Dalje je $m \leq c$ te $2^m - 2 = 2^{c-m}$ i slijedi $2^{m-1} - 1 = 2^{c-m-1}$. Za $m = 1$ dobivamo $2^{c-m-1} = 0$, što nije moguće. Zato je $m \geq 2$ pa je 2^{c-m-1} neparan, što je moguće jedino za $c - m - 1 = 0$, odnosno $c = m + 1$. Tada je $2^{c-m-1} = 1$ pa je $2^{m-1} = 2$ i $m = 2$.

Iz $a = 2^m - 1$ slijedi $a = 3$, dok $c = m + 1$ daje $c = 3$. Jedina uređena četvorka (a, b, c, p) s traženim svojstvom je $(3, 2, 3, 2)$. ◀

Prethodni se primjer pojavio 2001. godine u sklopu natjecanja u Sjedinjenim Američkim Državama.

U određenim situacijama nije moguće odmah primijeniti niti teorem 2.1 niti propoziciju 3.1, već je potrebno najprije provesti odgovarajuće transformacije. Do takvih se transformacija često može doći promatranjem ostataka pri dijeljenju s pojedinim prirodnim brojevima, što ćemo ilustrirati na iduća dva primjera. Pri tome ćemo se koristiti Binomnim teoremom, prema kojem za realne brojeve a i b te prirodan broj n vrijedi

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Primjer 3.4. *Odredimo sve uređene trojke prirodnih brojeva (a,b,n) takve da je $n \geq 2$ i vrijedi $3^b - 1 = a^n$.*

Rješenje. Iz $3^b - 1 = a^n$ slijedi da je $a^n + 1 = 3^b$ te je $a^n + 1$ djeljivo s 3. Prema tome, a ne može biti djeljiv s 3 te je ili $a = 3k+1$ ili $a = 3k-1$ za neki nenegativan cijeli broj k. Ako je n paran, možemo ga zapisati u obliku $n = 2m$, za neki prirodan broj m, te primjenom Binomnog teorema dobivamo

$$\begin{aligned}
(3k+1)^n = (3k+1)^{2m} &= \sum_{i=0}^{2m} \binom{2m}{i} (3k)^i \cdot 1^{2m-i} \\
&= \left(\sum_{i=1}^{2m} \binom{2m}{i} (3k)^i \right) + 1 = 3l_1 + 1, \\
(3k-1)^n = (3k+(-1))^{2m} &= \sum_{i=0}^{2m} \binom{2m}{i} (3k)^i \cdot (-1)^{2m-i} \\
&= \left(\sum_{i=1}^{2m} \binom{2m}{i} (3k)^i \cdot (-1)^{2m-i} \right) + (-1)^{2m} = 3l_2 + 1,
\end{aligned}$$

za

$$l_1 = \sum_{i=1}^{2m} \binom{2m}{i} 3^{i-1} k^i, l_2 = \sum_{i=1}^{2m} \binom{2m}{i} 3^{i-1} k^i \cdot (-1)^{2m-i}.$$

Dakle, za paran n je $a^n + 1$ oblika $3l + 2$, što nije djeljivo s 3. Zato n mora biti neparan i, prema drugom dijelu Propozicije 3.1, ukoliko je $(a,n) \neq (2,3)$, $a^n + 1$ ne može biti potencija prostog broja.

Preostaje provjeriti slučaj $(a,n) = (2,3)$. Tada je $3^b = 2^3 + 1 = 9$ te $b = 2$. Jedina je uređena trojka s danim svojstvom $(a,b,n) = (2,2,3)$. ◄

Kažemo da je prirodan broj *a potpun kvadrat* ako postoji prirodan broj b takav da je $a = b^2$. Primjerice, brojevi 1, 4 i 100 su potpuni kvadrati, dok brojevi 6, 17 i 50 nisu.

