Diofantski problemi sa sumama djelitelja

Bujačić Babić, Sanda

Doctoral thesis / Disertacija

2014

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:971358

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb



Sveučilište u Zagrebu

PRIRODOSLOVNO - MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Sanda Bujačić

Diofantski problemi sa sumama djelitelja

DOKTORSKI RAD

Zagreb, 2014.



University of Zagreb

FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Sanda Bujačić

Diophantine Problems With Sums of Divisors

DOCTORAL THESIS

Zagreb, 2014



Sveučilište u Zagrebu

PRIRODOSLOVNO - MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Sanda Bujačić

Diofantski problemi sa sumama djelitelja

DOKTORSKI RAD

Mentor: prof. dr. sc. Andrej Dujella

Zagreb, 2014.



University of Zagreb

FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Sanda Bujačić

Diophantine Problems With Sums of Divisors

DOCTORAL THESIS

Supervisor: prof. dr. sc. Andrej Dujella

Zagreb, 2014

Zahvala

Iznimno se zahvaljujem svom mentoru, akademiku Andreju Dujelli, koji mi je bio iznimna pomoć i potpora u izradi doktorskog rada od njegovog samog početka, odnosno od prijedloga teme doktorskog rada i razrade glavnog materijala pa sve do njegove finalne verzije.

Uz mentora podršku mi je uvijek nesebično pružala i moja obitelj, posebice mama Anka, tata Anton, sestra Lidija i dečko Arsen kojima se od srca zahvaljujem na svim konstruktivnim savjetima i konstantnom razumijevanju tijekom mog doktorskog studija.

Sadržaj

Uvod **1**

1 Fiksni koeficijenti linearnog polinoma $\delta n + \varepsilon$ **5**
1.1 Slučaj $\delta = 2$ 5
1.2 Slučaj $\delta = 4$ 8
1.3 Slučaj $\varepsilon = 0$ 17
1.4 Slučaj $\delta = 0$ 22

2 Jednoparametarske familije koeficijenata linearnog polinoma $\delta n + \varepsilon$ **27**
2.1 Slučaj $\varepsilon = \delta + 2$ 28
2.2 Slučaj $\varepsilon = \delta - 2$ 35

3 O verziji Subbaraove kongruencije **56**
3.1 Uvod 56
3.2 Verzija Subbaraove kongruencije za $n = 2^\alpha 5^\beta$ 57

Bibliografija **81**

Sažetak **83**

Summary **85**

Životopis **86**

Uvod

Diofantske jednadžbe, nazvane po starogrčkom matematičaru Diofantu iz Aleksandrije (3. stoljeće), jedan su od središnjih koncepata kako klasične, tako i moderne teorije brojeva. Matematički problemi koji se prikazuju diofantskim jednadžbama sežu daleko u povijest, te zauzimaju središnje mjesto u razrješavanju vrlo poznatog Arhimedovog problema stada, prilikom određivanja Pitagorinih trojki i u mnogim drugim klasičnim matematičkim problemima. Danas, u teoriji brojeva vrlo su aktualne moderne metode za rješavanje diofantskih jednadžbi koje proizlaze iz diofantskih aproksimacija (primjerice, Bakerova teorija linearnih formi u logaritmima) pomoću kojih je uvijek moguće dobiti gornje ograde za veličinu rješenja različitih diofantskih jednadžbi koje se kasnije reduciraju nekom od postojećih metoda za redukciju.

Y. F. Bilu i R. F. Tichy u [4] promatraju diofantsku jednadžbu oblika

$$f(x) = g(y), \tag{1}$$

gdje su f, g polinomi s racionalnim koeficijentima, te nastoje odrediti ima li navedena jednadžba konačno ili beskonačno mnogo rješenja u cijelim brojevima (ili racionalnim brojevima s ograničenim nazivnikom) x, y. Jedan od koraka koji se provodi prilikom odgovaranja na to pitanje je dekompozicija polinoma f i g.

U radu [2] objavljenom 2007. godine M. Ayad i F. Luca dokazuju da ne postoji neparan prirodan broj $n > 1$ te dva pozitivna djelitelja d_1, d_2 broja $(n^2 + 1)/2$ takva da vrijedi

$$d_1 + d_2 = n + 1.$$

Na taj je način dobiven alternativni dokaz tvrdnje da je za prost broj p i različite kompleksne brojeve a, b primitivna funkcija polinoma

$$((x - a)(x - b))^{(p^2-1)/2}$$

indekompozabilna nad poljem kompleksnih brojeva. Ovaj rezultat primjenom Bilu - Tichyjevog kriterija iz [4] ima direktne posljedice na konačnost rješenja izvjesnih diofantskih jednadžbi.

Problem iz [2] se može poopćiti. Ako se linearni polinom $n + 1$ zamijeni općenitim linearnim polinomom $\delta n + \varepsilon$, novi je problem pronaći (ili dokazati da ne postoje) besko-

načno mnogo neparnih prirodnih brojeva $n > 1$ te djelitelje d_1, d_2 od $(n^2+1)/2$ za koje vrijedi jednakost

$$d_1 + d_2 = \delta n + \varepsilon. \tag{2}$$

Budući da je broj $(n^2+1)/2$ neparan, a djelitelji d_1, d_2 dijele sumu kvadrata dva relativno prosta broja, znamo nešto više o djeliteljima d_1, d_2, preciznije vrijedi $d_1, d_2 \equiv 1 \pmod 4$. Stoga, iz (2) proizlaze dvije mogućnosti: ili su koeficijenti δ, ε neparni brojevi, ili su δ, ε parni brojevi, odnosno, preciznije, vrijedi kongruencija

$$\delta \equiv \varepsilon + 2 \equiv 0, 2 \pmod 4. \tag{3}$$

U članku [10] iz 2012. godine, A. Dujella i F. Luca promatraju navedeni problem za neparne koeficijente δ, ε. Postavljaju slutnju da, ako su $\delta > 0$ i ε relativno prosti cijeli brojevi i $(\delta, \varepsilon) \neq (1, 1)$, tada postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoje pozitivni djelitelji d_1, d_2 od $(n^2+1)/2$ takvi da je $d_1 + d_2 = \delta n + \varepsilon$. U prvom dijelu rada slutnju dokazuju za slučaj $\delta = 1$ prikazujući problem pellovskom, odnosno pripadnom Pellovom jednadžbom, kojoj određuju beskonačno mnogo rješenja putem kojih određuju i beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju navedena svojstva. Također, u radu je dokazana tvrdnja da ne postoji neparan prirodan broj n sa svojstvom da postoji par pozitivnih djelitelja d_1, d_2 od $(n^2+1)/2$ za koje vrijedi $d_1 + d_2 = \delta n + \delta$. Za općenite linearne polinome kojima su koeficijenti relativno prosti prirodni brojevi pristup problemu je već na samom početku dokaza korjenski drugačiji od prethodno navedenih dokaza. Pellova jednadžba čija se rješenja koriste u određivanju beskonačno mnogo neparnih prirodnih brojeva $n > 1$ koji zadovoljavaju spomenuto svojstvo je oblika

$$U^2 - abcV^2 = 1, \tag{4}$$

gdje se zahtijeva da su a, b, c prosti brojevi koji zadovoljavaju uvjete definirane Legendreovim, odnosno Jacobijevim simbolima određenima faktorizacijama $(U_0 - 1)(U_0 + 1) = abcV_0^2$, a gdje je (U_0, V_0) fundamentalno rješenje od (4). Tvrdnja je uvjetno dokazana, a uvjetovana je valjanostima poznatih slutnji o distribuciji prostih brojeva.

U prva dva poglavlja ovog doktorskog rada se ispituje postoji li beskonačno mnogo neparnih prirodnih brojeva $n > 1$ za koje postoje djelitelji d_1, d_2 od $(n^2+1)/2$ za koje vrijedi jednakost (2), gdje su koeficijenti linearnog polinoma δ, ε parni brojevi, odnosno vrijedi (3). U prvom poglavlju rada dokazujemo da postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoje djelitelji d_1, d_2 od $(n^2+1)/2$ za koje vrijedi (2) pri čemu je odabran fiksni koeficijent δ linearnog polinoma $\delta n + \varepsilon$. U prvom slučaju navedenu tvrdnju dokazujemo za $\delta = 2$, $\varepsilon \equiv 0 \pmod 4$, dok je u drugom slučaju poglavlja $\delta = 4$, te $\varepsilon \equiv 2 \pmod 4$. Bezuvjetno je dokazano da postoji beskonačno mnogo neparnih prirodnih

brojeva n koji zadovoljavaju navedeno svojstvo. Koristeći identitet

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1d_2,$$

u mogućnosti smo proučavane probleme prikazati pellovskom jednadžbom te uvjetujući da je njena desna strana potpuni kvadrat, ujedno i osigurati da promatarana pellovska jednadžba ima beskonačno mnogo rješenja. Rješavanjem pripadne Pellove jednadžbe dobivamo beskonačno mnogo rješenja koja koristimo prilikom određivanja traženih neparnih prirodnih brojeva n i djelitelja d_1, d_2 od $(n^2+1)/2$ koji zadovoljavaju (2). U radu su detaljno navedeni dokazi za slučajeve $\delta = 2$ i $\delta = 4$, te je određeno beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju navedeno svojstvo i gdje su djelitelji d_1, d_2 od $(n^2+1)/2$ relativno prosti brojevi. Dokaz slučaja $\delta = 4$ bitno je drugačiji od dokaza slučaja $\delta = 2$ i dokaza iz [10] jer se dokaz razlaže na dva podslučaja u ovisnosti o tome je li $\varepsilon \equiv 2 \pmod 8$ ili $\varepsilon \equiv 6 \pmod 8$. Podslučaj koji je bitno drugačiji je onaj u kojem je $\varepsilon \equiv 2 \pmod 8$. U tom podslučaju eksperimentalnim podacima koji su eksplicitno navedeni u radu utvrđen je $\mathrm{nzd}(d_1, d_2)$ na osnovu kojega je izgrađen dokaz za taj podslučaj. Dakle, i za $\delta = 2$ i $\delta = 4$ u radu dokazano je da možemo pronaći beskonačno mnogo neparnih prirodnih brojeva n i dva djelitelja d_1, d_2 od $(n^2+1)/2$ za koja vrijedi (2).

U nastavku poglavlja razmatra se slučaj u kojem je $\delta \equiv 2 \pmod 4$ te $\varepsilon = 0$. Za $\delta = 2$ dokazano je da postoji beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju navedeno svojstvo i pritom su djelitelji d_1, d_2 broja $(n^2+1)/2$ nužno relativno prosti brojevi, dok je u slučaju kad je $\delta \equiv 2 \pmod 4$, $\delta \geq 6$, dokazano uz pomoć kriterija za rješivost pellovskih jednadžbi iz [15], da takvi neparni prirodni brojevi n ne postoje.

Ovaj je dio doktorskog rada u cijelosti uvršten u članak [5] koji je prihvaćen za objavljivanje u časopisu Miskolc Mathematical Notes.

Za slučaj $\varepsilon = 0$ proučavani problem svodi se na pitanje možemo li svaki prirodni broj $\varepsilon \equiv 2 \pmod 4$ prikazati kao zbroj dvaju prirodnih brojeva d_1, d_2, gdje su svi prosti faktori od d_1, d_2 oblika $4k+1$, $k \in \mathbb{N}$. Ako zahtijevamo da djelitelji d_1, d_2 budu prosti brojevi, problem podsjeća na jaku (binarnu) formu Goldbachove slutnje. U potpoglavlju su pokazani rezultati za slučaj $\delta = 0$ drugih autora, posebice R. Dietmanna i C. Elsholtza iz [7].

U drugom poglavlju rada je promatran sličan, problem gdje su koeficijenti linearnog polinoma $\delta n + \varepsilon$ u međusobnoj ovisnosti. Naime, promatraju se jednoparametarske familije koeficijenata takve da je u jednom slučaju $\varepsilon = \delta + 2$, dok je u drugom slučaju $\varepsilon = \delta - 2$. U prvom od navedenih slučajeva dokazujemo da postoji beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju navedeno svojstvo. U poglavlju je dokazano i sljedeće zanimljivo svojstvo. Naime, svaka dva polinoma koja su generirana neparnim prirodnim brojevima n određenim susjednim članovima rekurzivnog niza $(U_m,\ m \geq 0)$, gdje je $U_m,\ m \geq 0$ niz prvih komponenti rješenja Pellove jednadžbe iz dokaza teorema,

imaju zajedničku nultočku.

U drugom dijelu drugog poglavlja razmatraju se slučajevi u kojima vrijedi $\varepsilon = \delta - 2$. Radna hipoteza je da postoji beskonačno mnogo neparnih prirodnih brojeva n te djelitelji d_1, d_2 od $(n^2+1)/2$ za koje vrijedi jednakost $d_1 + d_2 = \delta n + \delta - 2$. Problem ovakvog tipa razložen je na četiri podslučaja u ovisnosti o klasi ostataka kojoj pripada parni broj δ pri dijeljenju brojem 8. Određena je Pellova jednadžba oblika (4) koja se prikazuje kao $(U-1)(U+1) = 2abcV^2$. Uvjetovano je da su brojevi a, b, c prosti brojevi nakon čega su detaljno određeni uvjeti koje navedena faktorizacija treba zadovoljavati te se naposlijetku Legendreovim, odnosno Jacobijevim simbolima svi ostali, nepovoljni, uvjeti isključuju. Metoda dokaza počiva na valjanosti Schinzelove hipoteze H o distribuciji prostih brojeva iz [22]. Na ovaj način smo u mogućnosti dobiti beskonačno mnogo Pellovih jednadžbi oblika (4), a kao posljedicu toga i beskonačno mnogo neparnih prirodnih brojeva n koji zadovljavaju navedeno svojstvo. U radu su detaljno prikazani slučajevi $\delta \equiv 4, 6 \pmod 8$, dok su slučajevi $\delta \equiv 0, 2 \pmod 8$ izuzeti iz razmatranja jer na njih nije moguće primjeniti korištene metode.

U posljednjem poglavlju rada promatra se verzija Subbaraove kongruencije oblika

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)}, \tag{5}$$

gdje je φ Eulerova funkcija, a σ funkcija sume djelitelja prirodnog broja n. U radu [11] A. Dujella i F. Luca promatraju kongruenciju (5) i dokazuju da postoji samo konačno mnogo prirodnih brojeva n koji zadovoljavaju ovu verziju Subbaraove kongruencije i čiji su prosti faktori elementi konačnog i fiksiranog skupa. U radu se ispituje koji prirodni brojevi čiji su prosti faktori elementi skupa $\{2, 5\}$, odnosno koji su oblika $n = 2^\alpha 5^\beta,\ \alpha, \beta \geq 0$, zadovoljavaju kongruenciju (5). U dokazu glavnog teorema ovog poglavlja problem je prikazan diofantskom jednadžbom oblika

$$x^2 + y^2 - 501 = c(x-1)(y-1),\ \ c \equiv 17 \pmod{30}.$$

Uz pomoć Worleyjevog teorema i Leme iz [9] dobiva se konačno mnogo diofantskih jednadžbi navedenog oblika nakon čega je izračunavanjem svih njihovih rješenja dokazano da su jedini prirodni brojevi oblika $n = 2^\alpha 5^\beta,\ \alpha, \beta \geq 0$ koji zadovoljavaju verziju Subbaraove kongruencije brojevi $n = 1, 2, 5, 8$.

Poglavlje 1

Fiksni koeficijenti linearnog polinoma $\delta n + \varepsilon$

U jednom dijelu doktorskog rada ispitujemo postoji li beskonačno mnogo neparnih prirodnih brojeva n za koje vrijedi da postoje djelitelji d_1, d_2 broja $(n^2+1)/2$ takvi da je

$$d_1 + d_2 = \delta n + \varepsilon,$$

pri čemu je $\delta \equiv \varepsilon + 2 \equiv 0, 2 \pmod 4$. U prvom poglavlju doktorskog rada ispitujemo postoji li beskonačno mnogo neparnih prirodnih brojeva n s navedenim svojstvom za fiksne koeficijente linearnog polinoma $\delta n + \varepsilon$, odnosno, preciznije, ispitujemo postoji li beskonačno mnogo neparnih prirodnih brojeva n takvih da postoje djelitelji d_1, d_2 od $(n^2+1)/2$ takvi da vrijedi $d_1 + d_2 = \delta n + \varepsilon$ za $\delta = 2$, $\delta = 4$ te $\varepsilon = 0$.

U slučajevima kad su $\delta = 2$ i $\delta = 4$ dokazujemo da postoji beskonačno mnogo neparnih prirodnih brojeva n s navedenim svojstvom i navodimo jedan od načina generiranja beskonačno mnogo takvih neparnih prirodnih brojeva n. U slučaju kad je $\delta = 2,\ \varepsilon = 0$ određujemo način generiranja beskonačno mnogo neparnih prirodnih brojeva n s traženim svojstvom i ujedno određujemo sve takve neparne prirodne brojeve n, dok u slučaju kad je $\delta \equiv 2 \pmod 4,\ \delta \geq 6,\ \varepsilon = 0$ dokazujemo da ne postoji nijedan neparan prirodan broj n koji zadovoljava navedene uvjete.

1.1 Slučaj $\delta = 2$

U prvom potpoglavlju dokazujemo da postoji beskonačno mnogo neparnih prirodnih brojeva n takvih da postoje dva djelitelja d_1, d_2 broja $(n^2+1)/2$ za koje vrijedi $d_1 + d_2 = 2n + \varepsilon,\ \varepsilon \equiv 0 \pmod 4$. Koristeći poznati identitet $(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1d_2$, problem traženja beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju navedeno svojstvo pretvaramo u problem rješavanja pellovske jednadžbe. Određivanjem beskonačno mnogo rješenja pripadne Pellove jednadžbe u mogućnosti smo odrediti i beskonačno mnogo traženih neparnih prirodnih brojeva n. U dokazu teorema nisu navedeni apsolutno svi

neparni prirodni brojevi n koji zadovljavaju istaknuto svojstvo, već je navedeno beskonačno mnogo neparnih prirodnih brojeva n za koje vrijedi da su djelitelji d_1, d_2 broja $(n^2+1)/2$ međusobno relativno prosti.

Teorem 1.1 Za svaki cijeli broj $\varepsilon \equiv 0 \pmod 4$ postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoji par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da vrijedi

$$d_1 + d_2 = 2n + \varepsilon.$$

Dokaz.

Neka je $\varepsilon \equiv 0 \pmod 4$. Želimo naći neparan prirodan broj n i pozitivne djelitelje d_1, d_2 od $\frac{n^2+1}{2}$ tako da vrijedi

$$d_1 + d_2 = 2n + \varepsilon.$$

Stavimo $g = \text{nzd}(d_1, d_2)$ i pišemo $d_1 = gd_1', d_2 = gd_2'$. Budući je $gd_1'd_2' = \text{nzv}(d_1, d_2)$ i $\text{nzd}(d_1, d_2)$ dijeli $\frac{n^2+1}{2}$, zaključujemo da postoji $d \in \mathbb{N}$ takav da je

$$d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

Iz identiteta

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1d_2,$$

dobivamo:

$$(d_2 - d_1)^2 = (2n + \varepsilon)^2 - 4\frac{g(n^2+1)}{2d},$$

$$(d_2 - d_1)^2 = 4n^2 + 4\varepsilon n + \varepsilon^2 - 2\frac{g(n^2+1)}{d},$$

$$d(d_2 - d_1)^2 = 4n^2 d + 4d\varepsilon n + \varepsilon^2 d - 2n^2 g - 2g,$$

$$d(d_2 - d_1)^2 = (4d - 2g)n^2 + 4d\varepsilon n + \varepsilon^2 d - 2g,$$

$$d(4d-2g)(d_2 - d_1)^2 = (4d-2g)^2 n^2 + 4(4d-2g)d\varepsilon n + 4d^2\varepsilon^2 - 8dg - 2\varepsilon^2 dg + 4g^2. \quad (1.1)$$

Stavimo da je $X = (4d-2g)n + 2d\varepsilon, \quad Y = d_2 - d_1$. Tako (1.1) postaje:

$$X^2 - d(4d-2g)Y^2 = 8dg + 2\varepsilon^2 dg - 4g^2.$$

Za $g = 1$ prethodni izraz postaje:

$$X^2 - 2d(2d-1)Y^2 = 8d + 2\varepsilon^2 d - 4,$$

$$X^2 - 2d(2d-1)Y^2 = 2d(4 + \varepsilon^2) - 4. \quad (1.2)$$

Izraz (1.2) je pellovska jednadžba. Očito je da desna strana od (1.2) nikad nije jednaka

nuli.

Pokušavamo od desne strane od (1.2) napraviti potpuni kvadrat. Za izraz $2d(4+\varepsilon^2)-4$, ako umjesto d stavimo izraz $d = \frac{1}{8}\varepsilon^2 - \frac{1}{2}\varepsilon + 1$, dobivamo:

$$2d(4+\varepsilon^2) - 4 = 2\left(\frac{1}{8}\varepsilon^2 - \frac{1}{2}\varepsilon + 1\right)(4+\varepsilon^2) - 4 = \left(\frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)\right)^2.$$

Dakle, pellovska jednadžba (1.2) postaje:

$$X^2 - 2d(2d-1)Y^2 = \left(\frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)\right)^2. \tag{1.3}$$

Sad, slično kao u članku [10] tražimo rješenja od (1.3) u obliku

$$X = \frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)U, \quad Y = \frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)V.$$

Jednadžba (1.3) postaje:

$$U^2 - 2d(2d-1)V^2 = 1. \tag{1.4}$$

Dobivamo Pellovu jednadžbu (1.4) koja ima beskonačno mnogo (U, V) rješenja, a onda postoji i beskonačno mnogo (X, Y) rješenja. Kako bi riješili jednadžbu (1.4) razvijamo $\sqrt{2d(2d-1)}$ u verižni razlomak.

Dobivamo $\sqrt{2d(2d-1)} = [2d-1; \overline{2, 4d-2}]$. Tako dobivamo:
$(U_0, V_0) = (1, 0)$,
$(U_1, V_1) = (4d-1, 2)$,
$(U_2, V_2) = (32d^2 - 16d + 1, 16d - 4)$,
$(U_3, V_3) = (256d^3 - 192d^2 + 36d - 1, 128d^2 - 64d + 6), \ldots$.

Općenito,

$$U_0 = 1,\ U_1 = 4d-1,\ U_{m+2} = 2(4d-1)U_{m+1} - U_m,$$

$$V_0 = 0,\ V_1 = 2,\ V_{m+2} = 2(4d-1)V_{m+1} - V_m,\ m \in \mathbb{N}_0. \tag{1.5}$$

Dokazujemo matematičkom indukcijom da je $U_m \equiv 1 \pmod{(4d-2)}, m \geq 0$.
Vrijedi: $U_0 = 1 \equiv 1 \pmod{(4d-2)}$, $U_1 = 4d-1 \equiv 1 \pmod{(4d-2)}$.
Pretpostavimo da je $U_m \equiv U_{m-1} \equiv 1 \pmod{(4d-2)}$.
Tada za U_{m+1} vrijedi:

$$U_{m+1} = 2(4d-1)U_m - U_{m-1} \equiv 2 - 1 \equiv 1 \pmod{(4d-2)}.$$

Računamo pripadne vrijednosti za n. Znamo da je $X = (4d-2)n + 2d\varepsilon$ i također znamo da je $X = \frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)U$. Izjednačavanjem ovih izraza i izoliranjem broja n,

dobivamo izraz:

$$n = \frac{\frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)U - 2d\varepsilon}{4d - 2}.$$

Dokazujemo da je n prirodan broj, odnosno da se brojnik uvijek može podijeliti nazivnikom.
Za $d = \frac{1}{8}\varepsilon^2 - \frac{1}{2}\varepsilon + 1$ imamo $4d - 2 = \frac{1}{2}\varepsilon^2 - 2\varepsilon + 2$. Dakle,

$$\frac{1}{2}(\varepsilon^2 - 2\varepsilon + 4)U - 2d\varepsilon \equiv 4d + \varepsilon - 2 - 2d\varepsilon \equiv -(2d-1)\varepsilon \equiv 0 \pmod{(4d-2)},$$

što znači da su svi brojevi n generirani na navedeni način prirodni brojevi.

Na primjer, iz U_1, U_2, U_3, dobivamo:

$$\begin{cases} n = \frac{1}{2}(\varepsilon^2 - 3\varepsilon + 6), \\ d_1 = 1, \\ d_2 = \varepsilon^2 - 2\varepsilon + 5. \end{cases}$$

$$\begin{cases} n = \frac{1}{2}(\varepsilon^4 - 6\varepsilon^3 + 20\varepsilon^2 - 33\varepsilon + 34), \\ d_1 = \varepsilon^2 - 2\varepsilon + 5, \\ d_2 = \varepsilon^4 - 6\varepsilon^3 + 19\varepsilon^2 - 30\varepsilon + 29. \end{cases}$$

$$\begin{cases} n = \frac{1}{2}(\varepsilon^6 - 10\varepsilon^5 + 50\varepsilon^4 - 148\varepsilon^3 + 281\varepsilon^2 - 323\varepsilon + 198), \\ d_1 = \varepsilon^4 - 6\varepsilon^3 + 19\varepsilon^2 - 30\varepsilon + 29, \\ d_2 = \varepsilon^6 - 10\varepsilon^5 + 49\varepsilon^4 - 142\varepsilon^3 + 262\varepsilon^2 - 292\varepsilon + 169. \end{cases}$$

□

1.2 Slučaj $\delta = 4$

Dokaz sljedećeg teorema nešto je drugačiji od dokaza Teorema 1.1. Stavimo li da je $g = \text{nzd}(d_1, d_2)$ te $d_1 = gd_1', d_2 = gd_2'$, budući je $gd_1'd_2' = \text{nzv}(d_1, d_2)$ i $\text{nzd}(d_1, d_2)$ dijeli $(n^2+1)/2$, opet zaključujemo da postoji $d \in \mathbb{N}$ takav da je

$$d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

No, broj d kojeg definiramo i koji je izražen uz pomoć broja ε je prirodan broj ako je $\varepsilon \equiv 6 \pmod 8$, ali ne i u slučaju ako je $\varepsilon \equiv 2 \pmod 8$. Iz tog razloga razlikujemo dva podslučaja: u jednom podslučaju vrijedi $\varepsilon \equiv 6 \pmod 8$ i u dokazivanju tvrdnje Teorema 1.2 primjenjujemo metode iz članka [10], a u drugom podslučaju vrijedi $\varepsilon \equiv 2 \pmod 8$ i koristimo bitno drugačije metode od onih koje smo koristili u dokazu Teorema 1.1. U tom

podslučaju na osnovu eksperimentalnih podataka određujemo brojeve g, d_1 i d_2. Budući znamo da je $Y = d_2 - d_1$ jedna od nepoznanica pellovske jednadžbe koju nastojimo riješiti, u mogućnosti smo na osnovu određenih eksperimentalnih podataka odmah odrediti i broj Y. Poznavanje broja Y omogućuje nam određivanje i druge nepoznanice, X, početne pellovske jednadžbe. Na taj način dobivamo jedno rješenje (X, Y) pellovske jednadžbe i pomoću tog rješenja smo u mogućnosti odrediti i jedan neparan prirodan broj n koji zadovoljava svojstvo Teorema 1.2, odnosno za takav neparan prirodan broj n postoje djelitelji d_1, d_2 od $(n^2+1)/2$ za koje vrijedi $d_1 + d_2 = 4n + \varepsilon$, $\varepsilon \equiv 2 \pmod 8$. Koristeći svojstva pellovske jednadžbe kojoj znamo jedno rješenje, određujemo beskonačno mnogo njenih rješenja, a na taj način i beskonačno mnogo traženih prirodnih brojeva n.

Teorem 1.2 Za svaki cijeli broj ε takav da vrijedi $\varepsilon \equiv 2 \pmod 4$ postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoji par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da je

$$d_1 + d_2 = 4n + \varepsilon.$$

Dokaz.

