VILNIUS UNIVERSITY

ALBERTAS ZINEVIČIUS

CURVES OVER NUMBER FIELDS AND THEIR RINGS OF INTEGERS

Docotoral dissertation

Physical sciences, mathematics (01P)

Vilnius, 2013

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

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

Scientific advisor: dr. Paulius Drungilas (Vilnius University, physical sciences, mathematics 01P)

VILNIAUS UNIVERSITETAS

ALBERTAS ZINEVIČIUS

KREIVĖS VIRŠ SKAIČIŲ KŪNŲ IR JŲ SVEIKŲJŲ SKAIČIŲ ŽIEDŲ

Daktaro disertacija

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: dr. Paulius Drungilas (Vilniaus universitetas, Fiziniai mokslai, matematika 01P)

Abstract

In this document, the author collected his work that ranges through the years 2006 – 2013. The common theme that occurs in its five separate parts is that of families of algebraic curves defined over the rational numbers with points over a number field or over its ring of integers. In the first part, average number of rational points of small height on hyperelliptic curves of fixed genus is described. In the second part, this result is extended to describing how often, on average, values of homogeneous polynomials at pairs of small coprime integers are values of a given univariate polynomial with integer coefficients. Further, small families of curves that are defined over the rational numbers and do not have points over a given number field are constructed. In the subsequent part, congruent number curves are investigated. It is shown that, given a cyclic number field K, at least half of the prime numbers p that remain inert in K correspond to curves $16p^2 = x^4 - y^2$ that do not have nontrivial points over the ring of integers of K. In the last part, a short exposition to a classical technique of showing that a particular curve does not have integral points is given.

Table of Contents

Chapter 1

Notation

$A \times B$ - the cartesian product of sets A and B

x, y, z, t - free variables

$\mathbb{Z}$ - the set of all integers

$\mathbb{Q}$ - the set of all rational numbers

K, L - number fields

$K/\mathbb{Q}, L/K$ - field extensions

$[L : K]$ - degree of the field extension L/K

$Gal(L/K)$ - the Galois group of a Galois field extension L/K

$K(t)$ - field extension of K that is generated by t

$\mathcal{O}_K$ - the set of all integral elements of a number field K

$\mathbb{P}^1(\mathbb{Q})$ - the projective line over the field of rational numbers

$\mathbb{R}$ - the set of all real numbers

$\mathbb{C}$ - the set of all complex numbers

i - the complex number $\sqrt{-1}$

$||v||$ - the L_2-norm of a vector v

$O(f)$ - the set of all functions g that are bounded by a constant multiple of f for all large enough arguments

φ - the Euler's totient function

Chapter 2

Introduction

In this document, the author collected his work that ranges through the years 2006-2013. The common theme that occurs in its separate parts is that of families of algebraic curves defined over the rational integers with points over a number field or over its ring of integers. In general, this theme is a very rich and may give rise to problems that can be very difficult. The ones that are adressed here are but very modest. We will try to describe below some of the general as well as more immediate context in which these questions occur.

2.1 Literature review

Given an irreducible polynomial $F(x, y) \in \mathbb{Z}[x, y]$ in two variables x, y, the equation $F(x, y) = 0$ defines an algebraic curve. The problem of determining all integral or all rational solutions to the equation is an instance of a Diophantine problem. In 1900, D. Hilbert raised the famous question that asked for an algorithm that would solve any specified Diophantine problem. 70 years later a proof was given that no such algorithm exists. Thus, in a sense, the question "How to solve Diophantine equations?" has no answer. If, however, one restricts the question to a subfamily of Diophantine problems, then such an algorithm may sometimes be expected. The answer to this question for Diophantine equations in two variables, i.e., curves, up to this point is not known. However, according to [27], "there are quite good reasons to believe that there should be a positive answer".

By viewing curves over the complex numbers, one obtains an important topological classi-

fication. When the curve $F(x, y) = 0$ is nonsingular and irreducible in $\mathbb{C}[x, y]$, its complex points have a natural structure of a Riemann surface in $\mathbb{C}^2$. The surface can be turned into a compact Riemann surface by adding at most two additional points. The natural invariant of this surface - its genus - is then also an invariant of the curve and, as it turns out, can be a basis to infer information about rational or integral points on it. First, while curves of genus zero have rational parametrizations (that is, there exist functions $x(t), y(t) \in \mathbb{C}(t)$ that satisfy $F(x(t), y(t)) = 0$), it is not very difficult to show that curves of genus one or larger do not. Secondly, Siegel's theorem tells that a curve of genus one or larger has at most finitely many points over the ring of integers of a number field. Due to the work of Baker, the height of these points can be bounded in terms of the coefficients of the defining equation. Further, the theorem of Faltings says that a curve of genus at least two has at most finitely many points over a number field.

While, given a number field K, the K-rational points on a curve of genus zero can be parametrized by rational functions, the structure of K-rational points on curves of positive genus is more difficult to see. For a curve of genus one defined by the equation

$$y^2 = ax^3 + bx^2 + cx + d,$$

one has a natural addition operation on it that is induced by mapping the sum of any three collinear points to the point at infinity. One can show that this gives the curve the structure of an abelian group. The theorem of Mordell-Weil tells that the subgroup of its K-rational points is finitely generated. Rational points of finite order can be determined due to the theorem of Nagell-Lutz. In this case, all possible subgroups of points of finite order are described by the theorem of Mazur. The theorem of Merel says that K-rational points of finite order have order no larger than d^{3d^2}, where $d = [K : \mathbb{Q}]$ is the degree of the field extension $K/\mathbb{Q}$. The rank of the group of K-rational points can be arbitrarily large when K varies. It is also conjectured that there exist curves with arbitrarily large rank when $K = \mathbb{Q}$.

When the equation that defines the curve is more general (for instance, when genus of the curve is larger than one), there need not be very obvious group structure. However, when the genus is positive, the complex points on a curve can be embedded to a variety J that is called the Jacobian of the curve and has a group structure. Analogously to the above, the K-rational points on J comprise a finitely generated subgroup, as the Mordell-Weil

theorem guarantees. Analogues of theorems of Mazur and Merel are not known in this generality.

Given a curve and a number field K, knowledge about K-rational points on it can be obtained by studying the curve modulo powers of a prime ideal of $\mathcal{O}_K$. Obviously, if the curve has no points over the respective local field, then it does not have points over K. The Hasse principle ensures that the converse for curves of genus zero is also true: if the curve has a point over each local field, then it has a point over K. However, this principle needs not hold for curves of higher genus: as is asserted in [24], for every number field K there exists a curve defined over K that violates the Hasse principle.

Aside from when a given curve does not have points in some p-adic field, other well-known obstructions from it having (K-)rational points is descent, that is known at least since Fermat's proof that perfect squares are not congruent numbers, and the Brauer-Manin obstruction.

2.2 Methods

The work can be loosely divided into two parts: the first one, that is comprised of the first two chapters, investigates the average number of solutions of bounded height. The second part is concerned with showing that certain curves do not have points in a fixed ring or a field. The employed methods can be grouped into two parts according to this division as well.

The central idea of the first part is geometric and belongs to author's former supervisor prof. Michael Stoll. The geometric structure of hyperelliptic curves that have a fixed rational point is that of a translated lattice. By the method of geometry of numbers, one can estimate the number of intersection points of a translated lattice with a ball in the Euclidean space in terms of radius of the ball, the covolume (determinant) of the lattice, the length of its longest diagonal and its distance from the origin. When the radius of the ball is large compared to the length of the diagonals of the lattice, one obtains a good estimate for the number of points. The covolume of the lattice that is needed for this estimation can be expressed in terms of the x-coordinate of the rational point by using the recurrence for the determinants of tridiagonal matrices. The summation over all translations of a fixed lattice then is approximated by an integral. The convergence of the density constants

$\gamma(H)$ is proved by exploiting a suitable summation order. In the second work of the first part, a more general setting is considered. In order to be able to apply the methods of the first work, an additional lemma that bounds the difference of two integrals in terms of a derivative of a certain function is proved.

In the statements of the second part, a number of known results are used. In the proof of the existence of a genus four curve defined over the rationals without points over a number field 9, borrowed are Faltings' theorem and Schinzel's genralization of Hilbert's irreducibility theorem. In the subsequent theorem that proves a similar result for curves of genus zero, the Chebotarev density theorem and the unique factorization of ideals in rings of integers of number fields are employed. In the proof of the statement about congruent number curves over rings of integers of odd degree cyclic number fields, in addition to the Chebotarev density theorem and unique factorization of ideals, also is used Dirichlet's unit theorem as well as two recent results: the theorem of Green and Tao on arithmetic progressions in prime numbers and a theorem of Jarden and Narkiewicz that asserts existence of many terms in arithmetic progressions that are not sums of units of a finitely generated integral domain of zero characteristic. In the last chapter, the fact that the ring of Gaussian integers is a unique factorization domain plays a role.

2.3 Actuality and Novelty

The work "On the average number of rational points of bounded height on hyperelliptic curves" is a heuristic of a conjecture of Stoll (Conjecture 1 in [28]). It demonstrates that points of small height on hyperelliptic curves are "few". By now, major advnacements in the direction of the conjecture have been made by [1], [2], [23].

The subsequent work "How many integer homogeneous polynomials at small coprime integers have value of a univariate polynomial?" investigates how the average number of solutions changes in a slightly more general setting than that in the preceeding work.

In the next chapter, constructed are some special curves defined over the rational numbers that have no points over a given number field K. An analogous question for elliptic curves defined over number fields has been adressed in Theorem 1.1 of [20].

