VILNIAUS UNIVERSITETAS

ALBERTAS ZINEVIČIUS

KREIVĖS VIRŠ SKAIČIŲ KŪNŲ IR JŲ SVEIKŲJŲ SKAIČIŲ ŽIEDŲ

Daktaro disertacijos santrauka

Fiziniai mokslai, matematika (01P)

Vilnius, 2013 metai

Disertacija parengta 2009 - 2013 metais Vilniaus universitete.

Mokslinis vadovas:

prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

Konsultantas:

doc. dr. Paulius Drungilas (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

Disertacija ginama Vilniaus universiteto matematikos mokslo krypties taryboje:

Pirmininkas:

prof. habil. dr. Antanas Laurinčikas (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

Nariai:

prof. dr. Roma Kačinskaitė (Šiaulių universitetas, fiziniai mokslai, matematika - 01P)

prof. dr. Aleksandras Krylovas (Mykolo Romerio universitetas, fiziniai mokslai, matematika - 01P)

prof. habil. dr. Eugenijus Manstavičius (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

doc. dr. Darius Šiaučiūnas (Šiaulių universitetas, fiziniai mokslai, matematika - 01P)

Oponentai:

prof. dr. Ramūnas Garunkštis (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

doc. dr. Renata Macaitienė (Šiaulių universitetas, fiziniai mokslai, matematika - 01P)

Disertacija bus ginama viešame Matematikos mokslo krypties tarybos posedyje 2013 m. spalio men. 25 d. 16 val. Vilniaus universiteto Matematikos ir informatikos fakultete.

Adresas: Naugarduko 24, LT-03225 Vilnius, Lietuva.

Disertacijos santrauka išsiuntinėta 2013 m. rugsėjo mėn.

Su disertacija galima susipažinti Vilniaus universiteto bibliotekoje.

VILNIUS UNIVERSITY

ALBERTAS ZINEVIČIUS

CURVES OVER NUMBER FIELDS AND THEIR RINGS OF INTEGERS

Summary of docotoral dissertation

Physical sciences, mathematics (01P)

Vilnius, 2013

The dissertation was prepared during years 2009 - 2013 at Vilnius University.

Scientific supervisor:

prof. habil. dr. Artūras Dubickas (Vilnius University, physical sciences, mathematics - 01P)

Scientific advisor:

doc. dr. Paulius Drungilas (Vilnius University, physical sciences, mathematics - 01P)

The council for the defence of the doctoral thesis:

Chairman:

prof. habil. dr. Antanas Laurinčikas (Vilnius University, physical sciences, mathematics - 01P)

Members:

prof. dr. Roma Kačinskaitė (Šiauliai University, physical sciences, mathematics - 01P)

prof. dr. Aleksandras Krylovas (University of Mykolas Romeris, physical sciences, mathematics - 01P)

prof. habil. dr. Eugenijus Manstavičius (Vilnius University, physical sciences, mathematics - 01P)

doc. dr. Darius Šiaučiūnas (Šiauliai University, physical sciences, mathematics - 01P)

Opponents:

prof. dr. Ramūnas Garunkštis (Vilnius University, physical sciences, mathematics - 01P)

doc. dr. Renata Macaitienė (Šiauliai University, physical sciences, mathematics - 01P)

The doctoral thesis will be defended at a public meeting of the council on October 25th, 2013 in Vilnius University, Department of Mathematics and Informatics, at 4 p.m.

Adress: Naugarduko 24, LT-03225 Vilnius, Lithuania.

The summary of the dissertation was distributed in September, 2013.

The dissertation is available at the library of Vilnius University.

Anotacija

Disertaciją sudaro darbai, autoriaus atlikti 2006-2013 metais. Šiuos darbus jungianti tema yra algebrinių kreivių, apibrėžtų virš racionaliųjų skaičių, šeimos, einančios per taškus, kurių koordinatės priklauso duotam skaičių kūnui ar jo sveikųjų skaičių žiedui. Pirmoje disertacijos dalyje yra gaunama vidutinio mažo aukščio racionaliųjų taškų kiekio ant fiksuoto žanro hiperelipsinių kreivių asimptotika. Antroje dalyje šis rezultatas išplečiamas, apibūdinant vidutinį homogeninių daugianarių reikšmių taškuose, kurių koordinatės yra mažo aukščio tarpusavyje pirminiai skaičiai, sutampančių su duoto vieno kintamojo daugianario reikšmėmis sveikuosiuose taškuose, skaičių. Trečioje dalyje sukonstruojamos nedidelės kreivių, apibrėžtų virš racionaliųjų skaičių ir išvengiančių taškų, kurių koordinatės priklauso duotam skaičių kūnui, šeimos. Ketvirtoje dalyje tyrinėjamos kongruenčių skaičių kreivės. Įrodoma, kad bent pusė pirminių skaičių p, kurie lieka inertiški cikliniame skaičių kūne K, atitinka kreives $16p^2 = x^4 - y^2$, kurios neturi netrivialių taškų su koordinatėmis to kūno sveikųjų skaičių žiede. Paskutinėje dalyje iliustruojamas Gauso sveikųjų skaičių skaidymosi daugikliais vienatinumo taikymas įrodant, kad konkreti hiperelipsinė kreivė neturi taškų su sveikosiomis koordinatėmis.