Za početak promatramo podslučaj u kojem je $\varepsilon \equiv 6 \pmod 8$. Nastojimo dokazati da postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoje pozitivni djelitelji d_1, d_2 od $\frac{n^2+1}{2}$ takvi da vrijedi

$$d_1 + d_2 = 4n + \varepsilon.$$

Kao u dokazu Teorema 1.1, neka je $g = \text{nzd}(d_1, d_2)$, $d_1 = gd_1', d_2 = gd_2'$ te

$$d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

Koristeći poznati identitet

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1 d_2,$$

i uvrštavanjem definiranih vrijednosti, dobivamo:

$$(d_2 - d_1)^2 = (4n + \varepsilon)^2 - 4\frac{g(n^2+1)}{2d},$$

$$d(d_2 - d_1)^2 = (16d - 2g)n^2 + 8d\varepsilon n + \varepsilon^2 d - 2g,$$

$$d(16d-2g)(d_2-d_1)^2 = (16d-2g)^2 n^2 + 8(16d-2g)d\varepsilon n + 16d^2\varepsilon^2 - 32dg - 2\varepsilon^2 dg + 4g^2. \quad (1.6)$$

U slučaju kad je $X = (16d - 2g)n + 4d\varepsilon$, $Y = d_2 - d_1$, izraz (1.6) postaje:

$$X^2 - 2d(8d - g)Y^2 = 32dg + 2\varepsilon^2 dg - 4g^2. \quad (1.7)$$

Uvrštavanjem $g = 1$ u (1.7), dobivamo:

$$X^2 - 2d(8d-1)Y^2 = 2d(16+\varepsilon^2) - 4. \tag{1.8}$$

Izraz (1.8) je pellovska jednadžba. Desna strana od (1.8) je uvijek različita od nule.

Nastojimo da desna strana dobivene jednakosti (1.8) bude potpuni kvadrat kako bi na sličan način kao u Teoremu 1.1 mogli riješiti dobivenu pellovsku jednadžbu (1.8). Ako definiramo da je $d = \frac{1}{32}\varepsilon^2 - \frac{1}{8}\varepsilon + \frac{5}{8}$, dobivamo:

$$2d(16+\varepsilon^2) - 4 = 2\left(\frac{1}{32}\varepsilon^2 - \frac{1}{8}\varepsilon + \frac{5}{8}\right)(16+\varepsilon^2) - 4 = \left(\frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)\right)^2.$$

Dobivamo novu pellovsku jednadžbu:

$$X^2 - 2d(8d-1)Y^2 = \left(\frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)\right)^2. \tag{1.9}$$

Sad, slično kao u članku [10] tražimo rješenja od (1.9) u obliku

$$X = \frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)W, \quad Y = \frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)Z.$$

Pellovska jednadžba (1.8) postaje:

$$W^2 - 2d(8d-1)Z^2 = 1. \tag{1.10}$$

Dobivena Pellova jednadžba koja je pridružena pellovskoj jednadžbi (1.9) ima beskonačno mnogo (W, Z) rješenja, što implicira da onda postoji i beskonačno mnogo (X, Y) rješenja. Kako bi riješili jednadžbu (1.10) razvijamo $\sqrt{2d(8d-1)}$ u verižni razlomak.

Vrijedi $\sqrt{2d(8d-1)} = [4d-1; \overline{1, 2, 1, 8d-2}]$. Prvih par rješenja Pellove jednadžbe (1.10) je:
$(W_0, Z_0) = (1, 0)$,
$(W_1, Z_1) = (16d-1, 4)$,
$(W_2, Z_2) = (512d^2 - 64d + 1, 128d - 8), \ldots$.

Općenito,

$$W_0 = 1,\ W_1 = 16d-1,\ W_{m+2} = 2(16d-1)W_{m+1} - W_m,$$

$$Z_0 = 0,\ Z_1 = 4,\ Z_{m+2} = 2(16d-1)Z_{m+1} - Z_m,\ m \in \mathbb{N}_0.$$

Koristeći matematičku indukciju dokazujemo da je $W_m \equiv 1 \pmod{(16d-2)},\ m \geq 0$. Vrijedi: $W_0 = 1 \equiv 1 \pmod{(16d-2)}$, $W_1 = 16d-1 \equiv 1 \pmod{(16d-2)}$.

Pretpostavljamo da je $W_m \equiv W_{m-1} \equiv 1 \pmod{(16d-2)}$. Tada za W_{m+1} vrijedi:

$$W_{m+1} = 2(16d-1)W_m - W_{m-1} \equiv 2 - 1 \equiv 1 \pmod{(16d-2)}.$$

Sad smo u mogućnosti odrediti neparne prirodne brojeve n. Ranije smo odredili $X = (16d-2)n + 4d\varepsilon$ i $X = \frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)W$. Izjednačavanjem ovih izraza, dobivamo:

$$n = \frac{\frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)W - 4d\varepsilon}{16d-2}.$$

Dokazujemo da je n prirodan broj, odnosno da se brojnik uvijek može podijeliti nazivnikom.
Za $d = \frac{1}{32}\varepsilon^2 - \frac{1}{8}\varepsilon + \frac{5}{8}$ imamo $8d - 1 = \frac{1}{4}\varepsilon^2 - \varepsilon + 4$. Uočimo da je $\frac{\varepsilon}{2}$ neparan cijeli broj. Jednostavnim raspisom dobivamo,

$$\frac{1}{4}(\varepsilon^2 - 2\varepsilon + 16)W - 4d\varepsilon \equiv 8d - 1 + \frac{\varepsilon}{2} - 4d\varepsilon \equiv (8d-1)(1 - \frac{\varepsilon}{2}) \equiv 0 \pmod{(16d-2)},$$

što nam ukazuje da su svi brojevi n generirani na navedeni način su prirodni brojevi.

Iz W_1, W_2, W_3, dobivamo:

$$\begin{cases} n = \frac{1}{4}(\varepsilon^2 - 3\varepsilon + 18), \\ d_1 = 1 \\ d_2 = \varepsilon^2 - 2\varepsilon + 17. \end{cases}$$

$$\begin{cases} n = \frac{1}{4}(\varepsilon^4 - 6\varepsilon^3 + 44\varepsilon^2 - 105\varepsilon + 322), \\ d_1 = \varepsilon^2 - 2\varepsilon + 17, \\ d_2 = \varepsilon^4 - 6\varepsilon^3 + 43\varepsilon^2 - 102\varepsilon + 305. \end{cases}$$

$$\begin{cases} n = \frac{1}{4}(\varepsilon^6 - 10\varepsilon^5 + 86\varepsilon^4 - 388\varepsilon^3 + 1529\varepsilon^2 - 3155\varepsilon + 5778), \\ d_1 = \varepsilon^4 - 6\varepsilon^3 + 43\varepsilon^2 - 102\varepsilon + 305, \\ d_2 = \varepsilon^6 - 10\varepsilon^5 + 85\varepsilon^4 - 382\varepsilon^3 + 1486\varepsilon^2 - 3052\varepsilon + 5473. \end{cases}$$

U drugom podslučaju je $\varepsilon \equiv 2 \pmod 8$. Neka je $\varepsilon = 8k + 2,\ k \in \mathbb{N}_0$. Stavimo li za $g = \frac{1}{4}\varepsilon^2 + 4$ i ujedno $g = d_1$, dobivamo:

$$X^2 - 2d(8d-g)Y^2 = 32d\left(\frac{1}{4}\varepsilon^2 + 4\right) + 2\varepsilon^2 d\left(\frac{1}{4}\varepsilon^2 + 4\right) - 4\left(\frac{1}{4}\varepsilon^2 + 4\right)^2,$$

$$X^2 - 2d(8d-g)Y^2 = \varepsilon^4\left(\frac{d}{2} - \frac{1}{4}\right) + \varepsilon^2(16d-8) + 128d - 64,$$

$$X^2 - 2d(8d-g)Y^2 = \frac{2d-1}{4}\varepsilon^4 + 8\varepsilon^2(2d-1) + 64(2d-1),$$

i uočavamo da će desna strana biti potpuni kvadrat u slučaju kad vrijedi da je $2d-1$ potpuni kvadrat.

Pogledajmo primjere petorki (n, d_1, d_2, g, d) koje zadovoljavaju uvjete Teorema 1.2 i za koje vrijedi $\varepsilon \equiv 2 \pmod 8$. U navedenim tablicama istaknuti su oni podaci koje koristimo u dokazu drugog podslučaja Teorema 1.2, odnosno one petorke za koje vrijedi $g = d_1 = \frac{1}{4}\varepsilon^2 + 4$. Motivirani tim primjerima možemo odrediti i broj d_2. $\varepsilon = 2$

n	d_1	d_2	g	d
7	**5**	**25**	**5**	**1**
807	625	2605	5	1
1747	85	6905	5	13
79207	61405	255425	5	1
141877	6905	560605	5	13

$\varepsilon = 10$

n	d_1	d_2	g	d
99	**29**	**377**	**29**	**13**
157	145	493	29	5
240393	36221	925361	29	25
292477	278197	891721	29	5

$\varepsilon = 18$

n	d_1	d_2	g	d
11	1	61	1	1
43	5	185	5	5
463	221	1649	17	5
477	61	1865	1	1
1143	**85**	**4505**	**85**	**145**
1437	185	5581	1	1
2163	2465	6205	85	13
14443	1865	55925	5	5
43211	5811	167281	1	1
60337	4505	236861	17	29
220953	7565	876265	85	313
259849	1037	1038377	17	533
432957	55925	1675921	1	1
568143	1525	2271065	5	233

$\varepsilon = 26$

n	d_1	d_2	g	d
253	**173**	**865**	**173**	**37**
5443	**173**	**21625**	**173**	**685**
13747	**173**	**54149**	**173**	**1745**

$\varepsilon = 34$

n	d_1	d_2	g	d
13	1	85	1	1
47	1	221	1	1
109	13	457	1	1
207	5	857	1	5
667	85	2617	1	1
2189	3809	4981	293	37
3547	457	13765	1	1
8793	221	34985	1	5
16839	**293**	**67097**	**293**	**2113**
20269	2617	78493	1	1
34073	857	135469	1	5
106573	13765	412561	1	1
607675	78493	2352241	1	1

$\varepsilon = 42$

n	d_1	d_2	g	d
123	89	445	89	17
337	5	1385	5	41
657	**445**	**2225**	**445**	**97**
3149	2581	10057	89	17
13473	5785	48149	89	29
40707	**445**	**162425**	**445**	**5101**
147917	3205	588505	5	29
487309	401657	1547621	89	17
699485	12193	2785789	89	641

Motivirani navedenim podacima, uzimamo da je broj d u ovom slučaju jednak

$$d = \frac{1}{512}\varepsilon^4 - \frac{1}{64}\varepsilon^3 + \frac{7}{64}\varepsilon^2 - \frac{5}{16}\varepsilon + \frac{41}{32}.$$

Uvrštavajući za $\varepsilon = 8k + 2,\ k \in \mathbb{N}_0$, dobivamo $d = 8k^4 + 4k^2 + 1$, odnosno zaključujemo da je $d \in \mathbb{N}$. Također, vrijedi:

$$2d - 1 = 16k^4 + 8k^2 + 1 = (4k^2 + 1)^2.$$

Uvrstimo li sve dobiveno u (1.7), vrijedi:

$$X^2 - 2d(8d-g)Y^2 = \left(\frac{1}{32}(\varepsilon^2+16)(\varepsilon^2-4\varepsilon+20)\right)^2, \tag{1.11}$$

što još možemo zapisati i kao:

$$X^2 - 2d(8d-g)Y^2 = \left(2(4k^2+1)(16k^2+8k+5)\right)^2.$$

Promotrit ćemo i jednadžbu

$$U^2 - 2d(8d-g)V^2 = 1, \tag{1.12}$$

gdje je (1.12) pridružena Pellova jednadžba pellovskoj jednadžbi (1.11). U ovom slučaju ne možemo općenito razviti broj $\sqrt{2d(8d-g)}$ u verižni razlomak, stoga se odlučujemo na nešto drugačiji pristup u kojem ne određujemo eksplicitno fundamentalno rješenje Pellove jednadžbe (1.12).
Neka je (U_0, V_0) fundamentalno rješenje Pellove jednadžbe (1.12). Iz (1.12) je jasno i da vrijedi

$$U^2 \equiv 1 \pmod{(16d-2g)}.$$

Osim što smo utvrdili da postoji pravilnost za broj $g = \text{nzd}(d_1, d_2)$, $g = d_1 = \frac{1}{4}\varepsilon^2 + 4$, iz navedenih tablica uočavamo da postoji i pravilnost u formiranju broja d_2. Naime, vrijedi

$$d_2 = d_1^2 - 16kd_1, \;\; k \in \mathbb{N}_0.$$

Za $Y = d_2 - d_1$ tako dobivamo

$$Y = d_2 - d_1 = d_1^2 - 16kd_1 - d_1 = d_1^2 - (16k+1)d_1.$$

S obzirom da je $g = d_1$, možemo pisati

$$Y = g^2 - (16k+1)g.$$

U tom slučaju Y postaje

$$Y = \left(\frac{1}{4}\varepsilon^2+4\right)^2 - (2\varepsilon-3)\left(\frac{1}{4}\varepsilon^2+4\right) = \frac{\varepsilon^4}{16} - \frac{\varepsilon^3}{2} + \frac{11\varepsilon^2}{4} - 8\varepsilon + 28,$$

te je

$$Y^2 = \left(\frac{1}{16}(\varepsilon^2+16)(\varepsilon^2-8\varepsilon+28)\right)^2.$$

Uvrštavanjem dobivenog u (1.11), vrijedi:

$$X^2 = 2d(8d-g)\left(\frac{1}{16}(\varepsilon^2+16)(\varepsilon^2-8\varepsilon+28)\right)^2 + \left(\frac{1}{32}(\varepsilon^2+16)(\varepsilon^2-4\varepsilon+20)\right)^2,$$

$$X^2 = \left(\frac{(\varepsilon^2+16)(\varepsilon^6-16\varepsilon^5+140\varepsilon^4-768\varepsilon^3+3120\varepsilon^2-8704\varepsilon+14400)}{2048}\right)^2.$$

$$X = \frac{(\varepsilon^2+16)(\varepsilon^6-16\varepsilon^5+140\varepsilon^4-768\varepsilon^3+3120\varepsilon^2-8704\varepsilon+14400)}{2048}.$$

Ispitujemo vrijedi li kongruencija

$$X \equiv 4d\varepsilon \pmod{(16d-2g)} \tag{1.13}$$

za ovako definirani X. Znamo da je $X = (16d-2g)n + 4d\varepsilon$, odnosno $n = \frac{X-4d\varepsilon}{16d-2g}$.

$$16d - 2g = \frac{\varepsilon^4}{32} - \frac{\varepsilon^3}{4} + \frac{5\varepsilon^2}{4} - 5\varepsilon + \frac{25}{2},$$

$$X - 4d\varepsilon = \left(\frac{\varepsilon^4}{32} - \frac{\varepsilon^3}{4} + \frac{5\varepsilon^2}{4} - 5\varepsilon + \frac{25}{2}\right)\left(\frac{\varepsilon^4}{64} - \frac{\varepsilon^3}{8} + \frac{13\varepsilon^2}{16} - \frac{9\varepsilon}{4} + 9\right),$$

pa je

$$n = \frac{\varepsilon^4}{64} - \frac{\varepsilon^3}{8} + \frac{13\varepsilon^2}{16} - \frac{9\varepsilon}{4} + 9.$$

Uvrstimo li $\varepsilon = 8k+2$, dobivamo

$$n = 64k^4 + 28k^2 + 7,$$

iz čega je jasno da je $n \in \mathbb{N}$.

Budući vrijedi kongruencija za ovako definirani X, možemo definirati odgovarajuće fundamentalno rješenje od (1.11)

$$(X_0, Y_0) = \left(\frac{(\varepsilon^2+16)(\varepsilon^6-16\varepsilon^5+140\varepsilon^4-768\varepsilon^3+3120\varepsilon^2-8704\varepsilon+14400)}{2048},\right.$$

$$\left.\frac{1}{16}(\varepsilon^2+16)(\varepsilon^2-8\varepsilon+28)\right).$$

Na ovaj smo način dokazali da postoji barem jedan neparan $n \in \mathbb{N}$ za svaki $\varepsilon = 8k+2,\ k \in \mathbb{N}_0$, koji odgovara uvjetu Teorema 1.2. Preostaje dokazati da postoji beskonačno mnogo takvih brojeva n. To ćemo dokazati tako da dokažemo da postoji beskonačno mnogo parova rješenja $(X_i, Y_i),\ i \in \mathbb{N}$ od (1.11) koji zadovoljavaju kongruenciju (1.13).

Ako je (X_0, Y_0) rješenje jednadžbe (1.11), onda su i

$$(X_i, Y_i) = \left(X_0 + \sqrt{2d(8d-g)}Y_0\right)\left(U_0 + \sqrt{2d(8d-g)}V_0\right)^{2i}, \quad i = 0, 1, 2, \ldots \tag{1.14}$$

rješenja jednadžbe (1.11). Jednostavnim raspisom dobivamo da vrijedi

$$X_i = X_0\left(U_0^{2i} + \binom{2i}{2}2d(8d-g)U_0^{2i-2}V_0^2 + \binom{2i}{4}(2d(8d-g))^2U_0^{2i-4}V_0^4 + \cdots + (2d(8d-g))^iV_0^{2i}\right) +$$

$$+Y_0\left(4iU_0^{2i-1}V_0d(8d-g) + \binom{2i}{3}(2d(8d-g))^2U_0^{2i-3}V_0^3 + \binom{2i}{5}(2d(8d-g))^3U_0^{2i-5}V_0^5 + \cdots + \binom{2i}{2i-1}(2d(8d-g))^iV_0^{2i-1}U_0\right).$$

Ovako definiranih rješenja od (1.11) ima beskonačno mnogo. Ispitujemo vrijedi li (1.13) za $X_i,\ i \in \mathbb{N}$. Već znamo da vrijedi

$$X_0 \equiv 4d\varepsilon \pmod{(16d-2g)}.$$

Vrijedi

$$X_i \equiv U_0^{2i}X_0 \equiv X_0 \equiv 4d\varepsilon \pmod{(16d-2g)}.$$

Dakle, postoji beskonačno mnogo (X_i, Y_i) rješenja od (1.11) koji zadovoljavaju kongruenciju (1.13).

Koristeći

$$n = \frac{X_i - 4d\varepsilon}{16-2g}$$

dobivamo beskonačno mnogo prirodnih brojeva n koji zadovoljavaju uvjete Teorema 1.2. Vrlo je lako uočiti da su brojevi n neparni. Naime, s obzirom da je $d, g \equiv 1 \pmod 4$ znamo da vrijedi $16d - 2g \equiv 2 \pmod 4$. Imamo

$$X_0 = \frac{(\varepsilon^2+16)(\varepsilon^6 - 16\varepsilon^5 + 140\varepsilon^4 - 768\varepsilon^3 + 3120\varepsilon^2 - 8704\varepsilon + 14400)}{2048} =$$

$$= 2(256k^6 - 128k^5 + 160k^4 - 64k^3 + 52k^2 - 16k + 5)(16k^2 + 8k + 5) \equiv 10(4k^2+5) \equiv 2(4k^2+5) \equiv 2 \pmod 4.$$

Budući (1.12) implicira da je U_0 neparan te V_0 paran broj, iz (1.13) dobivamo da vrijedi

$$X_i - 4d\varepsilon \equiv X_i \equiv U_0^{2i}X_0 \equiv X_0 \equiv 2 \pmod 4$$

iz čega slijedi da je n neparan prirodan broj.

□

1.3 Slučaj $\varepsilon = 0$

U ovom potpoglavlju doktorskog rada promatramo slučaj u kojem je $\varepsilon = 0$. Ispitujemo postoji li beskonačno mnogo neparnih prirodnih brojeva n takvih da postoje djelitelji

d_1, d_2 broja $(n^2+1)/2$ za koje je $d_1 + d_2 = \delta n,\ \delta \equiv 2 \pmod 4$. Uočavamo da postoje dva bitno različita podslučaja. U slučaju kad je $\delta = 2$ dokazujemo da postoji beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju navedeno svojstvo i pritom su djelitelji d_1, d_2 broja $(n^2+1)/2$ međusobno relativno prosti. U slučaju kad je $\delta \equiv 2 \pmod 4,\ \delta \geq 6$ dokazujemo da ne postoje neparni prirodni brojevi n koji zadovoljavaju navedeno svojstvo. U dokazivanju navedenih tvrdnji problem opet svodimo na određivanje rješenja pellovske jednadžbe nešto drugačijeg tipa od prethodno dobivenih pellovskih jednadžbi. Novodobiveni tip pellovske jednadžbe zahtijeva primjenu kriterija iz članka [15] kojeg koristimo kako bi utvrdili postojanje njenih rješenja.

Propozicija 1.3 Postoji beskonačno mnogo neparnih prirodnih brojeva n sa svojstvom da postoji par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da je

$$d_1 + d_2 = 2n.$$

Pritom za sva rješenja vrijedi da je $\text{nzd}(d_1, d_2) = 1$ i $d_1 d_2 = \frac{n^2+1}{2}$.

Dokaz.

Želimo naći neparan pozitivan broj n i pozitivne djelitelje d_1, d_2 od $\frac{n^2+1}{2}$ tako da vrijedi

$$d_1 + d_2 = 2n.$$

Stavimo $g = \text{nzd}(d_1, d_2)$. Tada vrijedi $g|(2n)$, te $g|(n^2+1)$, iz čega zaključujemo da $g|((2n)^2+4)$ što znači da $g|4$. Budući je g najveći zajednički djelitelj brojeva d_1, d_2 koji su neparni, zaključujemo da je i g neparan broj pa slijedi da je $g = 1$. Kao i prije, definiramo d s $d_1 d_2 = \frac{n^2+1}{2d}$ pa iz identiteta:

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1 d_2,$$

dobivamo:

$$(d_2 - d_1)^2 = (2n)^2 - 2\frac{(n^2+1)}{d},$$
$$d(d_2 - d_1)^2 = 4n^2 d - 2n^2 - 2.$$

Stavljajući $d_2 - d_1 = 2y$ lako dobivamo:

$$(4d-2)n^2 - 4dy^2 = 2,$$

$$(2d-1)n^2 - 2dy^2 = 1. \tag{1.15}$$

Iskoristit ćemo sljedeću lemu, koja predstavlja Criterion 1 iz [15] kako bi provjerili postoji li rješenje za (1.15).

Lema 1.4 (Grelak, Grytczuk) Neka su $a > 1$, b prirodni brojevi takvi da vrijedi $\text{nzd}(a, b) = 1$ i $D = ab$ nije potpun kvadrat. Neka je (u_0, v_0) fundamentalno rješenje jednadžbe

$$u^2 - Dv^2 = 1.$$

Tada jednadžba $ax^2 - by^2 = 1$ ima rješenja u prirodnim brojevima ako i samo ako

$$2a|(u_0 + 1) \text{ i } 2b|(u_0 - 1).$$

□

Moramo riješiti pridruženu Pellovu jednadžbu oblika:

$$U^2 - 2d(2d-1)V^2 = 1. \tag{1.16}$$

Razvoj broja $\sqrt{2d(2d-1)}$ u verižni razlomak smo već odredili u Teoremu 1.1 i dobili smo da vrijedi:

$$\sqrt{2d(2d-1)} = [2d-1; \overline{2, 4d-2}].$$

Fundamentalno rješenje Pellove jednadžbe (1.16) je $(4d-1, 2)$. U našem slučaju, prema Lemi 1.4, treba vrijediti

$$2(2d-1)|4d \qquad \text{i} \qquad 4d|(4d-2),$$

što ne vrijedi za $d \in \mathbb{N}$. Dakle, za pellovsku jednadžbu (1.15) ne postoje cjelobrojna rješenja (n, y) u slučaju kad je $a = 2d-1 > 1$. Još ostaje provjeriti postoje li rješenja kad je $a = 1$ što je slučaj koji nije uključen u Lemu 1.4.

U slučaju kad je $a = 2d - 1 = 1$ vrijedi $d = 1$. Vratimo li se u početnu pellovsku jednadžbu (1.15) i uvrstimo li $d = 1$, dobivamo Pellovu jednadžbu:

$$n^2 - 2y^2 = 1, \tag{1.17}$$

koja ima beskonačno mnogo rješenja $n = U_m,\ y = V_m,\ m \in \mathbb{N}_0$ gdje je:

$$U_0 = 1,\ U_1 = 3,\ U_{m+2} = 6U_{m+1} - U_m,$$

$$V_0 = 0,\ V_1 = 2,\ V_{m+2} = 6V_{m+1} - V_m,\ m \in \mathbb{N}_0.$$

Prvih nekoliko rješenja jednadžbe (1.17) je:

$(U_0, V_0) = (1, 0)$, $(U_1, V_1) = (3, 2)$, $(U_2, V_2) = (17, 12)$, $(U_3, V_3) = (99, 70), \ldots$.

Za navedena početna rješenja ispisujemo pripadne trojke (n, d_1, d_2):

$$(n, d_1, d_2) = (3, 1, 5),\ \ (17, 5, 29),\ \ (99, 29, 169), \ldots .$$

Ovime je dokazano da postoji beskonačno mnogo neparnih brojeva n sa svojstvom da postoji par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da je $d_1 + d_2 = 2n$. Budući da smo dokazali da u slučaju kad je $\delta = 2$ i $\varepsilon = 0$ mora biti $g = 1$ i $d = 1$, zaključujemo da su u svim rješenjima brojevi d_1 i d_2 relativno prosti i zaključujemo da uvijek vrijedi $d_1 d_2 = \frac{n^2+1}{2}$.

□

Teorem 1.5 Neka je $\delta \geq 6$ prirodan broj takav da vrijedi $\delta = 4k + 2, k \in \mathbb{N}$. Tada ne postoji neparan prirodan broj n sa svojstvom da postoji par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da je

$$d_1 + d_2 = \delta n.$$

Dokaz.

Pretpostavimo suprotno, te neka je δ najmanji broj oblika $\delta = 4k + 2,\ k \in \mathbb{N}$, za kojeg postoji neparan prirodan broj n i par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da je $d_1 + d_2 = \delta n$. Neka je $g = \text{nzd}(d_1, d_2) > 1$. Budući vrijedi $d_1 = gd_1',\ d_2 = gd_2'$, tada $g|(n^2 + 1)$ i $g|(\delta n)$ pa zaključujemo da $g|((\delta n)^2 + \delta^2)$, odnosno $g|\delta^2$ što znači da g i δ imaju zajednički prosti faktor p. Neka je $d_1 = pd_1'', d_2 = pd_2'', \delta = p\delta''$. Tada vrijedi $pd_1'' + pd_2'' = p\delta''n$ pa je $d_1'' + d_2'' = \delta''n$ i d_1'', d_2'' su djelitelji od $\frac{n^2+1}{2}$. Očito je $\delta'' < \delta$ pa ako je $\delta'' \neq 2$, onda smo dobili kontradikciju s minimalnošću od δ. Dakle, ako je $\delta'' \neq 2$, onda mora biti $g = 1$.

Ako je $\delta'' = 2$, onda iz Propozicije 1.3 slijedi da je $\text{nzd}(d_1'', d_2'') = 1$ i $d_1''d_2'' = \frac{n^2+1}{2}$. No, $\text{nzv}(d_1, d_2) = pd_1''d_2''$ bi trebao dijeliti $\frac{n^2+1}{2}$ što je nemoguće zbog $p > 1$. Dakle, i u ovom slučaju mora biti $g = 1$.

Koristeći identitet

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1d_2,$$

i uzimanjem $g = 1$, dobivamo:

$$(d_2 - d_1)^2 = (\delta n)^2 - 2\frac{(n^2 + 1)}{d},$$

$$d(d_2 - d_1)^2 = \delta^2 n^2 d - 2n^2 - 2,$$

$$d(d_2 - d_1)^2 = (\delta^2 d - 2)n^2 - 2.$$

U izrazu

$$(\delta^2 d - 2)n^2 - d(d_2 - d_1)^2 = 2,$$

stavljamo $d_2 - d_1 = 2y$ (jer su d_1, d_2 neparni pa je njihova razlika sigurno paran broj) pa dobivamo:

$$(\delta^2 d - 2)n^2 - 4dy^2 = 2.$$

Čitav izraz dijelimo s 2:

$$(2d(2k+1)^2 - 1)n^2 - 2dy^2 = 1.$$

Definiramo $\delta' = \frac{\delta}{2} = 2k + 1$, pa prethodni izraz postaje:

$$(2\delta'^2 d - 1)n^2 - 2dy^2 = 1. \tag{1.18}$$

Pomoću Leme 1.4 ćemo dokazati da pellovska jednadžba (1.18) nema rješenja.