Primjer 3.5. *Odredimo sve nenegativne cijele brojeve k i l takve da je $3^k - 5^l$ potpun kvadrat.*

Rješenje. Neka je a prirodan broj takav da je $3^k - 5^l = a^2$. Ako je a paran, možemo ga zapisati u obliku $2t$, za neki prirodan broj t, te je $a^2 = (2t)^2 = 4t^2$. Ako je a neparan, možemo ga zapisati u obliku $2t + 1$, za neki nenegativan cijeli broj t, pa je $a^2 = (2t + 1)^2 = 4(t^2 + t) + 1$, odnosno a^2 je ili oblika $4n$ ili oblika $4n + 1$ za nenegativan cijeli broj n.

Pretpostavimo da je k neparan te ga zapišimo u obliku $k = 2m + 1$, za nenegativan cijeli broj m. Tada je

$$\begin{aligned} 3^k - 5^l &= (4-1)^{2m+1} - (4+1)^l \\ &= \sum_{i=0}^{2m+1} \binom{2m+1}{i} 4^i \cdot (-1)^{2m+1-i} - \sum_{j=0}^{l} \binom{l}{j} 4^j \cdot 1^{l-j} \\ &= \left(\sum_{i=1}^{2m+1} \binom{2m+1}{i} 4^i \cdot (-1)^{2m+1-i} \right) + (-1)^{2m+1} - \sum_{j=1}^{l} \binom{l}{j} 4^j - 1 \\ &= 4(n_1 + n_2) - 2 = 4(n_1 + n_2 - 1) + 2, \end{aligned}$$

za

$$n_1 = \sum_{i=1}^{2m+1} \binom{2m+1}{i} 4^{i-1} \cdot (-1)^{2m+1-i}, n_2 = \sum_{j=1}^{l} \binom{l}{j} 4^{j-1}.$$

Prema tome, ako je k neparan, $3^k - 5^l$ nije niti oblika $4n$ niti oblika $4n + 1$, za nenegativan cijeli broj n, pa ne može biti potpun kvadrat. Zato k mora biti paran te ga zapišimo u obliku $k = 2m$, za prirodan broj m. Sada je $3^{2m} - 5^l = a^2$ te $(3^m)^2 - a^2 = 5^l$, odakle je $(3^m - a)(3^m + a) = 5^l$.

Kako je desna strana prethodne jednakosti potencija prostog broja, i svi faktori s lijeve strane jednakosti moraju biti potencije istog prostog broja te postoje nenegativni cijeli brojevi r i s takvi da je $3^m - a = 5^r$ i $3^m + a = 5^s$. Zbog $3^m - a \leq 3^m + a$ dobivamo $r \leq s$.

Iz $5^r + 5^s = (3^m - a) + (3^m + a)$ slijedi $5^r + 5^s = 2 \cdot 3^m$. Ako je $r \geq 1$, zbog $r \leq s$ dobivamo da su i 5^r i 5^s djeljivi s 5, no tada je i $5^r + 5^s$ djeljivo s 5, što nije moguće jer je $5^r + 5^s = 2 \cdot 3^m$, a 5 ne dijeli $2 \cdot 3^m$. Zato je $r = 0$ te $5^s + 1 = 2 \cdot 3^m$.

Ukoliko je $s \geq 2$, možemo iskoristiti Korolar 2.1 te dobivamo da postoji prost djelitelj od $5^s + 1$ koji ne dijeli $5 + 1 = 6$ pa ne može dijeliti niti $2 \cdot 3^m$.

Za $s = 0$ dobivamo $2 \cdot 3^m = 5^0 + 1 = 2$ te je i $m = 0$. Zato je i $k = 2m = 0$, dok iz $3^m - a = 5^r$ slijedi $a = 0$. Koristeći $3^k - 5^l = a^2$ dobivamo $5^l = 1$ te $l = 0$. Prvo je rješenje $(k, l) = (0, 0)$.

Za $s = 1$ dobivamo $2 \cdot 3^m = 5 + 1 = 6$ pa je $m = 1$ te $k = 2$. Iz $3^m - a = 5^r$ je sada $a = 2$. Uvrstimo li $k = 2$ i $a = 2$ u $3^k - 5^l = a^2$ dobivamo $5^l = 5$ te $l = 1$. Drugo rješenje je $(k, l) = (2, 1)$. ◀

Idući je primjer bio zadan na češko-slovačkom natjecanju 1996. godine.