Further, the classical congruent number problem is investigated over rings of integers of

some number fields. It has been recently demonstrated in [16] that, conditionally on the Birch and Swinnerton-Dyer conjecture, every congruent number curve has a point over the number field $\mathbb{Q}(\sqrt{3},\sqrt{5})$. Here, it is shown that there are many congruent number curves that do not have nontrivial points over the ring of integers of a cyclic number field.

In the last chapter, a short exposition to a classical technique of showing that a particular curve does not have integral points is given.

2.4 Results and conclusions

As a heuristic of the conjecture of Stoll (Conjecture 1 in [28]) that most hyperelliptic curves do not have points over the rational numbers, we prove the following about the average number of rational points of small height:

let $\#C_N$ denote the number of hyperelliptic curves of genus $(n-2)/2$ and size at most N, where the size of a hyperelliptic curve $y^2 = f_n x^n + f_{n-1}x^{n-1} + ... + f_0$ is defined to be $N(f) = \sqrt{f_n^2 + f_{n-1}^2 + ... + f_0^2}$ and denote by $\#R_N(H)$ the number of rational points of height at most H on them, counted with multiplicities. Then

Theorem 1. *For any natural numbers H, N such that $H\sqrt{n} < N$ holds*

$$\sqrt{N}\frac{\#R_N(H)}{\#C_N} = \gamma(H) + O(N^{-\frac{1}{2}}H^2 + N^{-1}H^3), \tag{2.1}$$

where $\gamma(H)$ does not depend on N.

Moreover, we show that $\gamma(H)$ converges when H tends to infinity. Subsequently, we extend this result to the following:

Theorem 2. *Let a polynomial p of degree $m > 0$ be fixed. Then for any natural numbers H, N such that $H\sqrt{n} < N$ holds*

$$\begin{aligned}\#\{(a/b \in \mathbb{Q}, c \in \mathbb{Z}, f)|\, \text{height}(a/b) \leq H, N(f) \leq N, p(c) = b^n f(a/b)\} \\ = \gamma_p(H)N^{n+1/m} + O(N^{n+1/m-1}H^3 + N^n H^2),\end{aligned}$$

where $\gamma_p(H)$ does not depend on N.

More generally, one may expect that most hyperelliptic curves do not have points over any number field. We construct curves that do not have points over a given number field in the next chapter. In particular, we show that

Theorem 3. *Given a Galois extension K of the field of rational numbers, of finite degree d, the lower density of prime numbers p such that for any $a \in \mathbb{Z}$ that is not a square modulo p, the curve $y^2 = px^2 + a$ has no points over K, is at least $1/d$ in the set of all prime numbers.*

Further, we investigate a family of curves that arises from the congruent number problem. Conditionally on the conjecture of Birch and Swinnerton-Dyer, all of these curves have points over the number field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. We show that many of them do not have nontrivial points over rings of integers of cyclic number fields. Namely,

Theorem 4. *Let K be a finite Galois extension of the field of rational numbers with cyclic Galois group. Then, asymptotically, at least half of the prime numbers p that are inert in K correspond to curves*

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

that do not have points over $\mathcal{O}_K$ with $x \neq 0$.

2.5 Approbation

The work that is presented in this thesis has appeared in the following papers:

- 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 manuscript *A note on noncongruent numbers over rings of integers of cyclic number fields* is submitted for publication.

The work was presented in the following conferences:

- "27th Journées Arithmétiques" conference that took place during June 27 - July 1 of 2011 in Vilnius,
- "Elementare und Analytische Zahlentheorie" conference that took place during August 13 - 18 of 2012 in Schloss Schney (Germany),
- "54th Lithuanian Mathematical Society Conference" that took place during June 19 - 20 of 2013 in Vilnius,
- "28th Journées Arithmétiques" conference that took place during July 1 - 5 of 2013 in Grenoble (France).

2.6 Acknowledgements

I am thankful to prof. A. Dubickas for the supervision and encouragement throughout my graduate studies. I am indebted to many people for sharing their mathematical interest and knowledge during this time, in particular, to A. Balčiūnas, Ž. Darbėnas, dr. P. Drungilas, prof. R. Garunkštis, dr. J. Jankauskas, prof. R. Kašuba, prof. H. Markšaitis, P. Šarka, G. Šemetulskis, R. Šimėnas, J. Šiurys. I would also like to express gratitude to my undergraduate supervisor prof. M. Stoll, on whose ideas the first chapter of this work is built, and to my former mathematics teachers E. Jočaitienė, D. Micienė and L. Narkevičius. I would like to thank Vilniaus universitetas (Vilnius University) for the resources that enabled this work, I.Mustata and my family - for their caring support.

Chapter 3

On the average number of rational points of bounded height on hyperelliptic curves

3.1 Introduction

Fix an integer $g \geq 2$. Let $n = 2g + 2$. Consider the equation

$$y^2 = f_n x^n + f_{n-1} x^{n-1} + ... + f_0 \tag{3.1}$$

with integral coefficients $f_n, ..., f_0$. For the above to define a hyperelliptic curve of genus g we must impose two restrictions on the polynomial $f(x) = f_n x^n + ... + f_0$, namely, at least one of the coefficients f_n, f_{n-1} must be nonzero (C1) and f cannot have multiple roots (C2). Rational points on a curve given by (3.1) correspond to solutions of

$$y^2 = z^n f(\frac{x}{z}) = f_n x^n + f_{n-1} x^{n-1} z + ... + f_0 z^n = F_f(x, z) \tag{3.2}$$

in integers y, x, z with x coprime to z. The theorem of Faltings [12], proved in 1983, yields that the number of rational points on any hyperelliptic curve is finite. This fact gives rise to questions about the cardinality of rational points on varying families of curves. The Uniformity Conjecture stated in the work of Caporaso, Harris and Mazur [3] predicts the

existence of a uniform bound on the number of rational points a curve of genus $g \geq 2$ may have. In another direction, there arises a question of how many rational points "on average" there are on hyperelliptic curves of fixed genus, which can be made precise in the following way:

given the L_2-norm

$$N(f) = \sqrt{f_n^2 + f_{n-1}^2 + ... + f_0^2}$$

on the set of polynomials of degree at most n, let

$$C_N = \{f \in \mathbb{Z}[x] \mid f \text{ satisfies (C1), (C2), } N(f) \leq N\}$$

be the set of those polynomials that we can identify with curves of genus g by writing $y^2 = f(x)$.

Let

$$R_N = \{(f, (a : b)) \in C_N \times \mathbb{P}^1(\mathbb{Q}) | F_f(a, b) = y^2 \text{ for some } y \in \mathbb{Z}\}$$

be the subset of $C_N \times \mathbb{P}^1(\mathbb{Q})$ that consists of curves with rational points, each curve being taken as many times as there are rational points with different x-coordinates on it (we will further refer by a "rational point" to the x-coordinate $(a : b)$ only). In question then is the behaviour of the ratio $\frac{\#R_N}{\#C_N}$ when N tends to infinity. Conjecture 1 given in the work of Stoll [28] states that this ratio should be asymptotically equivalent to $\frac{\gamma}{\sqrt{N}}$ for some constant $\gamma = \gamma(g)$.

In this note we estimate the average number of rational points of small height. More precisely,

define the *height* of a rational point $(a : b) \in \mathbb{P}^1(\mathbb{Q})$ as

$$H(a : b) = \max\{|a|, |b|\}.$$

Denote by $R_N(H)$ the subset of R_N consisting of curves that have a rational point $(a : b)$ of height $H(a : b) \leq H$, each curve taken with respective multiplicity. We look at the ratio $\frac{\#R_N(H)}{\#C_N}$ and, in what follows, prove that

Theorem 5. *For any H, N such that $H\sqrt{n} < N$ holds*

$$\sqrt{N}\frac{\#R_N(H)}{\#C_N} = \gamma(H) + O(N^{-\frac{1}{2}}H^2 + N^{-1}H^3), \tag{3.3}$$

where $\gamma(H)$ does not depend on N.

Consequently, we will obtain the following bound for the lower limit:

Theorem 6.

$$\liminf_{N\to\infty} \sqrt{N}\frac{\#R_N}{\#C_N} \geq \gamma, \tag{3.4}$$

where $\gamma = \lim_{H\to\infty} \gamma(H)$.

3.2 Counting C_N

Let us prove the following lemma that will reocurr throughout the estimations of this paper:

Lemma 1. *Let $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 + ... + \mathbb{Z}w_k \subset \mathbb{R}^k$ be a k-dimensional lattice generated by the vectors $w_1, ...w_k$. Then, for $N > \delta$, we have*

$$\frac{\mathrm{vol}(B^k_{N-\delta})}{\Delta} \leq \#(\Lambda \cap B^k_N) \leq \frac{\mathrm{vol}(B^k_{N+\delta})}{\Delta}$$

where B^k_R is the k-dimensional ball of radius R, Δ is covolume of the lattice and δ is half the length of the longest diagonal of the fundamental parallelotope of Λ.

Proof. Let

$$\Lambda' = \frac{1}{2}(w_1 + w_2 + ... + w_n) + \Lambda,$$

then Λ' is a translation of Λ, and each of the parallelotopes that Λ' partitions $\mathbb{R}^k$ into, has at its centre a point of Λ. Call a parallelotope P cut by Λ' *inner* if the point of Λ at the centre of P lies inside the ball B^k_N, and *outer* otherwise. Moreover, if P intersects the boundary of B^k_N, call P *inner boundary parallelotope* (*outer boundary parallelotope* respectively).