Da bi mogli primijeniti Lemu 1.4, prvo moramo formirati jednadžbu oblika

$$x^2 - Dy^2 = 1.$$

U našem slučaju vrijedi $a = 2\delta'^2 d - 1$ i vrijedi da je $a > 1$ (jer je $\delta' \geq 3$) te također vrijedi da $D = ab = 2d(2\delta'^2 d - 1)$ nije potpun kvadrat jer je $2d(2\delta'^2 d - 1) \equiv 2 \pmod 4$. Zato tražimo najmanje (netrivijalno) rješenje jednadžbe:

$$u^2 - 2d(2\delta'^2 d - 1)v^2 = 1. \tag{1.19}$$

Prvi korak u traženju fundamentalnog rješenja jednadžbe (1.19) je razvijanje izraza $\sqrt{2d(2\delta'^2 d - 1)}$, $\delta' \geq 3$ u verižni razlomak.
Broj $\sqrt{2d(2\delta'^2 d - 1)}$ ima razvoj oblika:

$$\sqrt{2d(2\delta'^2 d - 1)} = [a_0; \overline{a_1, a_2, \ldots, a_{l-1}, 2a_0}].$$

Brojeve a_i računamo rekurzivno na sljedeći način:

$$a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor, \ s_{i+1} = a_i t_i - s_i, \ t_{i+1} = \frac{d - s_{i+1}^2}{t_i}.$$

$$a_0 = \lfloor \sqrt{2d(2\delta'^2 d - 1)} \rfloor = 2d\delta' - 1, \ s_0 = 0, \ t_0 = 1;$$

$$s_1 = 2d\delta' - 1, \ t_1 = 4d\delta' - 2d - 1, \ a_1 = 1;$$

$$s_2 = 2d\delta' - 2d, \ t_2 = 2d, \ a_2 = 2\delta' - 2;$$

$$s_3 = 2d\delta' - 2d, \ t_3 = 4d\delta' - 2d - 1, \ a_3 = 1;$$

$$s_4 = 2d\delta' - 1, \ t_4 = 1, \ a_4 = 2(2d\delta' - 1) = 2a_0.$$

Dakle, razvoj broja $\sqrt{2d(2\delta'^2 d - 1)}$ u verižni razlomak je

$$\sqrt{2d(2\delta'^2 d - 1)} = [2d\delta' - 1; \overline{1, 2\delta' - 2, 1, 2(2d\delta' - 1)}].$$

Sad tražimo fundamentalno rješenje jednadžbe (1.19). Budući je duljina perioda l razvoja u verižni razlomak jednaka $l = 4$, fundamentalno rješenje jednadžbe (1.19) je dano s (p_3, q_3), gdje brojeve $p_i, q_i,\ i = 0, 1, 2, 3$ računamo rekurzivno:

$$p_0 = a_0,\ p_1 = a_0 a_1 + 1,\ p_k = a_k p_{k-1} + p_{k-2},$$

$$q_0 = 1,\ q_1 = a_1,\ q_k = a_k q_{k-1} + q_{k-2},\ k = 2, 3.$$

Redom dobivamo:

$$(p_0, q_0) = (2d\delta' - 1, 1), \quad (p_1, q_1) = (2d\delta', 1), \quad (p_2, q_2) = (4\delta'^2 d - 2d\delta' - 1, 2\delta' - 1),$$

$$(p_3, q_3) = (4\delta'^2 d - 1, 2\delta').$$

Dobivamo fundamentalno rješenje $(p_3, q_3) = (u_0, v_0) = (4\delta'^2 d - 1, 2\delta')$ i primjenjujemo Lemu 1.4.

U našem slučaju je: $a = 2\delta'^2 d - 1,\ b = 2d$. Iz Leme 1.4 dobivamo:

$$(4\delta'^2 d - 2) | 4\delta'^2 d, \quad 4d | (4\delta'^2 d - 2).$$

Vidimo da $4d|(4\delta'^2 d - 2)$ ako i samo ako $4d|2$ što je nemoguće jer je $d \in \mathbb{N}$. Dakle, jednadžba (1.18) nema rješenja. Time smo pokazali da ne postoji neparan prirodan broj n sa svojstvom da postoji par pozitivnih djelitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da je $d_1 + d_2 = \delta n$, gdje je $\delta \equiv 2 \pmod 4,\ \delta \geq 6$.

□

1.4 Slučaj $\delta = 0$

U ovom potpoglavlju prikazujemo poznate rezultate drugih autora za slučaj u kojem je $\delta = 0$. Ovaj je slučaj bitno različit od svih do sad promatranih, budući da linearni polinom $\delta n + \varepsilon$ postaje konstantni polinom ε, što znači da promatrani polinom više ne ovisi o broju n.

Promatrajući ovaj problem pokušavamo odgovoriti na pitanje možemo li svaki prirodni broj $\varepsilon \equiv 2 \pmod 4$ prikazati kao zbroj dvaju prirodnih brojeva d_1, d_2 za koje vrijedi da su svi prosti faktori od d_1, d_2 oblika $4k + 1$. Ako se koncentriramo na slučaj u kojem zahtijevamo da su djelitelji d_1, d_2 prosti brojevi, problem koji promatramo nas podsjeća

na jaku (binarnu) Goldbachovu slutnju, odnosno slutnju da se svaki paran prirodan broj n, $n \geq 4$, može prikazati kao zbroj dvaju prostih brojeva. Ova se slutnja smatra jednim od najintrigantnijih neriješenih problema u teoriji brojeva već dugi niz godina, pa rješenje nećemo tražiti u obliku u kojem su d_1 i d_2 prosti brojevi.

U iznimno korisnom alatu eksperimentalne matematike naziva Enciklopedija cjelobrojnih nizova (On-Line Encyclopedia of Integer Sequences (OEIS), [19]) kod informacija o nizu numeriranom kao A071636 može se naći slutnja povezana s našim problemom.

Slutnja 1.6 Jedini prirodni brojevi oblika $n = 4k + 2, k \in \mathbb{N}_0$ za koje ne postoji par prostih brojeva $p, q \equiv 1 \pmod 4$ takvih da je $p + q = n$ su brojevi $2, 6, 14, 38, 62$.

□

Uz jaku (binarnu) Goldbachovu slutnju L. Euler i C. Goldbach u pismima koja su izmijenjivali formuliraju i slabu (ternarnu) Goldbachovu slutnju, odnosno slutnju da se svaki neparan prirodan broj $n \geq 5$ može prikazati kao suma triju prostih brojeva. I ovu su slutnju mnogi matematičari pokušavali dokazati dugi niz godina. I. M. Vinogradov je 1937. godine pokazao da slaba Goldbachova slutnja vrijedi za sve prirodne brojeve n koji su veći od vrlo velike konstante C. Iako je nekoliko puta tijekom 20. stoljeća ta konstanta smanjivana, njena je vrijednost ostala iznimno velika (M.-Ch. Liu i T. Wang su 2002. godine odredili da je $C = e^{3100}$). Naposlijetku, peruanski matematičar H. A. Helfgott 2013. godine ostvaruje iznimno značajan rezultat koristeći modernu interpretaciju poznatih rezultata G. H. Hardyja, J. E. Littlewooda i I. M. Vinogradova te u svom radu naslova "The Ternary Goldbach Conjecture Is True" dokazuje tu davno formuliranu slutnju.

No, za razliku od slučaja u kojem zahtijevamo da su $d_1, d_2 \in \mathbb{P}$ te oblika $4k+1$, postoje važni rezultati u dokazivanju da se svaki prirodni broj $\varepsilon \equiv 2 \pmod 4$ može prikazati kao zbroj prirodnih brojeva d_1, d_2 kojima su svi prosti faktori oblika $4k + 1$.

Značajne su rezultate dobili G. Greaves u svom radu [14] i R. Dietmann i C. Elsholtz u [7]. Prije predstavljanja glavnih teorema ovog dijela rada, navodimo neke poznate rezultate o prikazu prirodnih brojeva u obliku sume dva ili četiri kvadrata koji se koriste u dokazivanju glavnog rezultata ovog potpoglavlja.

Lema 1.7 Ako prosti broj p dijeli sumu dvaju kvadrata relativno prostih cijelih brojeva, tada je prosti broj p oblika $4k + 1$.

Dokaz.

Neka je $\text{nzd}(a, b) = 1$ i neka je p neparan prosti broj takav da $p|(a^2 + b^2)$. Tada vrijedi $a^2 \equiv -b^2 \pmod p$, odnosno

$$a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} \pmod p.$$

S obzirom da je $\text{nzd}(a, b) = 1$, brojevi a, b nisu djeljivi brojem p pa prema Malom Fermatovom teoremu vrijedi

$$a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$$

što povlači da je $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ što za $p > 2$ daje $(-1)^{(p-1)/2} = 1$. Dakle, broj $(p-1)/2$ je paran broj, odnosno prosti broj p je oblika $4k + 1$.

□

Korolar 1.8 Ako je p prosti broj oblika $p \equiv 3 \pmod{4}$ i $p|n = a^2 + b^2$, tada $p|a$ i $p|b$.

□

Korolar 1.9 Ako je p prosti broj oblika $p \equiv 3 \pmod{4}$ za kojeg vrijedi da $p|n$, tada n ne možemo prikazati kao sumu dvaju kvadrata relativno prostih cijelih brojeva.

□

Teorem 1.10 Prirodni broj $n = \prod p_i^{a_i}$ moguće je prikazati kao sumu dvaju kvadrata cijelih brojeva ako i samo ako su eksponenti a_i parni za svaki $p_i \equiv 3 \pmod{4}$.

□

Tvrdnja najvažnijeg teorema ovog poglavlja, Teorema 1.14, ima i povijesni značaj. L. Euler je u pismu C. Goldbachu 15. travnja 1747. godine napisao: "Teorem '*Bilo koji broj se može prikazati kao suma četiriju kvadrata*' ovisi o sljedećoj činjenici: *'Svaki se broj oblika* $4m + 2$ *može prikazati kao suma brojeva* $4x + 1$ *i* $4y + 1$ *od kojih nijedan od navedenih brojeva ne smije imati faktor oblika* $4p - 1$'". Kasnije je L. Euler doradio svoje komentare i tvrdio da uvijek možemo odabrati da navedena dva pribrojnika budu prosti brojevi. Danas to zapažanje poznajemo kao jaku formu Goldbachove slutnje. Euler je tada imao u cilju dokazati Teorem o četiri kvadrata. Predstavio je problem u obliku

$$4m + 2 = a^2 + b^2 + c^2 + d^2$$

i utvrdio da bi, bez smanjenja općenitosti, brojevi a, b trebali biti parni, a brojevi c, d neparni. Na taj način brojevi $a^2 + c^2 = 4x + 1$ i $b^2 + d^2 = 4y + 1$ zadovoljavaju Eulerove uvjete, osim u slučaju kad brojevi a, c ili brojevi b, d imaju zajednički prosti faktor oblika $4p - 1$ što je pokušavao kroz dokaz isključiti.

L. Euler nije uspio dokazati Teorem o četiri kvadrata. Nakon njega je J. L. Lagrange proučavao isti problem i 1770. godine dokazuje Teorem o četiri kvadrata koristeći Eulerov identitet o četiri kvadrata.

Teorem 1.11 (Teorem o četiri kvadrata, Lagrange) Svaki prirodan broj može se prikazati u obliku sume kvadrata četiri cijela broja.

□

Nekoliko godina kasnije A. M. Legendre je poboljšao Lagrangeov rezultat dokazujući da se svaki prirodni broj n može prikazati kao suma kvadrata triju cijelih brojeva ako i samo ako prirodni n nije oblika $n = 4^a(8b + 7),\ \ a, b \in \mathbb{N}$.

Definicija 1.12 Neka su zadane dvije funkcije $f, g : \mathbb{R} \to \mathbb{R}$. Pišemo $f(x) = O(g(x))$, za $x \to \infty$, ako postoje konstante $C_1, C_2 \in \mathbb{R}$ za koje vrijedi

$$|f(x)| < C_1|g(x)|,\ \ x > C_2.$$

Teorem 1.13 (Greaves) Neka je $n \not\equiv 0, 1, 5 \pmod 8$ i neka je $S(n)$ broj parova (p, q), $p, q \in \mathbb{P}$ za koje je

$$1 < p < \sqrt{n/2},\ \ 1 < q < \sqrt{n/2}$$

te vrijedi da se broj $n - p^2 - q^2$ može prikazati kao suma $x^2 + y^2$. Tada vrijedi

$$S(n) > A\frac{n}{\log^{5/2} n}\left(1 + O\left(\frac{\log\log n}{(\log n)^{1/10}}\right)\right),$$

gdje je $A > 0$. Svaki dovoljno veliki broj n zadanog oblika moguće je prikazati kao sumu

$$x^2 + y^2 + p^2 + q^2,$$

gdje su p, q neparni prosti brojevi.

□

Konstanta $A > 0$ je eksplicitno izražena u dokazu glavnog Teorema 1.13 u [14], no nije precizirano i što izraz "dovoljno velik" za broj n znači.

Koristeći rezultate iz [14], R. Dietmann i C. Elsholtz su dokazali sljedeći teorem koji garantira da se svaki dovoljno velik prirodan broj n oblika $n \equiv 2 \pmod 4$ može prikazati kao suma dvaju prirodnih brojeva d_1, d_2. Iako nije eksplicitno naznačeno što znači "dovoljno velik" broj n, ovaj je teorem najvažniji rezultat ovog potpoglavlja.

Teorem 1.14 (Dietmann, Elsholtz) Neka je n dovoljno velik prirodan broj za koji vrijedi $n \equiv 2 \pmod 4$. Tada se broj n može prikazati kao suma dvaju prirodnih brojeva od kojih nijedan broj ne sadrži proste faktore oblika $p \equiv 3 \pmod 4$ u svojoj faktorizaciji.

Dokaz.
Prema Teoremu 1.13 znamo da se svaki dovoljno veliki broj n oblika $n \equiv 2 \pmod 4$ može prikazati u obliku

$$n = x^2 + y^2 + p^2 + q^2,$$

gdje su $p, q \in \mathbb{P}$, te $x, y \in \mathbb{N}$, te uočavamo da je broj takvih reprezentacija najmanje reda $n(\log n)^{-5/2}$.

Neka je $a = p^2 + x^2$ te $b = q^2 + y^2$. Broj prikaza broja a kao sume dvaju relativno prostih kvadrata, gdje pritom ne razlikujemo prikaze koji se razlikuju samo u poretku pribrojnika, označavamo s $r_2(a)$.

Iz [18] možemo uočiti da vrijedi nejednakost $r_2(a) \leq \tau(a)$, gdje je $\tau(a)$ broj djelitelja od a. Naime, neka je $a = \prod_p p^{\alpha(p)}$. Znamo da je

$$\tau(a) = \prod_p (\alpha(p) + 1).$$

Ako je $\alpha(2) = 0$ ili 1, te $\alpha(p) = 0$ za sve proste brojeve oblika $p \equiv 3 \pmod 4$, onda je $r_2(a) = 2^{t-1}$, gdje je t broj prostih faktora od a oblika $4k + 1$. U protivnom je $r_2(a) = 0$. Slijedi $r_2(a) \leq \tau(a)$.

U knjizi [21] (Poglavlje 1, Teorem 5.2.) dokazano je da za svaki $\eta > 0$ i $k > k_0(\eta)$ vrijedi nejednakost

$$\tau(k) < \exp\left\{(1+\eta)\log 2 \frac{\log k}{\log\log k}\right\},$$

odnosno

$$\tau(k) \ll k^\eta, \ \ \eta > 0,$$

gdje je $\tau(k)$ broj djelitelja od k, a oznaka $\tau(k) \ll k^\eta, \ \eta > 0$, ekvivalentna je oznaci $\tau(k) = O(k^\eta)$.

U našem slučaju možemo zaključiti

$$r_2(a) \leq \tau(a) \ll a^\eta \ll n^\eta, \ \ \eta > 0.$$

Analogne nejednakosti vrijede i za broj reprezentacija broja b kao sume dvaju kvadrata, što označavamo s $r_2(b)$.

Dakle, postoji barem $n^{1-2\eta}$ parova brojeva (a, b) takvih da je $n = a + b$ i da su a i b sume kvadrata prostog broja i kvadrata cijelog broja.

Neka je w prosti broj oblika $w \equiv 3 \pmod 4$ te neka $w|a = p^2 + x^2$. Prema Korolaru 1.8 i činjenici da je p prost broj, jasno je da je $p = w$ i $w|x$. U tom slučaju možemo zaključiti da je najviše $O(1 + \frac{\sqrt{n}}{w})$ brojeva a djeljivo s w, a za svaki takav broj a postoji točno jedan broj b budući vrijedi $n = a + b$. Analogne zaključke donosimo i u slučaju ako $w|b$. Očito je $w \leq \sqrt{n}$. Sumirajući po svim takvim brojevima w zaključujemo da je broj parova (a, b) takvih da je $n = a + b$ gdje je jedan od brojeva a, b djeljiv prostim brojem $p \equiv 3 \pmod 4$ jednak najviše $O(\sqrt{n}\log\log n)$ što je manjeg reda veličine od izraza $n^{1-2\eta}$, za $0 < \eta < 1/4$, kojeg smo dobili na početku dokaza. Dobili smo kontradikciju za dovoljno veliki n, što dokazuje tvrdnju teorema.

□

Poglavlje 2

Jednoparametarske familije koeficijenata linearnog polinoma $\delta n + \varepsilon$

U drugom poglavlju doktorskog rada promatramo sličan, ali općenitiji problem. Ispitujemo postoji li beskonačno mnogo neparnih prirodnih brojeva n za koje postoje djelitelji d_1, d_2 broja $(n^2+1)/2$ za koje vrijedi da su koeficijenti δ, ε linearnog polinoma $\delta n + \varepsilon$ u međusobnoj ovisnosti. Naime, promatramo jednoparametarske familije koeficijenata takve da je u jednom slučaju $\varepsilon = \delta + 2$, a u drugom slučaju $\varepsilon = \delta - 2$.

U slučaju u kojem je $\varepsilon = \delta + 2$ dokazujemo da postoji beskonačno mnogo neparnih prirodnih brojeva n s traženim svojstvom, a u dokazu koristimo vrlo slične metode kao u dokazima teorema iz prethodnog poglavlja.

U slučaju kad je $\varepsilon = \delta - 2$ metode dokazivanja su bitno različite od svih metoda koje smo primjenjivali u dokazima prethodnih teorema. Problem razlažemo na četiri podslučaja koji odgovaraju četirima klasama ostataka pri dijeljenju brojem 8 za parne brojeve $\varepsilon = \delta - 2$. U radu detaljno prikazujemo dokaze za slučajeve $\delta \equiv 4, 6 \pmod 8$, dok ekvivalentan problem za $\delta \equiv 0, 2 \pmod 8$ ostaje za buduće promatranje, s obzriom da prikazane metode u tim slučajevima ne mogu biti primjenjene. Promatrane probleme prikazujemo pellovskim i pridruženim Pellovim jednadžbama oblika

$$U^2 - 2abcV^2 = 1$$

koje onda predstavljamo kao

$$(U-1)(U+1) = 2abcV^2$$

i postavljamo uvjet da su brojevi a, b, c prosti brojevi. Navodimo sve mogućnosti za vrijednosti izraza $U \pm 1$ i određujemo samo one koje će garantirati postojanje beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju traženo svojstvo. Uz pomoć kvadratnih kongruencija, odnosno Legendreovih i Jacobijevih simbola, dokazujemo da postoje brojevi koji istovremeno čine faktorizacije koje osiguravaju rješenja mogućima, te

faktorizacije koje nam ne osiguravaju rješenja nemogućima. U radu su prikazani uvjetni dokazi tvrdnji koji su uvjetovani valjanošću Schinzelove hipoteze H o distribuciji prostih brojeva kojom osiguravamo tvrdnju da su brojevi a, b, c prosti brojevi.

2.1 Slučaj $\varepsilon = \delta + 2$

U ovom potpoglavlju doktorskog rada promatramo jednoparametarske familije koeficijenata linearnog polinoma $\delta n+\varepsilon$ za koje vrijedi $(\delta, \varepsilon) = (\delta, \delta+2)$. Određujemo beskonačno mnogo neparnih prirodnih brojeva n koji zadovoljavaju traženo svojstvo, odnosno za djelitelje d_1, d_2 od $(n^2+1)/2$ vrijedi

$$d_1 + d_2 = \delta(n+1) + 2.$$

U dokazu Teorema 2.1 navodimo beskonačno mnogo neparnih prirodnih brojeva n za koje vrijedi da djelitelji d_1, d_2 broja $(n^2+1)/2$ imaju svojstvo

$$d_1 d_2 = \frac{n^2+1}{2},$$

pri čemu ne vrijedi nužno da $\text{nzd}(d_1, d_2) = d = 1$ kao što je to bio slučaj u dokazima teorema iz prethodnog poglavlja.

Teorem 2.1 Za svaki paran prirodni broj δ postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoji par pozitivnih djeljitelja d_1, d_2 od $\frac{n^2+1}{2}$ takvih da vrijedi

$$d_1 + d_2 = \delta(n+1) + 2.$$

Dokaz.

Neka je δ paran prirodan broj. Stavimo $g = \text{nzd}(d_1, d_2)$ i pišemo $d_1 = gd_1', d_2 = gd_2'$. Budući je $gd_1'd_2' = \text{nzv}(d_1, d_2)$ i $\text{nzd}(d_1, d_2)$ dijeli $\frac{n^2+1}{2}$, zaključujemo da postoji $d \in \mathbb{N}$ takav da je

$$d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

Iz poznatog identiteta

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1 d_2,$$

uvrštavanjem relacija koje vrijede u ovom slučaju dobivamo:

$$(d_2 - d_1)^2 = (\delta(n+1) + 2)^2 - 2\frac{g(n^2+1)}{d},$$

$$d(d_2 - d_1)^2 = d(\delta^2(n+1)^2 + 4\delta(n+1) + 4) - 2g(n^2+1),$$

$$d(d_2 - d_1)^2 = (\delta^2 d - 2g)n^2 + 2d\delta(\delta + 2)n + \delta^2 d + 4d\delta + 4d - 2g,$$

$$d(\delta^2 d - 2g)(d_2 - d_1)^2 =$$

$$= (\delta^2 d - 2g)^2 n^2 + 2d\delta(\delta^2 d - 2g)(\delta + 2)n + \delta^4 d^2 + 4\delta^3 d^2 + 4d^2\delta^2 - 4\delta^2 dg - 8d\delta g - 8dg + 4g^2.$$

Definiramo li $X = (\delta^2 d - 2g)n + d\delta(\delta + 2)$, $Y = d_2 - d_1$ prethodna jednadžba postaje

$$X^2 - d(\delta^2 d - 2g)Y^2 = 4\delta^2 dg + 8d\delta g + 8dg - 4g^2. \tag{2.1}$$

U slučaju kad je $d = g$ desna strana jednadžbe (2.1) postaje potpuni kvadrat, odnosno $4\delta^2 dg + 8d\delta g + 8dg - 4g^2 = (2d(\delta + 1))^2$ i vrijedi

$$X^2 - d(\delta^2 d - 2d)Y^2 = (2d(\delta + 1))^2.$$

Rješenja tražimo u obliku $X = dX'$ pa u tom slučaju cijeli izraz možemo podijeliti s d^2 nakon čega dobivamo

$$X'^2 - (\delta^2 - 2)Y^2 = 4(\delta + 1)^2. \tag{2.2}$$

Broj δ je paran broj pa uočavamo da $\delta^2 - 2 \equiv 2 \pmod 4$ sigurno nije potpun kvadrat. Također, desna strana izraza nikad nije jednaka nuli. Jednadžba (2.2) je pellovska jednadžba. Da bi dobili Pellovu jednadžbu, tražimo rješenja u obliku $X' = 2(\delta+1)U$ i $Y' = 2(\delta+1)V$. Dijeljenjem s $(2(\delta + 1))^2$ jednadžba (2.2) postaje

$$U^2 - (\delta^2 - 2)V^2 = 1 \tag{2.3}$$

što je Pellova jednadžba pridružena pellovskoj jednadžbi (2.2) i kao takva jednadžba (2.3) ima beskonačno mnogo rješenja (U, V). Također, jednadžba (2.2) ima beskonačno mnogo rješenja (X, Y).

Kako bi odredili o kojim se (U, V) rješenjima radi, prvi je korak razviti izraz $\sqrt{\delta^2 - 2}$ u verižni razlomak.

Stavimo $D = \delta^2 - 2$. Dobivamo redom:
$a_0 = \lfloor\sqrt{D}\rfloor = \lfloor\sqrt{\delta^2 - 2}\rfloor = \delta - 1,\ s_0 = 0,\ t_0 = 1,$
$s_1 = a_0 t_0 - s_0 = \delta - 1,\ t_1 = \frac{D - s_1^2}{t_0} = 2\delta - 3,\ a_1 = \lfloor\frac{a_1 + \sqrt{D}}{t_1}\rfloor = 1,$
$s_2 = \delta - 2,\ t_2 = 2,\ a_2 = \delta - 2,$
$s_3 = \delta - 2,\ t_3 = 2\delta - 3,\ a_3 = 1,$
$s_4 = \delta - 1,\ t_4 = 1,\ a_4 = 2\delta - 2.$
Razvoj u verižni razlomak izraza $\sqrt{\delta^2 - 2}$ je

$$\sqrt{\delta^2 - 2} = [\delta - 1; \overline{1, \delta - 2, 1, 2\delta - 2}].$$

Duljina razvoja u verižni razlomak broja $\sqrt{\delta^2 - 2}$ je $l = 4$ pa je fundamentalno rješenje jednažbe $(U_1, V_1) = (p_3, q_3)$ gdje vrijednosti (p_i, q_i) dobivamo rekurzivno: $p_0 = a_0 = \delta - 1,\ p_1 = a_0a_1 + 1 = \delta,\ p_2 = a_2p_1 + p_0 = \delta^2 - \delta - 1,\ p_3 = a_3p_2 + p_1 = \delta^2 - 1$ te $q_0 = q_1 = 1,\ q_2 = a_2q_1 + q_0 = \delta - 1,\ q_3 = a_3q_2 + q_1 = \delta$. Dakle, fundamentalno rješenje je $(U_1, V_1) = (\delta^2 - 1, \delta)$. Sva rješenja jednadžbe definirana su s

$$U_0 = 1,\ U_1 = \delta^2 - 1,\ U_{m+2} = 2(\delta^2 - 1)U_{m+1} - U_m,$$

$$V_0 = 0,\ V_1 = \delta,\ V_{m+2} = 2(\delta^2 - 1)V_{m+1} - U_m,\ m \in \mathbb{N}_0.$$

Znamo da je $X = 2d(\delta + 1)U$ i $X = (\delta^2 d - 2d)n + d\delta(\delta + 2)$ pa izjednačavanjem navedenih vrijednosti i izražavanjem broja n dobivamo

$$n = \frac{2(\delta + 1)U - \delta(\delta + 2)}{\delta^2 - 2}.$$

Treba dokazati da se radi o broju n koji je prirodan broj, odnosno treba dokazati da $(\delta^2 - 2)|(2(\delta + 1)U - \delta(\delta + 2))$.

Prije toga moramo odrediti ostatak pri dijeljenju U_m brojem $\delta^2 - 2$. Budući znamo kako su $U_m,\ m \in \mathbb{N}_0$ generirani, dokaz provodimo matematičkom indukcijom po m.

Znamo $U_0 = 1 \equiv 1 \pmod{\delta^2 - 2}, U_1 = \delta^2 - 1 \equiv 1 \pmod{\delta^2 - 2}$.
Pretpostavimo da je $U_{m-1} \equiv U_m \equiv 1 \pmod{\delta^2 - 2}$.
Dokazujemo da vrijedi $U_{m+1} \equiv 1 \pmod{\delta^2 - 2}$.
Znamo

$$U_{m+1} = 2(\delta^2 - 1)U_m - U_{m-1} \equiv 2 - 1 \equiv 1 \pmod{\delta^2 - 2}.$$

Dakle, $U_m \equiv 1 \pmod{\delta^2 - 2}, m \in \mathbb{N}_0$. Također, $\delta^2 + 2\delta \equiv 2\delta + 2 \pmod{\delta^2 - 2}$ pa je iz svega zaključenog jasno da je $n \equiv 0 \pmod{\delta^2 - 2}$. Dokazali smo da je n neparan prirodan broj.