Primjer 3.6. *Odredimo sve uređene trojke prirodnih brojeva (a, b, p) takve da je p prost i vrijedi $p^a - b^p = 1$.*

Rješenje. Pogledajmo najprije slučaj $p = 2$. Tada je $2^a - b^2 = 1$, odnosno $b^2 + 1 = 2^a$. Ako je b paran, zapišimo ga u obliku $2k$, za neki prirodan broj k, odakle je $b^2 + 1 = 4k^2 + 1$. Ako je b neparan, zapišimo ga u obliku $2k + 1$, za neki nenegativan cijeli broj k, te dobivamo $b^2 + 1 = 4k^2 + 4k + 2 = 4(k^2 + k) + 2$. Zato $b^2 + 1$ nije djeljiv s 4 te slijedi $a = 1$. Dalje je $b^2 + 1 = 2$ i $b = 1$. Jedna tražena uređena trojka (a, b, p) je $(1, 1, 2)$.

Neka je sada p neparan prost broj. Uočimo kako je tada $b > 1$ zbog $b^p + 1 = p^a$. Primjenom drugog dijela Propozicije 3.1 dobivamo da $b^p + 1$ nije potencija prostog broja za $(b, p) \neq (2, 3)$. Ako je $(b, p) = (2, 3)$, dobivamo $3^a = 2^3 + 1$, odakle je $a = 2$. Druga je tražena uređena trojka $(a, b, p) = (2, 2, 3)$. ◀

Primjer 3.7. *Odredimo sve prirodne brojeve a, m i n takve da $a^m + 1$ dijeli $(a + 1)^n$.*

Rješenje. Ako je $m \geq 2$, $a \geq 2$ i $(a, m) \neq (2, 3)$, prema korolaru 2.1 postoji prost djelitelj od $a^m + 1$ koji ne dijeli $a + 1$ pa ne dijeli niti $(a + 1)^n$. Dakle, uz navedene uvjete $a^m + 1$ ne dijeli $(a + 1)^n$.

Pogledajmo preostale slučajeve.

Za $m = 1$ je $a^m + 1 = a + 1$ što očito dijeli $(a + 1)^n$.

Za $a = 1$ je $a^m + 1 = 2$, što dijeli 2^n.

Za $(a, m) = (2, 3)$ dobivamo $a^m + 1 = 9$ što dijeli $(a + 1)^n = 3^n$ čim je $n \geq 2$.

Sveukupno zaključujemo da $a^m + 1$ dijeli $(a + 1)^n$ jedino ako je $m = 1$, $a = 1$ ili $(a, m) = (2, 3)$ uz $n \geq 2$. ◀

Napomenimo kako se prethodni primjer nalazio u užem izboru za Međunarodnu matematičku olimpijadu 2000. godine.

Kao idući primjer navodimo zadatak koji je 2011. godine bio zadan na Japanskoj matematičkoj olimpijadi te iz kojeg možemo vidjeti kako primjenom Zsigmondyjeva teorema efikasno zaobilazimo dubinsku analizu problema te ga svodimo na proučavanje nekolicine specijalnih slučajeva.

Primjer 3.8. *Odredimo sve uređene petorke prirodnih brojeva (a, n, p, q, r) takve da je*

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1). \tag{2}$$

Rješenje. Ako je $a \geq 3$, tada je $a^p - 1 \geq 2$, $a^q - 1 \geq 2$ i $a^r - 1 \geq 2$, odakle je i $a^n - 1 > a^p - 1$, $a^n - 1 > a^q - 1$ i $a^n - 1 > a^r - 1$, odnosno n je veći od svakog od brojeva p, q i r. Ukoliko je, uz $a \geq 3$, također i $n \geq 3$, po teoremu 2.1 postoji prost djelitelj od $a^n - 1$ koji ne dijeli niti $a^p - 1$ niti $a^q - 1$ niti $a^r - 1$ pa ne dijeli niti njihov produkt te u tom slučaju ne postoji tražena uređena petorka.

Ovim smo ispitivanje sveli na slučajeve u kojima je $a \leq 2$ ili $n \leq 2$.