We claim that $B^k_{N-\delta}$ contains no interior point of any outer boundary parallelotope. Assume it contained such a point. Then, since that point is distanced from the centre of the parallelotope by a distance less than δ, increasing the radius of the ball by δ would also make the centre point of the parallelotope a point of B^k_N, contradicting the assumption

that it is an outer parallelotope. Therefore the volume of $B^k_{N-\delta}$ is bounded by the sum of volumes of inner parallelotopes, which leads to

$$\#(\Lambda \cap B^k_N) \geq \frac{\mathrm{vol}(B^k_{N-\delta})}{\Delta}.$$

In the same way we deduce that $B^k_{N+\delta}$ contains completely all inner boundary parallelotopes of B^k_N to get the second inequality. □

Now, due to the lemma, without restrictions (C1), (C2), the set of polynomials

$$P_N = \{f | f \text{ - polynomial of degree } \deg(f) \leq n, N(f) \leq N\}$$

satisfies

$$\mathrm{vol}(B^{n+1}_{N-\delta}) \leq \#P_N \leq \mathrm{vol}(B^{n+1}_{N+\delta}),$$

where $\delta = \frac{\sqrt{n+1}}{2}$ is half of the diagonal length of $n+1$-dimensional unit cube.

Let P'_N be the set of polynomials of degree $\deg(f) \leq n-2$ in P_N. In the same way we infer from Lemma 1 that

$$\#P'_N \leq \mathrm{vol}(B^{n-1}_{N+\sqrt{n-1}/2}).$$

Next, let

$$P''_N = \{f \in P_N | \mathrm{disc}(f) = 0\}$$

be the set of polynomials with zero discriminant. The following lemma will allow us to see that $\#P''_N = O(N^n)$:

Lemma 2. *Let $f(x_1, x_2, ...x_m) \in \mathbb{C}[x_1, x_2, ...x_m]$ be a polynomial of degree $d > 0$. Then the number of its integral zeroes in $[-N, N]^m$ does not exceed $md(2N+1)^{m-1}$.*

Proof. We proceed by induction on m:

when $m = 1$, f is a one variable polynomial, thus the number of its zeroes does not exceed d, which gives the inequality.

Assumed that the inequality is true for $m \leq k$, consider $m = k+1$. Fix x_{k+1} at any integer in $[-N, N]$. There are at most d values of x_{k+1} for which f turns into the zero polynomial (were there more, $f(x_1, x_2, ...x_m)$ had to be the zero polynomial itself). These values give

at most $d(2N+1)^k$ zeroes of f. The remaining values, by the inductive hypothesis, yield no more than $(2N+1)kd(2N+1)^{k-1}$ zeroes. Thus in total there are no more than

$$d(2N+1)^k + (2N+1)kd(2N+1)^{k-1} = (k+1)d(2N+1)^k$$

integral zeroes in the hypercube $[-N,N]^{k+1}$, which completes the inductive step. □

As $\mathrm{disc}(f)$ is a homogeneous polynomial of degree $d = 2n-2$ in $n+1$ variables $f_n, f_{n-1}, ...f_0$, Lemma 2 now guarantees that its zero set in the hypercube $[-N,N]^{n+1}$ is of order $O(N^n)$.

We can now estimate the size of C_N:

$$\mathrm{vol}(B^{n+1}_{N+\sqrt{n+1}/2}) \geq \#C_N \geq \#P_N - \#P'_N - \#P''_N \geq \mathrm{vol}(B^{n+1}_{N-\sqrt{n+1}/2}) - \mathrm{vol}(B^{n-1}_{N+\sqrt{n-1}/2}) - O(N^n)$$

and hence

$$\#C_N = \mathrm{vol}(B^{n+1}_N) + O(N^n) = N^{n+1}(\mathrm{vol}(B^{n+1}_1) + O(\frac{1}{N})). \tag{3.5}$$

3.3 Counting $R_N(H)$

Fix $(a:b) \in \mathbb{P}^1(\mathbb{Q})$. Set

$$P_N(a:b) = \{f \in P_N | f \text{ has } (a:b) \text{ as a rational point}\}.$$

The linear map $M : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}$ defined by $f \mapsto F_f(a:b)$ has n-dimensional kernel spanned by the vectors

$$\begin{aligned} v_1 &= (a, -b, 0, 0, ..., 0), \\ v_2 &= (0, a, -b, 0, ..., 0), \\ &\vdots \\ v_n &= (0, 0, ..., 0, a, -b). \end{aligned}$$

It is easy to see that $\ker(M_{|\mathbb{Z}^{n+1}})$ is the n-dimensional lattice

$$\Lambda(a:b) = \mathbb{Z}v_1 + \mathbb{Z}v_2 + ... + \mathbb{Z}v_n$$

(the inclusion $\ker(M_{|\mathbb{Z}^{n+1}}) \subset \Lambda(a:b)$ is immediate from the fact that $gcd(a,b) = 1$). More generally, the hyperplane

$$h_y(a:b) = \{f \in \mathbb{R}^{n+1} | F_f(a,b) = y^2\}$$

is a translation of $\ker(M)$ and its integral points have the same structure as $\Lambda(a:b)$.

Let $\Delta(a:b)$ denote the covolume of $\Lambda(a:b)$.

Claim 1. $\Delta(a:b) = \sqrt{a^{2n} + a^{2n-2}b^2 + ... + b^{2n}}$.

Proof. Let

$$A = \begin{pmatrix} a & -b & 0 & 0 & ... & 0 \\ 0 & a & -b & 0 & ... & 0 \\ & & & \vdots & & \\ 0 & 0 & ... & 0 & a & -b \end{pmatrix}.$$

The covolume of $\Lambda(a:b)$ is given by

$$\Delta(a:b) = \sqrt{\det(AA^T)} = \begin{vmatrix} a^2+b^2 & -ab & 0 & 0 & ... & 0 \\ -ab & a^2+b^2 & -ab & 0 & ... & 0 \\ 0 & -ab & a^2+b^2 & -ab & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & ... & 0 & -ab & a^2+b^2 & -ab \\ 0 & ... & ... & 0 & -ab & a^2+b^2 \end{vmatrix}^{\frac{1}{2}}.$$

By expanding the determinant with respect to the n-th row we get the recurrence relation

$$\det(T_n) = (a^2+b^2)\det(T_{n-1}) - a^2b^2\det(T_{n-2}),$$

where T_k is a $k \times k$ tridiagonal matrix of the same form. We leave it as an easy exercise for the reader to see inductively that $\det(T_k) = a^{2k} + a^{2k-2}b^2 + ... + b^{2k}$.

□

Now, by Lemma 1, for $N > \delta$ we have

$$\frac{\mathrm{vol}(h_y(a:b) \cap B^{n+1}_{N-\delta})}{\Delta(a:b)} \leq \#(P_N \cap h_y(a:b)) \leq \frac{\mathrm{vol}(h_y(a:b) \cap B^{n+1}_{N+\delta})}{\Delta(a:b)}.$$

Summing this over y gives

$$\frac{\sum_{y=0}^{\infty} \mathrm{vol}(h_y(a:b) \cap B^{n+1}_{N-\delta})}{\Delta(a:b)} \leq \#P_N(a:b) \leq \frac{\sum_{y=0}^{\infty} \mathrm{vol}(h_y(a:b) \cap B^{n+1}_{N+\delta})}{\Delta(a:b)}. \tag{3.6}$$

Here δ can be taken to be half the length of the longest diagonal of the paralellotope

$$F = \{t_1 v_1 + ... + t_n v_n | (t_1, ..., t_n) \in [0,1]^n\}.$$

Clearly, it is at most $\frac{\sqrt{a^2+(n-2)(|a|+|b|)^2+b^2}}{2} \leq \frac{H\sqrt{4n-6}}{2}$. We allow ourselves to set $\delta = \frac{H\sqrt{4n-6}}{2}$ uniformly for all $(a:b)$ with $H(a:b) \leq H$ and assume $N \geq H\sqrt{n}$ here and for the rest of our considerations in order for $N > \delta$ to hold.

Let $\mathbf{e} = \frac{1}{\Delta(a:b)}(a^n, a^{n-1}b, ...b^n)$ and let $v(\rho)$ denote the n-dimensional volume of the intersection of B^{n+1}_1 with the hyperplane $\{\mathbf{x} | \mathbf{e} \cdot \mathbf{x} = \rho^2\}$. Then

$$\mathrm{vol}(h_y(a:b) \cap B^{n+1}_t) = t^n v(\frac{y}{\sqrt{t\Delta(a:b)}})$$

and therefore

$$\frac{\sum_{y=0}^{\infty} \mathrm{vol}(h_y(a:b) \cap B^{n+1}_t)}{\Delta(a:b)} = \frac{t^n}{\Delta(a:b)} \sum_{y=0}^{\infty} v(\frac{y}{\sqrt{t\Delta(a:b)}}).$$

The last sum is monotonically decreasing. Therefore one can approximate it by an integral as follows:

$$\sum_{y=0}^{\infty} v(\frac{y}{\sqrt{t\Delta(a:b)}}) = \int_0^{\infty} v(\frac{\rho}{\sqrt{t\Delta(a:b)}})d\rho + O(1) = \sqrt{t\Delta(a:b)}\int_0^{\infty} v(\rho)d\rho + O(1).$$

Notice that $\int_0^{\infty} v(\rho)d\rho = \mathrm{vol}(B_1^{n+1})/2$. Hence we can write:

$$\frac{t^n}{\Delta(a:b)}\sum_{y=0}^{\infty} v(\frac{y}{\sqrt{t\Delta(a:b)}}) = t^{n+\frac{1}{2}}\,\mathrm{vol}(B_1^{n+1})\gamma(a:b) + O(\frac{t^n}{\Delta(a:b)}), \tag{3.7}$$

where $\gamma(a:b) := \frac{1}{2\sqrt{\Delta(a:b)}}$.