Generirajmo prvih nekoliko neparnih prirodnih brojeva n za U_1, U_2, U_3.
Budući znamo da vrijedi

$$d_1 + d_2 = \delta n + \delta + 2,\ d_1d_2 = \frac{n^2 + 1}{2}, \tag{2.4}$$

pomoću Viéteovih formula možemo odrediti i izraze za d_1, d_2 za svaki neparni prirodni broj n.
Na početku dobivamo kvadratnu jednadžbu oblika

$$d^2 - (d_1 + d_2)d + d_1d_2 = 0,$$

$$d^2 - (\delta n + \delta + 2)d + \frac{n^2 + 1}{2} = 0. \tag{2.5}$$

Rješenja kvadratne jednažbe (2.5) su djelitelji d_1, d_2 broja $\frac{n^2+1}{2}$ za koje su zadovoljeni uvjeti (2.4).
Iz (2.5) lako dobivamo:

$$d_{1,2} = \frac{2\delta n + 2\delta + 4 \pm \sqrt{4(\delta n + \delta + 2)^2 - 8(n^2+1)}}{4}. \tag{2.6}$$

Za $U = U_1 = \delta^2 - 1$ vrijedi

$$n = \frac{2(\delta+1)(\delta^2-1) - \delta(\delta+2)}{\delta^2 - 2} = 2\delta + 1.$$

Uvrštavajući $n = 2\delta + 1$ u (2.6), dobivamo:

$$d_{1,2} = \frac{2\delta(2\delta+1) + 2\delta + 4 \pm 4\delta(1+\delta)}{4} = \frac{4\delta^2 + 4\delta + 4 \pm (4\delta^2 + 4\delta)}{4},$$

iz čega slijedi

$$d_1 = 1, \;\; d_2 = 2\delta^2 + 2\delta + 1.$$

Za $U = U_2 = 2\delta^4 - 4\delta^2 + 1$ vrijedi da je

$$n = \frac{2(\delta+1)(2\delta^4 - 4\delta^2 + 1) - \delta(\delta+2)}{\delta^2 - 2} = 4\delta^3 + 4\delta^2 - 1.$$

Uvrštavajući dobiveni broj n u (2.6), dobivamo:

$$d_{1,2} = \frac{2\delta(4\delta^3 + 4\delta^2 - 1) + 2\delta + 4 \pm \sqrt{4(\delta(4\delta^3 + 4\delta^2 - 1) + \delta + 2)^2 - 8((4\delta^3 + 4\delta^2 - 1)^2 + 1)}}{4}.$$

Pojednostavljivanjem prethodnog izraza određujemo vrijednosti traženih brojeva d_1, d_2:

$$d_{1,2} = \frac{8\delta^4 + 8\delta^3 + 4 \pm 8\delta(\delta-1)(\delta+1)^2}{4},$$

odnosno

$$d_1 = 2\delta^2 + 2\delta + 1, \;\; d_2 = 4\delta^4 + 4\delta^3 - 2\delta^2 - 2\delta + 1.$$

Za $U = U_3 = 4\delta^6 - 12\delta^4 + 9\delta^2 - 1$ vrijedi da je

$$n = \frac{2(\delta+1)(4\delta^6 - 12\delta^4 + 9\delta^2 - 1) - \delta(\delta+2)}{\delta^2 - 2} = 8\delta^5 + 8\delta^4 - 8\delta^3 - 8\delta^2 + 2\delta + 1,$$

te analognim postupkom dobivamo:

$$d_1 = 4\delta^4 + 4\delta^3 - 2\delta^2 - 2\delta + 1, \;\; d_2 = 8\delta^6 + 8\delta^5 - 12\delta^4 - 12\delta^3 + 4\delta^2 + 4\delta + 1.$$

Dakle, na navedeni način možemo dobiti beskonačno mnogo neparnih prirodnih brojeva

n koji zadovoljavaju zadana svojstva. Tako dobivamo:

$$\begin{cases} n = 2\delta + 1, \\ d_1 = 1, \\ d_2 = 2\delta^2 + 2\delta + 1. \end{cases}$$

$$\begin{cases} n = 4\delta^3 + 4\delta^2 - 1, \\ d_1 = 2\delta^2 + 2\delta + 1, \\ d_2 = 4\delta^4 + 4\delta^3 - 2\delta^2 - 2\delta + 1. \end{cases}$$

$$\begin{cases} n = 8\delta^5 + 8\delta^4 - 8\delta^3 - 8\delta^2 + \delta + 1, \\ d_1 = 4\delta^4 + 4\delta^3 - 2\delta^2 - 2\delta + 1, \\ d_2 = 8\delta^6 - 12\delta^4 - 12\delta^3 + 4\delta^2 + 4\delta + 1. \end{cases}$$

□

Možemo primjetiti da je djelitelj d_2 broja $\frac{n^2+1}{2}$ koji je dobiven pomoću broja U_1 ujedno i djelitelj d_1 broja $\frac{n^2+1}{2}$ koji je dobiven pomoću broja U_2. Također, djelitelj d_2 broja $\frac{n^2+1}{2}$ koji je dobiven pomoću broja U_2 ujedno i djelitelj d_1 broja $\frac{n^2+1}{2}$ koji je dobiven pomoću broja U_3. Nastojimo općenito dokazati da dvije kvadratne jednadžbe oblika (2.5) koje nastaju koristeći susjedne brojeve n (generirane susjednim članovima rekurzivnog niza $U_m, m \geq 1$) imaju zajedničku nultočku.

Definicija 2.2 Neka su zadana dva polinoma $f, g \in K[x]$ pozitivnog stupnja, odnosno neka je zadano:

$$f(x) = a_0 x^l + \cdots + a_l, \;\; a_0 \neq 0, \;\; l > 0,$$

$$g(x) = b_0 x^m + \cdots + b_m, \;\; b_0 \neq 0, \;\; m > 0. \tag{2.7}$$

Definiramo rezultantu od f i g, u oznaci $\mathrm{Res}(f, g)$, kao determinantu tipa $(l+m) \times (l+m)$

$$\mathrm{Res}(f,g) = \det \begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & a_2 & \ddots & a_0 & \vdots & b_2 & \ddots & b_0 \\ a_l & \vdots & \ddots & a_1 & b_m & \vdots & \ddots & b_1 \\ & a_l & & a_2 & & b_m & & b_2 \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_l & & & & b_m \end{bmatrix},$$

gdje su na praznim mjestima nule.

Tri su osnovna svojstva rezultante:

- (Cjelobrojni polinom) $\mathrm{Res}(f, g)$ je cjelobrojni polinom u koeficijentima od f i g,
- (Zajednički faktor) $\mathrm{Res}(f, g) = 0$ ako i samo ako f i g imaju zajednički faktor u $K[x]$,
- (Eliminacija) Postoje polinomi $A, B \in K[x]$ takvi da je $Af + Bg = \mathrm{Res}(f, g)$. Koeficijenti od A, B su cjelobrojni polinomi u koeficijentima od f i g.

Prvo svojstvo rezultante proizlazi iz njene definicije. Dokaz svojstva zajedničkog faktora rezultante možemo naći u [12], dok je dokaz trećeg svojstva rezultante u [16].

Prema drugom svojstvu rezultante poznato je da ako dva polinoma imaju zajedničku nultočku, njihova je rezultanta jednaka nuli. Vrijedi i obrat tvrdnje. Pogledajmo je li to svojstvo općenito potvrđeno i na kvadratnim polinomima koje smo dobili djelitelje d_1, d_2 za brojeve $\frac{n^2+1}{2}$ generirane članovima U_1, U_2 rekurzivnog niza $U_i, m \geq 1$. Koristimo li U_1 dobivamo $n = 2\delta + 1$ pa kvadratna jednadžba

$$2d^2 - 2(\delta n + \delta + 2)d + n^2 + 1 = 0$$

postaje

$$2d^2 - 2(\delta(2\delta + 1) + \delta + 2)d + (2\delta + 1)^2 + 1 = 0,$$

$$2d^2 - 2(2\delta^2 + 2\delta + 2)d + 4\delta^2 + 4\delta + 2 = 0. \tag{2.8}$$

Analogno, za neparan prirodan broj n generiran brojem U_2 dobivamo:

$$2d^2 - 2(4\delta^4 + 4\delta^3 + 2)d + 16\delta^6 + 32\delta^5 + 16\delta^4 - 8\delta^3 - 8\delta^2 + 2 = 0. \tag{2.9}$$

Odredimo rezultantu kvadratnih polinoma (2.8) i (2.9). Znamo da dva promatrana polinoma imaju jednu nultočku zajedničku. U skladu s tim i rezultanta tih dvaju polinoma bi trebala biti jednaka nuli. Zaista, vrijedi

$$\begin{vmatrix} 2 & 0 & 2 & 0 \\ -2(2\delta^2+2\delta+2) & 2 & -2(4\delta^4+4\delta^3+2) & 2 \\ 4\delta^2+4\delta+2 & -2(2\delta^2+2\delta+2) & 16\delta^6+32\delta^5+16\delta^4-8\delta^3-8\delta^2+2 & -2(4\delta^4+4\delta^3+2) \\ 0 & 4\delta^2+4\delta+2 & 0 & 16\delta^6+32\delta^5+16\delta^4-8\delta^3-8\delta^2+2 \end{vmatrix} = 0.$$

Idućom propozicijom dokazujemo da ovo svojstvo vrijedi općenito.

Propozicija 2.3 Svaka dva polinoma oblika (2.5) generirana susjednim vrijednostima broja n, odnosno, susjednim članovima rekurzivnog niza U_i, $m \geq 1$, imaju zajedničku nultočku. Dakle, svaka dva susjedna broja oblika $\frac{n^2+1}{2}$ imaju zajednički djelitelj.

Dokaz.

Neka su $U_{m-1},\ U_m$ dva susjedna člana rekurzije kojima generiramo dvije vrijednosti za neparan prirodni broj n. Dobivamo dva kvadratna polinoma oblika:

$$2d^2 - 2\left(\delta\frac{2(\delta+1)U_{m-1}-\delta(\delta+2)}{\delta^2-2}+\delta+2\right)d+\left(\frac{2(\delta+1)U_{m-1}-\delta(\delta+2)}{\delta^2-2}\right)^2+1=0, \tag{2.10}$$

$$2d^2 - 2\left(\delta\frac{2(\delta+1)U_{m}-\delta(\delta+2)}{\delta^2-2}+\delta+2\right)d+\left(\frac{2(\delta+1)U_{m}-\delta(\delta+2)}{\delta^2-2}\right)^2+1=0. \tag{2.11}$$

Pripadajuća rezultanta je oblika

$$\begin{vmatrix} 2 & 0 & 2 & 0 \\ -2\left(\delta\frac{2(\delta+1)U_{m-1}-\delta(\delta+2)}{\delta^2-2}+\delta+2\right) & 2 & -2\left(\delta\frac{2(\delta+1)U_{m}-\delta(\delta+2)}{\delta^2-2}+\delta+2\right) & 2 \\ \left(\frac{2(\delta+1)U_{m-1}-\delta(\delta+2)}{\delta^2-2}\right)^2+1 & -2\left(\delta\frac{2(\delta+1)U_{m-1}-\delta(\delta+2)}{\delta^2-2}+\delta+2\right) & \left(\frac{2(\delta+1)U_{m}-\delta(\delta+2)}{\delta^2-2}\right)^2+1 & -2\left(\delta\frac{2(\delta+1)U_{m}-\delta(\delta+2)}{\delta^2-2}+\delta+2\right) \\ 0 & \left(\frac{2(\delta+1)U_{m-1}-\delta(\delta+2)}{\delta^2-2}\right)^2+1 & 0 & \left(\frac{2(\delta+1)U_{m}-\delta(\delta+2)}{\delta^2-2}\right)^2+1 \end{vmatrix}$$

$$= \frac{64(1+\delta^4)(U_m-U_{m-1})^2(\delta^4+(U_m+U_{m-1})^2-2\delta^2(1+U_mU_{m-1}))}{(\delta^2-2)^4}.$$

Uvjet da rezultanta bude jednaka nuli je

$$\delta^4 - 2\delta^2(U_mU_{m-1}+1)+(U_m+U_{m-1})^2=0. \tag{2.12}$$

Matematičku indukciju koristimo kako bi dokazali da vrijedi (2.12).

Promatramo prva dva člana rekurzije, $U_0,\ U_1$. Znamo da je po definiciji $U_0 = 1$.

Uvrstimo li $U_0,\ U_1$ u prethodnu jednakost, dobivamo:

$$\delta^4 - 2\delta^2 + (2-2\delta^2)(\delta^2-1)+1+(\delta^2-1)^2 = \delta^4-2\delta^4-2+2\delta^2+1+\delta^4-2\delta^2+1=0.$$

Pretpostavimo da vrijedi

$$\delta^4 - 2\delta^2 + (2-2\delta^2)U_{m-1}U_m + U_{m-1}^2 + U_m^2 = 0.$$

Tvrdnja će i općenito biti dokazana ako dokažemo da vrijedi

$$\delta^4 - 2\delta^2 + (2-2\delta^2)U_{m}U_{m+1} + U_{m+1}^2 + U_m^2 = 0.$$

Rekurzija je zadana tako da vrijedi

$$U_{m+1} = 2(\delta^2-1)U_m - U_{m-1}.$$

Tako dobivamo:

$$\delta^4 - 2\delta^2 + (2 - 2\delta^2)U_m(2(\delta^2 - 1)U_m - U_{m-1}) + (2(\delta^2 - 1)U_m - U_{m-1})^2 + U_m^2 = 0,$$

$$\delta^4 - 2\delta^2(2\delta^2 U_m - 2U_m - U_{m-1})U_m - 2\delta^2 + 4(\delta^2 - 1)^2 U_m^2 -$$
$$-4(\delta^2 - 1)U_{m-1}U_m + U_{m-1}^2 + 2(2\delta^2 U_m - 2U_m - U_{m-1})U_m + U_m^2 = 0.$$

Jednostavnim operacijama dolazimo do izraza

$$\delta^4 - 2\delta^2 + (2 - 2\delta^2)U_{m-1}U_m + U_{m-1}^2 + U_m^2 = 0,$$

što znamo da vrijedi prema pretpostavci indukcije. Na ovaj je način dokazana tvrdnja propozicije.

□

Primjer 2.4 Kao ilustraciju za slučaj $\delta \equiv 2 \pmod 4$, uzmimo $\delta = 10$. Dobivamo sljedeće vrijednosti:

$$(n, \frac{n^2+1}{2}, d_1, d_2, \delta, \varepsilon) = (21, 221, 1, 221, 10, 12), (4399, 9675601, 221, 43781, 10, 12), ...$$

Primjer 2.5 Kao primjer slučaja kad je $\delta \equiv 0 \pmod 4$ uzmimo da je $\delta = 8$. Dobivamo sljedeće vrijednosti:

$$(n, \frac{n^2+1}{2}, d_1, d_2, \delta, \varepsilon) = (17, 145, 1, 145, 8, 10), (2303, 2651905, 145, 18289, 8, 10), ...$$

2.2 Slučaj $\varepsilon = \delta - 2$

U ovom potpoglavlju doktorskog rada promatramo parne koeficijente δ, ε linearnog polinoma $\delta n + \varepsilon$ takve da za slobodni koeficijent ε vrijedi $\varepsilon = \delta - 2$. Nastojimo dokazati da postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoje djelitelji d_1, d_2 od $(n^2 + 1)/2$ takvi da je

$$d_1 + d_2 = \delta n + \delta - 2. \tag{2.13}$$

Problem prikazujemo Pellovom jednadžbom čije je svojstvo beskonačnost njenih rješenja koje onda koristimo za određivanje neparnih prirodnih brojeva n. Pellova jednadžba koja se javlja u dokazima propozicija ovog potpoglavlja je

$$U^2 - 2abcV^2 = 1.$$

Tu jednadžbu prikazujemo u obliku

$$(U-1)(U+1) = 2abcV^2$$

te uvjetujemo da su a, b, c prosti brojevi što možemo učiniti koristeći Schinzelovu hipotezu H o distribuciji prostih brojeva. Određujemo uvjete koje navedena faktorizacija treba zadovoljavati, a onda Legendreovim i Jacobijevim simbolima isključujemo sve ostale uvjete koji se javljaju. Na taj način dobivamo beskonačno mnogo Pellovih jednadžbi što rezultira i s beskonačno mnogo neparnih prirodnih brojeva n za koje postoje djelitelji d_1, d_2 od $(n^2+1)/2$ za koje vrijedi (2.13).

Potpoglavlje se sastoji od propozicija u kojima je uvjetno dokazano da za svaki $\delta \equiv 4, 6 \pmod 8$ postoji beskonačno mnogo neparnih prirodnih brojeva n sa svojstvom (2.13). U slučaju u kojem je $\delta \equiv 0, 2 \pmod 8$ navedenim metodama ne možemo dokazati analognu tvrdnju pa navedeni problemi ostaju otvoreni za buduće promatranje. U potpoglavlju navodimo i razloge zbog kojih primjenjivane metode za slučaj $\delta \equiv 0, 2 \pmod 8$ ne daju rezultate.

Neka je $g = \text{nzd}(d_1, d_2)$ i broj $d \in \mathbb{N}$ takav da vrijedi jednakost

$$d_1 d_2 = \frac{g(n^2+1)}{2d}.$$

Vrijede kongruencije $g \equiv d \equiv d_1 \equiv d_2 \equiv 1 \pmod 4$.
Iz identiteta

$$(d_2 - d_1)^2 = (d_1 + d_2)^2 - 4d_1 d_2,$$

dobivamo

$$(d_2 - d_1)^2 = (\delta n + \varepsilon)^2 - \frac{2g(n^2+1)}{d},$$

$$d(d_2 - d_1)^2 = d(\delta n + \varepsilon)^2 - 2g(n^2+1),$$

$$d(d_2 - d_1)^2 = (\delta^2 d - 2g)n^2 + 2d\delta\varepsilon n + \varepsilon^2 d - 2g,$$

$$d(\delta^2 d - 2g)(d_2 - d_1)^2 = (\delta^2 d - 2g)^2 n^2 + 2d\delta\varepsilon(\delta^2 d - 2g)n + d^2\delta^2\varepsilon^2 - 2\delta^2 dg - 2\varepsilon^2 dg + 4g^2.$$

Prethodna jednakost postaje

$$X^2 - d(d\delta^2 - 2g)Y^2 = 2dg(\delta^2 + \varepsilon^2) - 4g^2, \tag{2.14}$$

gdje je $X = n(d\delta^2 - 2g) + d\delta\varepsilon$ te $Y = d_2 - d_1$.

U općenitom slučaju, budući je $g = \text{nzd}(d_1, d_2)$ i vrijedi $d_1 + d_2 = \delta n + \varepsilon$, zaključujemo da $g|(\delta n + \varepsilon)$, što povlači $g|(\delta^2 n^2 - \varepsilon^2)$. S obzirom da $g|(n^2+1)$ vrijedi i $g|\delta^2(n^2+1)$

naposlijetku možemo zaključiti da $g|(\delta^2 n^2 + \delta^2 - \delta^2 n^2 + \varepsilon^2)$, odnosno

$$g|(\delta^2 + \varepsilon^2).$$

Koeficijenti δ, ε su parni pa vrijedi $\delta^2 + \varepsilon^2 \equiv 0 \pmod 4$, dok je $g \equiv 1 \pmod 4$. Zaključujemo da općenito vrijedi $g|\frac{\delta^2+\varepsilon^2}{4}$. U ovom potpoglavlju je $\varepsilon = \delta - 2$ pa sve do sad zaključeno možemo prikazati kao

$$g \mid \frac{\delta^2 - 2\delta + 2}{2}.$$

Definirajmo stoga $g = \frac{\delta^2+\varepsilon^2}{4} = \frac{\delta^2-2\delta+2}{2}$ pa (3.5) postaje

$$X^2 - d(d\delta^2 - 2g)Y^2 = 4g^2(2d - 1). \tag{2.15}$$

Za $d = 2k^2 - 2k + 1, \ \ k \in \mathbb{N}$, desna strana od (3.6) je potpun kvadrat. Preciznije,

$$X^2 - d(d\delta^2 - 2g)Y^2 = (2g(2k - 1))^2, \ \ k \in \mathbb{N}.$$

Pogledajmo što se događa s lijevom stranom jednakosti (3.6). Vrijedi:
$d\delta^2 - 2g = (2k^2 - 2k + 1)\delta^2 - (\delta^2 - 2\delta + 2) = 2(\delta k - 1)(\delta k - \delta + 1)$ pa (3.6) postaje

$$X^2 - 2(2k^2 - 2k + 1)(\delta k - 1)(\delta k - \delta + 1)Y^2 = (2g(2k - 1))^2. \tag{2.16}$$

Pripadna Pellova jednadžba od (2.16) je

$$U^2 - 2(2k^2 - 2k + 1)(\delta k - 1)(\delta k - \delta + 1)V^2 = 1. \tag{2.17}$$

Pellova jednadžba (2.17) ima beskonačno mnogo rješenja. Budući da razvoj broja

$$\sqrt{2(2k^2 - 2k + 1)(\delta k - 1)(\delta k - \delta + 1)}$$

u verižni razlomak nema uvijek jednaku duljinu perioda za svaki $k \in \mathbb{N}$, pristup kojeg smo primjenjivali u nekim od dosadašnjih slučajeva nije moguć.

Neka je (U_0, V_0) fundamentalno rješenje od (2.17), a (X, Y) rješenje od (2.16). Rješenja jednadžbe (2.16) moraju zadovoljavati i dodatan uvjet

$$X \equiv d\delta\varepsilon \equiv d\delta(\delta - 2) \pmod{2(\delta k - 1)(\delta k - \delta + 1)}, \tag{2.18}$$

koji je nužan s obzirom da zahtijevamo da je n prirodan broj. Neka je

$$a = 2k^2 - 2k + 1, \ \ b = \delta k - 1, \ \ c = \delta k - \delta + 1.$$

U tom slučaju jednadžbu (2.17) možemo zapisati u obliku

$$U^2 - 2abcV^2 = 1. \tag{2.19}$$

Za (U_0, V_0) fundamentalno rješenje te jednadžbe vrijedi:

$$U_0^2 - 1 = 2abcV_0^2,$$

$$(U_0 - 1)(U_0 + 1) = 2abcV_0^2.$$

U_0 je neparan broj, odnosno vrijedi da $4|(U_0 - 1)(U_0 + 1)$, što povlači da $4|2abcV_0^2$. Očito je da su a, b, c redom neparni brojevi, to jest $2|V_0^2$ i čega zaključujemo da je V_0 paran broj. Stoga, možemo pisati $V_0 = 2st, \;\; s, t \in \mathbb{N}$.
Uvođenjem novih oznaka prethodna jednadžba postaje:

$$(U_0 - 1)(U_0 + 1) = 8abcs^2t^2.$$

Pretpostavimo da su a, b, c prosti brojevi. Na taj način je broj faktorizacija jednadžbe (2.19) najmanji mogući te ih sve možemo jednoznačno navesti. Uz tu pretpostavku određujemo rješenja jednadžbe (2.19).

Očito je $a, b, c \neq 2$, pa onda u obzir dolaze sljedeće faktorizacije:

$1^{\pm})$ $\;U_0 \pm 1 = 2abcs^2, \;\; U_0 \mp 1 = 2^2t^2,$

$2^{\pm})$ $\;U_0 \pm 1 = 2^2abcs^2, \;\; U_0 \mp 1 = 2t^2,$

$3^{\pm})$ $\;U_0 \pm 1 = 2abs^2, \;\; U_0 \mp 1 = 2^2ct^2,$

$4^{\pm})$ $\;U_0 \pm 1 = 2acs^2, \;\; U_0 \mp 1 = 2^2bt^2,$

$5^{\pm})$ $\;U_0 \pm 1 = 2bcs^2, \;\; U_0 \mp 1 = 2^2at^2,$

$6^{\pm})$ $\;U_0 \pm 1 = 2as^2, \;\; U_0 \mp 1 = 2^2bct^2,$

$7^{\pm})$ $\;U_0 \pm 1 = 2bs^2, \;\; U_0 \mp 1 = 2^2act^2,$

$8^{\pm})$ $\;U_0 \pm 1 = 2cs^2, \;\; U_0 \mp 1 = 2^2abt^2.$

Odredimo uvjete

$$U_0 \equiv -1 \pmod{(\delta k - 1)}, \ U_0 \equiv 1 \pmod{(\delta k - \delta + 1)}.$$

Definiramo

$$D := d\delta^2 - 2g = 2(\delta k - 1)(\delta k - \delta + 1).$$

U tom slučaju lako možemo dobiti

$$X_0 = 2g(2k-1)U_0 \equiv 2g(2k-1) \equiv d\delta^2(2k-1) \equiv$$

$$\equiv 2d\delta(\delta k - \delta + 1) + d\delta(\delta - 2) \equiv d\delta(\delta - 2) \pmod{(\delta k - \delta + 1)},$$

$$X_0 = 2g(2k-1)U_0 \equiv -2g(2k-1) \equiv -d\delta^2(2k-1) \equiv$$

$$-d(2\delta(\delta k - 1) - \delta(\delta - 2)) \equiv d\delta(\delta - 2) \pmod{(\delta k - 1)}.$$

Iz dobivenih kongruencija zaključujemo da je

$$X_0 \equiv d\delta(\delta - 2) \pmod{(\delta k - 1)(\delta k - \delta + 1)},$$

pa je stoga i

$$X_0 \equiv d\delta(\delta - 2) \pmod{2(\delta k - 1)(\delta k - \delta + 1)},$$

čime je dokazano da vrijedi (2.18).

Zbog značajnih različitosti u dokazima koji se javljaju u ovisnosti o tome kojoj klasi ostataka modulo 8 paran broj δ pripada, odlučili smo razložiti problem na četiri slučaja i razmatrati svaki takav slučaj posebno.

1. Slučaj $\delta \equiv 4 \pmod 8$

Neka je $\delta \equiv 4 \pmod 8$, te neka je $k \equiv 3 \pmod 8$. Uz navedene pretpostavke za brojeve a, b, c vrijede sljedeće kongruencije:

$$a = 2k^2 - 2k + 1 \equiv 5 \pmod 8,$$

$$b = \delta k - 1 \equiv 3 \pmod 8,$$

$$c = \delta k - \delta + 1 \equiv 1 \pmod 8. \tag{2.20}$$

Dokazujemo da uvijek možemo pronaći prirodne brojeve k takve da su samo slučajevi $3^+), 4^-), 7^+), 8^-)$ iz ranije naznačenih faktorizacija valjani. Promatramo svaku od ranije navedenih faktorizacija posebno.

Dobivamo redom
$1^+)$ $U_0 + 1 = 2abcs^2$, $U_0 - 1 = 2^2t^2$.
Vrijedi $2abcs^2 - 2^2t^2 = 2$, pa nakon dijeljenja izraza brojem 2 dobivamo $abcs^2 - 2t^2 = 1$ i nakon uvrštavanja poznatih ostataka, dobivamo da bi trebalo vrijediti $7s^2 - 2t^2 \equiv 1 \pmod 8$ što nije moguće pa zaključujemo da ovaj slučaj nema rješenja.

$1^-)$ $U_0 + 1 = 2^2t^2$, $U_0 - 1 = 2abcs^2$.
Vrijedi $2^2t^2 - 2abcs^2 = 2$. Dijeljenjem ovog izraza s 2 dobivamo $2t^2 - abcs^2 = 1$ i nakon uvrštavanja poznatih ostataka je $2t^2 - 7s^2 \equiv 1 \pmod 8$ što je moguće za slučaj kad je $t^2 \equiv 4 \pmod 8, s^2 \equiv 1 \pmod 8$, tako da ćemo dodatno razraditi ovaj slučaj.
Da bi izraz $2^2t^2 = 2abcs^2 + 2$ imao rješenja, moralo bi vrijedi $\left(\frac{2}{a}\right) = \left(\frac{2}{b}\right) = \left(\frac{2}{c}\right) = 1$. No, budući želimo odrediti uvjete koji određuju da ovaj slučaj nema rješenja, trebalo bi vrijediti ili $\left(\frac{2}{a}\right) = -1$ ili $\left(\frac{2}{b}\right) = -1$ ili $\left(\frac{2}{c}\right) = -1$.
Poznavajući klase ostataka brojeva $a, b, c \pmod 8$ uočavamo da vrijedi $\left(\frac{2}{a}\right) = \left(\frac{2}{b}\right) = -1$ pa ni ovaj slučaj nema rješenja.

$2^+)$ $U_0 + 1 = 2^2abcs^2$, $U_0 - 1 = 2t^2$.
Vrijedi $2abcs^2 - t^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $6s^2 - t^2 \not\equiv 1 \pmod 8$ jer su kvadratni ostaci mod 8 samo $0, 1, 4$. Zaključujemo da ni ovaj slučaj ne vrijedi.

$2^-)$ $U_0 + 1 = 2t^2$, $U_0 - 1 = 2^2abcs^2$.
Dobivamo $t^2 - 2abcs^2 = 1$ što je kontradikcija s minimalnošću od (U_0, V_0).