Ako je $a = 1$, tada je jednakost (2) ispunjena za sve prirodne brojeve n, p, q, r. Nadalje možemo pretpostaviti da je $a \geq 2$.

Za $n = 1$ dobivamo $a - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$. Iz $a \geq 2$ slijedi $a^m - 1 \geq a - 1$ i $a^m - 1 \geq 1$, za svaki prirodan broj m, pa je $a - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$ jedino ako je $a^p - 1 = a^q - 1 = a^r - 1 = a - 1 = 1$, tj. $a = 2$ i $p = q = r = 1$, odnosno $(a, n, p, q, r) = (2, 1, 1, 1, 1)$.

Za $n = 2$ dobivamo $a^2 - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$. Ako je neki od p, q, r veći ili jednak 3, produkt $(a^p - 1)(a^q - 1)(a^r - 1)$ je veći ili jednak $a^3 - 1$, što je veće od $a^2 - 1$ zbog pretpostavke $a \geq 2$. Ako je jedan od p, q, r jednak 2, dobivamo da je produkt dvaju faktora s lijeve strane jednakosti (2) jednak 1, što je moguće jedino za $a = 2$ i $(p, q, r) \in \{(2, 1, 1), (1, 2, 1), (1, 1, 2)\}$, odnosno

$$(a, n, p, q, r) \in \{(2, 2, 2, 1, 1), (2, 2, 1, 2, 1), (2, 2, 1, 1, 2)\}.$$

Preostaje još mogućnost $p = q = r = 1$, koja vodi na $a^2 - 1 = (a - 1)^3$, odnosno $a + 1 = (a - 1)^2$. Iz navedene jednakosti dobivamo kvadratnu jednadžbu $a^2 - 3a = 0$, čija su rješenja $a = 0$ i $a = 3$, čime dobivamo traženu uređenu petorku $(a, n, p, q, r) = (3, 2, 1, 1, 1)$.

Za $a = 2$ dobivamo $2^n - 1 = (2^p - 1)(2^q - 1)(2^r - 1)$ te odmah dobivamo rješenja

$$(a, n, p, q, r) \in \{(2, n, n, 1, 1), (2, n, 1, n, 1), (2, n, 1, 1, n) : n \in \mathbb{N}\}.$$

Nadalje možemo pretpostaviti i $n \geq 3$, jer smo već riješili slučajeve $n \in \{1, 2\}$, te $p < n, q < n$ i $r < n$. Ako je $n \neq 6$, prema teoremu 2.1 postoji prost djelitelj od $2^n - 1$ koji ne dijeli niti $2^p - 1$ niti $2^q - 1$ niti $2^r - 1$ pa ne dijeli niti $(2^p - 1)(2^q - 1)(2^r - 1)$. Za $n = 6$ dobivamo $63 = (2^p - 1)(2^q - 1)(2^r - 1)$, odnosno

$$3 \cdot 3 \cdot 7 = (2^p - 1)(2^q - 1)(2^r - 1),$$

što daje preostala rješenja

$$(a, n, p, q, r) \in \{(2, 6, 2, 2, 3), (2, 6, 2, 3, 2), (2, 6, 3, 2, 2)\}. \qquad \blacktriangleleft$$

Pogledajmo na koji nam način rezultat koji je osnova ovog rada može pružiti i kombinatorne temelje za dobivanje informacija o broju djelitelja prirodnog broja.

Primjer 3.9. *Ako su p i q različiti neparni prosti brojevi te a prirodan broj veći od 1, dokažimo da $a^{pq}-1$ ima barem 8 pozitivnih djelitelja.*

Rješenje. Osnova za dobivanje broja djelitelja je upravo poznavanje prostih djelitelja promatranog broja. Možemo uzeti da je $p > q$. Kako su p i q neparni, njihov je umnožak pq također neparan. Zato, prema teoremu 2.1, postoji prost djelitelj d_1 od $a^{pq}-1$ koji ne dijeli a^k-1 za $k \in \{1, 2, \ldots, pq-1\}$.