1 Įvadas

1.1 Mokslinė problema ir tyrimo objektas

Šio darbo tyrimo objektas yra algebrinės kreivės. Sprendžiama problema, ar tam tikro pavidalo kreivės eina per taškus su koordinatėmis, priklausančiomis fiksuotam skaičių kūnui arba jo sveikųjų skaičių žiedui, kaip dažnai tai atsitinka ir koks yra vidutinis mažo aukščio tokių taškų kiekis.

1.2 Tikslai ir uždaviniai

Pagrindiniai šio darbo uždaviniai - gauti asimptotinį įvertį mažo aukščio vidutiniam racionaliųjų taškų kiekiui ant hiperelipsinių kreivių bei šiek tiek bendresnio pavidalo lygčių, sukonstruoti kuo didesnes kreivių šeimas, išvengiančias taškų su koordinatėmis duotame skaičių kūne, tyrinėti kongruenčių skaičių kreives virš skaičių kūnų sveikųjų skaičių žiedų.

1.3 Aktualumas ir naujumas

Darbas *On the average number of rational points of bounded height on hyperelliptic curves* yra heuristinis M. Stoll hipotezės apie vidutinį racionaliųjų taškų skaičių ant hiperelipsinių kreivių argumentas, įrodantis ją mažo aukščio taškams. Paskutiniu metu dideli žingsniai link visos hipotezės įrodymo žengti M. Bhargava ir B. Gross, M. Bhargava ir A. Shankar, B. Poonen ir M. Stoll darbuose.

Darbe *How many integer homogeneous polynomials at small coprime integers have value of a univariate polynomial?* pagrindinis pirmojo darbo rezultatas išplečiamas šiek tiek bendresnio pavidalo lygtims.

Tolesniame skyriuje sukonstruojamos kreivės, neturinčios sprendinių virš pasirinkto skaičių kūno. Analogiškas klausimas elipsinėms kreivėms yra atsakinėjamas viename iš B. Mazur ir K. Rubin darbe įrodytų teiginių.

Skyriuje *On the congruent number curves* klasikinis kongruenčių skaičių uždavinys yra nagrinėjamas virš tam tikrų skaičių kūnų sveikųjų skaičių žiedų. Neseniai T. Jedrzejak darbe buvo įrodyta, kad, jei Birch ir Swinnerton-Dyer hipotezė yra teisinga, tuomet visos kongruenčių skaičių kreivės turi taškų, kurių koordinatės priklauso skaičių kūnui $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Čia įrodome, kad daug kongruenčių skaičių kreivių, kurių parametras yra pirminis skaičius, išvengs taškų, kurių koordinatės priklauso fiksuoto ciklinio skaičių kūno sveikųjų skaičių žiedui (išskyrus

trivialius taškus, tai yra, tuos, kurių pirmoji koordinatė lygi nuliui).

Paskutiniame skyriuje iliustruojamas Gauso sveikųjų skaičių skaidymosi daugikliais vienatinumo taikymas, įrodant, kad konkreti hiperelipsinė kreivė neturi taškų su sveikosiomis koordinatėmis.

Visi įrodinėjami teiginiai, išskyrus paskutiniojo skyriaus, kiek autoriui žinoma, yra nauji. Rezultatai yra publikuoti recenzuojamuose žurnaluose ir pristatyti mokslinėse konferencijose (žr. skyrius „Publikacijų sąrašas“ ir „Rezultatų aprobavimas“).

1.4 Tyrimų metodika

Pagal tyrimų tematiką disertaciją galima skirti į dvi dalis. Pirmuose dviejuose skyriuose ieškoma vidutinio mažo aukščio sprendinių skaičiaus ant aprėžto aukščio kreivių asimptotika. Likusiuose trijuose skyriuose įrodinėjama, kad tam tikros kreivės neturi sprendinių fiksuotame kūne ar žiede. Atitinkamai į dvi dalis galime skirti ir naudojamus metodus.

Idėja, kuria pagrįsta pirmoji dalis, yra geometrinė ir priklauso M. Stoll. Visos hiperelipsinės kreivės, einančios per duotą racionalųjį tašką, gali būti sutapatintos su pastumtos gardelės taškais. Skaičių geometrijos metodu galima įvertinti pastumtos gardelės taškų skaičių Euklidinės erdvės rutulyje to rutulio spindulio, gardelės fundamentalaus lygiagretainio tūrio bei šio lygiagretainio ilgiausios įstrižainės ilgio terminais. Kai rutulio spindulys yra pakankamai didelis palyginus su ilgiausios įstrižainės ilgiu, taip gaunamas įvertis yra pakankamai geras. Gardelės fundamentalaus lygiagretainio tūrį, reikalingą šiam įverčiui, galima išreikšti per racionaliojo taško pirmosios koordinatės skaitiklį ir vardiklį, pasinaudojus rekurentine formule trijstrižaininių matricų determinantams. Sumuojant gautuosius įverčius per visus duotos gardelės pastūmimus, gauname monotoninę sumą, kurią galima įvertinti integralu. Tankio konstantų sekos $\gamma(H)$ konvergavimas įrodomas pasinaudojus tinkama sumuojamų elementų perstata. Antrame pirmosios dalies darbe nagrinėjamos šiek tiek bendresnio pavidalo lygtys. Kad galėtume joms pritaikyti pirmo darbo metodus, įrodome papildomą lemą, skirtą aprėžti skirtumą tarp šiame ir pirmame darbe sutinkamų integralų per tam tikros funkcijos išvestinę.