$3^-)$ $U_0 + 1 = 2^2ct^2$, $U_0 - 1 = 2abs^2$.
Vrijedi $2ct^2 - abs^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $2t^2 - 7s^2 \equiv 1 \pmod 8$ što je moguće za slučaj kad vrijedi $t^2 \equiv 4 \pmod 8, s^2 \equiv 1 \pmod 8$ tako da slučaj moramo dodatno razmotriti.
Početnu jednakost $2^2ct^2 - 2abs^2 = 2$ množimo brojem c i dobivamo $(2ct)^2 = 2abcs^2 + 2c$. Ako želimo da ova jednakost nema rješenja, trebao bi vrijediti jedan od uvjeta $\left(\frac{2c}{a}\right) = -1$ ili $\left(\frac{2c}{b}\right) = -1$. Jednostavnim raspisom dobivamo da bi trebao vrijediti jedan od uvjeta

$$\left(\frac{2c}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{c}{a}\right) = -\left(\frac{c}{a}\right) = -1, \quad \boxed{\left(\frac{c}{a}\right) = 1},$$

ili

$$\left(\frac{2c}{b}\right) = \left(\frac{2}{b}\right)\left(\frac{c}{b}\right) = -\left(\frac{c}{b}\right) = -1, \quad \boxed{\left(\frac{c}{b}\right) = 1}.$$

$4^+)$ $U_0 + 1 = 2acs^2$, $U_0 - 1 = 2^2bt^2$.
Vrijedi $acs^2 - 2bt^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $5s^2 - 6t^2 \not\equiv 1 \pmod 8$ jer su kvadratni ostaci mod 8 samo $0, 1, 4$. Zaključujemo da ni ovaj slučaj ne vrijedi.

$5^+)$ $U_0 + 1 = 2bcs^2$, $U_0 - 1 = 2^2at^2$.
Vrijedi $2bcs^2 - 2^2at^2 = 2$. Uvrštavanjem poznatih ostataka dobivamo $3s^2 - 2t^2 \equiv 1 \pmod 8$ što vrijedi za $s^2, t^2 \equiv 1 \pmod 8$ pa ovaj slučaj još moramo dodatno promotriti.
Jednakost $2bcs^2 - 2^2at^2 = 2$ množimo brojem a i dobivamo $(2at)^2 = 2abcs^2 - 2a$. U situaciji da ova jednakost nema rješenja, trebalo bi vrijediti $\left(\frac{-2a}{b}\right) = -1$ ili $\left(\frac{-2a}{c}\right) = -1$. U raspisu dobivamo da bi trebalo vrijediti

$$\left(\frac{-2a}{b}\right) = \left(\frac{-1}{b}\right)\left(\frac{2}{b}\right)\left(\frac{a}{b}\right) = \left(\frac{a}{b}\right), \quad \boxed{\left(\frac{a}{b}\right) = -1},$$

ili

$$\left(\frac{-2a}{c}\right) = \left(\frac{-1}{c}\right)\left(\frac{2}{c}\right)\left(\frac{a}{c}\right) = \left(\frac{a}{c}\right), \quad \boxed{\left(\frac{a}{c}\right) = -1}.$$

$5^-)$ $U_0 + 1 = 2^2at^2$, $U_0 - 1 = 2bcs^2$.
Vrijedi $2at^2 - bcs^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $2t^2 - 3s^2 \not\equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj ne vrijedi.

$6^+)$ $U_0 + 1 = 2as^2$, $U_0 - 1 = 2^2bct^2$.
Vrijedi $as^2 - 2bct^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $5s^2 - 6t^2 \not\equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj nije moguć.

$6^-)$ $U_0 + 1 = 2^2bct^2$, $U_0 - 1 = 2as^2$.
Vrijedi $2bct^2 - as^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $6t^2 - 5s^2 \not\equiv 1 \pmod 8$ što znači da ovaj slučaj moramo dodatno razmotriti.
Množenjem izraza $2bct^2 - as^2 = 1$ brojem a, dobivamo $(as)^2 = 2abct^2 - a$. Budući ne želimo da ovaj izraz ima rješenja, trebalo bi vrijediti

$$\left(\frac{-a}{b}\right) = -1, \text{ odnosno } \boxed{\left(\frac{a}{b}\right) = 1},$$

ili

$$\left(\frac{-a}{c}\right) = -1, \text{ odnosno } \boxed{\left(\frac{a}{c}\right) = -1}.$$

$7^-)$ $U_0 + 1 = 2^2act^2$, $U_0 - 1 = 2bs^2$.
Vrijedi $2act^2 - bs^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $2t^2 - 3s^2 \not\equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj ne vrijedi.

8^+) $U_0 + 1 = 2cs^2$, $U_0 - 1 = 2^2abt^2$.
Vrijedi $cs^2 - 2abt^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $s^2 - 6t^2 \not\equiv 1 \pmod 8$. Ovaj slučaj je moguć za $s^2 \equiv 1 \pmod 8$ te $t^2 \equiv 0 \pmod 8$ pa ga valja dodatno razmotriti. Jednakost $2 = 2cs^2 - 2^2abt^2$ dijelimo brojem 2 i dobivamo $1 = cs^2 - 2abt^2$. Množeći dobivenu jednakost brojem c dobivamo $(cs)^2 = 2abct^2 + c$. Ukoliko želimo da navedena jednakost nema rješenja, morao bi vrijediti jedan od uvjeta

$$\boxed{\left(\frac{c}{a}\right) = -1},$$

ili

$$\boxed{\left(\frac{c}{b}\right) = -1}.$$

Od svih istaknutih uvjeta, biramo uvjete

$$\left(\frac{a}{c}\right) = -1, \ \left(\frac{c}{b}\right) = 1.$$

Sada ćemo pokazati kako se ovi uvjeti mogu zadovoljiti i to, pretpostavljajući neke standardne slutnje o prostim brojevima, na beskonačno mnogo načina.

Neka je broj k takav da vrijedi sljedeće:

(i) $k \equiv 3 \pmod 8$,

(ii) $\left(\frac{\delta k - \delta + 1}{A}\right) = -1$, gdje je $A = \frac{\delta^2}{2} - \delta + 1$,

(iii) $\left(\frac{\delta k - \delta + 1}{B}\right) = 1$, gdje je $B = \frac{\delta}{2} - 1$,

(iv) $2k^2 - 2k + 1$ je prost broj,

(v) $\delta k - 1$ je prost broj,

(vi) $\delta k - \delta + 1$ je prost broj.

Vidjeli smo već da uvjet (i) povlači pretpostavljene ostatke modulo 8 brojeva a, b, c definirane u (2.20), odnosno, kongruencije

$$a \equiv 5 \pmod 8, \ b \equiv 3 \pmod 8, \ c \equiv 1 \pmod 8.$$

Pokažimo još da je uvjet (ii) ekvivalentan s prvim postavljenim uvjetom na Legendreove simbole $(a/c) = -1$, pa da je uvjet (iii) ekvivalentan s drugim uvjetom $(b/c) = 1$. Detaljnije, vrijedi

$$\left(\frac{a}{c}\right) = \left(\frac{2k^2 - 2k + 1}{\delta k - \delta + 1}\right) = \left(\frac{2\delta^2 k^2 - 2\delta^2 k + \delta^2}{\delta k - \delta + 1}\right) = \left(\frac{2\delta k(\delta k - \delta + 1) - 2\delta k + \delta^2}{\delta k - \delta + 1}\right) =$$

$$= \left(\frac{-2\delta k + \delta^2}{\delta k - \delta + 1}\right) = \left(\frac{-2(\delta k - \delta + 1) - 2\delta + 2 + \delta^2}{\delta k - \delta + 1}\right) =$$

$$= \left(\frac{\delta^2/2 - \delta + 1}{\delta k - \delta + 1}\right) = \left(\frac{\delta k - \delta + 1}{\delta^2/2 - \delta + 1}\right) = \left(\frac{c}{A}\right),$$

gdje je $A = \frac{\delta^2}{2} - \delta + 1$.
Nadalje, vrijedi:

$$\left(\frac{c}{b}\right) = \left(\frac{\delta k - \delta + 1}{\delta k - 1}\right) = \left(\frac{\delta k - 1}{\delta k - \delta + 1}\right) = \left(\frac{\delta k - \delta + 1 + \delta - 2}{\delta k - \delta + 1}\right) = \left(\frac{\delta - 2}{\delta k - \delta + 1}\right) =$$

$$= \left(\frac{\delta/2 - 1}{\delta k - \delta + 1}\right) = \left(\frac{\delta k - \delta + 1}{\delta/2 - 1}\right) = \left(\frac{c}{B}\right),$$

gdje je $B = \delta/2 - 1$.

Provjerimo mogu li istovremeno biti zadovoljeni uvjeti (i), (ii) i (iii).

Iz $A = B \cdot \delta + 1$ slijedi da je $\mathrm{nzd}(A, B) = 1$. Vrijedi i da je $\mathrm{nzd}(AB, \delta) = 1$.

Neka je

$$A = p_1^{a_1} p_2^{a_2} \cdot \cdots \cdot p_r^{a_r}$$

rastav broja A na proste faktore. Provjeravamo je li broj A potpuni kvadrat (u slučaju da je broj A potpun kvadrat, uvjet $\left(\frac{c}{A}\right) = -1$ nije moguć). Neka je $\delta = 8l + 4,\ l \in \mathbb{N}_0$. Tada je $A = \frac{\delta^2}{2} - \delta + 1 = 32l^2 + 24l + 5 \equiv 5 \pmod 8$. Ako je A potpuni kvadrat pri dijeljenju s 8 imao bi ostatak $0, 1$, ili 4, a broj $A \equiv 5 \pmod 8$ što implicira da A nije potpuni kvadrat. S obzirom da broj A nije potpun kvadrat, onda je neki od eksponenata a_i u njegovom rastavu na proste faktore neparan. Bez smanjenja općenitosti, neka je broj a_1 neparan te x_1 neki kvadratni neostatak modulo p_1. Po Kineskom teoremu o ostacima postoji beskonačno mnogo cijelih brojeva koji zadovoljavaju sustav kongruencija

$$x \equiv x_1 \pmod{p_1},\ \ x \equiv 1 \pmod{p_i},\ \ i = 2, \ldots r,$$

$$x \equiv 1 \pmod{B}.$$

Sad definiramo k s $x = \delta k - \delta + 1$, odnosno s

$$k = \frac{x + \delta - 1}{\delta}.$$

Budući je $k \equiv 3 \pmod 8$, i taj uvjet uvrštavamo u kongruencije koje zadovoljava x. Uz navedene kongruencije vrijedi i

$$x = \delta k - \delta + 1 = \delta(8l + 3) - \delta + 1 \equiv 2\delta + 1 \pmod{8\delta},$$

pa su rješenja oblika

$$x \equiv x_0 \pmod{8p_1 \dots p_r B\delta}.$$

Na ovaj je način jednoznačno određeno kojim klasama ostataka broj k pripada modulo p_i, $i = 1, \dots r$, modulo B i modulo 8, a to je upravo $k \equiv 3 \pmod 8$. Pitamo se mogu li istovremeno brojevi a, b, c biti prosti. U odgovoru na to pitanje koristimo poznatu slutnju iz [22].

Slutnja 2.6 (Schinzelova hipoteza H) Neka su $f_1(x), \dots, f_s(x)$ polinomi s cjelobrojnim koeficijentima kojima su vodeći koeficijenti prirodni brojevi. Ako su zadovoljena sljedeća dva svojstva

- $f_i(x)$ je ireducibilan za sve $i = 1, 2, \dots, s$,
- za svaki p prosti broj postoji prirodan broj n za koji vrijedi

  $$f_1(n) f_2(n) \dots f_s(n) \not\equiv 0 \pmod p,$$

  tada postoji beskonačno mnogo prirodnih brojeva t takvih da su svi

  $$f_1(t), f_2(t), \dots f_s(t)$$

  istovremeno prosti brojevi.

□

Propozicija 2.7 Ako Schinzelova hipoteza H vrijedi, tada za sve brojeve $\delta \equiv 4 \pmod 8$ postoji beskonačno mnogo neparnih prirodnih brojeva n sa svojstvom da postoje djelitelji d_1, d_2 od $\frac{n^2+1}{2}$ za koje je $d_1 + d_2 = \delta n + \delta - 2$.

Ideja dokaza Propozicije 2.7 ilustrirana je u sljedećem primjeru.

Primjer 2.8 Neka je $\delta = 12$. Tada je $A = 12^2/2 - 12 + 1 = 61$, $B = 12/2 - 1 = 5$. Prema napisanom, kvadratni neostaci $\pmod{61}$ su

$$x \equiv 2, 6, 7, 8, 10, 11, 17, 18, 21, 23, 24, 26, 28, 29, 30, 31, 32, 33,$$

$$35, 37, 38, 40, 43, 44, 50, 51, 53, 54, 55, 59 \pmod{61}.$$

Za

$$x \equiv 24 \pmod{61}, \ \ x \equiv 1 \pmod{5}, \ \ x \equiv 25 \pmod{96}$$

vrijedi

$$x \equiv 16921 \pmod{29280}.$$

Možemo pisati $x = 29280s + 16921, \ \ s \in \mathbb{Z}$. Za brojeve k određene s $x = \delta k - \delta + 1$ vrijedi

$$k \equiv 1411 \pmod{2440}.$$

Broj k možemo zapisati i kao $k = 2440u + 1411, \ \ u \in \mathbb{Z}$.
Uvrštavajući dobiveni izraz za k dobivamo tri polinoma. Prvi je polinom oblika:

$$f_1(u) = 2(2440u + 1411)^2 - 2(2440u + 1411) + 1 = 11907200u^2 + 13766480u + 3979021.$$

Drugi polinom je

$$f_2(u) = 12(2440u + 1411) - 1 = 29280u + 16931,$$

dok je treći polinom oblika

$$f_3(u) = 12(2440u + 1411) - 11 = 29280u + 16921.$$

Diskriminanta kvadratnog polinoma f_1 nije potpun kvadrat što povlači da polinom f_1 nije ireducibilan, a polinomi f_2, f_3 su linearni polinomi te su oni po definiciji ireducibilni.
Uz ireducibilnost polinoma koja mora biti ispunjena prema Schinzelovoj hipotezi H, drugi uvjet Schinzelove hipoteze H jest da za svaki p prosti broj postoji prirodan broj n za koji p ne dijeli produkt ova tri polinoma. Pokazat ćemo da je dovoljno uzeti $n = 1, 2, 3$.
Zaista, za $n = 1$ dobivamo

$$f_1(1) \cdot f_2(1) \cdot f_3(1) = (13 \cdot 2280977) \cdot (11 \cdot 4201) \cdot (47 \cdot 983).$$

Za $n = 2$ dobivamo

$$f_1(2) \cdot f_2(2) \cdot f_3(2) = 79140781 \cdot (13 \cdot 5807) \cdot (7 \cdot 41 \cdot 263).$$

Za $n = 3$ dobivamo da vrijedi

$$f_1(3) \cdot f_2(3) \cdot f_3(3) = (641 \cdot 237821) \cdot (17 \cdot 6163) \cdot 104761.$$

Ako postoji prosti broj p koji dijeli tri produkta $f_1(n)f_2(n)f_3(n), \ \ n = 1, 2, 3$, tada taj

prosti broj dijeli i njihov zajednički djelitelj. Uočavamo da je

$$\text{nzd}(f_1(1)\cdot f_2(1)\cdot f_3(1),\ \ f_1(2)\cdot f_2(2)\cdot f_3(2), f_1(3)\cdot f_2(3)\cdot f_3(3)) = 1,$$

te je na taj način pokazano da takav djelitelj p ne postoji.
Budući tri navedena ireducibilna polinoma, f_1, f_2, f_3 zadovoljavaju oba uvjeta Schinzelove hipoteze H, u slučaju da je ona valjana, vrijedi da postoji beskonačno mnogo prirodnih brojeva u takvih da su brojevi

$$f_1(u), f_2(u), f_3(u)$$

istovremeno prosti brojevi.

Za $k \leq 10^9$ postoje 153 broja k koji zadovoljavaju sve navedene uvjete. Prvih nekoliko brojeva k koje dobivamo su:

$$1411, 16051, 240531, 360091, 425971, 626051, 1314131, 1975371, 2241331, 2426771, 2495091\ldots$$

Uzmemo li najmanji $k = 1411$, za njega određujemo pripadnu Pellovu jednadžbu i njena rješenja.
Za početak određujemo brojeve

$$a = 2\cdot 1411^2 - 2\cdot 1411 + 1 = 3979021,\ \ b = 12\cdot 1411 - 1 = 16931,\ \ c = 12\cdot 1411 - 11 = 16921.$$

Odgovarajuća Pellova jednadžba je

$$U^2 - 2279895083614942V^2 = 1.$$

Fundamentalno rješenje koje ovom jednadžbom dobivamo vrlo je veliko što će u konačnici rezultirati i vrlo velikim brojem n.
Fundamentalno rješenje se može naći u programskom paketu PARI/GP [20], pomoću funkcije `quadunit`.

Vrijedi

$$U_0 \approx 2.58023\cdot 10^{1502988},\ \ V_0 \approx 1.54982\cdot 10^{1502980}.$$

Uz fundamentalno rješenje Pellove jednadžbe u mogućnosti smo odrediti i rješenje početne pellovske jednadžbe (X_0, Y_0). Znamo da je $X_0 = 2g(2k-1)U_0$. Naposlijetku, iz izraza

$$n = \frac{X_0 - d\delta(\delta-2)}{d\delta^2 - 2g},$$

što je u našem slučaju

$$n = \frac{X_0 - 120d}{144d - 2\cdot 61},\ \ d = 2k^2 - 2k + 1 = 3979021,$$

dobivamo i vrijednost broja

$$n \approx 1.54982 \cdot 10^{1502985}.$$

Traženi djelitelji broja $(n^2+1)/2$ su

$$d_1 \approx 9.89977 \cdot 10^{1502978}, \;\; d_2 \approx 1.85979 \cdot 10^{1502986}.$$

2. Slučaj $\delta \equiv 6 \pmod 8$

Neka je $\delta \equiv 6 \pmod 8$ te neka je $k \equiv 2 \pmod 8$. Za zadane brojeve a, b, c tada vrijede sljedeće kongruencije:

$$\begin{aligned} a &= 2k^2 - 2k + 1 \equiv 5 \pmod 8, \\ b &= \delta k - 1 \equiv 3 \pmod 8, \\ c &= \delta k - \delta + 1 \equiv 7 \pmod 8. \end{aligned} \tag{2.21}$$

Dokazujemo da možemo pronaći prirodne brojeve k takve da su samo slučajevi $3^+), 4^-), 7^+), 8^-)$ iz ranije navedenih faktorizacija valjani. Promatramo svaku faktorizaciju posebno.
Dobivamo redom
$1^+)$ $U_0 + 1 = 2abcs^2, \;\; U_0 - 1 = 2^2t^2$.
Vrijedi $(2t)^2 = 2abcs^2 - 2$. Da bi ova jednakost imala rješenja, trebalo bi vrijediti

$$\left(\frac{-2}{a}\right) = \left(\frac{-2}{b}\right) = \left(\frac{-2}{c}\right) = 1,$$

odnosno trebalo bi vrijediti

$$\left(\frac{-1}{a}\right)\left(\frac{2}{a}\right) = 1 \;\; \Rightarrow \;\; \left(\frac{2}{a}\right) = 1,$$

što je kontradikcija s $a \equiv 5 \pmod 8$. Dakle, ovaj slučaj nema rješenja.

$1^-)$ $U_0 + 1 = 2^2t^2, \;\; U_0 - 1 = 2abcs^2$.
Vrijedi $(2t)^2 = 2abcs^2 + 2$, a da bi ova jednakost imala rješenja, trebalo bi vrijediti

$$\left(\frac{2}{a}\right) = \left(\frac{2}{b}\right) = \left(\frac{2}{c}\right) = 1,$$

što je u kontradikciji s $\left(\frac{2}{a}\right) = \left(\frac{2}{b}\right) = -1$ jer $a \equiv 5 \pmod 8, b \equiv 3 \pmod 8$. Ni ovaj slučaj nema rješenja.

$2^+)$ $U_0 + 1 = 2^2abcs^2, \;\; U_0 - 1 = 2t^2$.

Vrijedi $2abcs^2 - t^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $2s^2 - t^2 \equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj vrijedi za $s^2, t^2 \equiv 1 \pmod 8$ pa ga moramo još dodatno razmotriti.
Vrijedi $2abcs^2 - 1 = t^2$. Ako zahtijevamo da ova jednakost nema rješenja, trebalo bi vrijediti

$$\left(\frac{-1}{a}\right) = -1, \text{ ili } \left(\frac{-1}{b}\right) = -1, \text{ ili } \left(\frac{-1}{c}\right) = -1.$$

Vrijedi $\left(\frac{-1}{b}\right) = -1$ budući $b \equiv 3 \pmod 4$. Ovaj slučaj nema rješenja.

$2^-)$ $U_0 + 1 = 2t^2$, $U_0 - 1 = 2^2abcs^2$.
Dobivamo $t^2 - 2abcs^2 = 1$ što je kontradikcija s minimalnošću od (U_0, V_0).

$3^-)$ $U_0 + 1 = 2^2ct^2$, $U_0 - 1 = 2abs^2$.
Vrijedi $2ct^2 - abs^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $7t^2 - 6s^2 \equiv 1 \pmod 8$ što je moguće za $s^2, t^2 \equiv 1 \pmod 8$ pa ovaj slučaj moramo dodatno razmotriti.
Vrijedi $2 = 2^2ct^2 - 2abs^2$ i ako jednakost množimo brojem c, dobivamo $(2ct)^2 = 2c + 2abcs^2$. Da bi ova jednakost imala rješenja, mora vrijediti $\left(\frac{2c}{a}\right) = \left(\frac{2c}{b}\right) = 1$. Budući tražimo brojeve a, b za koje ova jednakost neće imati rješenja, onda bi trebalo vrijediti $\left(\frac{2c}{a}\right) = -1$ ili $\left(\frac{2c}{b}\right) = -1$. Jednostavnim raspisom dobivamo da bi trebali vrijediti sljedeći uvjeti:

$$\left(\frac{2c}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{c}{a}\right) = -\left(\frac{c}{a}\right) = -1, \quad \boxed{\left(\frac{c}{a}\right) = 1},$$

ili

$$\left(\frac{2c}{b}\right) = \left(\frac{2}{b}\right)\left(\frac{c}{b}\right) = -\left(\frac{c}{b}\right) = -1, \quad \boxed{\left(\frac{c}{b}\right) = 1}.$$

$4^+)$ $U_0 + 1 = 2acs^2$, $U_0 - 1 = 2^2bt^2$.
Vrijedi $acs^2 - 2bt^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $3s^2 - 6t^2 \not\equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj nema rješenja.

$5^+)$ $U_0 + 1 = 2bcs^2$, $U_0 - 1 = 2^2at^2$.
Vrijedi $2bcs^2 - 2^2at^2 = 2$. Uvrštavanjem poznatih ostataka dobivamo $5s^2 - 2t^2 \not\equiv 1 \pmod 8$ pa ovaj slučaj ne vrijedi.

$5^-)$ $U_0 + 1 = 2^2at^2$, $U_0 - 1 = 2bcs^2$.
Vrijedi $2at^2 - bcs^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $2t^2 - 5s^2 \not\equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj ne vrijedi.

$6^+)$ $U_0 + 1 = 2as^2$, $U_0 - 1 = 2^2bct^2$.
Vrijedi $as^2 - 2bct^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $5s^2 - 2t^2 \equiv 1 \pmod 8$

što znači da ni ovaj slučaj nema rješenja.

6^-) $U_0 + 1 = 2^2 bct^2,\ U_0 - 1 = 2as^2$.
Vrijedi $2bct^2 - as^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $2t^2 - 5s^2 \equiv 1 \pmod 8$ što znači da ovaj slučaj nema rješenja.

7^-) $U_0 + 1 = 2^2 act^2,\ U_0 - 1 = 2bs^2$.
Vrijedi $2act^2 - bs^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $6t^2 - 3s^2 \not\equiv 1 \pmod 8$. Zaključujemo da ovaj slučaj također ne može vrijediti.

8^+) $U_0 + 1 = 2cs^2,\ U_0 - 1 = 2^2 abt^2$.
Vrijedi $cs^2 - 2abt^2 = 1$. Uvrštavanjem poznatih ostataka dobivamo $7s^2 - 6t^2 \equiv 1 \pmod 8$ vrijedi za $s^2, t^2 \equiv 1 \pmod 8$ pa ovaj slučaj dodatno razmatramo.
Vrijedi $1 = cs^2 - 2abt^2$ i ako jednakost množimo brojem c, dobivamo $(cs)^2 = c + 2abct^2$. Da bi ova jednakost imala rješenja, mora vrijediti $\left(\frac{c}{a}\right) = \left(\frac{c}{b}\right) = 1$. Budući tražimo brojeve a, b za koje ova jednakost neće imati rješenja, onda bi trebalo vrijediti $\left(\frac{c}{a}\right) = -1$ ili $\left(\frac{c}{b}\right) = -1$. Dakle, trebalo bi vrijediti

$$\boxed{\left(\frac{c}{a}\right) = -1},$$

ili

$$\boxed{\left(\frac{c}{b}\right) = -1}.$$

Od istaknutih uvjeta, odaberimo

$$\left(\frac{c}{a}\right) = 1,\ \left(\frac{c}{b}\right) = -1.$$

Navedeni uvjeti garantiraju da i uvjeti koje smo dodatno razmatrali nemaju rješenja.

Znamo da je $\delta \equiv 6 \pmod 8$ što možemo prikazati kao $\delta = 8l + 6,\ l \in \mathbb{N}_0$. Dobivamo da vrijedi

$$\left(\frac{c}{a}\right) = \left(\frac{\delta k - \delta + 1}{2k^2 - 2k + 1}\right) = \left(\frac{2k^2 - 2k + 1}{\delta k - \delta + 1}\right) = \left(\frac{\delta^2 - 2\delta k}{\delta k - \delta + 1}\right) = \left(\frac{\delta^2 - 2\delta + 2}{\delta k - \delta + 1}\right) =$$

$$= \left(\frac{\delta^2/2 - \delta + 1}{\delta k - \delta + 1}\right) = \left(\frac{\delta k - \delta + 1}{\delta^2/2 - \delta + 1}\right) = \left(\frac{c}{A}\right) = \left(\frac{-c}{A}\right),$$

gdje je $A = \delta^2/2 - \delta + 1$. Uočimo da je $A \equiv 1 \pmod 4$, gdje A može biti i složen broj. Promatrajući drugi uvjet na Jacobijev simbol, možemo također primjetiti

$$\left(\frac{c}{b}\right) = -\left(\frac{b}{c}\right) = -\left(\frac{\delta k - 1}{\delta k - \delta + 1}\right) = -\left(\frac{\delta - 2}{\delta k - \delta + 1}\right) = -\left(\frac{8l + 4}{\delta k - \delta + 1}\right) = -\left(\frac{(\delta - 2)/4}{\delta k - \delta + 1}\right) =$$

$$= \begin{cases} \left(\frac{\delta k-\delta+1}{B}\right) = \left(\frac{c}{B}\right) = -\left(\frac{-c}{B}\right), & \text{za } \delta \equiv 14 \pmod{16},\ B \equiv 3 \pmod 4 \\ -\left(\frac{\delta k-\delta+1}{B}\right) = -\left(\frac{c}{B}\right) = -\left(\frac{-c}{B}\right), & \text{za } \delta \equiv 6 \pmod{16},\ B \equiv 1 \pmod 4 \end{cases}$$

gdje je $B = (\delta - 2)/4$, te ni B nije nužno prost broj.

Neka je broj k takav da vrijede sljedeći uvjeti

(i) $k \equiv 2 \pmod 8$,

(ii) $\left(\frac{-c}{A}\right) = 1$, gdje je $A = \frac{\delta^2}{2} - \delta + 1$,

(iii) $\left(\frac{-c}{B}\right) = 1$, gdje je $B = (\delta - 2)/4$,

(iv) $2k^2 - 2k + 1$ je prost broj,

(v) $\delta k - 1$ je prost broj,

(vi) $\delta k - \delta + 1$ je prost broj.