We now use the last equality to rewrite (3.6) into

$$\begin{aligned}(N-\delta)^{n+\frac{1}{2}}\,\mathrm{vol}(B_1^{n+1})\gamma(a:b) + O(\frac{(N-\delta)^n}{\Delta(a:b)}) &\le \#P_N(a:b)\\ &\le (N+\delta)^{n+\frac{1}{2}}\,\mathrm{vol}(B_1^{n+1})\gamma(a:b) + O(\frac{(N+\delta)^n}{\Delta(a:b)}).\end{aligned}$$

From this we deduce that

$$\#P_N(a:b) = N^{n+\frac{1}{2}}\,\mathrm{vol}(B_1^{n+1})\gamma(a:b) + O(N^{n-\frac{1}{2}}H + N^n).$$

By summing up the last equality over all points $(a:b)$ that satisfy $H(a:b) \le H$ we get

$$\begin{aligned}\#P_N(H) &= \sum_{H(a:b)\le H} \#P_N(a:b)\\ &= N^{n+\frac{1}{2}}\,\mathrm{vol}(B_1^{n+1}) \sum_{H(a:b)\le H} \gamma(a:b) + O(N^{n-\frac{1}{2}}H^3 + N^nH^2).\end{aligned} \tag{3.8}$$

Define $\gamma(H) := \sum_{H(a:b)\le H}\gamma(a:b)$, then

$$\#P_N(H) = N^{n+\frac{1}{2}}\,\mathrm{vol}(B_1^{n+1})\gamma(H) + O(N^{n-\frac{1}{2}}H^3 + N^nH^2). \tag{3.9}$$

From (3.5), we can see that the difference between $\#P_N(H)$ and $\#R_N(H)$ is bounded by $O(N^n H^2)$. That enables us to replace $P_N(H)$ by $R_N(H)$ in (3.9) to obtain

$$\#R_N(H) = N^{n+\frac{1}{2}} \operatorname{vol}(B_1^{n+1})\gamma(H) + O(N^{n-\frac{1}{2}}H^3 + N^n H^2). \tag{3.10}$$

3.4 Evaluation of the ratio

Proof of Theorem 1. From (3.5) and (3.10) we obtain

$$\begin{aligned}
\frac{\#R_N(H)}{\#C_N} &= \frac{\operatorname{vol}(B_1^{n+1})\gamma(H)}{\operatorname{vol}(B_1^{n+1}\sqrt{N}) + O(\frac{1}{\sqrt{N}})} + \frac{O(N^{n-\frac{1}{2}}H^3 + N^n H^2)}{N^{n+1}\operatorname{vol}(B_1^{n+1}) + O(N^n)} \\
&= \frac{\gamma(H)}{\sqrt{N}} + O(N^{-\frac{3}{2}}) + \frac{O(N^{n-\frac{1}{2}}H^3 + N^n H^2)}{N^{n+1}\operatorname{vol}(B_1^{n+1}) + O(N^n)} \\
&= \frac{\gamma(H)}{\sqrt{N}} + O(N^{-\frac{3}{2}}) + O(N^{-\frac{3}{2}}H^3 + N^{-1}H^2),
\end{aligned}$$

hence it follows that

$$\sqrt{N}\frac{\#R_N(H)}{\#C_N} = \gamma(H) + O(N^{-\frac{1}{2}}H^2 + N^{-1}H^3), \tag{3.11}$$

as claimed. □

Proof of Theorem 2. We first show that $\lim_{H\to\infty}\gamma(H) < \infty$:

$$\gamma(H) = \sum_{H(a:b)\le H}\gamma(a:b) = \frac{1}{2}\sum_{H(a:b)\le H}\frac{1}{\sqrt[4]{a^{2n} + a^{2n-2} + \ldots + b^{2n}}} < \frac{1}{2}\sum_{H(a:b)\le H}\frac{1}{\sqrt[4]{\max\{|a|^{2n}, |b|^{2n}\}}}.$$

To prove that the sum is bounded when H tends to infinity, we can allow ourselves to drop the condition that a is coprime to b, which leads to the following inequality:

$$\gamma(H) \leq \frac{1}{2} \sum_{(a,b):H(a:b)\leq H} \frac{1}{\max\{|a|^{\frac{n}{2}}, |b|^{\frac{n}{2}}\}} = \frac{1}{2} \sum_{m=1}^{H} \frac{8m}{m^{\frac{n}{2}}} = 4 \sum_{m=1}^{H} \frac{1}{m^g}.$$

Since $g \geq 2$, the last sum converges. This implies that the limit $\gamma := \lim_{H\to\infty} \gamma(H)$ is finite.

Now, let $H = N^{1/4-u}$, $\frac{1}{4} > u > 0$, then (3.11) turns into

$$\sqrt{N} \frac{\#R_N(H)}{\#C_N} = \gamma(H) + O(N^{-\frac{1}{4}-3u} + N^{-2u})$$

and the claim is immediate: pick any $\epsilon > 0$, then for $N > 0$ big enough both $O(N^{-1/4-3u} + N^{-2u}) < \frac{\epsilon}{2}$ and $\gamma - \gamma(N^{1/4-u}) < \frac{\epsilon}{2}$ hold simultaneously. Therefore

$$\liminf_{N\to\infty} \sqrt{N} \frac{\#R_N}{\#C_N} \geq \liminf_{N\to\infty} \sqrt{N} \frac{\#R_N(N^{1/4-u})}{\#C_N} > \gamma(N^{1/4-u}) - \frac{\epsilon}{2} > (\gamma - \frac{\epsilon}{2}) - \frac{\epsilon}{2} = \gamma - \epsilon,$$

which completes the proof. □

Chapter 4

How many integer homogeneous polynomials at small coprime integers have value of a univariate polynomial?

4.1 Introduction

Given a polynomial $f(x) \in \mathbb{Z}[x]$ with integer coefficients, an interesting and possibly very difficult question is to determine all rational values of x for which the value of the polynomial is a square of a rational number. If a/b (where $a \in \mathbb{Z}, b \in \mathbb{N}$ are coprime) is such a value of x, then $b^{\deg(f)+(\deg(f) \mod 2)} f(a/b)$ is a square of an integer. We are lead in this way into investigating values of a two-variable homogeneous polynomial at coprime integers.

Let $n \in \mathbb{N}$ be a fixed natural number throughout this note. We denote by P_n the $\mathbb{Z}$-module

$$\mathbb{Z}x^n + \mathbb{Z}x^{n-1} + ... + \mathbb{Z} \subset \mathbb{Z}[x]$$

of polynomials, coefficients of which are integers and degree is at most n. Let us further identify P_n with $\mathbb{Z}^{n+1}$ (by identifying $x^n, x^{n-1}, ..., 1$ with the standard basis of $\mathbb{Z}^{n+1}$). When a rational number a/b is fixed, polynomials $f \in P_n$ that have it as a root comprise an n-dimensional lattice $\Lambda(a : b) \subset \mathbb{Z}^{n+1}$ (see Section 2). If we vary a/b over the rational numbers, the disjoint union of the resulting lattices corresponds to polynomials $f \in P_n$

that have a rational root taken with multiplicities equal to the number of distinct rational roots that they have. It is well-known that for $n > 1$ this set, viewed as a weighted subset of $\mathbb{Z}^{n+1}$, has zero density (this can be derived from estimates for the number of reducible polynomials, for instance, from [22]).

When a rational number a/b is fixed, polynomials $f \in P_n$ that satisfy $y^2 = b^n f(a/b)$ for an integer value of y comprise a union of translations of $\Lambda(a : b)$ by distances proportional to y^2 along the direction $v_{a,b}$ (see Section 2). If we again vary a/b over the rational numbers, the disjoint union of the resulting unions of translations of $\Lambda(a : b)$ correspond to those polynomials that are squares of a rational number at some rational value of x taken with the occuring (possibly infinite) multiplicities.

If $n = 6$ and we discard from the above set those polynomials $f \in P_6$ that are of degree less than 5 or have a multiple root, then the equation $y^2 = f(x)$ defines a hyperelliptic curve. Due to the theorem of Faltings, there are at most finitely many rational points on such a curve. Therefore, the multiplicities of the remaining polynomials are finite. It was conjectured in [28] that this set, viewed as a weighted subset of $\mathbb{Z}^7$, has zero density. Uniformity Conjecture, stated in [3], predicts a uniform bound on the multiplicities.

Let $H(a/b) = \max\{|a|, |b|\}$ denote the height of a rational number. It may be interesting to see what one can say about the cardinality of the above set when only the rational numbers a/b of height at most H are taken. Let $N(f)$ denote the Euclidean norm of the vector that corresponds to the polynomial $f \in P_n$ and let $\#S$ denote the cardinality of a set S. In (9) of [33] we showed that for any natural numbers H, N such that $H\sqrt{n} < N$ holds

$$\#\{(a/b \in \mathbb{Q}, c \in \mathbb{Z}, f \in P_n) | H(a/b) \leq H, N(f) \leq N, c^2 = b^n f(a/b)\} = \gamma_n(H) N^{n+1/2} + O(N^{n-1/2} H^3 + N^n H^2),$$

where the number $\gamma_n(H)$ does not depend on N and the implied constant does not depend on any of H, N. We also showed that for $n \geq 6$ the number $\gamma_n(H)$ converges when H tends to infinity (Theorem 2 of [33]).

In this work we look at the setting when y^2 is replaced by an arbitrary polynomial $p(y)$ of degree $m > 0$. We show the following.