Keli žinomi skaičių teorijos rezultatai naudojami antroje disertacijos dalyje. Įrodinėdami žanro $g = 4$ kreivės, neturinčios taškų duotame skaičių kūne, egzistavimą, pasiskoliname Faltings'o teoremą bei Hilberto neredukuojamumo teoremos apibendrinimą, įrodytą A. Schinzel. Įrodinėdami analogišką teiginį žanro $g = 0$ kreivėms, pasinaudojame Čebotariovo tankio teorema bei idealų skaidymosi pirminiais daugikliais vienatinumu skaičių kūnų sveikųjų skaičių žieduose. Teiginio apie kongruenčių skaičių kreives ciklinių plėtinių sveikųjų skaičių žieduose įrodyme, be pastarųjų dviejų rezultatų, dar naudojama Dirichlė teorema apie apverčiamų e-

lementų struktūrą skaičių kūnų sveikųjų skaičių žieduose. Be to, pasiskolinamos dvi neseniai įrodytos teoremos: B. Green ir T. Tao teorema apie pasirinkto ilgio aritmetinių progresijų, kurių elementai priklauso pirminių skaičių aibės teigiamo tankio poaibiui, egzistavimą, bei M. Jarden ir W. Narkiewicz teorema, tvirtinančia, kad baigtinai generuotose nulinės charakteristikos sveikumo srityse visos aritmetinės progresijos, kurių nariai yra fiksuoto skaičiaus apverčiamų elementų sumos, yra aprėžto ilgio. Paskutiniame skyriuje svarbų vaidmenį vaidina faktas, kad Gauso sveikieji skaičiai skaidosi į neredukuojamus daugiklius vieninteliu būdu.

1.5 Disertacijos struktūra

Disertacija parašyta anglų kalba. Ją sudaro anotacija, naudojamų žymėjimų paaiškinimai, įvadas, penki skyriai bei cituotos literatūros sąrašas. Disertacijos apimtis - 55 puslapiai.

2 Vidutinis mažo aukščio taškų ant hiperelipsinių kreivių kiekis

Tegu $g \geq 2$ būna sveikasis skaičius, o $n = 2g + 2$. Lygtis

$$y^2 = f_n x^n + f_{n-1} x^{n-1} + ... + f_0$$

su sveikaisiais koeficientais $f_n, f_{n-1}, ..., f_0$ ir nežinomaisiais x, y apibrėžia žanro g hiperelipsinę kreivę, jei daugianaris $f_n x^n + f_{n-1} x^{n-1} + ... + f_0$ neturi kartotinių šaknų ir bent vienas iš skaičių f_n, f_{n-1} yra nelygus nuliui. 1983 metais G. Faltings įrodė 1922 metais L. Mordell iškeltą hipotezę, teigiančią, kad hiperelipsinė kreivė gali eiti tik per baigtinį skaičių taškų, kurių abi koordinatės priklauso duotam baigtinio laipsnio racionaliųjų skaičių kūno plėtiniui. Vadinasi, galime klausti, kiek iš viso racionaliųjų taškų yra ant pasirinktos baigtinės aibės tokių kreivių ir kalbėti apie vidutinį racionaliųjų taškų skaičių. Galima tikėtis, kad surikiavus visas žanro g kreives pagal dydį, kurį čia apibrėžiame kaip vektoriaus $(f_n, f_{n-1}, ..., f_0)$ ilgį, vidutinis racionaliųjų taškų kiekis ant visų aprėžto dydžio kreivių artės į tam tikrą ribą, kai rėžį didinsime. Hipotezėje, iškeltoje M. Stoll, spėjama, kad ši riba turėtų būti nulis. Dar daugiau - kad egzistuoja konstanta γ, su kuria $\gamma/\sqrt{N}$ yra vidutinio skaičiaus racionaliųjų taškų ant kreivių, kurių dydis ne didesnis už N, asimptotika. Kita labai stipri hipotezė (angl. *Uniformity conjecture*) spėja, kad racionaliųjų taškų skaičius ant žanro g hiperelipsinės kreivės negali būti kiek norimai didelis. Spėjama, kad ir taškų, priklausančių kuriam nors baigtinio laipsnio racionaliųjų skaičių kūno plėtiniui, skaičius ant žanrdo g hiperelipsinės kreivės taip pat

negali būti kiek norimai didelis. Iš kitos pusės, yra žinoma, kad žanro $g = 2$ kreivė, apibrėžta lygtimi

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + \\ 567207969x^3 + 567207969x^2 - 985905640x + 247747600$$

turi ne mažiau nei 642 racionaliuosius taškus.

Racionaliojo skaičiaus, užrašyto nesuprastinama trupmena a/b, aukščiu vadinsime didesniąją iš reikšmių $|a|, |b|$. Galime nagrinėti vidutinį skaičių racionaliųjų taškų, kurių aukštis ne didesnis už H, ant kreivių, kurių dydis ne didesnis už N. Šiuo atveju galime įrodyti teiginį, analogišką iškeltąjai hipotezei:

2.1 TEOREMA. *Tegu H, N - natūralieji skaičiai, tenkinantys nelygybę $H\sqrt{2g+2} < N$. Tuomet vidutinis skaičius racionaliųjų taškų, kurių aukštis yra ne didesnis už H, įskaičiuojant taškų kartotinumą, ant visų žanro g hiperelipsinių kreivių, kurių dydis ne didesnis už N, yra lygus*

$$\gamma(H)/\sqrt{N} + O(N^{-3/2}H^3 + N^{-1}H^2),$$

čia $\gamma(H)$ - skaičius, nepriklausantis nuo N. Be to, $\gamma(H)$ konverguoja kai H neaprėžtai didėja.