Uvjet (i) povlači pretpostavljene ostatke modulo 8 brojeva a, b, c, odnosno vrijedi

$$a \equiv 5 \pmod 8,\ b \equiv 3 \pmod 8,\ c \equiv 7 \pmod 8.$$

Također, već je pokazano da je uvjet (ii) ekvivalentan s prvim postavljenim uvjetom na Legendreov simbol $(c/a) = 1$ te da je uvjet (iii) ekvivalentan s drugim uvjetom $(c/b) = -1$. Preostaje nam provjeriti jesu li istovremeno zadovoljeni uvjeti (i), (ii) i (iii).
Iz $A = 2B\delta + 1$ slijedi $\text{nzd}(A, B) = 1$, te je također $\text{nzd}(AB, \delta) = 1$.
Prema Kineskom teoremu u ostacima postoji beskonačno mnogo cijelih brojeva x koji zadovoljavaju sljedeći sustav kongruencija

$$x \equiv 1 \pmod A,\ x \equiv 1 \pmod B.$$

Definiramo broj k u obliku $x = -(\delta k - \delta + 1) = \delta - \delta k - 1$, odnosno

$$k = \frac{\delta - x - 1}{\delta}.$$

S obzirom da je $k \equiv 2 \pmod 8$, taj uvjet kombiniramo sa svim do sad navedenim kongruencijama. Naime, vrijedi

$$x = \delta - \delta k - 1 = \delta - \delta(8k + 2) - 1 \equiv -\delta - 1 \pmod{8\delta}.$$

Kineskim teoremom o ostacima dobivamo da su rješenja oblika

$$x \equiv x_0 \pmod{(8AB\delta)}.$$

Na ovaj je način određeno jednoznačno kojim klasama ostataka broj k pripada modulo A, B i 8, a ovo posljednje je upravo $k \equiv 2 \pmod 8$. Na kraju preostaje odgovoriti na pitanje jesu li za ovako definirane brojeve k kojih je beskonačno mnogo, svi brojevi oblika $2k^2 - 2k + 1,\ \delta k - 1,\ \delta k - \delta + 1$ uz sve navedene uvjete istovremeno i prosti brojevi. Potvrdan odgovor na to pitanje, uz uvjet da vrijedi, daje Schinzelova hipoteza H 2.6.

Propozicija 2.9 Ako Schinzelova hipoteza H vrijedi, tada za sve brojeve $\delta \equiv 6 \pmod 8$ postoji beskonačno mnogo neparnih prirodnih brojeva n sa svojstvom da postoje djelitelji d_1, d_2 od $\frac{n^2+1}{2}$ za koje je $d_1 + d_2 = \delta n + \delta - 2$.

Ideja dokaza ove propozicije bit će prikazana u primjeru koji slijedi.

Primjer 2.10 Neka je $\delta = 14$. Tada je $A = 14^2/2 - 14 + 1 = 85,\ B = (14-2)/4 = 3$. Vrijede sljedeće kongruencije:

$$x \equiv 1 \pmod{85},\ x \equiv 1 \pmod 3,\ x \equiv -15 \pmod{112}.$$

Dakle,

$$x \equiv 8161 \pmod{28560}.$$

Također, $k \equiv -582 \pmod{2040},\ k = 2040u - 582,\ u \in \mathbb{Z}$. Uvrštavajući dobiveni izraz za k dobivamo tri polinoma. Prvi je polinom oblika:

$$f_1(u) = 2(2040u - 582)^2 - 2(2040u - 582) + 1 = 8323200u^2 - 4753200u + 678613,$$

Drugi i treći polinom su redom:

$$f_2(u) = 14(2040u - 582) - 1 = 28560u - 8149,$$

$$f_3(u) = 14(2040u - 582) - 14 + 1 = 28560u - 8161.$$

Diskriminanta kvadratnog polinoma f_1 nije jednaka potpunom kvadratu, što povlači da polinom f_1 nije ireducibilan, kao što to nisu ni polinomi f_2, f_3 koji su linearni polinomi. Uz prvi uvjet Schinzelove hipoteze H koji je zadovoljen, drugi uvjet te hipoteze je da za svaki prosti broj p postoji prirodan broj n za koji p ne dijeli produkt ovih triju polinoma. Dovoljno je uzeti samo prirodne brojeve $n = 1, 2$ kako bi dokazali da i drugi uvjet Schinzelove hipoteze H vrijedi.
Zaista, za $n = 1$ dobivamo

$$f_1(1) \cdot f_2(1) \cdot f_3(1) = (181 \cdot 23473) \cdot (20411) \cdot (20399).$$

Za $n = 2$ vrijedi

$$f_1(2) \cdot f_2(2) \cdot f_3(2) = 24465013 \cdot (13 \cdot 3767) \cdot (173 \cdot 283).$$

Na ovom primjeru uočavamo da je

$$\text{nzd}(f_1(1) \cdot f_2(1) \cdot f_3(1), f_1(2) \cdot f_2(2) \cdot f_3(2)) = 1,$$

te možemo zaključiti da je i drugi uvjet Schinzelove hipoteze H zadovoljen. Dakle, postoji beskonačno mnogo prirodnih brojeva u takvih da su brojevi

$$f_1(u), \;\; f_2(u), \;\; f_3(u)$$

istovremeno prosti brojevi.

Neki od brojeva k koji zadovoljavaju sve navedene uvjete su brojevi

$$119778, 519618, 1101018, 1200978, 1313178, 1531458....$$

Uočavamo da se radi o relativno velikim brojevima k za koje bi računanje rješenja početne Pellove jednadžbe $U^2 - 2abcV^2 = 1$ iznimno dugo trajalo. Stoga, pokušavamo naći manje brojeve k tako da kongruencije $\pmod A$ i/ili $\pmod B$ zamijenimo neki drugim kvadratima. U slučaju u kojem je

$$x \equiv 16 \pmod{85}, \;\; x \equiv 1 \pmod 3, \;\; x \equiv -15 \pmod{112},$$

dobivamo

$$x \equiv 28321 \pmod{28560},$$

odnosno

$$k \equiv -2022 \equiv 18 \pmod{2040}.$$

Za te uvjete za brojeve k dobivamo redom:

$$18, 1410, 2346, 2826, 5586, 5826, 6210, 8730, 10770, 11706, \ldots,$$

što će zahtijevati puno manje procesorskog vremena od bilo kojeg broja k kojeg smo dobili u prethodnom sustavu kongruencija.
Odabiremo najmanji $k = 18$ i za njega određujemo Pellovu jednadžbu te njena rješenja. Vrijedi

$$a = 2 \cdot 18^2 - 2 \cdot 18 + 1 = 613, \;\; b = 14 \cdot 18 - 1 = 251, \;\; c = 14 \cdot 18 - 14 + 1 = 239.$$

Odgovarajuća Pellova jednadžba je

$$U^2 - 73546514V^2 = 1.$$

Vrijedi

$$U_0 \approx 2.91573 \cdot 10^{691},$$

odnosno, preciznije

$U_0 = 291573388084965623066415414222126493136822343845493123412752236765274077$
$047669911769682451511507081003076621967400385067946380722339816957898527792310$
$242019306518318827256909550055996787540244985198454803117431608746874726122824$
$153967234011379557977600800213886457303490508397077246328333679634053574864041$
$520657503187757886344638828603422833555896881265832379330923158130855807053054$
$244383288931527023415438326412636349360055549692288183042949659508297035880327$
$503057266985056117173224849650918405905402874753750161096833033042080558687518$
$518439947137127139222463825005313529954301388448259569761169303032693778858708$
$236036555985997956168697062677089133739814280630549875823002622587926511 99,$

te je

$$V_0 \approx 3.39990 \cdot 10^{687},$$

odnosno, preciznije

$V_0 = 339990542978751282739828119424302553299657872399320657989287591779880879$
$309967012712446699097444187277631381601256181416786620057449703681269597367507$
$081003560227526431522393329115182701036227498219884797473847790357015709897314$
$277932290655203257819564009723755430664517338349896914895701883566997903415685$
$406555613744183305811551677327737415208498848248290426354870483394484713326412$
$332325509177292810250465316795707516271674119874122325987330043301485370243621$
$129034741052529669969882404543797108787906213047585398206502595358277973250388$
$540579916467941702063275101805230853575000119725236410800100656457368048242988$
$905250623356226464040395278986537710257089164265534681156377474923372 0.$

Nakon određivanja fundamentalnog rješenja Pellove jednadžbe, u mogućnosti smo odrediti i rješenje (X_0, Y_0) početne pellovske jednadžbe iz jednakosti $X_0 = 2g(2k-1)U_0$. Koristeći

$$n = \frac{X_0 - d\delta(\delta - 2)}{d\delta^2 - 2g},$$

dobivamo i vrijednost broja

$$n \approx 1.44598 \cdot 10^{690},$$

ili preciznije,

$n = 144598314616475141879775601745457720095691955681932027897270817045906812 7$

851469415250804802958431655777147394277311082993782997964561762072626848559107
453045453153075582338938657781577360736516412951379485029520472123143093259433
992986249452156537004054711090887013415599964128931650513915379338394347664611
051952978018602930329394580831790711345068632192320806330321217955451876148687
887846579491728307958007336474342194979354982304351372006159857702551604034030
108178781577525794046148340048145922700117608882306304927700533931536885254575
992863429517000182011418559053839456590452634038860824550298682295527500216134
628363123336518227678197271940422698954720840280527897736973115402959497.

Traženi djelitelji d_1, d_2 broja $\frac{n^2+1}{2}$ koji zadovoljavaju svojstva Propozicije 2.9 su redom

$d_1 = 716336953540927007440556930903944603361519385545237762765133776202073548876727856034432256005701893049815730380618380707903904280364999061741823041651146225530261773858136906329435616932784681861808367035967154174078428337093818241809917279883889635368835448503163980893299308833545027661925057280703563651864133724076716441209966532234687696263968995960546025485164470224291158004832824215841763705075470818064809675577317980987532040592005021569867146349048216846792472992287671903684515905747246061342401047853785045152561198849258297286779149169773563769749563467125830227691487644624255054909624646199306628402246733581850789028854562135373346201253464324506403851975658192885039948 5,
te
$d_2 = 202366006767711105930941786750550413673632586016150315279902630486649330544318045349509229188579861619495653625785489781058829324610610190261584615970878311740888404404141637721456477268809833829627012291200536150679832190222611377193893931573926791604122669179331561785905648119547717445386914869480602689182087003550196738601994244663227230818683211607328858283696454066740833545015821016099544665592606573945299926939739377899423855988021661877921370509929859393460350173554382399270399155149854453410331003418097311373559494295279009810910322965215402669104623641920824940899894220000978089931550853056753919367418623297479082033648989491404534324557728314485188633520485610416867910334 85.

Napomena za slučaj $\delta \equiv 0 \pmod 8$
Neka je $\delta \equiv 0 \pmod 8$. Analognom metodom kao u prethodnim slučajevima, uz izbor $k \equiv 3 \pmod 8$ za kojeg vrijede kongruencije

$$a \equiv 5 \pmod 8, \quad b \equiv 7 \pmod 8, \quad c \equiv 1 \pmod 8,$$

nismo u mogućnosti eliminirati slučaj 5^-) iz ranije navedenih faktorizacija, odnosno slučaj

u kojem vrijedi

$$U_0 + 1 = 2^2 at^2, \;\; U_0 - 1 = 2bcs^2.$$

Nadalje, iako smo za male vrijednosti δ eksperimentalno pronašli sporadična rješenja, već za $\delta = 40$, nismo našli nijedno rješenje pa u ovom slučaju nemamo niti dobro fundiranu hipotezu o tome što bi trebalo vrijediti.

Napomena za slučaj $\delta \equiv 2 \pmod 8$
Analogna metoda prikazana u prethodnim slučajevima dovodi do kompliciranijih uvjeta na Legendreove simbole, primjerice

$$\left(\frac{a}{c}\right) - 1, \;\; \left(\frac{a}{b}\right) = 1, \;\; \left(\frac{c}{b}\right) = 1,$$

pa ne možemo direktnom primjenom Kineskog teorema o ostacima i Schinzelove hipoteze H doći do dokaza o egzistenciji beskonačno mnogo rješenja kao što je to bio slučaj za $\delta \equiv 4, 6 \pmod 8$.

Poglavlje 3

O verziji Subbaraove kongruencije

3.1 Uvod

U teoriji brojeva osim Wilsonovog teorema koji je vrlo jednostavna karakterizacija prostih brojeva izražena preko kongruencija, nije poznata slična, jednostavna karakterizacija prostih brojeva koja uključuje i koncept kongruencije.

Lehmerova kongruencija

$$n - 1 \equiv 0 \pmod{\varphi(n)}, \tag{3.1}$$

gdje je φ Eulerova funkcija, zadovoljena je za svaki prosti broj, iako je još otvoreno pitanje postoji li složeni broj n koji zadovoljava tu kongruenciju. Lehmer je 1932. godine u [17] dokazao da, ako i postoji složeni prirodni broj n koji zadovoljava kongruenciju (3.1), tada je taj broj n neparan, kvadratno slobodan i ima barem sedam različitih prostih faktora. Lehmerov je rezultat poboljšao F. Schuh 1944. godine kad je pokazao da broj n mora imati barem 11 različitih prostih faktora.

U teoriji brojeva postoji mnoštvo neriješenih problema o karakterizacijama prirodnih brojeva n koji zadovoljavaju određene kongruencije i koji uključuju Eulerovu funkciju φ i funkciju sume djeljitelja σ.

Jedan je takav problem predstavio M. V. Subbarao u [23] u kojem se pita koji složeni brojevi n zadovoljavaju kongruenciju

$$n\sigma(n) \equiv 2 \pmod{\varphi(n)}. \tag{3.2}$$

U tom radu dokazuje da su jedini prirodni složeni brojevi koji zadovoljavaju (3.2) brojevi $n = 4, 6$ i 22.

U radu [11] autori A. Dujella i F. Luca promatraju kongruenciju

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)}$$

koja je vrlo slična Subbaraovoj kongruenciji. Dokazuju da postoji samo konačno mnogo

prirodnih brojeva n koji zadovoljavaju navedenu kongruenciju i čiji su prosti faktori elementi konačnog i fiksiranog skupa. U slučaju kad je taj skup prostih faktora $\{2, 3\}$ koristeći Worleyjev teorem i razvoj kvadratnih iracionalnosti u verižni razlomak, nalaze sve takve prirodne brojeve n koji zadovoljavaju navedenu kongruenciju.

U posljednjem poglavlju doktorske disertacije promatramo problem slične prirode. Zadana je verzija Subbaraove kongruencije $n\varphi(n) \equiv 2 \pmod{\sigma(n)}$ koja vrijedi za sve proste brojeve. Ispitujemo koji prirodni brojevi oblika $n = 2^\alpha 5^\beta$ zadovoljavaju tu kongruenciju za $\alpha, \beta \geq 0$. U prvom dijelu dokaza glavnog teorema poglavlja, prema uzoru na [6], [11], promatramo potencije prostih brojeva $n = 2^\alpha$ i $n = 5^\beta$ s eksponenatima $\alpha \geq 2$, $\beta \geq 2$ i dokazujemo da je jedini broj takvog oblika koji zadovoljava verziju Subbaraove kongruencije broj $n = 2^3$. U nastavku dokaza dokazujemo da ne postoje brojevi oblika $n = 2^\alpha 5^\beta,\ \alpha, \beta \in \mathbb{N}$ koji zadovoljavaju zadanu kongruenciju. U glavnom teoremu ovog poglavlja dokazano je da su jedini prirodni brojevi oblika $n = 2^\alpha 5^\beta,\ \alpha, \beta \in \mathbb{N}_0$, koji zadovoljavaju verziju Subbaraove kongruencije brojevi $n = 1, 2, 5, 8$.

3.2 Verzija Subbaraove kongruencije za $n = 2^\alpha 5^\beta$

Definicija 3.1 Aritmetička funkcija f je multiplikativna ako je $f(1) = 1$ te ako vrijedi

$$f(mn) = f(m)f(n)$$

za sve $m, n \in \mathbb{N}$ za koje je $\text{nzd}(m, n) = 1$.

Definicija 3.2 Eulerova funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ je aritmetička funkcija koja prirodnom broju n pridružuje broj svih prirodnih brojeva manjih od n koji su relativno prosti s brojem n. Definiramo $\varphi(1) = 1$.

Teorem 3.3 Eulerova funkcija φ je multiplikativna funkcija.

□

Definicija 3.4 Suma djelitelja prirodnog broja n je aritmetička funkcija $\sigma : \mathbb{N} \to \mathbb{N}$ definirana s

$$\sigma(n) = \sum_{d|n} d.$$

Teorem 3.5 Funkcija sume djelitelja σ je multiplikativna funkcija.

□

U [11] A. Dujella i F. Luca proučavaju kongruenciju

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)}. \tag{3.3}$$

Vrlo je lako uočiti da svi prosti brojevi zadovoljavaju promatranu kongruenciju.
Neka je p prost broj. Tada vrijedi $\varphi(p) = p - 1$ te $\sigma(p) = p + 1$. Uvrštavajući dobivene vrijednosti u (3.3) dobivamo

$$p(p-1) - 2 = (p+1)(p-2) \equiv 0 \pmod{(p+1)},$$

što povlači da kongruencija (3.3) vrijedi za sve proste brojeve, odnosno

$$p(p-1) \equiv 2 \pmod{(p+1)}.$$

U [6] je pokazano da jedini prirodni brojevi n koji su potencije prostih brojeva s eksponentima $a \geq 2$ i koji zadovoljavaju (3.3) jesu brojevi $n = 8, 9$. Pokazano je također da, ako je n složen prirodni broj koji zadovoljava (3.3) i ako je

$$k := \frac{n\varphi(n) - 2}{\sigma(n)},$$

tada n možemo ograditi koristeći broj k. Naime, vrijedi

$$n \ll k(\log\log k)^2.$$

Promotrimo zadovoljavaju li prirodni brojevi $n = \{p_1^{a_1} \dots p_k^{a_k},\ a_i \geq 0\}, k$ konačan, kongruenciju (3.3).

Neka je $\mathcal{P} = \{p_1, \dots p_k\}$ konačan skup prostih brojeva i neka je $\mathcal{S}_\mathcal{P} = \{p_1^{a_1} \dots p_k^{a_k} : a_i \geq 0\}$ skup svih prirodnih brojeva čiji su prosti faktori elementi iz $\mathcal{P}$. U [11] je dokazan sljedeći teorem:

Teorem 3.6 (Dujella, Luca) Za svaki konačan skup prostih brojeva $\mathcal{P}$ postoji samo konačno mnogo prirodnih brojeva $n \in \mathcal{S}_\mathcal{P}$ koji zadovoljavaju kongruenciju (3.3).

Dokaz.

Neka je $n = p^a$, p prost broj i $a \geq 2$. Definiramo $D := \sigma(p^a) = \frac{p^{a+1}-1}{p-1}$. U tom slučaju vrijedi $p^{a+1} \equiv 1 \pmod{D}$. Također, zbog kongruencije $n\varphi(n) \equiv 2 \pmod{D}$ u ovom slučaju je

$$p^a \cdot p^a \left(1 - \frac{1}{p}\right) \equiv 2 \pmod{D},$$

$$p^{2a-1}(p-1) \equiv 2 \pmod{D}.$$

Množeći brojem p^3 prethodna kongruencija postaje

$$p^{2(a+1)}(p-1) \equiv 2p^3 \pmod{D}.$$

Od ranije znamo $p^{a+1} \equiv 1 \pmod{D}$ iz čega je lako zaključiti da vrijedi $2p^3 \equiv p - 1$

(mod D), odnosno $D|(2p^3-p+1)$. Broj $2p^3-p+1\neq 0$ za svaki prost broj p, što povlači $D\leq 2p^3-p+1$. U tom slučaju je

$$p^{a+1}-1\leq (p-1)(2p^3-p+1).$$

Za $a\geq 4$, vrijede nejednakosti

$$p^5-1\leq p^{a+1}-1\leq (p-1)(2p^3-p+1),$$

što nije moguće za $p\geq 2$. Zaključujemo da je $a\in\{2,3\}$.

Za $a=2$ analogno dobivamo nejednakost

$$p^3-1\leq (p-1)(2p^3-p+1),$$

$$p^2+p+1\leq 2p^3-p+1,$$

pa zaključujemo da $(p^2+p+1)|(2p^3-p+1)$ što povlači $(p^2+p+1)|(p-3)$. To je moguće jedino u slučaju kad je $p=3$. Dobiveni rezultat odgovara rješenju $n=3^2$ zadane kongruencije (3.3).

Ako je $a=3$, analognim zaključivanjem dobivamo da $(p^3+p^2+p+1)|(2p^3-p+1)$. Vrijedi $(p^3+p^2+p+1)|(2p^2+3p+1)$ što je moguće u slučaju $p^3\leq p^2+2p$, odnosno $p\leq 2$. Na ovaj način dobivamo još jedno rješenje kongruencije (3.3), preciznije vrijedi da i $n=2^3$ zadovoljava verziju Subbaraove kongruencije.

Promotrimo sad općenit slučaj. Neka je $\mathcal{P}=\{p_1,\dots p_k\}$ konačan skup prostih brojeva uz pretpostavku da vrijedi $p_1<p_2<\cdots<p_k$. Bez smanjenja općenitosti možemo pretpostaviti da se skup $\mathcal{P}$ sastoji od svih prostih brojeva p za koje vrijedi $p\leq p_k$. Dakle, p_j je j-ti prosti broj. Neka broj $n=p_{i_1}^{a_{i_1}}\dots p_{i_s}^{a_{i_s}}\in\mathcal{S}_{\mathcal{P}}$ zadovoljava kongruenciju (3.3), gdje je $1\leq i_1<\cdots<i_s\leq k$ i a_j su pozitivni brojevi za $j=1,\dots s$. Bez smanjenja općenitosti možemo pretpostaviti $s\geq 2$.

Neka je

$$u_j:=p_{i_j}^{a_j+1},\ \ j=1,\dots s,\ \ v:=n\varphi(n)/2=p_{i_1}^{2a_1-1}\dots p_{i_s}^{2a_s-1}(p_{i_1}-1)\dots(p_{i_s}-1)/2.$$

Uočimo da su $u_j,v\in\mathcal{S}_{\mathcal{P}}$ za sve $j=1,\dots s$. Također, u_j i v su multiplikativno nezavisni jer je u_j potencija samo jednog prostog broja, a v ima najmanje dva prosta faktora, primjerice p_{i_1} i p_{i_2}. Neka je j takav da je $u_j=\max\{u_t:1\leq t\leq s\}$. Možemo pretpostaviti da je $a_j\geq 3$, inače $u_t\leq p_i^3$, za sve $i=1,\dots,s$ pa imamo samo konačno mnogo izbora za n. Vrijedi

$$v<p_{i_1}^{2a_{i_1}}\dots p_{i_s}^{2a_{i_s}}<u_1^2\dots u_s^2<u_j^{2k},$$

iz čega slijedi $u_j>v^{1/2k}$.

Budući $\frac{u_j-1}{p_{i_j}-1}|2(v-1)$, slijedi

$$\text{nzd}(u_j-1, v-1) \geq \frac{u_j-1}{2(p_{i_j}-1)} > u_j^{1/2} > v^{1/4k},$$

gdje koristimo pretpostavku da je $a_j \geq 3$. Hernándezov i Lucin rezultat iz [13] tvrdi da, ako je $\varepsilon > 0$ fiksiran, postoji samo konačno mnogo parova $(u, v) \in \mathcal{S}_{\mathcal{P}}$ takvih da je

$$\text{nzd}(u-1, v-1) < \max\{u, v\}^{\varepsilon},$$

u, v multiplikativno nezavisni. Uočimo da je $u_j < v$ za $a_j \geq 3$. Budući već znamo da su u_j i v multiplikativno nezavisni, navedeni rezultat možemo primijeniti za $\varepsilon := \frac{1}{4}k$ te smo u mogućnosti odabrati samo konačno mnogo brojeva v što implicira da postoji samo konačno mnogo mogućnosti za odabir broja $n\varphi(n)$, odnosno, specijalno, samo konačno mnogo mogućnosti za odabir broja n što je trebalo i pokazati.

□

U [11] A. Dujella i F. Luca dokazuju da, ako je skup $\mathcal{P} = \{2, 3\}$, tada su jedini prirodni brojevi $n \in \mathcal{S}_{\mathcal{P}}$ koji zadovoljavaju kongruenciju (3.3) brojevi $n = 1, 2, 3, 8, 9$.
U ovom dijelu doktorske disertacije ispitujemo sličan problem. Neka je skup $\mathcal{P} = \{2, 5\}$. Pokušavamo pronaći sve prirodne brojeve $n \in \mathcal{S}_{\mathcal{P}}$ koji zadovoljavaju kongruenciju (3.3).

Teorem 3.7 Ako je $\mathcal{P} = \{2, 5\}$, tada su jedini prirodni brojevi $n \in \mathcal{S}_{\mathcal{P}}$ koji zadovoljavaju kongruenciju (3.3) brojevi $n = 1, 2, 5, 8$.

Dokaz.

Kongruencija (3.3) vrijedi za sve proste brojeve pa tako i za brojeve $n = 2, 5$.

Rezultat u kojem je $a = 0$ ili $b = 0$ za $n = 2^a 5^b$ specijalan je slučaj prvog dijela dokaza prethodnog Teorema 3.6 iz [11] o potencijama prostih brojeva p^a, $p \in \mathbb{P}$, $a \geq 2$, odnosno dokaza iz [6] u kojem je pokazano da jedini prirodni brojevi n koji su potencije prostih brojeva s eksponentima $a \geq 2$ i koji zadovoljavaju (3.3) jesu brojevi $n = 8, 9$.

Neka je $b = 0$, odnosno $n = 2^a$, $a \geq 2$. Definiramo $D := \sigma(2^a) = 2^{a+1} - 1$. Jednostavno zaključujemo da je $2^{a+1} \equiv 1 \pmod{D}$. Uz navedeno, zbog kongruencije (3.3), također vrijedi

$$2^a \cdot 2^a \left(1 - \frac{1}{2}\right) \equiv 2 \pmod{D},$$

$$2^{2a-1} \equiv 2 \pmod{D},$$

$$2^{2(a+1)} \equiv 2^4 \pmod{D},$$

$$(2^{a+1} - 1)(2^{a+1} + 1) - 15 \equiv 0 \pmod{D}.$$

Uočavamo da $D|((2^{a+1}-1)(2^{a+1}+1)-15)$ ako i samo ako $D|15$, odnosno ako $(2^{a+1}-1)|15$.

Uz pretpostavku da je $a \geq 2$, navedeni uvjet je moguć ako i samo ako je $a = 3$. Prirodni broj $n = 2^3$ zadovoljava verziju Subbaraove kongruencije (3.3).

Neka je $a = 0$. Tada je $n = 5^b,\ \ b \geq 2$. Kao u prethodnom slučaju za $a = 0$, definiramo $D := \sigma(5^b) = \frac{5^{b+1}-1}{4}$. Vrijedi $5^{b+1} \equiv 1 \pmod{D}$. Zbog (3.3), zaključujemo

$$5^{2b-1} \cdot 2^2 \equiv 2 \pmod{D},\ \ 5^{2(b+1)} \cdot 2^2 \equiv 5^3 \cdot 2 \pmod{D}.$$

S obzirom da vrijedi $5^{b+1} \equiv 1 \pmod{D}$, lako je uočiti da $D|246$, što nije moguće za $b \geq 2$. Brojevi oblika $n = 5^b,\ \ b \geq 2$, ne zadovoljavaju kongruenciju (3.3).

U nastavku promatramo općenit slučaj. Neka je $n = 2^a 5^b$, gdje su $a, b \in \mathbb{N}$. Definiramo: $M := 2^{a+1} - 1$ te $N := \frac{5^{b+1}-1}{4}$. Tada je

$$2^{a+1} \equiv 1 \pmod{M}$$

i

$$5^{b+1} \equiv 1 \pmod{N}.$$

Uz sve navedeno, budući je zadovoljena i kongruencija (3.3)

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)},$$

u našem slučaju lako je zaključiti

$$2^{2a+1} \cdot 5^{2b-1} \equiv 2 \pmod{MN}. \tag{3.4}$$

Množeći prethodni izraz s $2 \cdot 5^3$ dobivamo

$$2^{2(a+1)} \cdot 5^{2(b+1)} \equiv 500 \pmod{MN}.$$

Zbog $2^{a+1} \equiv 1 \pmod{M}$, vrijedi i kongruencija $5^{2(b+1)} \equiv 500 \pmod{M}$. Također, zbog $5^{b+1} \equiv 1 \pmod{N}$, zaključujemo da je $2^{2(a+1)} \equiv 500 \pmod{N}$. S obzirom da M dijeli $2^{a+1} - 1$, također slijedi da $M|(2^{2(a+1)} - 1)$. Analogno, $N|(5^{2(b+1)} - 1)$. Brojevi M, N dijele izraz

$$2^{2(a+1)} + 5^{2(b+1)} - 501. \tag{3.5}$$

Nastojimo dokazati da su brojevi M, N međusobno relativno prosti i ispitujemo parnost, odnosno neparnost eksponenata a, b.