Theorem 7. *Let a natural number n and a polynomial p of degree $m > 0$ be fixed. Then for any natural numbers H, N such that $H\sqrt{n} < N$ holds the equality*

$$\#\{(a/b \in \mathbb{Q}, c \in \mathbb{Z}, f \in P_n) | H(a/b) \leq H, N(f) \leq N, p(c) = b^n f(a/b)\} = \gamma_{n,p}(H) N^{n+1/m} + O(N^{n+1/m-1} H^3 + N^n H^2),$$

where the number $\gamma_{n,p}(H)$ does not depend on N and the implied constant does not depend on any of H, N.

Notice that when $p(y) = y^2$, we recover the previous result. Furthermore, notice that the larger the degree m of the polynomial p is, the sparser is the set

$$\{(a/b \in \mathbb{Q}, c \in \mathbb{Z}, f \in P_n) | H(a/b) \leq H, p(c) = b^n f(a/b)\}.$$

In particular, for p of degree at least 2 it has zero density. If, additionally, $n > 2m/(m-1)$ is satisfied, then $\gamma_{n,p}(H)$ (which is a strictly increasing function of variable $H \in \mathbb{N}$, as can be seen from (4.10)) converges to a constant $\gamma_{n,p}$ when $H \to \infty$ (the proof is the same as that for $\gamma(H)$ in Theorem 2 of [33]). If we also discard $a/b = 0/1$, the resulting constant $\gamma'_{n,p}$ converges to zero if we let n tend to infinity and keep p fixed (this can be seen from (4.10) as well). For any fixed n, p, the number $\gamma_{n,p}(H)$ is trivially $O(H^2)$. This tells that the contribution of polynomials f with degree smaller than n to the cardinality of Theorem 1 is in its "error term". When $N \to \infty, N \gg H^{\max\{3,2m\}}$, the term $\gamma_{n,p}(H) N^{n+1/m}$ is an asymptotic for the cardinality in the theorem. The restriction that the height H is not too large compared with N is an essential limitation of our proof (we cannot use Lemma 1 for lattices with long diagonals). Finally, a variant of Theorem 1 with $b = 1$ may also be mentioned.

Theorem 8. *Let a natural number n and a polynomial p of degree $m > 0$ be fixed. Then for any natural numbers N, H such that $N > H\sqrt{n}$ holds the equality*

$$\#\{(a, c \in \mathbb{Z}, f \in P_n) | H(a) \leq H, N(f) \leq N, p(c) = f(a)\} = \gamma''_{n,p}(H) N^{n+1/m} + O(N^{n+1/m-1} H^2 + N^n H),$$

where the number $\gamma''_{n,p}(H)$ does not depend on N.

We remark that $\gamma''_{n,p}(H)$ equals the sum in (4.10) with the restriction $b = 1$.

The structure of the proof of Theorem 1 is as follows: in Section 2 we estimate, by standard technique, the number of points of a fixed lattice in a ball. Further, we sum the obtained inequality over translations of the lattice. The sum then is replaced by an integral, an asymptotic of which is described in Section 4. In Section 5 we use this asymptotic to obtain the theorem. In comparison to the proof of (9) in [33], Lemma 2 proved in Section 4 is the main novelty that appears in this note.

4.2 Estimating the number of points of a lattice in a ball

In this section we fix a rational number $a/b \in \mathbb{Q}$ (where $a \in \mathbb{Z}, b \in \mathbb{N}, \gcd(a,b) = 1$) of height $H(a/b) \leq H$ and an integer $c \in \mathbb{Z}$. We identify polynomials $f \in P_n$ with points of $\mathbb{Z}^{n+1}$. Then all f that satisfy $f(a/b) = 0$ comprise a lattice $\Lambda(a:b)$. Let

$$\begin{aligned} v_1 &= (b, -a, 0, 0, ..., 0), \\ v_2 &= (0, b, -a, 0, ..., 0), \\ &\vdots \\ v_n &= (0, 0, ..., 0, b, -a). \end{aligned}$$

Then

$$\Lambda(a:b) = \mathbb{Z}v_1 + \mathbb{Z}v_2 + ... + \mathbb{Z}v_n$$

(the inclusion $\Lambda(a:b) \subset \mathbb{Z}v_1 + \mathbb{Z}v_2 + ... + \mathbb{Z}v_n$ is immediate from the fact that $gcd(a,b) = 1$). All polynomials f that satisfy

$$p(c) = b^n f(a/b)$$

comprise the translated lattice

$$\Lambda_{p(c)}(a:b) := (p(c)u, 0, ..., 0, p(c)v) + \Lambda(a:b),$$

where $u, v \in \mathbb{Z}$ are such that $ua^n + vb^n = 1$.

Let $v_{a,b} = (a^n, a^{n-1}b, ..., b^n)$. The translated lattice lies in the real hyperplane

$$h_{p(c)}(a : b) = \{\mathbf{x} \in \mathbb{R}^{n+1} | \mathbf{x} \cdot v_{a,b} = p(c)\}.$$

Let $\Delta(a : b)$ denote the covolume of $\Lambda(a : b)$.

Claim 2. $\Delta(a : b) = \sqrt{a^{2n} + a^{2n-2}b^2 + ... + b^{2n}}$.

Proof. See Claim 1 of [33].

Lemma 3. *Let $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 + ... + \mathbb{Z}w_k \subset \mathbb{R}^k$ be a k-dimensional lattice generated by the vectors $w_1, w_2, ..., w_k$. Then, for $N > \delta$, we have*

$$\frac{\text{vol}(B^k_{N-\delta})}{\Delta} \leq \#(B^k_N \cap \Lambda) \leq \frac{\text{vol}(B^k_{N+\delta})}{\Delta}, \tag{4.1}$$

where B^k_R is a k-dimensional Euclidean ball of radius R, Δ is covolume of the lattice and δ is half the length of the longest diagonal of the fundamental parallelotope of Λ.

Proof. See Lemma 1 of [33]. From Lemma 1, for $N > \delta$, one has

$$\frac{\text{vol}(B^{n+1}_{N-\delta} \cap h_{p(c)}(a : b))}{\Delta(a : b)} \leq \#(B^{n+1}_N \cap \Lambda_{p(c)}(a : b)) \leq \frac{\text{vol}(B^{n+1}_{N+\delta} \cap h_{p(c)}(a : b))}{\Delta(a : b)}. \tag{4.2}$$

Here, δ can be taken to be $H\sqrt{n}$ (as each diagonal is a difference between a pair of vertices of the fundamental parallelotope, each coordinate of a diagonal vector is in absolute value at most $\max\{|2a|, |2b|\} \leq 2H$; in addition, the first and the last coordinates are in absolute value each at most $\max\{|a|, |b|\} \leq H$. Hence the length of a diagonal is at most $\sqrt{4H^2(n-1) + 2H^2} < 2H\sqrt{n}$).

4.3 Summing over translations and approximating by an integral

Next, we sum the inequality (4.2) over the translated lattices (notice that since |p(c)| tends to infinity, the sum has only finitely many nonzero terms):

$$\frac{1}{\Delta(a:b)} \sum_{c=-\infty}^{\infty} \mathrm{vol}(B_{N-\delta}^{n+1} \cap h_{p(c)}(a:b)) \leq \sum_{c=-\infty}^{\infty} \#(B_N^{n+1} \cap \Lambda_{p(c)}(a:b)) \leq \frac{1}{\Delta(a:b)} \sum_{c=-\infty}^{\infty} \mathrm{vol}(B_{N+\delta}^{n+1} \cap h_{p(c)}(a:b)). \tag{4.3}$$

For a vector $v \in \mathbb{R}^{k+1}$ of Euclidean length $||v|| = 1$, denote by

$$\mathrm{Vol}_k(t, \rho) = \mathrm{vol}(B_t^{k+1}(0) \cap \{\mathbf{x} | \mathbf{x} \cdot v = \rho\})$$

the k-dimensional volume of the intersection of $k+1$-dimensional Euclidean ball of radius t centered at the origin with the hyperplane that is perpendicular to v at the distance ρ along the direction v from the origin.

When

$$v = \frac{v_{a,b}}{||v_{a,b}||},$$

we have

$$\mathrm{vol}(B_t^{n+1}(0) \cap h_{p(c)}(a:b)) = \mathrm{Vol}_n(t, p(c)/||v_{a,b}||).$$

Thus

$$\sum_{c=-\infty}^{\infty} \mathrm{vol}(B_t^{n+1}(0) \cap h_{p(c)}(a:b)) = \sum_{c=-\infty}^{\infty} \mathrm{Vol}_n(t, p(c)/||v_{a,b}||).$$

This sum is again finite. Moreover, there exists a constant $C_p \in \mathbb{N}$ such that p is monotone on both $(-\infty, -C_p]$ and $[C_p, \infty)$, and therefore the summand is.

When $c \in [-C_p + 1, C_p - 1]$, we have the bound:

$$\sum_{c=-C_p+1}^{C_p-1} \mathrm{vol}(B_t^{n+1}(0) \cap h_{p(c)}(a:b)) \leq (2C_p - 1)\,\mathrm{vol}(B_t^{n+1}(0) \cap h_0(a:b)) = (2C_p - 1)\,\mathrm{vol}(B_t^n).$$

The last quantity is clearly $O(t^n)$. Therefore, we can approximate the sum by an integral as follows:

$$\sum_{c=-\infty}^{\infty} \mathrm{vol}(B_t^{n+1}(0) \cap h_{p(c)}(a:b)) = \int_{-\infty}^{\infty} \mathrm{Vol}_n(t, p(\rho)/||v_{a,b}||)d\rho + O(t^n). \tag{4.4}$$

4.4 Approximation of the integral

In this section, we will describe an asymptotic of the integral when t tends to infinity. We will see first what the asymptotic is when the polynomial in ρ involved in it is a monomial ρ^l. To describe the general case, we will make use of the idea that the polynomial $p(\rho)$ can be "replaced" by its leading term $p_m\rho^m$ and that would be a sufficiently good approximation.