Jei tikėsimės, kad didelio aukščio taškų ant kreivių turi būti „mažai“, ši teorema gali būti suprasta kaip heuristinis M. Stoll hipotezės argumentas. Neseniai (2013 m.) B. Poonen ir M. Stoll darbe *Chabauty's method proves that most odd degree hyperelliptic curves have only one rational point*, pasirėmus M. Bhargava ir B. Gross darbu, įrodoma, kad hiperelipsinių kreivių, atsirandančių iš nelyginio laipsnio daugianarių ir neturinčių (afiniųjų) racionaliųjų taškų, tankis tarp visų tokių kreivių artėja į vienetą, kai žanras didinamas, taip žengiant didelį žingsnį link visos hipotezės įrodymo. Naujausiame M. Stoll darbe įrodoma, kad jei hiperelipsinės kreivės Jakobio daugdaros K-racionaliųjų taškų grupės generatorių skaičius yra nedidelis, t.y., jei kreivės žanras yra ne mažesnis už 3, o generatorių skaičius bent 3 mažesnis už žanrą, tuomet ta kreivė turi ne daugiau negu $C(d, g)$ taškų bet kuriame skaičių kūne K, kurio laipsnis $[K : \mathbb{Q}]$ yra ne didesnis už d, čia $C(d, g)$ yra skaičius, priklausantis vien nuo g ir d.

3 Homogeninių daugianarių reikšmės taškuose, kurių koordinatės yra mažo aukščio tarpusavyje pirminiai skaičiai

Pirmasis rezultatas gali būti interpretuojamas kaip dviejų kintamųjų homogeninių daugianarių su sveikaisiais koeficientais, įgyjančių reikšmę, kuri yra sveikojo skaičiaus kvadratas, taške, kurio koordinatės yra mažo aukščio tarpusavyje pirminiai skaičiai, kiekio (įskaitant kartotinumus) asimptotika. Galima klausti, kaip ši asimptotika pasikeis, jei, užuot skaičiavę daugianarius, įgyjančius reikšmę, kuri yra sveikojo skaičiaus kvadratas, skaičiuosime daugianarius, įgyjančius vieną arba daugiau kurio nors kito fiksuoto vieno kintamojo daugianario reikšmių sveikuosiuose taškuose. Į šį klausimą atsakoma šia teorema:

1.2 TEOREMA. *Tegu n - bet koks natūralusis skaičius, H, N - natūralieji skaičiai, tenkinantys nelygybę $H\sqrt{n} < N$, o $p \in \mathbb{Z}[x]$ - fiksuotas laipsnio $m > 0$ daugianaris su sveikaisiais koeficientais. Tuomet skaičius trejetų $(a/b, c, f)$, kur a/b - racionalusis skaičius, užrašytas supaprastintąja trupmena, o skaičiai a, b yra absuliučiu didumu ne didesni už H, c - sveikasis skaičius, o f - dviejų kintamųjų homogeninis daugianaris su sveikaisiais koeficientais, kurio laipsnis ne didesnis už n, o dydis - ne didesnis už N, tenkinančių lygybę $p(c) = f(a, b)$, yra lygus*

$$\gamma_p(H)N^{n+1/m} + O(N^{n+1/m-1}H^3 + N^nH^2),$$

čia $\gamma_p(H)$ - skaičius, nepriklausantis nuo N.

Kai $n = 2g + 2$, o $p(x) = x^2$, iš šios teoremos nesunkiai gauname įrodytąją aukščiau: tereikia abi lygybės puses padalinti iš žanro g hiperelipsinių kreivių skaičiaus, kurių aukštis neviršija N, o tokių kreivių iš viso yra $\mathrm{vol}(B_1^{n+1})N^{n+1} + O(N^n)$. Jei $m > 1$ ir papildomai yra tenkinama nelygybė $n > 2m(m-1)$, tuomet $\gamma_p(H)$ konverguoja kai H neaprėžtai didėja. Jei neįskaičiuosime pavidalo $(0, c, f)$ trejetų, tuomet taip modifikuotų konstantų $\gamma_p(H)$ ribos, neaprėžtai didinant n reikšmę, sudarys konverguojančią į nulį seką. Taipogi galime matyti, kad kai $N >> H^{\max\{3,2m\}}, N \to \infty$, narys $\gamma_p(H)N^{n+1/m}$ yra teoremoje skaičiuojamo dydžio asimptotika. Pažymėsime, kad reikalavimas $N > H\sqrt{n}$ tiek šioje, tiek ir ankstesnėje teoremoje yra esminis, nes pirmoji įrodyme naudojama lema negali būti efektyviai taikoma gardelėms, turinčioms ilgą įstrižainę.