Iz $a^{pq}-1 = (a^p)^q - (1^p)^q = (a^q)^p - (1^q)^p$ i tvrdnje (1) slijedi da i a^p-1 i a^q-1 dijele $a^{pq}-1$. Kako je p neparan, prema teoremu 2.1 postoji prost djelitelj d_2 od a^p-1 koji ne dijeli a^q-1. Zbog toga što a^p-1 dijeli $a^{pq}-1$ je d_2 i prost djelitelj od $a^{pq}-1$ te je $d_1 \neq d_2$ jer d_1 ne dijeli a^p-1.

Svaki prirodan broj veći od 1 ima prost djelitelj pa tako postoji i prost djelitelj d_3 od a^q-1. Na isti način kao i za d_2 možemo zaključiti da je d_3 prost djelitelj od $a^{pq}-1$ koji je različit i od d_1 i od d_2.

Na ovaj smo način došli do tri različita prosta djelitelja d_1, d_2, d_3 broja $a^{pq}-1$. Sada su 1, d_1, d_2, d_3, d_1d_2, d_1d_3, d_2d_3 i $d_1d_2d_3$ traženih 8 pozitivnih djelitelja broja $a^{pq}-1$. ◀

Kažemo da je niz realnih brojeva (a_n) *geometrijski niz* ako kvocijent $\frac{a_{n+1}}{a_n}$ ne ovisi o prirodnom broju n, odnosno ukoliko postoji realan broj q takav da je $\frac{a_{n+1}}{a_n} = q$ za svaki prirodan broj n. Takav broj q nazivamo *kvocijent* geometrijskog niza. Za prirodan broj n, $n \geq 2$, vrijedi

$$\frac{a_n}{a_{n-1}} = \frac{a_{n+1}}{a_n},$$

odakle dobivamo da su tri uzastopna člana geometrijskog niza povezana relacijom $a_n^2 = a_{n-1}a_{n+1}$. Često je vrlo interesantno ispitivati postoje li u danom nizu članovi s određenim svojstvom, pri čemu također od pomoći može biti Zsigmondyjev teorem. Pogledajmo takvu situaciju na primjeru zadatka s rumunjskog matematičkog natjecanja iz 1994.

Primjer 3.10. *Pokažimo da niz (a_n), pri čemu je $a_n = 3^n - 2^n$, ne sadrži tri uzastopna člana geometrijskog niza.*

Rješenje. Pretpostavimo suprotno, odnosno neka postoje prirodni brojevi k, l i m takvi da je $k < l < m$ te

$$(3^l - 2^l)^2 = (3^k - 2^k)(3^m - 2^m). \tag{3}$$

Prema teoremu 2.1 postoji prost broj p koji dijeli $3^m - 2^m$ te koji ne dijeli $3^n - 2^n$ za $n \in \{1, 2, \ldots, m-1\}$. Zato p dijeli desnu stranu jednakosti (3), ali ne i lijevu stranu te jednakosti, što nije moguće. Zato promatrani niz ne sadrži tri uzastopna člana nekog geometrijskog niza. ◀

Primijetimo kako nam poznavanje iskaza teorema 2.1 omogućava i generalizaciju brojnih rezultata. Primjerice, u prethodnom smo primjeru umjesto niza čiji je n-ti član dan s $3^n - 2^n$ mogli promatrati i mnogo općenitiji niz s n-tim članom oblika $a^n - b^n$, pri čemu je $(a, b) \neq (2, 1)$ te $a + b$ nije potencija broja 2. Na taj način izbjegavamo posebne slučajeve navedene u teoremu 2.1 i rješenje može ići na potpuno isti način. Konkretno, mogli smo promatrati i niz dan s $a_n = 11^n - 7^n$ ili s $a_n = 2023^n - 2022^n$.

Literatura

[1] G. D. Birkhoff, H. S. Vandiver, *On the integral divisors of $a^n - b^n$*, Ann. of Math., **5**(4) (1904), 173–180.

[2] A. Loo, *Zsigmondy's Theorem*, Math. Excalibur, **16**(4) (2012).

[3] I. Matić, *Uvod u teoriju brojeva*, Sveučilište J. J. Strossmayera u Osijeku, Odjel za matematiku, Osijek, 2015.

[4] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc., **125** (1997), 1913–1919.