Claim 3. *Let $l \in \mathbb{N}$. Then*

$$\int_{-\infty}^{\infty} \mathrm{Vol}_k(t, \rho^l)d\rho = t^{k+1/l} \int_{-\infty}^{\infty} \mathrm{Vol}_k(1, \rho^l)d\rho. \tag{4.5}$$

Proof. Observe that the following scaling equality holds:

$$\int_{-\infty}^{\infty} \mathrm{Vol}_k(t, \rho^l)d\rho = t^k \int_{-\infty}^{\infty} \mathrm{Vol}_k(1, \frac{\rho^l}{t})d\rho.$$

By the change of variable, the last integral is

$$\int_{-\infty}^{\infty} \mathrm{Vol}_k(1, \frac{\rho^l}{t})d\rho = \int_{-\infty}^{\infty} \mathrm{Vol}_k(1, \big(\frac{\rho}{t^{1/l}}\big)^l)d\rho = t^{1/l} \int_{-\infty}^{\infty} \mathrm{Vol}_k(1, \rho^l)d\rho.$$

□

We will need the following lemma to describe the general case.

Lemma 4. *Let $p(\rho) = \rho^l + p_{l-1}\rho^{l-1} + ... + p_0 \in \mathbb{R}[\rho]$ be a monic polynomial in a real variable ρ. Then*

$$\int_0^\infty \mathrm{Vol}_k(t, p(\rho))d\rho = \int_0^\infty \mathrm{Vol}_k(t, \rho^l)d\rho + O(t^k), \tag{4.6}$$

where the implied constant of the term $O(t^k)$ may depend on k and p but not on t.

In the use of O-notation in the proof below we will allow, in the same manner, the implied constants to depend on k and p.

Proof. Initially, observe that the integrands are zero everywhere but on finite intervals. To be more precise, let

$$C = \inf\{b \in \mathbb{R}_{\geq 0} \mid p(b) \geq 0, p \text{ is increasing on } [b, \infty)\}.$$

Let p^{-1} denote the inverse of the restricion of the polynomial p to the interval $[C, \infty)$. We assume without a loss of generality that $t \geq \max\{p(C), C^l\}$ (as both integrals are $O(t^k)$ on bounded intervals of integration). Then the precise upper bounds of integration are $p^{-1}(t)$ and $t^{1/l}$ respectively.

We will need the following two propositions for the proof of this lemma. In the first proposition we bound the difference between the lengths of the intervals of integration.

Proposition 1. *The term $|p^{-1}(t) - t^{1/l}|$ is $O(1)$.*

Proof. Assume first that

$$p^{-1}(t) - t^{1/l} > |p_{l-1}|/l + 1.$$

Since p is increasing on $[C, \infty)$,

$$t = p(p^{-1}(t)) > p(t^{1/l} + |p_{l-1}|/l + 1).$$

The last term, viewed as a polynomial in $t^{1/l}$, has t as its leading term and a positive coefficient in front of its second leading term. It follows that t that satisfy the last inequality

must be bounded by a constant C_p. But then the difference $p^{-1}(t) - t^{1/l}$ is bounded above by

$$\max\{p^{-1}(\theta) - \theta^{1/l} | C \leq \theta \leq C_p\}.$$

Assume, in the opposite direction, that

$$p^{-1}(t) - t^{1/l} < -|p_{l-1}|/l - 1.$$

Again, since p is increasing on $[C, \infty)$,

$$t = p(p^{-1}(t)) < p(t^{1/l} - |p_{l-1}|/l - 1).$$

The right hand side, viewed as a polynomial in $t^{1/l}$, has t as its leading term and a negative coefficient in front of its second leading term. It follows that t that satisfy the last inequality must be bounded by a constant, call it C_p again. But then the difference $p^{-1}(t) - t^{1/l}$ is bounded below by

$$\min\{p^{-1}(\theta) - \theta^{1/l} | C \leq \theta \leq C_p\}.$$

This ends the proof of the proposition.

□

In the second proposition we bound the main error term.

Proposition 2. *The term* $\int_0^{\min\{p^{-1}(t), t^{1/l}\}} (\mathrm{Vol}_k(t, p(\rho)) - \mathrm{Vol}_k(t, \rho^l))d\rho$ *is* $O(t^k)$.

Proof. Initially, we write out the integral more explicitly:

$$\int_0^{\min\{p^{-1}(t), t^{1/l}\}} (\mathrm{Vol}_k(t, p(\rho)) - \mathrm{Vol}_k(t, \rho^l))d\rho =$$
$$\mathrm{vol}(B_1^k) \int_0^{\min\{p^{-1}(t), t^{1/l}\}} \left(\sqrt{(t^2 - p^2(\rho))^k} - \sqrt{(t^2 - \rho^{2l})^k} \right) d\rho.$$

We will bound the integrand for $\rho \in [1, t^{1/l} - (|p_{l-1}| + 1)/l]$ (one can see that the remain-

ing values of ρ comprise two intervals of bounded length, as follows from the preceeding proposition, hence the integral on them is $O(t^k)$).

Notice that

$$\rho^{2l} \leq t^2 - 2(|p_{l-1}| + 1)t^{(2l-1)/l} + O(t^{(2l-2)/l}).$$

Hence

$$t^2 - \rho^{2l} \geq 2(|p_{l-1}| + 1)t^{(2l-1)/l} + O(t^{(2l-2)/l}).$$

In the meanwhile,

$$|p^2(\rho) - \rho^{2l}| \leq |p_{l-1}|t^{(2l-1)/l} + O(t^{(2l-2)/l}).$$

Therefore, when t is larger than some constant,

$$|p^2(\rho) - \rho^{2l}| \leq \frac{1}{2}(t^2 - \rho^{2l}) \tag{4.7}$$

holds. Thus one obtains

$$t^2 - p^2(\rho) = (t^2 - \rho^{2l}) + (p^2(\rho) - \rho^{2l}) \geq (t^2 - \rho^{2l}) - \frac{1}{2}(t^2 - \rho^{2l}) = \frac{1}{2}(t^2 - \rho^{2l}).$$

Therefore,

$$\sqrt{(t^2 - p^2(\rho))^k} \geq 2^{-k/2}\sqrt{(t^2 - \rho^{2l})^k}.$$

Now observe that for any two real numbers $A, B > 0$ the inequality

$$|B - A| \leq \max\{|B^2 - A^2|/(2A), |B^2 - A^2|/(2B)\}$$

holds. If additionally A, B satisfy $A \geq 2^{-k/2}B$, then one can conclude that

$$|B - A| \leq 2^{k/2} \frac{|B^2 - A^2|}{2B}.$$

When $A = \sqrt{(t^2 - p^2(\rho))^k}, B = \sqrt{(t^2 - \rho^{2l})^k}$, this yields

$$\left| \sqrt{(t^2 - \rho^{2l})^k} - \sqrt{(t^2 - p^2(\rho))^k} \right| \leq 2^{k/2} \frac{|(t^2 - \rho^{2l})^k - (t^2 - p^2(\rho))^k|}{2\sqrt{(t^2 - \rho^{2l})^k}}.$$

We claim that the last term is at most $-c' \frac{d}{d\rho} \sqrt{(t^2 - \rho^{2l})^k}$ for some constant $c' > 0$.

To see that, it suffices to show that

$$2^{k/2} |(t^2 - \rho^{2l})^k - (t^2 - p^2(\rho))^k| \leq -c' \frac{d}{d\rho} (t^2 - \rho^{2l})^k.$$

We rewrite the left hand side (without the constant factor) by the binomial expansion:

$$|(t^2 - \rho^{2l})^k - ((t^2 - \rho^{2l}) + (\rho^{2l} - p^2(\rho)))^k| = \left| \sum_{j=1}^{k} \binom{k}{j} (t^2 - \rho^{2l})^{k-j} (\rho^{2l} - p^2(\rho))^j \right|.$$

From here, one can see that it suffices to show that the inequality holds term-wise, that is,

$$|(t^2 - \rho^{2l})^{k-j} (\rho^{2l} - p^2(\rho))^j| \leq -c'_j \frac{d}{d\rho} (t^2 - \rho^{2l})^k = -c'_j k (t^2 - \rho^{2l})^{k-1} (-2l) \rho^{2l-1} \qquad (4.8)$$

for some $c'_j > 0, j = 1, ..., k$.

Since $\rho \geq 1$, one sees that

$$|\rho^{2l} - p^2(\rho)| = O(\rho^{2l-1}).$$

Furthermore, from (4.7) one has

$$|\rho^{2l} - p^2(\rho)| = O(t^2 - \rho^{2l}).$$

The last two equalities together give

$$|(t^2 - \rho^{2l})^{k-j}(\rho^{2l} - p^2(\rho))^j| = O((t^2 - \rho^{2l})^{k-1}\rho^{2l-1}).$$

Hence (4.8) is satisfied. Therefore, the claim holds.