Teorema įrodinėjama analogiškai, kaip ir pirmoji, bet tam, kad galėtume pasinaudoti ankstesniu metodu, reikalinga papildoma lema, kuri ir sudaro šios darbo dalies pagrindą:

3.2 LEMA. *Tegu $p(\rho) = \rho^l + p_{l-1}\rho^{l-1} + ... + p_0 \in \mathbb{R}[\rho]$ - kintamojo ρ daugianaris su realiaisiais koeficientais, o $Vol_k(t, \rho) = \mathrm{vol}(B_t^{k+1}(0) \cap \{\boldsymbol{x} | \boldsymbol{x} \cdot e = \rho\})$ - sankirtos tarp $(k+1)$-mačio euklidinio*

rutulio, kurio spindulys lygus t, o centras koordinačių pradžioje, ir hiperplokštumos, kuri yra statmena vienetiniam vektoriui e atstumu ρ nuo koordinačių pradžios vektoriaus e kryptimi, k-matis tūris. Tuomet teisinga lygybė

$$\int_0^\infty \mathrm{Vol}_k(t, p(\rho))d\rho = \int_0^\infty \mathrm{Vol}_k(t, \rho^l)d\rho + O(t^k),$$

čia liekamojo nario $O(t^k)$ neišreikštąjai konstantai leidžiama priklausyti nuo k ir p, bet ne nuo t.

Lema leidžia daugiamačio rutulio pjūvių, išsidėsčiusių atstumais, atitinkančiais daugianario $p(\rho)$ reikšmes sveikuosiuose taškuose, bendrą tūrį įvertinti per pjūvių atstumais, kurie yra vienanario ρ^m reikšmės svekuosiuose taškuose, bendrą tūrį, taip supaprastinant įvertinimą iki jau gauto ankstesniame darbe.

Paminėsime ir lygiagrečiai gaunamą įrodytos teoremos variantą, kai imame $b = 1$:

3.3 TEOREMA. *Tegu n - bet koks natūralusis skaičius, H, N - natūralieji skaičiai, tenkinantys nelygybę $H\sqrt{n} < N$, o $p \in \mathbb{Z}[x]$ - fiksuotas laipsnio $m > 0$ daugianaris su sveikaisiais koeficientais. Tuomet skaičius trejetų (a, c, f), kur a - sveikasis skaičius, absoliučiu didumu ne didesnis už H, c - sveikasis skaičius, o f - vieno kintamojo daugianaris su sveikaisiais koeficientais, kurio laipsnis ne didesnis už n, o dydis - ne didesnis už N, tenkinančių lygybę $p(c) = f(a)$, yra lygus*

$$\gamma_p(H)N^{n+1/m} + O(N^{n+1/m-1}H^2 + N^nH),$$

čia $\gamma_p''(H)$ - skaičius, nepriklausantis nuo N.

4 Kreivės, išvengiančios taškų, kurių koordinatės priklauso duotam skaičių kūnui

Galima tikėtis, kad tiek aukščiau įrodytų teoremų, tiek ir Stoll hipotezės analogai turėtų galioti ir baigtinio laipsnio racionaliųjų skaičių kūno plėtiniams. Vis dėlto pirmiau susiduriame su elementaresniu klausimu: ar kiekvienam skaičių kūnui K egzistuoja kreivė su racionaliaisiais koeficientais, neinantį per nė vieną tašką, kurio koordinatės būtų to skaičių kūno elementai? Jei taip, kaip sukonstruoti kuo daugiau tokių krevių?

Vienas būdas įrodyti, kad egzistuoja daug kreivių, išvengiančių aibės $K \times K$ taškų - pasinaudoti dviem gerai žinomomis teoremomis. Pagal aukščiau minėtą Faltings'o teoremą, lygtis

$y^2 = x^5 + 1$ turi tik baigtinį skaičių sprendinių kūne K. Pažymėkime $p_\alpha(x)$ bet kurio tokio sprendinio x-koordinatės α minimalųjį daugianarį virš racionaliųjų skaičių. Galime įrodyti, kad daugianaris $p_\alpha(x^d+y)$ yra neredukuojamas žiede $\mathbb{Q}[x, y]$ su visomis natūraliosioms d reikšmėmis. Imkime $d > [K : \mathbb{Q}]$. Pagal Hilberto neredukuojamumo teoremą, egzistuoja toks natūralusis n_K, su kuriuo visi daugianariai $p_\alpha(x^d+n_K)$ yra neredukuojami virš racionaliųjų skaičių. Tuomet kreivė

$$y^2 = (x^d + n_K)^5 + 1$$

išvengs aibės $K \times K$ taškų.

Matome, kad tokios kreivės žanras priklauso nuo plėtinio $K/\mathbb{Q}$ laipsnio. Galime to išvengti, pasinaudoję ta pačia konstrukcija bei šiek tiek benresniu Hilberto neredukuojamumo teoremos variantu, įrodytu A. Schinzel, ir įrodyti, kad

4.1 TEOREMA. *Egzistuoja be galo daug žanro $g = 4$ kreivų su racionaliaisiais koeficientais, išvengiančių aibės $K \times K$ taškų.*

Galima ir šiek tiek paprastesnė tokių kreivių konstrukcija. Iš Čebotariovo tankio teoremos žinome, kad pirminių skaičių, kurie visiškai suskyla Galua plėtinyje K, tankis pirminių skaičių aibėje yra lygus $1/[K : \mathbb{Q}]$. Galime įrodyti, kad jei p yra visiškai suskylantis pirmins skaičius, o sveikasis skaičius a nėra kvadratinė liekana moduliu p, tuomet lygtis

$$y^2 = px^2 + az^2$$

kūno K sveikųjų skaičių žiede $\mathcal{O}_K$ turi vienintelį sprendinį $(x, y, z) = (0, 0, 0)$. Iš čia seka tokia teorema:

4.2 TEOREMA. *Tegu K - baigtinio laipsnio d Galua plėtinys. Tuomet pirminiai skaičiai p, su kuriais visos kreivės $y^2 = px^2 + a$ išvengia taškų su koordinatėmis kūne K, kai a yra sveikasis skaičius, kuris nėra kvadratinė liekana moduliu p, sudaro aibę, kurios apatinis tankis visų pirminių skaičių aibėje yra ne mažesnis už $1/[K : \mathbb{Q}]$.*

Iš šios teoremos galime padaryti tokią išvadą;

4.3 IŠVADA. *Egzistuoja be galo daug bet kurio žanro kreivių, apibrėžtų virš racionaliųjų skaičių kūno ir išvengiančių taškų, kurių koordinatės priklauso pasirinktam baigtinio laipsnio racionaliųjų skaičių plėtiniui K.*

Pridursime, kad šio skyriaus metodais negalime sukonstruoti daugianario $f(x) \in \mathbb{Z}[x]$, kurio

laipsnis būtų lygus 9 arba būtų lygus nelyginiam pirminiam skaičiui, o kreivė $y^2 = f(x)$ išvengtų taškų su koordinatėmis duotame skaičių kūne K.

5 Kongruenčių skaičių kreivės

Natūralusis skaičius n yra vadinamas kongruenčiu, jei egzistuoja statusis trikampis, kurio kraštinių ilgiai yra racionalūs skaičiai, o plotas yra lygus n. Klausimas, kurie natūralieji skaičiai yra kongruentūs minimas rašytiniuose šaltiniuose jau dešimtame amžiuje, bet iki šiol nėra iki galo išspręstas. P. Fermat įrodė, kad sveikųjų skaičių kvadratai nėra kongruentūs skaičiai. Šiuo metu žinoma daug kongruenčių ir nekongruenčių skaičių. Pavyzdžiui, visi pavidalo $8m + 5$ pirminiai skaičiai yra kongruentūs, o visi pavidalo $8m + 3$ pirminiai skaičiai - nekongruentūs.

Skaičius n yra kongruentus tuomet ir tik tuomet, kai lygčių sistema

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2n \end{cases} \tag{1}$$

turi sprendinį teigiamais racionaliaisiais skaičiais a, b, c. Ši lygčių sistema yra ekvivalenti sistemai

$$\begin{cases} c^2 - 4n = (a - b)^2 \\ c^2 + 4n = (a + b)^2. \end{cases}$$

Taigi, jei n yra kongruentus skaičius, tuomet kreivė

$$16n^2 = x^4 - y^2$$

turi racionalųjį tašką su nelygiomis nuliui koordinatėmis. Teisingas ir atvirkščias teiginys: jei ši kreivė turi racionalųjį tašką su nelygiomis nuliui koordinatėmis, tuomet n yra kongruentus skačius. Tokio pavidalo kreives vadinsime kongruenčių skaičių kreivėmis.

Kongruentaus skaičiaus sąvoką galima apibendrinti: jei k yra racionaliųjų skaičių kūno plėtinys, o $S \subset k$ - bet koks jo poaibis, sakysime, kad natūralusis skaičius n yra S-kongruentus, jei (1) lygtis turi sprendinį nelygiais nuliui skaičiais a, b, c, priklausančiais aibei S. Kai aibė S sudaro žiedą, tuomet jei n yra S-kongruentus skaičius, tai ir jį atitinkanti kreivė turi tašką su koordinatėmis aibėje S.

E. Girondo ir bendraautorių straipsnyje *Right triangles with algebraic sides and elliptic*

curves over number fields buvo iškeltas klausimas, ar egzistuoja toks baigtinio laipsnio racionaliųjų skaičių kūno plėtinys K, kad visi natūralieji skaičiai būtų K-kongruentūs. Nors žinoma, kad kreivė $16n^2 = x^4 - y^2$ neturi sprendinių racionaliųjų funkcijų kūne $\mathbb{C}(n)$, neseniai (2012 m.) T. Jedrzejak straipsnyje *Congruent numbers over real number fields* į šį klausimą buvo sąlyginai atsakyta teigiamai, parodant, kad jei teisinga yra silpna Birch ir Swinnerton-Dyer hipotezė kongruenčių skaičių kreivėms, tuomet visi natūralieji skaičiai yra $\mathbb{Q}(\sqrt{3}, \sqrt{5})$-kongruentūs.

Galime klausti, kurios kongruenčių skaičių kreivės turės taškų virš duoto racionaliųjų skaičių kūno plėtinio sveikųjų skaičių žiedo. Šiame darbe įrodome tokią teoremą kongruenčių skaičių kreivėms, atitinkančioms pirminius skaičius:

5.1 TEOREMA. *Tegu K - ciklinis racionaliųjų skaičių kūno plėtinys. Tuomet pirminiai skaičiai p, su kuriais kreivė $16p^2 = x^4 - y^2$ neturi sprendinių skaičių kūno K sveikųjų skaičių žiede $\mathcal{O}_K$ su nelygia nuliui x koordinate, sudaro bet pusę (asmptotine prasme) visų inertiškų kūne K pirminių skaičių.*

Pažymėkime ciklinio plėtinio $K/\mathbb{Q}$ laipsnį d. Iš įrodytos teoremos išplaukia, kad

5.2 IŠVADA. *Pirminiai skaičiai, kurie nėra $\mathcal{O}_K$-kongruentūs, turi ne mažesnį už $\varphi(d)/(2d)$ apatinį tankį pirminių skaičių aibėje (čia φ - Oilerio funkcija).*