Neka je $D := \text{nzd}(M, N)$. Vrijedi $2^{a+1} \equiv 5^{b+1} \equiv 1 \pmod{D}$. Iz (3.5) zaključujemo da $D|(1 + 1 - 501)$, odnosno $D| - 499$. Budući je $499 \in \mathbb{P}$, broj D je $D = 1$ ili $D = 499$.
Za početak, pretpostavimo da je $D = 499$. U tom slučaju znamo da $499|M$, odnosno $499|\,(2^{a+1} - 1)$. Zaključujemo da $166|(a + 1)$, pa posebno vrijedi $2|(a + 1)$. Dakle, a je neparan broj. Broj M možemo prikazati kao $M = 2^{a+1} - 1 = 2^{2k} - 1$ za $k \in \mathbb{N}$, nakon

čega zaključujemo da $3|M$. Slijedi da $3|(n\varphi(n)-2)$, odnosno $3|(2^{2a+1}\cdot 5^{2b-1}-2)$, što nije moguće. Stoga, $499 \nmid M$, odnosno, $\text{nzd}(M,N)=1$. Dokazano je i da je $a+1$ neparan broj iz čega jasno slijedi da je a paran broj.

Preostaje nam još dokazati da je i broj b paran. Pretpostavimo suprotno, neka je b neparan broj. U tom slučaju možemo pisati $5^{b+1}-1=5^{2k}-1$. Uočavamo da $24|(5^{2k}-1)$, što povlači da $6|N|(2^{2a+1}\cdot 5^{2b-1}-2)$ što je nemoguće. Broj b je paran broj. Dakle, brojevi M,N su neparni brojevi.

Budući brojevi M,N dijele (3.5) i dokazano je da su međusobno relativno prosti, zaključujemo

$$MN|(2^{2(a+1)}+5^{2(b+1)}-501).$$

Broj $2^{2(a+1)}+5^{2(b+1)}-501$ je paran pa možemo izraziti u obliku

$$2MN=(2^{a+1}-1)(5^{b+1}-1).$$

Definirajmo $x:=2^{a+1}$ i $y:=5^{b+1}$. Uz navedene oznake prethodni problem možemo prikazati kao jednadžbu oblika:

$$x^2+y^2-501=c(x-1)(y-1), \tag{3.6}$$

za neki $c\in\mathbb{N}$. Iz (3.6) ćemo pokušati saznati nešto više o prirodnom broju c.

Budući su eksponenti broja n parni brojevi, možemo primjetiti da vrijede kongruencije $x\equiv 0 \pmod 8$, $x^2\equiv 0 \pmod 8$, kao i $y\equiv 5 \pmod 8$, $y^2\equiv 1 \pmod 8$. Uvrštavanjem dobivenih ostataka u (3.6), dobivamo $4c\equiv 4 \pmod 8$ što vrijedi za svaki c neparan broj, odnosno za

$$c\equiv 1 \pmod 2. \tag{3.7}$$

Također, možemo uočiti da je $x\equiv 2 \pmod 3$ iz čega slijedi $x^2\equiv 1 \pmod 3$. Za y vrijede kongruencije $y\equiv 2 \pmod 3$ te $y^2\equiv 1 \pmod 3$. Iz (3.6) slijedi

$$c\equiv 2 \pmod 3. \tag{3.8}$$

Možemo primjetiti i sljedeće

$$x\equiv 3 \pmod 5,\ x^2\equiv 4 \pmod 5,\ \text{za } a\equiv 2 \pmod 4,$$

$$x\equiv 2 \pmod 5,\ x^2\equiv 4 \pmod 5,\ \text{za } a\equiv 0 \pmod 4.$$

Očito je $y\equiv y^2\equiv 0 \pmod 5$. Korištenjem jednadžbe (3.6) zaključujemo da broj c može biti element dviju klasa ostataka pri dijeljenju brojem 4. Preciznije,

$$c\equiv 1 \pmod 5,\ \text{za } a\equiv 2 \pmod 4,$$

te

$$c \equiv 2 \pmod 5, \text{ za } a \equiv 0 \pmod 4. \tag{3.9}$$

Pokušajmo za broj c pobliže utvrditi koja nam od dvije navedene klase ostataka zadovoljava već definirane uvjete. Neka je $t = 2^a \cdot 5^{b-1}$, odnosno $5t^2 = 2^{2a} \cdot 5^{2b-1}$. Prema (3.4) možemo zaključiti da je $5t^2 \equiv 1 \pmod M$, što povlači $\left(\frac{5}{M}\right) = \left(\frac{M}{5}\right) = 1$. U tom slučaju je $M \equiv 1, 4 \pmod 5$. Budući je $M = 2^{a+1} - 1$, vrijedi $2^{a+1} - 1 \equiv 1 \pmod 5$ ili $2^{a+1} - 1 \equiv 4 \pmod 5$. Prvu je kongruenciju moguće ostvariti za $a \equiv 0 \pmod 4$, dok druga mogućnost vrijedi za $a \equiv 3 \pmod 4$ što ne uzimamo u obzir budući je dokazano da je a paran broj. Zbog ove činjenice promatramo samo one brojeve c za koje je $c \equiv 2 \pmod 5$.

Temeljem kongruencija (3.7), (3.8) i (3.9) određujemo sve prirodne brojeve c za koje vrijedi

$$c \equiv 17 \pmod{30}. \tag{3.10}$$

"Dijagonalizirajmo" jednadžbu (3.6). Neka je

$$X := cy - c - 2x, \tag{3.11}$$

$$Y := cy - c - 2y. \tag{3.12}$$

Tada vrijedi

$$(c+2)Y^2 - (c-2)X^2 - (-1996c + 4008) = -4(c-2)(x^2 + y^2 - 501 - c(x-1)(y-1)) = 0.$$

Ovim smo postupkom dobili pellovsku jednadžbu oblika

$$(c+2)Y^2 - (c-2)X^2 = -1996c + 4008. \tag{3.13}$$

Iz (3.13) je jasno da je $\frac{X}{Y}$ dobra aproksimacija iracionalnog broja $\sqrt{\frac{c+2}{c-2}}$. Zaključujemo

$$\left|\frac{X}{Y} - \sqrt{\frac{c+2}{c-2}}\right| = \frac{1996c - 4008}{(\sqrt{c+2}Y - \sqrt{c-2}X)\sqrt{c-2}Y} \leq \frac{1996(c-2)}{\sqrt{c^2-4}Y^2} < \frac{1996}{Y^2}.$$

No, racionalna aproksimacija oblika

$$\left|\frac{X}{Y} - \sqrt{\frac{c+2}{c-2}}\right| < \frac{1996}{Y^2} \tag{3.14}$$

nije dovoljno dobra aproksimacija od $\sqrt{\frac{c+2}{c-2}}$ da bi mogli zaključiti da je $\frac{X}{Y}$ konvergenta razvoja u verižni razlomak broja $\sqrt{\frac{c+2}{c-2}}$.
Iz tog razloga koristimo Worleyjev teorem iz [24], odnosno iz [8].

Teorem 3.8 (Worley) Neka je α iracionalan broj te neka su $a, b \neq 0$ relativno prosti cijeli

brojevi koji zadovoljavaju nejednakost

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

gdje je c pozitivan realan broj. Tada je

$$(a, b) = (rp_{m+1} \pm sp_m,\ \ rq_{m+1} \pm sq_m),$$

za $m, r, s \in \mathbb{N}_0$ za koje vrijedi uvjet $rs < 2c$.

□

Prema Worleyjevom teoremu znamo da postoji konvergenta $\frac{X}{Y}$ oblika

$$\frac{X}{Y} = \frac{rp_{k+1} + up_k}{rq_{k+1} + uq_k},$$

gdje je $k \geq -1$, $u \in \mathbb{Z}$, r je nenegativni cijeli broj, te vrijedi $|ru| < 2 \cdot 1996 = 3992$.

Kako bi odredili sva rješenja, koristimo i lemu iz [9].

Lema 3.9 (Dujella, Jadrijević) Neka je $\alpha\beta$ prirodan broj koji nije potpun kvadrat i neka je p_k/q_k k-ta konvergenta razvoja u verižni razlomak broja $\sqrt{\frac{\alpha}{\beta}}$. Neka su $(s_k)_{k\geq -1}$ i $(t_k)_{k\geq -1}$ nizovi iz razvoja u verižni razlomak kvadratne iracionalnosti $\frac{\sqrt{\alpha\beta}}{\beta}$. Tada je

$$\alpha(rq_{k+1} + uq_k)^2 - \beta(rp_{k+1} + up_k)^2 = (-1)^k(u^2t_{k+1} + 2rus_{k+2} - r^2t_{k+1}). \tag{3.15}$$

□

Primjenjujući Lemu 3.9, lako je uočiti da je u našem slučaju

$$(c+2)Y^2 - (c-2)X^2 = d^2(-1)^k(u^2t_{k+1} + 2rus_{k+1} - r^2t_{k+2}), \tag{3.16}$$

gdje su $(s_k)_{k\geq -1}$ i $(t_k)_{k\geq -1}$ nizovi cijelih brojeva koji se pojavljuju u razvoju u verižni razlomak kvadratne iracionalnosti $\sqrt{\frac{c+2}{c-2}}$.

Iz tog razloga određujemo razvoj broja $\sqrt{\frac{c+2}{c-2}}$ u verižni razlomak za c neparan broj.

Dobivamo redom vrijednosti:

$$s_0 = 0,\ \ t_0 = c-2,\ \ a_0 = 1,$$

$$s_1 = c-2,\ \ t_1 = 4, a_1 = \frac{c-3}{2},$$

$$s_2 = c-4,\ \ t_2 = 2c-5,\ \ a_2 = 1,$$

$$s_3 = c-1,\ \ t_3 = 1,\ \ a_3 = 2c-2,$$

$$s_4 = c-1,\ \ t_4 = 2c-5,\ \ a_4 = 1,$$
$$s_5 = c-4,\ \ t_5 = 4,\ \ a_5 = \frac{c-3}{2},$$
$$s_6 = c-2,\ \ t_6 = c-2,\ \ a_6 = 2,$$

odnosno

$$\sqrt{\frac{c+2}{c-2}} = \left[1; \overline{\frac{c-3}{2}, 1, 2c-2, 1, \frac{c-3}{2}, 2}\right],\ \ c \text{ neparan broj.}$$

Uočavamo da je duljina razvoja l broja $\sqrt{\frac{c+2}{c-2}}$ u verižni razlomak $l = 6$ pa promatramo jednakost (3.16) za $k = 0, 1, 2, 3, 4, 5$. Određujemo brojeve $c \in \mathbb{N}$ koji zadovoljavaju kongruenciju (3.10) za svaki takav k.

Za $k = 0$ jednakost (3.16) postaje:

$$d^2(u^2t_1 + 2rus_1 - r^2t_2) = -1996c + 4008,$$

$$d^2(4u^2 - 4ru + 2cru - 2r^2c + 5r^2) = -1996c + 4008.$$

Provjerimo je li moguće da su ove dvije strane jednakosti identički jednake. Mogućnosti za broj d u svim promatranim slučajevima, za $k = 0, 1, 2, 3, 4, 5$, su $d = 1$ ili $d = 2$.
Za $d = 1$ prethodna jednakost postaje

$$4u^2 - 4ru + 2cru - 2r^2c + 5r^2 = -1996c + 4008,$$

čime je određen sustav jednadžbi

$$\begin{cases} 4u^2 - 4ru + 5r^2 = 4008, \\ 2ru - 2r^2 = -1996. \end{cases}$$

Ovaj sustav ne rezultira cjelobrojnim rješenjima.
Za $d = 2$ dobivamo jednakost

$$4u^2 - 4ru + 2cru - 2r^2c + 5r^2 = -499c + 1002,$$

odnosno sustav

$$\begin{cases} 4u^2 - 4ru + 5r^2 = 1002, \\ 2ru - 2r^2 = -499, \end{cases}$$

koji također nema cjelobrojna rješenja.

Općenito, za sve vrijednosti broja d definiramo broj c. U slučaju $k = 0$ dobivamo da je

$$c = \frac{4008 - 4d^2u^2 + 4d^2ru - 5d^2r^2}{1996 + 2d^2ru - 2d^2r^2}. \tag{3.17}$$

Nastojimo odrediti prirodni broj c koji zadovoljava kongruenciju (3.10) i koji je definiran pomoću trojki (d, r, u) za koje vrijedi $d \in \mathbb{N},\ d \leq 64$, $u \in \mathbb{Z}$, $r \in \mathbb{N}$ i koje zadovoljavaju nejednakost $d^2ru < 3992$. S tim ciljem je napisan računalni program koji u prvom koraku određuje sve povoljne trojke (d, r, u) za koje vrijedi uvjet nejednakosti $d^2ru < 3992$. Drugi dio računalnog programa uvrštava sve takve trojke (d, r, u) u (3.17) i sve analogne izraze za određivanje broja c za svaki $k = 0, 1, 2, 3, 4, 5$. Uz navedeno, program ispituje je li svaki dobiveni broj c prirodan broj te zadovoljava li kongruenciju (3.10). U slučaju potvrdnih odgovora, program ispisuje povoljne brojeve c.

Koristeći program za $k = 0$ ne nalazimo brojeve c koji zadovoljavaju navedene uvjete.

Za slučaj kad je $k = 1$ jednakost (3.16) je oblika:

$$-d^2(u^2t_2 + 2rus_2 - r^2t_3) = -1996c + 4008,$$

$$-d^2(u^2(2c-5) + 2ru(c-4) - r^2) = -1996c + 4008.$$

Za $d = 1$ vrijedi $5u^2 + 8ru + r^2 = 4008,\ -2u^2 - 2ru = -1996$, dok za $d = 2$ dobivamo sustav $5u^2 + 8ru + r^2 = 1002,\ -2u^2 - 2ru = -499$. Oba sustava nemaju cjelobrojna rješenja.
Broj c općenito predstavljamo kao:

$$c = \frac{5d^2u^2 + 8d^2ru + d^2r^2 - 4008}{2d^2u^2 + 2d^2ru - 1996}.$$

Upotrebom programa saznajemo da je jedini broj $c \in \mathbb{N}$ koji je određen na navedeni način i koji zadovoljava kongruenciju (3.10) broj

$$c = 77.$$

Za $c = 77$ iz (3.13) određujemo pellovsku jednadžbu

$$79Y^2 - 75X^2 = -149684$$

kojoj, u nastavku rada, nastojimo odrediti rješenja.

Za $k = 2$ i $u \in \mathbb{Z}$ dobivamo jednakost:

$$d^2(u^2t_3 + 2rus_3 - r^2t_4) = -1996c + 4008,$$

$$d^2(u^2 + 2ru(c-1) - r^2(2c-5)) = -1996c + 4008.$$

Za $d = 1$ određen je sustav $u^2 - 2ru + 5r^2 = 4008,\ 2ru - 2r^2 = -1996$ koji nema cjelobrojna

rješenja. Za slučaj kad je $d = 2$ sustav $u^2 - 2ru + 5r^2 = 1002,\ \ 2ru - 2r^2 = -499$ također ne rezultira cjelobrojnim rješenjima.
Broj c je u ovom slučaju definiran s

$$c = \frac{d^2u^2 - 2d^2ru + 5d^2r^2 - 4008}{2d^2r^2 - 2d^2ru - 1996}.$$

Brojevi c koje smo odredili opisanim računalnim programom su

$$c \in \{17, 227, 497, 647, 857, 2537, 3107, 4937\}.$$

Za svaki navedeni broj c definirana je po jedna pellovska jednadžba oblika (3.13) kojoj u nastavku rada određujemo rješenja.

Za iduću vrijednost broja k, konkretnije za $k = 3$, vrijedi:

$$-d^2(u^2t_4 + 2rus_4 - r^2t_5) = -1996c + 4008,$$

$$-d^2(u^2(2c - 5) + 2ru(c - 1) - 4r^2) = -1996c + 4008.$$

Sustavi koje dobivamo za $d = 1$, $d = 2$ su redom $5u^2 + 2ru + 4r^2 = 4008,\ \ -2u^2 - 2ru = -1996$, odnosno $5u^2 + 2ru + 4r^2 = 1002,\ \ -2u^2 - 2ru = -499$, respektivno. Kao i u svim prethodnim slučajevima, ni ovi sustavi nemaju cjelobrojna rješenja. Traženi broj c je:

$$c = \frac{5d^2u^2 + 2d^2ru + 4d^2r^2 - 4008}{2d^2u^2 + 2d^2ru - 1996}.$$

Kao i za $k = 0$, ni u ovom slučaju ne postoje prirodni brojevi c koji zadovoljavaju zadanu kongruenciju.

Za $k = 4$ analognim postupkom dobivamo jednakosti

$$d^2(u^2t_5 + 2rus_5 - r^2t_0) = -1996c + 4008,$$

$$d^2(4u^2 + 2ru(c - 4) - r^2(c - 2)) = -1996c + 4008.$$

Za $d = 1$ vrijedi $4u^2 - 8ru + 2r^2 = 4008,\ \ 2ru - r^2 = -1996$, dok je za $d = 2$ $4u^2 - 8ru + 2r^2 = 1002,\ \ 2ru - r^2 = -499$. Oba sustava nemaju cjelobrojna rješenja. Općenito,

$$c = \frac{4d^2u^2 - 8d^2ru + 2d^2r^2 - 4008}{d^2r^2 - 2d^2ru - 1996}.$$

Nijedan prirodan broj c određen na ovaj način ne zadovoljava zadanu kongruenciju.

Naposlijetku, za $k = 5$ uvrštavanjem odgovarajućih vrijednosti dobivenih razvojem

kvadratne iracionalnosti $\sqrt{\frac{c+2}{c-2}}$, c neparan broj, u verižni razlomak u (3.9), vrijedi:

$$-d^2(u^2t_0 + 2rus_0 - r^2t_1) = -1996c + 4008,$$

$$-d^2(u^2(c-2) - 4r^2) = -1996c + 4008.$$

Za $d = 1$ određen je sustav $4r^2 + 2u^2 = 4008$, $-u^2 = -1996$, dok je za $d = 2$ određen sustav $4r^2 + 2u^2 = 1002$, $-u^2 = -499$. Kao i svi sustavi određeni na ovaj način za $k = 0, 1, 2, 3, 4$, ni ovi sustavi ne rezultiraju cjelobrojnim rješenjima.
Broj c je u ovom slučaju:

$$c = \frac{2d^2u^2 + 4d^2r^2 - 4008}{d^2u^2 - 1996}.$$

No, ne postoji takav prirodan broj c.

U sljedećem dijelu dokaza preostaje nam za svaki dobiveni prirodni broj c odrediti pellovsku jednadžbu (3.13), izračunati njena rješenja, te ispitati postoje li rješenja koja zadovoljavaju kongruencije koje slijede iz oblika brojeva x, y i njihove veze s rješenjima X, Y.

Promatramo sljedeće pellovske jednadžbe:

$$19Y^2 - 15X^2 = -29924, \text{ za } c = 17,$$

$$79Y^2 - 75X^2 = -149684, \text{ za } c = 77,$$

$$229Y^2 - 225X^2 = -449084, \text{ za } c = 227,$$

$$499Y^2 - 495X^2 = -988004, \text{ za } c = 497,$$

$$649Y^2 - 645X^2 = -1287404, \text{ za } c = 647,$$

$$859Y^2 - 855X^2 = -1706564, \text{ za } c = 857,$$

$$2539Y^2 - 2535X^2 = -5059844, \text{ za } c = 2537,$$

$$3109Y^2 - 3105X^2 = -6197564, \text{ za } c = 3107,$$

$$4937Y^2 - 4935X^2 = -9850244, \text{ za } c = 4937.$$

Općeniti oblik diofantske jednadžbe drugog stupnja je

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{3.18}$$

Ako vrijedi $a = b = c = 0$, jednadžbu (3.18) zovemo linearna diofantska jednadžba. Za $a = c = 0$, $b \neq 0$, jednadžba (3.18) je jednostavna hiperbolička diofantska jednadžba. Uz navedene slučajeve, razlikujemo još tri tipa diofantskih jednadžbi: eliptičke diofantske jednadžbe, gdje vrijedi $b^2 - 4ac < 0$, paraboličke diofantske jednadžbe za koje je $b^2 - 4ac = 0$ te hiperboličke diofantske jednadžbe koje karakterizira nejednakost $b^2 - 4ac > 0$. Možemo

primjetiti da sve pellovske jednadžbe koje promatramo u dokazu teorema odgovaraju hiperboličkom tipu diofantskih jednadžbi.

Ako je zadana jednadžba

$$ax^2 + bxy + cy^2 + f = 0, \quad f \neq 0,$$

te vrijedi $b^2 - 4ac = k^2$, za neki $k \in \mathbb{Z}$, postupak rješavanja takve diofantske jednadžbe za početak uključuje određivanje svih pozitivnih i negativnih djelitelja u_i broja $-4af$ te generiranje njenih rješenja

$$x = \frac{u_i - (b+k)y}{2a}, \quad y = \frac{u_i + 4af/u_i}{2k},$$

ne uključujući one djelitelje u_i za koje $x, y \notin \mathbb{Z}$.

Za slučaj kad je $f \neq 0$ i $b^2 - 4ac \neq k^2, \ k \in \mathbb{Z}$, ispitujemo je li slobodni koeficijent f višekratnik od $\text{nzd}(a, b, c)$. Ako je odgovor negativan, polazna diofantska jednadžba nema rješenja. U suprotnom, cijelu diofantsku jednadžbu možemo podijeliti brojem $\text{nzd}(a, b, c)$. U slučaju da je zadovoljena nejednakost $4f^2 < b^2 - 4ac$, rješenja polazne diofantske jednadžbe nalaze se među konvergentama razvoja u verižni razlomak korijena jednadžbe $at^2 + bt + c = 0$. Budući je razvoj kvadratne iracionalnosti u verižni razlomak periodičan, a broj $b^2 - 4ac \neq k^2, \ k \in \mathbb{Z}$, broj rješenja diofantske jednadžbe je, ili beskonačan, ili jednadžba nema rješenja.

Ako je zadovoljena nejednakost $4f^2 \geq b^2 - 4ac$, postupak određivanja rješenja pellovske jednadžbe je nešto drugačiji. Definiramo $G = \text{nzd}(x, y), \ x = Gu, \ y = Gv$. Početna jednadžba postaje

$$au^2 + buv + cv^2 + \frac{f}{g^2} = 0.$$

Neka je $x = sy - fz$. Nakon supstitucije, polazna diofantska jednadžba poprima oblik

$$-\frac{(as^2 + bs + c)}{f} y^2 + (2as + b)yz - afz^2 = 1.$$

Određujemo vrijednosti $0 < s < f - 1$ za koje je $as^2 + bs + c \equiv 0 \pmod{f}$. Vrijednosti y, z određuju se razvojem rješenja jednadžbe

$$-\frac{(as^2 + bs + c)}{f} t^2 + (2as + b)t - af = 0$$

u verižni razlomak. Ako je duljina perioda razvoja u verižni razlomak paran broj, razmatraju se konvergente do kraja prvog perioda. U slučaju da je duljina perioda neparan broj, razmatraju se konvergente dva perioda. Nakon toga smo u mogućnosti odrediti i broj x. Ako polazna jednadžba ima rješenja, tada postoje i rješenja navedene kongruencije, osim ako je $\text{nzd}(a, b, f) > 1$. U ovom slučaju, ako vrijedi $\text{nzd}(b, c, f) = 1$, definiramo

supstituciju $y = sx - fz$ i na analogan način dobivamo diofantsku jednadžbu

$$-\frac{cs^2 + bs + a}{f}x^2 + (2cs + b)xz - cfz^2 = 1.$$

Određujemo $0 < s < f - 1$ takve da kongruencija $cs^2 + bs + a \equiv 0 \pmod{f}$ ima rješenja. Vrijednosti x, z određujemo razvojem rješenja kvadratne jednadžbe

$$-\frac{cs^2 + bs + a}{f}t^2 + (2cs + b)t - cf = 0$$

u verižni razlomak. Naposlijetku, u mogućnosti smo odrediti i vrijednost y. Ako jednadžbe

$$y = sx - fz, \quad -\frac{cs^2 + bs + a}{f}x^2 + (2cs + b)xz - cfz^2 = 1$$

nemaju rješenja za $\text{nzd}(a, b, f) > 1$ i $\text{nzd}(b, c, f) > 1$, tada je nužno koristiti drugačije pristupe. Više o određivanju rješenja diofantskih jednadžbi može se naći na internetskoj stranici [1] koja je ujedno i kalkulator rješenja diofantskih jednadžbi drugog stupnja.

Prva pellovska jednadžba koju promatramo je

$$19Y^2 - 15X^2 = -29924.$$

Prema (3.18) vrijedi

$$(a, b, c, d, e, f) = (-15, 0, 19, 0, 0, 29924).$$

Prvi korak u rješavanju zadane pellovske jednadžbe je odrediti najveći zajednički djelitelj svih koeficijenata jednadžbe ne uključujući i slobodni koeficijent te njime podijeliti polaznu diofantsku jednadžbu. S obzirom da je $\text{nzd}(-15, 0, 19, 0, 0) = 1$, polazna diofantska jednadžba ostaje nepromijenjena.

Budući da vrijedi nejednakost $4f^2 \geq b^2 - 4ac$, rješenje tražimo koristeći supstituciju $x = sy - fz$.

Neka je $x = sy - fz$. Tada je

$$-\frac{(as^2 + bs + c)}{f}y^2 + (2as + b)yz - afz^2 = 1. \tag{3.19}$$

Dakle, $-15s^2 + 19$ je višekratnik broja 29924, što vrijedi za $s \equiv 5751, 9211, 20713, 24173 \pmod{29924}$.

- Neka je $s = 5751$.

Uvrštavajući s u (3.19), dobivamo

$$16579y^2 - 172530yz + 448860z^2 = 1. \tag{3.20}$$

Određujemo razvoj u verižni razlomak rješenja jednadžbe

$$16579t^2 - 172530t + 448860 = 0.$$

Rješenja dobivene jednadžbe su

$$t_1 = \frac{\sqrt{1140} + 172530}{33158}, \quad t_2\frac{\sqrt{1140} + 172530}{33158}.$$

Za rješenje t_1 dobivamo razvoj u verižni razlomak

$$\frac{\sqrt{1140} + 172530}{33158} = [5; 4, 1, 8, 1, 1, \overline{7, 1, 32, 1, 7, 2}],$$

gdje je duljina perioda $l = 6$.

Konvergente razvoja broja t_1 u verižni razlomak su

$$\left\{5, \frac{21}{4}, \frac{26}{5}, \frac{229}{44}, \frac{255}{49}, \frac{484}{93}, \frac{3643}{700}, \frac{4127}{793}, \frac{135707}{26076}, \frac{139834}{26869}, \frac{1114545}{214159}\right\}.$$

Neka je $\frac{y}{z}$ konvergenta razvoja u verižni razlomak broja $\frac{\sqrt{1140}+172530}{33158}$. Budući je duljina perioda razvoja u verižni razlomak $l = 6$ paran broj, promatramo konvergente do kraja prvog perioda. Svaku konvergentu uvrštavamo u jednadžbu (3.20) i provjeravamo vrijedi li jednakost. U slučaju da među konvergentama razvoja u verižni razlomak ne postoji rješenje jednadžbe, zaključujemo da polazna pellovska jednadžba nema rješenja.

Ako postoji konvergenta $\frac{y}{z}$ koja zadovoljava jednadžbu (3.20) označimo s $y = Y_0, \ z = Z_0$.