Consequently, from the claim, for $\rho \in [1, t^{1/l} - (|p_{l-1}| + 1)/l]$, we have a bound for the integrand:

$$\left|\mathrm{Vol}_k(t, p(\rho)) - \mathrm{Vol}_k(t, \rho^l)\right| \leq \mathrm{vol}(B_1^k)(-c')\frac{d}{d\rho}\sqrt{(t^2 - \rho^{2l})^k}.$$

Therefore,

$$\begin{aligned}
\int_0^{\min\{p^{-1}(t), t^{1/l}\}} \left|\mathrm{Vol}_k(t, p(\rho)) - \mathrm{Vol}_k(t, \rho^l)\right| d\rho \leq \\
\mathrm{vol}(B_1^k) \int_0^{\min\{p^{-1}(t), t^{1/l}\}} -c'\frac{d}{d\rho}\sqrt{(t^2 - \rho^{2l})^k} d\rho + O(t^k) \leq \\
\mathrm{vol}(B_1^k)\Big|_0^{t^{1/l}} - c'\sqrt{(t^2 - \rho^{2l})^k} + O(t^k) = \\
\mathrm{vol}(B_1^k)c't^k + O(t^k) = O(t^k).
\end{aligned}$$

Finally, the condition that t is larger than some constant can be dropped, as otherwise the length of the interval of integration is $O(1)$ and therefore the integral is $O(t^k)$ on it. This ends the proof of the second proposition.

□

Now one can use the propositions to have a transition between the two integrals:

$$\int_0^\infty \mathrm{Vol}_k(t,p(\rho))d\rho = \int_0^{\min\{p^{-1}(t),t^{1/l}\}} \mathrm{Vol}_k(t,p(\rho))d\rho + O(t^k|p^{-1}(t)-t^{1/l}|) =$$
$$\int_0^{\min\{p^{-1}(t),t^{1/l}\}} \mathrm{Vol}_k(t,p(\rho))d\rho + O(t^k) =$$
$$\int_0^{\min\{p^{-1}(t),t^{1/l}\}} \mathrm{Vol}_k(t,\rho^l)d\rho + O(t^k) =$$
$$\int_0^{\infty} \mathrm{Vol}_k(t,\rho^l)d\rho + O(t^k).$$

This completes the proof of Lemma 2.

□

Corollary 1. *We have*

$$\int_{-\infty}^\infty \mathrm{Vol}_k(t,p(\rho))d\rho = t^{k+1/l}\int_{-\infty}^\infty \mathrm{Vol}_k(1,\rho^l)d\rho + O(t^k). \tag{4.9}$$

Proof. It follows from (4.6) (by using it also when ρ is substituted with $-\rho$) that

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

Now (4.5) yields the conclusion.

□

Now we can use Corollary 1 to approximate the integral in (4.4). By the change of variable one obtains

$$\int_{-\infty}^\infty \mathrm{Vol}_n(t,p(\rho)/||v_{a,b}||)d\rho = \sqrt[m]{||v_{a,b}||/|p_m|}\int_{-\infty}^\infty \mathrm{Vol}_n(t,p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||)d\rho.$$

By symmetry of the function Vol_n in the second argument we have

$$\mathrm{Vol}_n(t, p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||) = \mathrm{Vol}_n(t, \mathrm{sign}(p_m)p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||).$$

The polynomial $\mathrm{sign}(p_m)p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||$ is a monic polynomial in ρ. We obtain now from Corollary 1 (with $k = n$ and $l = m$) that

$$\int_{-\infty}^{\infty} \mathrm{Vol}_n(t, \mathrm{sign}(p_m)p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||)d\rho = t^{n+1/m}\int_{-\infty}^{\infty} \mathrm{Vol}_n(1, \rho^m)d\rho + O(t^n).$$

Corollary 1 allows the implied constant here to be dependent on the polynomial

$$\mathrm{sign}(p_m)p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||$$

and thus on $||v_{a,b}||$. However, since $||v_{a,b}|| \geq 1$, notice that when $||v_{a,b}|| > 1$, the absolute value of every but the leading coefficient of this polynomial is smaller than the absolute value of the respective coefficient of the polynomial $\mathrm{sign}(p_m)p(\rho/\sqrt[m]{|p_m|})$, while when $||v_{a,b}|| = 1$, the two polynomials coincide. Therefore, for all $|\rho|$ larger than some constant that depends on p but not on $||v_{a,b}||$ holds

$$\begin{aligned}|\,\mathrm{Vol}_n(t, \mathrm{sign}(p_m)p\big(\sqrt[m]{||v_{a,b}||/|p_m|}\rho\big)/||v_{a,b}||) - \mathrm{Vol}_n(t, \rho^m)| \leq \\ |\,\mathrm{Vol}_n(t, \mathrm{sign}(p_m)p(\rho/\sqrt[m]{|p_m|})) - \mathrm{Vol}_n(t, \rho^m)|.\end{aligned}$$

We thus conclude that the implied constant above does not depend on $||v_{a,b}||$.

Define

$$\gamma(a:b) := |p_m|^{-1/m}\Delta(a:b)^{1/m-1}\int_{-\infty}^{\infty} \mathrm{Vol}_n(1, \rho^m)d\rho.$$

Then we can write

$$\frac{1}{\Delta(a:b)}\int_{-\infty}^{\infty} \mathrm{Vol}_n(t, p(\rho)/||v_{a,b}||)d\rho = \gamma(a:b)t^{n+1/m} + O(t^n),$$

where the implied constant does not depend on a/b.

4.5 Proof of Theorem 1

Equality (4.4) together with the last equality of the previous section give

$$\frac{1}{\Delta(a:b)} \sum_{c=-\infty}^{\infty} \mathrm{vol}(B_t^{n+1}(0) \cap h_{p(c)}(a:b)) = \gamma(a:b)t^{n+1/m} + O(t^n).$$

This together with (4.3) give

$$\sum_{c=-\infty}^{\infty} \#(B_N^{n+1}(0) \cap \Lambda_{p(c)}(a:b)) = \gamma(a:b)N^{n+1/m} + O(N^{n+1/m-1}H + N^n).$$

To complete the proof, we sum the last equality over rational numbers a/b of height at most H to obtain Theorem 1 with

$$\gamma_{n,p}(H) := \sum_{a/b \in \mathbb{Q}, H(a/b) \leq H} \gamma(a:b). \tag{4.10}$$

Chapter 5

Curves without points in a number field

In view of the arguments given in the preceeding chapters, one may expect that few hyperelliptic curves will have points over any number field. It is thus of interest to construct families of hyperelliptic curves that do not have points over a given number field.

For a given finite extension K of the field of rational numbers, it is not very difficult to show (relying on two well-known theorems) that there exists a hyperelliptic curve that has no points over K. To see that, we consider the curve

$$y^2 = x^5 + 1.$$

It may or may not itself have points over K. Suppose that it has, then, by the theorem of Faltings, there are only finitely many of them. Thus, there exists a finite set of the x-coordinates of the points. For each element α of the set, we can look at its minimal polynomial $p_\alpha(x)$ over the rational numbers. Suppose that the degree of the extension $K/\mathbb{Q}$ is d. Then, by [5], the polynomial $p_\alpha(x^{d+1} + y)$ is irreducible over $\mathbb{Q}[x, y]$. By Hilbert's irreducibility theorem, there exists a natural number $n_K \neq -1$ such that all the polynomials $p_\alpha(x^{d+1} + n_K)$ are irreducible over $\mathbb{Q}[x]$. Since their degrees each is larger than the degree of the extension $K/\mathbb{Q}$, none of them has roots in K. Then, consequently, the hyperelliptic curve

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

has no points over K.

We see that the genus of such a curve depends on the extension K. We can avoid this.

Theorem 9. *There exists a hyperelliptic curve of genus 4 that has no points over K.*

Proof. We may again look at the curve

$$y^2 = x^5 + 1.$$

Let the x-coordinates of its points over K be denoted by $\alpha_1, ..., \alpha_s$. Then one can note that the polynomials $x^2 + y - \alpha_i$ are irreducible over $\mathbb{C}[x, y]$. By a generalized Hilbert's irreducibility theorem [25] (known to us from [11]), there exists an arithmetic progression of rational integers such that for any number n_K in it, each of the polynomials $x^2 + n_K - \alpha_i$ are irreducible over $K[x]$. Then the curve

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

has no points over K. □

There exist simpler reasons why a hyperelliptic curve may have no points over a number field. For instance, $y^2 = 7x^2 + 3z^2$ does not have integer solutions other than $(x, y, z) = (0, 0, 0)$ (since 3 is not a square modulo 7). Hence $y^2 = 7x^2 + 3$ does not have rational solutions. One can then construct a hyperelliptic curve $y^2 = 7f(x)^2 + 3$ (where $f(x) \in \mathbb{Q}[x]$) that will not have rational solutions for the same reason.

Let $K = \mathbb{Q}(\sqrt{2})$. We could verify that $y^2 = 7x^2 + 3z^2$ does not have solutions in $\mathcal{O}_K$ other than $(x, y, z) = (0, 0, 0)$. Indeed, observe that $7 = (2\sqrt{2} + 1)(2\sqrt{2} - 1)$. Thus, the ideal $7\mathbb{Z}$ splits completely in $\mathcal{O}_K$. Let $\wp_1, \wp_2$ denote its two prime factors. In the field $\mathcal{O}_K/\wp_1$ the equation simplifies to $y^2 = 3z^2$. Since 3 is not a square in this field, we must have $y, z \in \wp_1$. Then

$$\wp_1^2 | (y^2 - 3z^2)\mathcal{O}_K = 7\mathcal{O}_K x^2 \mathcal{O}_K.$$

Since $\wp_1^2$ does not divide $7\mathcal{O}_K$, the uniqueness of factorization of ideals yields that $\wp_1$ divides $x\mathcal{O}_K$. Thus, $x, y, z \in \wp_1$. In the same way, $x, y, z \in \wp_2$. Therefore, $x, y, z \in p\mathcal{O}_K$. Then we can divide x, y, z by p and obtain a smaller solution. We can continue in this way to conclude that $(x, y, z) = (0, 0, 0)$.