5.3 PAVYZDYS. *Daugianaris $f(x) = x^3 - 3x + 1$ yra neredukuojamas žiede $\mathbb{Q}[x]$. Be to, jo diskriminantas yra racionaliojo skaičiaus kvadratas, todėl šio daugianario skaidymosi kūno laipsnis lygus trim, taigi, yra ciklinis racionaliųjų skaičių kūno plėtinys. Tegu $\alpha = 2\cos(2\pi/9)$ būna daugianario $f(x)$ šaknis. Iš teoremos išplaukia, kad pirminiai skaičiai, kurie nėra $\mathbb{Z}[\alpha]$-kongruentūs, sudaro aibę, kurios apatinis tankis visų pirminių skaičių aibėje yra ne mažesnis už $1/3$.*

Teoremos įrodymui pasiskoliname du teiginius, kuriuos suformuluosime čia kaip lemas. Pirmoji yra B. Green ir T. Tao teorema.

5.4 LEMA. *Tegu A - pirminių skaičių poaibis, turintis teigiama apatinį tankį pirminių skaičių aibėje. Tuomet aibėje A yra be galo daug bet kurio (baigtinio) ilgio aritmetinių progresijų.*

Antroji yra teorema, įrodyta M. Jarden ir W. Narkiewicz.

5.5 LEMA. *Jei R yra baigtinai generuota nulinės charakteristikos sveikumo sritis, o l - natūralusis skaičius, tuomet egzistuoja tokia konstanta $A_l(R)$, kad kiekvienoje aritmetinėje progresijoje iš žiedo R elementų, turinčioje daugiau nei $A_l(R)$ narių, bus bent vienas narys, kurio negalima užrašyti l šio žiedo apverčiamų elementų suma.*

Greta šių teiginių įrodyme taip pat naudojama Dirichlė teorema apie multiplikatyviosios apverčiamų elementų grupės skaičių kūnų sveikųjų skaičių žieduose struktūrą, Čebotariovo tankio teorema, nusakanti pirminių idealų skaidymosi tipų skaičių kūnų sveikųjų skaičių žieduose dažnį bei idealų skaidymosi nebesiskaidančiais dalikliais vienatinumas.

Teoremos įrodymas suskyla į du atvejus. Pirmuoju atveju pradinė lygtis suvedama į lygčių sistemą

$$\begin{cases} x^2 - y = pr \\ x^2 + y = 16p/r \end{cases}$$

su nežinomaisiais $x, y, r \in \mathcal{O}_K$ bei sąlyga, kad r dalija 16. Imdami patį didžiausią kūno K pokūnį K', kurio, kaip racionaliųjų skaičių kūno plėtinio, laipsnis yra nelyginis, pastebime, kad prijungę prie K' kompleksinį skaičių $\sqrt{-1}$, vėl gausime ciklinį plėtinį. Iš Čebotariovo teoremos galime išvesti, kad šiame pletinyje inertiškais liks pusė (asimptotine prasme) pirminių skaičių, kurie yra inertiški pradiniame plėtinyje K. Būtent šiems pirminiams (išskyrus $p = 2$) galime įrodyti, kad nagrinėjamoji lygtis negali turėti sprendinių su nelygia nuliui x reikšme.

Antruoju atveju pradinė lygtis suvedama į lygčių sistemą

$$\begin{cases} x^2 - y = 16p^2/r \\ x^2 + y = r. \end{cases}$$

Šiuo atveju prijungiame prie kūno K visus pavidalo $\sqrt{r}$ skaičius (čia $r \in \mathcal{O}_K$, kaip ir aukščiau, dalija 16). Dirichlė teorema leidžia padaryti išvadą, kad taip gautas plėtinys tebebus baigtinio laipsnio racionaliųjų skaičių kūno plėtinys. Šiame plėtinyje galime kairiąją išvestos lygties $2x^2r - 16p^2 = r^2$ pusę išskaidyti dauginamaisiais ir padaryti išvadą, kad $8p$ yra dviejų sveikųjų algebrinių skaičių, kurie yra 16^2 dalikliai, suma. Tuomet lemų pagalba nebesunku išvesti, kad tokių pirminių skaičių tankis pirminių skaičių aibėje turi būti lygus nuliui.

6 Lygčių $x^{2n+1} - y^2 = 4$ sveikieji sprendiniai ir Gauso sveikieji skaičiai

Paskutiniame disertacijos skyrelyje įrodome, kad hiperelipsinė kreivė $y^2 = x^5 - 4$ išvengia taškų su sveikosiomis koordinatėmis. Šis rezultatas yra žinomas, bet čia įrodomas kitu būdu, nei tai daroma žurnale „Mathematical Excalibur“ pateiktame sprendime: čia pasinaudojame Gauso sveikųjų skaičių skaidymosi daugikliais vienatinumu. Pats įrodymo būdas taip pat yra gerai

žinomas ir taikomas panašiems uždaviniams spręsti, kai duotosios lygties abi puses pavyksta išskaidyti į daugiau dauginamųjų kuriame nors racionaliųjų skaičių plėtinyje, kurio sveikųjų skaičių žiedas yra principinių idealų žiedas. Naudodamiesi ta pačia idėja įrodome ir truputį bendresnį teiginį:

6.1 TEOREMA. *Tegu n žymi neneigiamą sveikąjį skaičių. Tuomet lygtis $x^{2n+1} - y^2 = 4$ turi sveikąjį sprendinį (x, y) tada ir tik tada, kai lygtis $y + 2i = \pm(l + 2i)^{2n+1}$ turi sveikąjį sprendinį (y, l).*

Paskutinioji lygtis gali būti intepretuojama geometriškai per posūkio ir homotetijos transformacijas plokštumoje. Gali būti įdomu klausti, ar yra be galo daug natūraliųjų skaičių n, su kuriais ši lygtis turi sveikąjį sprendinį. Pasirodo, kad atsakymas į šį klausimą yra neigiamas: T. Nagell įrodė, kad lygtis neturi sveikųjų sprendinių kai $n \geq 2$. S. S. Pillai iškelta hipotezė spėja, kad, ir daug bendriau, bet kuris natūralusis skaičius gali tik baigtiniu skaičium būdų būti užrašytas kaip dviejų natūraliųjų skaičių laipsnių skirtumas.