U našem slučaju vrijedi $Y_0 = 4127, Z_0 = 793$ pa iz jednakosti $X_0 = 5751Y_0 - 29924Z_0$ izračunavamo X_0. Rješenja početne diofantske jednadžbe su

$$(X_0, Y_0) = (4645, 4127), (-4645, -4127).$$

Promatramo i drugo rješenje t_2 jednadžbe (3.20). Iz konvergenti razvoja broja t_2 u verižni razlomak analognim postupkom dobivamo $Y_0 = -463, Z_0 = -89$ te iz $X_0 = 5751Y_0 - 29924Z_0$ možemo odrediti broj X_0. Vrijedi

$$(X_0, Y_0) = (523, -463), (-523, 463).$$

- Za $s = 9211$ dobivamo još neka rješenja zadane pellovske jednadžbe

$$(X_0, Y_0) = (47, 13), (-47, -13), (78689, -69917), (-78689, 69917).$$

- Za $s = 20713$ rješenja su

$$(X_0, Y_0) = (-47, 13), (47, -13), (78689, 69917), (-78689, -69917).$$

- Za $s = 24173$ dobivamo

$$(X_0, Y_0) = (47, 13), (-47, -13), (78689, -69917), (-78689, 69917).$$

Budući $4|29924$, rješenja početne jednadžbe bit će i dvostruka rješenja jednadžbe

$$15u^2 + 19v^2 + 7481 = 0.$$

Tako dobivamo i rješenja:

$$(X_0, Y_0) = (8844, 7858), (-8844, -7858), (-8844, 7858), (8844, -7858), (276, -242),$$

$$(-276, 242), (276, 242), (-276, -242).$$

Beskonačno mnogo rješenja pellovske jednadžbe dobivamo putem jednakosti

$$X_{n+1} = PX_n + QY_n, \;\; Y_{n+1} = RX_n + SY_n,$$

gdje vrijednosti P, Q, R, S određujemo na sljedeći način. Vrijedi

$$P = m, \;\; Q = -Cn, \;\; R = An, \;\; S = m + Bn,$$

gdje je (m, n) fundamentalno rješenje jednadžbe

$$m^2 + bmn + acn^2 = 1.$$

U našem slučaju vrijedi $m^2 - 285n^2 = 1$ pa je fundamentalno rješenje Pellove jednadžbe $(m, n) = (2431, 144)$. Tada je

$$P = 2431, \;\; Q = -2736, \;\; R = -2160, \;\; S = 2431,$$

pa sva ostala rješenja možemo odrediti pomoću već određenih rješenja i konstanti P, Q, R, S.

Fundamentalna rješenja prve pellovske jednadžbe su

$$(X_0, Y_0) = (\pm 47, 13), \ \ (\pm 276, 242), \ \ (\pm 523, 463).$$

Za fundamentalno rješenje $(X_0, Y_0) = (47, 13)$ koristeći vrijednosti P, R, S, Q dobivamo $(X_1, Y_1) = (78689, -69917)$. Sva rješenja pellovske jednadžbe mogu se dobiti iz rekurzivnih relacija

$$X_{n+1} = 4862 \cdot X_n - X_{n-1}, \ \ Y_{n+1} = 4862 \cdot Y_n - Y_{n-1}, \ \ n \geq 2.$$

Pretpostavimo da su X, Y definirani s (3.11) i (3.12). Lako možemo utvrditi da iz (3.11) i (3.12) za brojeve X, Y vrijede sljedeće kongruencije

$$X \equiv 0 \pmod 4, \ \ X \equiv 1 \pmod 3, \ \ X \equiv 4 \pmod 5, \ \text{odnosno} \ X \equiv 4 \pmod{60},$$

te X možemo prikazati kao $X = 60x + 4, \ \ x \in \mathbb{Z}$.

Za Y vrijedi

$$Y \equiv 2 \pmod 4, \ \ Y \equiv 1 \pmod 3, \ \ Y \equiv 3 \pmod 5,$$

odnosno vrijedi $Y \equiv 58 \pmod{60}$. Uvrštavanjem $X = 60x + 4$ u polaznu pellovsku jednadžbu dobivamo

$$19Y^2 - 15(60x + 4)^2 = -29924,$$

$$19Y^2 - 54000x^2 - 7200x + 29684 = 0.$$

Budući je $\text{nzd}(-54000, 0, 19, -7200, 0) = 1$, promatranu pellovsku jednadžbu ne možemo podijeliti djeliteljem većim od 1, te je promatramo upravo kako je i zadana. Određujemo djelitelje brojeva 19, 54000 te provjeravamo postoje li rješenja polazne jednadžbe $\pmod{19}$, $\pmod 9$, $\pmod{16}$, $\pmod{25}$. Budući rješenja tih jednadžbi postoje, postupak rješavanja pellovske jednadžbe se nastavlja. Nastojimo supstitucijama dobiti oblik

$$x'^2 + By^2 + Cy + D = 0.$$

Za $x' = -108000x - 7200$, $y' = -y$ vrijedi

$$-x'^2 + 414000y'^2 + 6463584000 = 0.$$

Određujemo razvoj u verižni razlomak rješenja jednadžbi $t^2 - 1026000 = 0$ i $-t^2 + 4104000 = 0$. Definiramo $x' = sy' - fz'$ i u mogućnosti smo zaključiti da bi broj $-s^2 + 4104000$ trebao biti višekratnik broja 6463584000. Za tako odabrane brojeve s dobivamo pellovsku jednadžbu oblika

$$\frac{-as^2 + bs + c}{f'} y'^2 + (2as + b)y'z - af'z^2 = 1$$

te nalazimo razvoje u verižne razlomke rješenja kvadratne jednadžbe

$$\frac{-as^2+bs+c}{f'}t^2-(2as+b)t+c=1.$$

Za sve definirane vrijednosti broja s vrijedi da, ili među konvergentama razvoja u verižni razlomak ne postoje rješenja jednadžbe, ili broj X_0 određen pomoću brojeva Y_0, Z_0 nije cijeli broj. Zaključujemo da početna jednadžba nema rješenja.

Zadana je i pellovska jednadžba

$$79Y^2-75X^2=-149684.$$

Za ovu pellovsku jednadžbu je vrlo lako odmah utvrditi da je nerješiva te za nju nije potrebno ni definirati kojim klasama ostataka pripadaju brojevi X, Y.

Određujemo $\text{nzd}(-75,0,79,0,0)=1$ pa zadana pellovska jednadžba ostaje nepromijenjena. Promatramo sve djelitelje brojeva $75, 79$ i utvrđujemo da polazna pellovska jednadžba modulo navedeni djelitelji ima rješenja. Uvodimo supstituciju oblika $x=sy-fz$. Zaključujemo da bi broj $-75s^2+79$ trebao biti višekratnik broja 149684, no to nije moguće. S obzirom da $4|149684$, rješenja polazne jednadžbe bi trebala biti dvostruko veća od rješenja jednadžbe

$$-75x^2+79y'^2=37421.$$

Analognim zaključivanjem utvrđujemo da bi broj $-75s^2+79$ trebao biti višekratnik broja 37421, no ni to nije moguće što znači da polazna pellovska jednadžba nema rješenja.

Pellovskoj jednadžbi

$$229Y^2-225X^2=-449084$$

na već opisani način možemo odrediti funadamentalna rješenja. Tako dobivamo

$$(X_0,Y_0)=(\pm 283,277),\ \ (\pm 404,398),\ \ (\pm 63837,63277).$$

Također, vrijedi

$$P=5848201,\ \ Q=-5899956,\ \ R=-5796900,\ \ S=5848201.$$

Znamo da vrijedi $Y=60y+58,\ \ y\in\mathbb{Z}$. Uvrštavanjem u zadanu jednadžbu dobivamo

$$229(60y+58)^2-225X^2=-449084,$$

$$824400y^2-225X^2+1593840y+1219440=0,$$

što je diofantska jednadžba koja nema rješenja. Za detaljniji postupak može se pogledati internetska stranica i kalkulator rješenja diofantskih jednadžbi [1].

Sljedeća pellovska jednadžba čija rješenja promatramo je

$$499Y^2 - 495X^2 = -988004.$$

Njena su fundamentalna rješenja

$$(X_0, Y_0) = (\pm 497, 493), \ \ (\pm 501, 497), \ \ (\pm 246508, 245518).$$

Uz sva navedena rješenja određujemo i konstante P, Q, R, S.

$$P = 61380991, \ \ Q = -61628496, \ \ R = -61134480, \ \ S = 61380991.$$

S obzirom da jednadžba može imati rješenja za $X \equiv 4 \pmod{60}$, $Y \equiv 58 \pmod{60}$, potrebno je odrediti dodatne uvjete za barem jednu od navedenih varijabli te nakon toga provjeriti je li dobivena jednadžba rješiva.
Znamo da vrijedi $Y = cy - c - 2y = c(y-1) - 2y \equiv -2 \pmod{(c-2)}$. U našem je slučaju $c - 2 = 495 = 3^2 \cdot 5 \cdot 11$, što povlači $Y \equiv -2 \pmod{3^2 \cdot 5 \cdot 11}$, a posebno i $Y \equiv -2 \pmod 9$, $Y \equiv -2 \pmod 5$, $Y \equiv -2 \pmod{11}$. U ranijim smo slučajevima odredili da vrijedi $Y \equiv 2 \pmod 4$. Također, možemo lako dobiti da je $Y = c(y-1) - 2y = 497(y-1) - 2y \equiv -2y \equiv 21, 28, 34, 61, 69 \pmod{71}$. Za svaki dobiveni ostatak pri dijeljenju brojem 71 dobivamo po jednu pellovsku jednadžbu koja nije rješiva.

Za

$$Y \equiv 2 \pmod 4, \ \ Y \equiv 7 \pmod{3^2}, \ \ Y \equiv 9 \pmod{11}, \ \ Y \equiv 21 \pmod{71},$$

vrijedi $Y \equiv 11878 \pmod{140580}$. Dobivamo jednadžbu

$$9861605463600y^2 - 495X^2 + 1666469621520y + 70403343120 = 0$$

koja nema rješenja.
Za

$$Y \equiv 2 \pmod 4, \ \ Y \equiv 7 \pmod{3^2}, \ \ Y \equiv 9 \pmod{11}, \ \ Y \equiv 28 \pmod{71},$$

vrijedi $Y \equiv 27718 \pmod{140580}$. Vrijedi

$$9861605463600y^2 - 495X^2 + 3888803247120y + 383376462480 = 0$$

koja nije rješiva.

Za slučaj kad je

$$Y \equiv 2 \pmod 4,\ Y \equiv 7 \pmod{3^2},\ Y \equiv 9 \pmod{11},\ Y \equiv 34 \pmod{71},$$

vrijedi $Y \equiv 61387 \pmod{140580}$. Definiramo $Y = 140580y + 61387,\ y \in \mathbb{Z}$. Uvrštavajući u polaznu jednadžbu dobivamo

$$9861605463600y^2 - 495X^2 + 8612524891080y + 1880414508735 = 0.$$

Ova pellovska jednadžba nema rješenja.

Za

$$Y \equiv 2 \pmod 4,\ Y \equiv 7 \pmod{3^2},\ Y \equiv 9 \pmod{11},\ Y \equiv 61 \pmod{71},$$

vrijedi $Y \equiv 1978 \pmod{140580}$. Vrijedi

$$9861605463600y^2 - 495X^2 + 277511105520y + 1953317520 = 0$$

što je pellovska jednadžba koja nema rješenja. Za

$$Y \equiv 2 \pmod 4,\ Y \equiv 7 \pmod{3^2},\ Y \equiv 9 \pmod{11},\ Y \equiv 69 \pmod{71},$$

vrijedi $Y \equiv 140578 \pmod{140580}$. Dobivamo jednadžbu

$$9861605463600y^2 - 495X^2 + 19722930329520y + 9861325855920 = 0$$

što je pellovska jednadžba bez rješenja.

Budući za sve klase ostataka modulo 71 koje su moguće za varijablu Y pripadne pellovske jednadžbe nemaju rješenja, možemo zaključiti da ni polazna pellovska jednadžba nije rješiva.

Sljedeća pellovska jednadžba je

$$649Y^2 - 645X^2 = -1287404.$$

Fundamentalna rješenja su joj

$$(X_0, Y_0) = (\pm 135, 127),\ (\pm 2461, 2453),\ (\pm 84884, 84622),$$

te su odgovarajuće konstante

$$P = 135419041,\ Q = -135838296,\ R = -135001080, S = 135419041.$$

U ovom slučaju dovoljno je promatrati $Y \equiv 58 \pmod{60}$. Uvrštavanjem $Y = 60y + 58$ u početni izraz, dobivamo pellovsku jednadžbu oblika

$$2336400y^2 - 645X^2 + 4517040y + 3470640 = 0$$

koja nema rješenja.

Fundamentalna rješenja iduće pellovske jednadžbe

$$859Y^2 - 855X^2 = -1706564,$$

su

$$(X_0, Y_0) = (\pm 107, 97), \ \ (\pm 4188, 4178), \ \ (\pm 87511, 87307)$$

te je lako odrediti

$$P = 314710111, \ \ Q = -315445416, \ \ R = -313976520, \ \ S = 314710111.$$

Budući znamo da vrijedi $X = 60x + 4$, uvrštavanjem u početnu pellovsku jednadžbu dobivamo

$$859Y^2 - 855(60x + 4)^2 = -1706564,$$

$$859Y^2 - 3078000x^2 - 410400x + 1692884 = 0.$$

Kao i u svim prethodnim slučajevima zaključujemo da ni ova pellovska jednadžba nije rješiva.

Za pellovsku jednadžbu

$$2539Y^2 - 2535X^2 = -5059844$$

dobivamo

$$(X_0, Y_0) = (\pm 173, 167), \ \ (\pm 7444, 7438), \ \ (\pm 431457, 431117).$$

Vrijedi

$$P = 8164530271, \ \ Q = -8170969176, \ \ R = -8158096440, \ \ S = 8164530271.$$

U ovom slučaju nije dovoljno promatrati X, Y i klase ostataka pri dijeljenju brojem 60 jer tako dobivane jednadžbe imaju rješenja, već moramo odrediti dodatne uvjete za Y.
Znamo da vrijedi $Y \equiv -2 \pmod{(c-2)}$. U našem slučaju je $Y \equiv -2 \pmod{2535}$, odnosno $Y \equiv -2 \pmod{3 \cdot 5 \cdot 11^2}$. Zaključujemo da je $Y \equiv 1 \pmod 3$, $Y \equiv 3 \pmod 5$, $Y \equiv 167 \pmod{169}$ te od ranije znamo $Y \equiv 2 \pmod 4$. Koristeći Kineski teorem o ostacima dobivamo da vrijedi $Y \equiv 10138 \pmod{10140}$, odnosno možemo pisati $Y = 10140y + 10138$.

Uvrštavanjem ovog izraza u polaznu jednadžbu, dobivamo:

$$2539(10140y + 10138)^2 - 2535X^2 = -5059844,$$

$$261058964400y^2 - 2535X^2 + 522014946960y + 260961052560 = 0,$$

te dobivamo pellovsku jednadžbu koja nema rješenja.

Pretposljednja pellovska jednadžba koju promatramo je

$$3109Y^2 - 3105X^2 = -6197564.$$

Njena su fundamentalna rješenja

$$(X_0, Y_0) = (\pm 625, 623), \ \ (\pm 2484, 2482), \ \ (\pm 1939391, 1938143).$$

Dobivamo

$$P = 14996628361, \ \ Q = -15006284916, \ \ R = -14986978020, \ \ S = 14996628361.$$

Uvrštavajući $X = 60x + 4$ u zadanu pellovsku jednadžbu, dobivamo

$$3109Y^2 - 11178000x^2 - 1490400x + 6147884 = 0.$$

Jednadžba nema rješenja.

Posljednja pellovska jednadžba koju promatramo je

$$4937Y^2 - 4935X^2 = -9850244.$$

Ta jednadžba nema rješenja.

Budući nijedna pellovska jednadžba oblika (3.13) koja je trebala dati brojeve $n = 2^\alpha 5^\beta$ koji zadovoljavaju kongruenciju (3.3) nema rješenja, zaključujemo da takvi brojevi ne postoje što dokazuje tvrdnju teorema.

□

U ovom smo poglavlju doktorskog rada problem određivanja svih prirodnih brojeva $n = 2^\alpha 5^\beta$ koji zadovoljavaju verziju Subbaraove kongruencije nakon supstitutcija i postupka "dijagonalizacije" uspjeli prikazati kao problem u kojem ispitujemo rješivost nekoliko pellovskih jednadžbi oblika

$$(c + 2)Y^2 - (c - 2)X^2 = -1996c + 4008,$$

za brojeve c koje smo algoritamski izračunali. U dokazu glavnog teorema ovog poglavlja

pokazali smo da nijedna dobivena pellovska jednadžba nije rješiva što ima za posljedicu i tvrdnju da ne postoje prirodni brojevi $n = 2^\alpha 5^\beta,\ \ a, b \in \mathbb{N}$ koji zadovoljavaju verziju Subbaraove kongruencije. Dakle, jedini prirodni brojevi oblika $n = 2^\alpha 5^\beta,\ \ a, b \in \mathbb{N}_0$ koji zadovoljavaju promatranu kongruenciju su brojevi $n = 1, 2, 5, 8$.

Bibliografija

[1] D. Alpern, Quadratic Diophantine equation solver, http://www.alpertron.com.ar

[2] M. Ayad and F. Luca, *Two divisors of* $(n^2+1)/2$ *summing up to* $n+1$, J. Théor. Nombres Bordeaux **19** (2007), 561–566.

[3] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367.

[4] Y. F. Bilu and R. F. Tichy, *The Diophantine Equation* $f(x) = g(y)$, Acta Arith. **95** (2000), 261–288.

[5] S. Bujačić, *Two divisors of* $(n^2+1)/2$ *summing up to* $\delta n+\varepsilon$*, for* δ *and* ε *even*, Miskolc Math. Notes, prihvaćeno za objavljivanje

[6] M. Diaz, *Two variations of Subbarao's Problem*, preprint 2010.

[7] R. Dietmann and C. Elsholtz (31. 08. 2010), *Euler and the Four-Squares Theorem (odgovor)*, MathOverflow.
http://mathoverflow.net/questions/37278/euler-and-the-four-squares-theorem
(posjećeno 15. 05. 2014.)

[8] A. Dujella, *Continued fractions and RSA with small secret exponents*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[9] A. Dujella and B. Jadrijević, *Solutions of a class of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.

[10] A. Dujella and F. Luca, *On the sum of two divisors of* $(n^2+1)/2$, Period. Math. Hungar. **65** (2012), 83–96.

[11] A. Dujella and F. Luca, *On a variation of a congruence of Subbarao*, J. Aust. Math. Soc. **93** (2012), 85–90.

[12] J. P. Escofier, Galois theory. Translated from the 1997 French original by Leila Schneps. Graduate Texts in Mathematics, 204. Springer-Verlag, New York, 2001.

[13] S. H. Hernández and F. Luca, *On the largest prime factor of* $(ab+1)(ac+1)(bc+1)$, Bol. Soc. Math. Mexicana **9** (2003), 235–244.

[14] G. Greaves, *On the representation of a number in the form* $x^2 + y^2 + p^2 + q^2$ *where* p, q *are odd primes*, Acta Arith. **29** (1976), 266-274.

[15] A. Grelak and A. Grytczuk, *On the Diophantine equation* $ax^2 - by^2 = c$, Publ. Math. Debrecen **44** (1994), 291–299.

[16] S. Lang, Algebra. Revisited third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[17] D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), 745–751.

[18] I. Niven, H. S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers. Fifth edition. Wiley, New York, 1991.

[19] The On-Line Encyclopedia of Integer Sequences (OEIS), `http://www.oeis.org`

[20] The PARI Group, PARI/GP version `2.7.0`, Bordeaux, 2014, `http://pari.math.u-bordeaux.fr/`

[21] K. Prachar, Primzahlverteilung. Springer-Verlag, Berlin, 1957.

[22] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208, Corrigendum, 5 (1959), 259.

[23] M. V. Subbarao, *On two congruences for primality*, Pacific J. Math. **54** (1974), 261–268.

[24] R. T. Worley, *Estimating* $|\alpha - \frac{p}{q}|$, J. Austral. Math. Soc. Ser. A **31** (1981), 202–206.

Sažetak

Ključne riječi: funkcija sume djelitelja; verižni razlomci; Pellova jednadžba; Legendreov simbol; Eulerova funkcija; Subbaraova kongruencija

Ayad i Luca su dokazali da ne postoji neparan prirodan broj $n > 1$ i dva pozitivna djelitelja d_1, d_2 od $(n^2+1)/2$ takvi da vrijedi $d_1 + d_2 = n + 1$. Dujella i Luca promatraju općenitiji problem, gdje je linearni polinom $n+1$ koji je suma djelitelja d_1 i d_2 zamijenjen proizvoljnim linearnim polinomom $\delta n + \varepsilon$, gdje su koeficijenti δ i ε cijeli brojevi i $\delta > 0$. Budući je broj $(n^2+1)/2$ neparan te brojevi d_1, d_2 dijele sumu kvadrata dva relativno prosta broja, za brojeve d_1, d_2 vrijedi $d_1, d_2 \equiv 1 \pmod 4$. Dujella i Luca su se fokusirali na slučaj u kojem su koeficijenti δ, ε linearnog polinoma neparni brojevi.

U ovom radu promatramo drugi slučaj, odnosno slučaj u kojem su koeficijenti linearnog polinoma parni brojevi. Preciznije, u jednom slučaju vrijedi

$$\delta \equiv 0 \pmod 4 \quad \text{i} \quad \varepsilon \equiv 2 \pmod 4,$$

a u drugom vrijedi

$$\delta \equiv 2 \pmod 4 \quad \text{i} \quad \varepsilon \equiv 0 \pmod 4.$$

U radu promatramo slučajeve kad je jedan od koeficijenata δ, ε fiksiran, odnosno u potpunosti rješavamo slučajeve $\delta = 2$, $\delta = 4$, $\varepsilon = 0$. Dokazujemo da za $\varepsilon \equiv 0 \pmod 4$ postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoji par djelitelja d_1, d_2 od $(n^2+1)/2$ takvih da vrijedi $d_1 + d_2 = 2n + \varepsilon$ te dokazujemo i analogan rezultat za slučaj kad je $\varepsilon \equiv 2 \pmod 4$ i djelitelji d_1, d_2 od $(n^2+1)/2$ takvi da vrijedi $d_1 + d_2 = 4n + \varepsilon$. U slučaju kad je vodeći koeficijent oblika $\delta = 4k+2$, $k \in \mathbb{N}$, dokazujemo da ne postoji neparan prirodan broj n sa svojstvom da postoji par pozitivnih djelitelja d_1, d_2 od $(n^2+1)/2$ takvih da je $d_1 + d_2 = \delta n$. S druge strane, dokazujemo i da postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoji par djelitelja d_1, d_2 od $(n^2+1)/2$ takvih da vrijedi $d_1 + d_2 = 2n$.

Nadalje, promatramo i slučaj u kojem jednoparametarske familije koeficijenata nisu fiksirane, ali su koeficijenti međusobno povezani. Dokazujemo da postoji beskonačno

mnogo neparnih prirodnih brojeva n za koje postoji par djelitelja d_1, d_2 od $(n^2+1)/2$ takvih da vrijedi $d_1 + d_2 = \delta n + (\delta + 2)$. Također promatramo i jednoparametarsku familiju koeficijenata za koju vrijedi $\varepsilon = \delta - 2$ i za nju dokazujemo analogan rezultat, odnosno da postoji beskonačno mnogo neparnih prirodnih brojeva n za koje postoji par djelitelja d_1, d_2 od $(n^2+1)/2$ takvih da vrijedi $d_1+d_2 = \delta n+(\delta-2)$, $\delta \equiv 4, 6 \pmod 8$.

U posljednjem poglavlju rada promatramo verziju Subbaraove kongruencije oblika

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)},$$

gdje je φ Eulerova, a σ funkcija sume djelitelja prirodnog broja n. Dujella i Luca su promatrali navedenu kongruenciju i dokazali da postoji samo konačno mnogo prirodnih brojeva n koji je zadovoljavaju i čiji su prosti faktori elementi konačnog i fiksiranog skupa. U radu ispitujemo koji prirodni brojevi čiji su prosti faktori elementi skupa $\{2, 5\}$, odnosno koji su oblika $n = 2^\alpha 5^\beta$, $\alpha, \beta \geq 0$, zadovoljavaju navedenu verziju Subbaraove kongruencije. Dokazano je da su jedini takvi prirodni brojevi n brojevi $n = 1, 2, 5, 8$.

Summary

Keywords: sum of divisors; continued fractions; Pell's equations; Legendre symbol; Euler's (Totient) function; Subbarao's congruence

Ayad and Luca have proved that there does not exist an odd integer $n > 1$ and two positive divisors d_1, d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = n+1$. Dujella and Luca have dealt with a more general issue, where $n+1$ was replaced with an arbitrary linear polynomial $\delta n + \varepsilon$, where $\delta > 0$ and ε are given integers. The reason that d_1 and d_2 are congruent to 1 modulo 4 comes from the fact that $(n^2+1)/2$ is odd and is a sum of two coprime squares $((n+1)/2)^2 + ((n-1)/2)^2$. Such numbers have the property that all their prime factors are congruent to 1 modulo 4. Since $d_1 + d_2 = \delta n + \varepsilon$, then there are two cases: it is either $\delta \equiv \varepsilon \equiv 1 \pmod 2$, or $\delta \equiv \varepsilon + 2 \equiv 0 \text{ or } 2 \pmod 4$. Dujella and Luca have focused on the first case.

We deal with the second case, the case where $\delta \equiv \varepsilon + 2 \equiv 0 \text{ or } 2 \pmod 4$. We completely solve cases when $\delta = 2, \delta = 4$ and $\varepsilon = 0$. We prove that there exist infinitely many positive odd integers n with the property that there exists a pair of positive divisors d_1, d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = 2n + \varepsilon$ for $\varepsilon \equiv 0 \pmod 4$ and we prove an analogous result for $\varepsilon \equiv 2 \pmod 4$ and divisors d_1, d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = 4n + \varepsilon$. In the case when $\delta \geq 6$ is a positive integer of the form $\delta = 4k+2, \ k \in \mathbb{N}$ we prove that there does not exist an odd integer n such that there exists a pair of divisors d_1, d_2 of $(n^2+1)/2$ with the property $d_1 + d_2 = \delta n$. We also prove that there exist infinitely many odd integers n with the property that there exists a pair of positive divisors d_1, d_2 of $(n^2+1)/2$ such that $d_1 + d_2 = 2n$.

The second part of the doctoral thesis deals with the similar problem or, more specifically, it deals with one-parametric families of coefficients $\delta, \ \varepsilon$. We prove that there exist infinitely many odd integers n with the property that there exists a pair of positive divisors d_1, d_2 of $(n^2+1)/2$ such that

$$d_1 + d_2 = \delta n + (\delta + 2).$$

We also prove that there exist infinitely many odd integers n with the property that there

exists a pair of positive divisors d_1, d_2 of $(n^2+1)/2$ such that

$$d_1 + d_2 = \delta n + (\delta - 2), \;\; \delta \equiv 4, 6 \pmod 8.$$

The third part of the doctoral thesis deals with the version of Subbarao's congruence, or, more precisely, with the congruence of the form

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)},$$

where $\varphi(n)$ is Euler's totient function and $\sigma(n)$ is sum of divisors of n. Dujella and Luca have proved that there exist only finitely many integers n whose prime factors belong to a fixed finite set and satisfy the congruence. We prove that the only integers of the form $n = 2^\alpha 5^\beta, \;\; \alpha, \beta \geq 0$, that satisfy that congruence are integers $n = 1, 2, 5, 8$.

Životopis

Sanda Bujačić je rođena u Beogradu, Srbija, 28. prosinca 1984. godine. Osnovnu školu pohađa u Opatiji, nakon čega upisuje opći smjer opatijske gimnazije Eugen Kumičić gdje maturira kao učenica generacije 2003. godine.

Dodiplomski studij matematike i informatike započela je akademske godine 2003./04. na Filozofskom fakultetu u Rijeci. Diplomirala je s radom naslova Ciklotomički polinomi 2008. godine.

Od prosinca 2008. godine je asistentica na Odjelu za matematiku Sveučilišta u Rijeci. U isto vrijeme upisuje i poslijediplomski doktorski studij matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu.

Član je Seminara za konačnu algebru i teoriju brojeva čiji su voditelji prof. dr. sc. Andrej Dujella i prof. dr. sc. Ivica Gusić. Sudjelovala je na ljetnoj školi "Four Faces of Number Theory", Wuerzburg, Njemačka, u kolovozu 2012. godine s posterom i na Arctic Number Theory Workshopu "Diophantine and Transcedental Methods", Saariselka, Finska u lipnju 2013. godine s usmenim izlaganjem. U srpnju 2014. godine jedan je od četiri pozvana predavača na ljetnoj školi "Diophantine Analysis" na kojoj održava seriju predavanja pod naslovom "Linearne forme u logaritmima". U kolovozu 2014. godine sudjeluje na konferenciji ELementare und Analytische Zalentheorie (ELAZ) s predavanjem kojim predstavlja dio svoje doktorske disertacije.

Na Odjelu za matematiku Sveučilišta u Rijeci vodi auditorne vježbe iz kolegija Računarski praktikum I, Elementarna matematika II, Matematika II, Uvod u teoriju brojeva, Uvod u numeričku matematiku.

Autor je članka "Two divisors of $(n^2+1)/2$ summing up to $\delta n + \varepsilon$ for δ and ε even" koji je prihvaćen za objavljivanje u časopisu Miskolc Mathematical Notes.