7 Išvados

Šiame darbe

- radome vidutinio mažo aukščio racionaliųjų taškų ant hiperelipsinių kreivių kiekio asimptotiką. Šį rezultatą apibendrinome platesnei lygčių klasei.
- Sukonstravome nedideles kiekvieno žanro kreivių, išvengiančių taškų su koordinatėmis duotame skaičų kūne, šeimas.
- Įrodėme, kad bent pusė kongruenčių skaičių kreivių, atsirandančių iš pirminių skaičių, kurie yra inertiški duotame cikliniame skaičių kūne, neturi netrivialių taškų su koordinatėmis to kūno sveikųjų skaičių žiede.

8 Publikacijų sąrašas

- Zinevičius A., *On the average number of rational points of bounded height on hyperelliptic curves*, Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry **53**(1), 225-233 (2012),
- —, *How many integer homogeneous polynomials at small coprime integers have value of a univariate polynomial?*, Lithuanian Mathematical Journal **52**(4), 477-487 (2012),
- —, $x^5 - y^2 = 4$ *and Gaussian integers*, Šiauliai Mathematical Seminar **7**(15), 157-161 (2012),
- —, *A note on noncongruent numbers over rings of integers of cyclic number fields* (atiduota publikavimui).

9 Rezultatų aprobavimas

Pranešimai disertacijos temomis buvo perskaityti šiose konferencijose:

- *27th Journées Arithmétiques* konferencijoje, vykusioje 2011 m. birželio 27 d. - liepos 1 d. Vilniuje,
- *Elementare und Analytische Zahlentheorie* konferencijoje, vykusioje 2012 m. rugpjūčio 13 - 18 d. Schloss Schney (Vokietijoje),
- 54-ojoje Lietuvos matematikų draugijos konferencijoje, vykusioje 2013 m. birželio 19 - 20 d. Vilniuje,
- *28th Journées Arithmétiques* konferencijoje, vykusioje 2013 m. liepos 1 - 5 d. Grenoblyje (Prancūzijoje).

Pranešimai disertacijos temomis taip pat perskaityti Vilniaus universiteto Matematikos ir informatikos fakulteto Tikimybių teorijos ir skaičių teorijos katedroje.

10 Summary

This thesis is comprised of research work that the author pursued as a graduate student at the Department of Mathematics and Informatics of Vilnius University and as an undergraduate student at Jacobs University. The object of investigation is solvability of certain families of two-variable algebraic equations in rational numbers or algebraic numbers and, more restrictedly, rational or algebraic integers, as well as the number of solutions with restrictions on their heigth.

The thesis consists of an abstract, explication of used notation, introduction, five sections and bibliography. In the first section, average number of rational points of small height on hyperelliptic curves of fixed genus is described. It is shown that when only rational points of height that is small compared to the number of curves considered are counted, this average decreases proportionally to $1/\sqrt{N}$, where N is the bound on the size of the curves that are considered. Furthermore, the constant of proportionality is expressed explicitly and the error term is estimated. In the second section, a genaralization of this result is obtained to a wider class of equations. In the third section, some families of curves that do not have points in a given number field are constructed. In the fourth section, curves that arise from the congruent number problem are investigated. It is shown that, asymptotically, at least half of the curves that correspond to prime numbers that remain inert in a given cyclic extension of the field of rational numbers, do not have nontrivial points over the ring of integers of that extension. In the last section, integral solutions of a particular family of hyperelliptic curves are investigated.

11 Trumpos žinios apie autorių

Gimimo data ir vieta:

1985 m. vasario 13 d., Kaunas.

Išsilavinimas ir kvalifikacija:

1992-1995 m. - Kauno "Aušros" vidurinė mokykla.

1995-2001 m. - Kauno Petro Vileišio vidurinė mokykla.

2001-2004 m. - Kauno Technologijos universiteto Gimnazija.

2004-2007 m. - Jacobs University (Bremenas, Vokietija). Matematikos bakalauro kvalifikacinis laipsnis.

2007-2009 m. - Vilniaus universitetas, Matematikos ir informatikos fakultetas. Matematikos magistro kvalifikacinis laipsnis.

2009-2013 m. - Vilniaus universitetas, Matematikos ir informatikos fakultetas. Matematikos krypties doktorantūros studijos.

Darbo patirtis:

2006-2007 m. - Jacobs University (Bremenas, Vokietija), Matematikos fakultetas, asistentas.

2008 m. - UAB "Dora ir draugai", administratorius.

2009 m. - Nacionalinė moksleivių akademija, matematikos sekcijos mokytojas.

2012-2013 m. - Vilniaus universitetas, Matematikos ir informatikos fakultetas, asistentas.