This approach generalizes to Galois closure of an arbitrary number field with the help of the Chebotarev density theorem.

Theorem 10. *Let K be a Galois extension of the field of rational numbers of finite degree d. Then the lower density of prime numbers p such that for any $a \in \mathbb{Z}$ that is not a square modulo p, the curve $y^2 = px^2 + a$ has no points over K, is at least $1/d$ in the set of all prime numbers.*

Proof. Let us assume that the curve has a K-rational point. Then the equation

$$y^2 = px^2 + az^2 \tag{5.1}$$

has a solution in $\mathcal{O}_K$ with $z \neq 0$. It follows from Chebotarev density theorem that the density of prime numbers that split completely over K is $1/d$. Let p be such a prime. Write

$$p\mathcal{O}_K = \mathfrak{p}_1 ... \mathfrak{p}_d.$$

Modulo $\mathfrak{p}_j$, the above equation reduces to $y^2 = az^2$. Then, since a is not a square modulo p, we must have $y, z \in \mathfrak{p}_j$. Since this is true for $i = 1, ..., d$, we conclude that $y, z \in p\mathcal{O}_K$. We thus can write py, pz instead of y, z to obtain

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

After dividing both sides by p one can see that $x^2 \in p\mathcal{O}_K$ and thus that $p\mathcal{O}_K$ divides $(x\mathcal{O}_K)^2$. Therefore $(p\mathcal{O}_K)^2$ divides $(x\mathcal{O}_K)^2$ and thus $p|x$. We have obtained a descent. Consequently, the equation (5.1) cannot have solutions in $\mathcal{O}_K$ other than $(0, 0, 0)$. A contradiction. □

This allows to conclude the following.

Corollary 2. *Given a number fied K, there exist infinitely many curves of every genus that are defined over the rational numbers and have no points over K.*

We remark that the result given in [26] enables a different construction of quadratic curves that do not have points over a chosen number field. The observations above do not seem to

extend to tell whether there is a polynomial $f(x) \in \mathbb{Q}[x]$ of degree 9 or, of any odd prime degree (and nonzero discriminant), such that the curve $y^2 = f(x)$ has no points over K.

Chapter 6

On the congruent number curves

6.1 Introduction

A positive integer n is called a *congruent number* if it is the area of a right triangle with rational sides. The question of what positive integers are congruent numbers dates back at least to 10th century AD (see, for instance, [4]) and is not fully resolved. P.Fermat proved that perfect squares are not congruent numbers. By now, many families of congruent and not congruent numbers are known. For instance, prime numbers of the form $8m + 5$ are congruent numbers while prime numbers of the form $8m + 3$ are not.

Thus an integer n is a congruent number if and only if the system of equations

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2n \end{cases} \tag{6.1}$$

in unknowns a, b, c has a solution in nonzero rational numbers. The system of equations is equivalent to

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

Hence, if n is a congruent number, the curve

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

has a rational point with nonzero coordinates. Conversely, if the curve has a rational point (x, y) with nonzero coordinates, then $(a, b, c) = (y/(2x), 4nx/y, (x^4 + 16n^2)/(2xy))$ would give a solution in nonzero rational numbers to the above system of equations (alternatively, one may obtain a similar mapping from the curve $y^2 = x^3 - n^2x$).

Resolution of the congruent number problem is related with the famous Birch and Swinnerton-Dyer conjecture that we briefly state here. For an elliptic curve E, let the number $p+1-a_p$ be the number of points on E over the finite field $\mathbb{F}_p$. Let the $L(E, s)$ be a function of the complex variable s, defined by

$$L(E, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where the product is taken over all primes p such that the reduced curve remains elliptic over $\mathbb{F}_p$. The function $L(E, s)$ is called the L-function of the curve E. It is a deep fact that the function is holomorphic on the whole complex plane. The weak Birch and Swinnerton-Dyer conjecture asserts that the order of vanishing of the L-function at the point $s = 1$ equals the rank of the group of rational points on E.

In 1983 Tunnell proved the following theorem.

Theorem 11. *(Tunnell [31]). Let n be a squarefree positive integer. Define*

$A_n = \{(x, y, z) \in \mathbb{Z}^3 | x^2 + 2y^2 + 8z^2 = n\}$,
$B_n = \{(x, y, z) \in \mathbb{Z}^3 | x^2 + 2y^2 + 32z^2 = n\}$,
$C_n = \{(x, y, z) \in \mathbb{Z}^3 | 2x^2 + 8y^2 + 16z^2 = n\}$,
$D_n = \{(x, y, z) \in \mathbb{Z}^3 | x^2 + 8y^2 + 64z^2 = n\}$.

If n is an odd congruent number, then $\#A_n = 2\#B_n$. If n is an even congruent number, then $\#C_n = 2\#D_n$. Moreover, if the weak Birch and Swinnerton-Dyer conjecture holds for the curve $y^2 = x^3 - n^2x$, then the converse is true: if n is odd and $\#A_n = 2\#B_n$ then n is a congruent number; if n is even and $\#C_n = 2\#D_n$, then n is a congruent number.

Would the Birch and Swinnerton-Dyer conjecture be proven to be true, the theorem would

provide a complete solution to the congruent number problem.

As an illustration, one can easily draw from the theorem the following corollary.

Corollary 3. *For all $m \in \mathbb{N}$, the number $n = 64m^2 + 64m + 26$, whenever it is squarefree, is not congruent.*

Proof. In this case, $(1, 1, 2m+1)$ belongs to the set C_n of the above theorem, while the set D_n is empty, as the equation

$$x^2 + 8y^2 + 64z^2 = 64m^2 + 64m + 26$$

has no solutions modulo 16. □

We refer the reader to [4] for a more detailed survey of the main facts related to the congruent number problem.

One may ask, quite generally, if a set contains lengths of a right triangle with area equal to n.

Definition 1. *Let k be a field extension of the rational numbers and $S \subset k$ be its subset. We will say that a positive integer n is a S-congruent number if (6.1) has a solution in S with $a, b, c \neq 0$.*

In [13], the following question was stated: given a number field K, what positive integers are K-congruent numbers? In particular, this asks whether all positive integers are K-congruent numbers for some number field K.

One may first wonder if for some number field K there may exist rational functions $a(n), b(n), c(n) \in K(n)$ that for every $n \in \mathbb{N}$ would evaluate to side lengths of a rational right triangle with area n. Were that the case, the curve $n^2 = x^4 - y^2$ would also have a parametric solution $(x(n), y(n)) \in K(n) \times K(n)$. However, the following (folklore) proposition tells us that such a parametrization does not exist.

Proposition 3. *The curve $n^2 = x^4 - y^2$ does not have solutions in $\mathbb{C}(n)$ with $x \neq 0$.*

Proof. If $(x(n), y(n))$ is a solution, then

$$1 = x(n)^4/n^2 - y^2(n)/n^2.$$

Set $n = t^2$, then

$$1 = (x(t^2)/t)^4 - (y(t^2)/t^2)^2.$$

Thus $(x(t^2)/t, y(t^2)/t^2) \in \mathbb{C}(t)$ is a point on the curve $1 = x^4 - y^2$. As it is known that a curve of genus one (or larger) cannot have nonconstant rational parametrizations, it follows that there must exist constants $c_1, c_2 \in \mathbb{C}$ such that $x(t^2)/t = c_1, y(t^2)/t^2 = c_2$. Thus $x(n) = c_1 t \notin \mathbb{C}(n)$, unless $c_2 = 0$. □

In contrast to this, Jedrzejak ([16], Corollary 6) recently proved the following generalization of a result of Tada [29].

Theorem 12. *Let $m_1, ..., m_s$ be square-free positive integers that are not multiples of each other. Let $K = \mathbb{Q}(\sqrt{m_1}...., \sqrt{m_s})$ and assume that $\sqrt{2} \notin K$. Then a positive integer n is a K-congruent number if and only if one of the numbers $nm_1^{e_1}...m_s^{e_s}$, where $e_i \in \{0, 1\}$, is a congruent number (over the rational numbers).*

This allows one to conclude ([16], Remark 8) via the Tunnell's theorem above that, conditionally on the weak Birch and Swinnerton-Dyer conjecture for the curves $y^2 = x^3 - n^2 x$, every positive integer is a $\mathbb{Q}(\sqrt{3}, \sqrt{5})$-congruent number.

It may be interesting to ask what numbers are congruent over rings of integers of a number field K, that is, are $\mathcal{O}_K$-congruent. We will prove the following theorem.

Theorem 13. *Let K be a finite Galois extension of the field of rational numbers with cyclic Galois group. Then, asymptotically, at least half of the prime numbers p that are inert in K correspond to curves*

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

that do not have points over $\mathcal{O}_K$ with $x \neq 0$.

Corollary 4. *For a finite Galois extension K of the field of rational numbers with cyclic*

Galois group $Gal(K/\mathbb{Q})$ of cardinality d, the set of prime numbers that are not $\mathcal{O}_K$-congruent has lower density at least $\varphi(d)/(2d)$ among the prime numbers.

Example 1. *The polynomial $f(x) = x^3 - 3x + 1$ is irreducible in the ring $\mathbb{Q}[x]$. Moreover, its discriminant is a perfect square and thus the splitting field of $f(x)$ is a cyclic extension of degree 3 of the rational numbers. Let $\alpha = 2\cos(2\pi/9)$ be a root of $f(x)$. Then the theorem implies that the (rational) prime numbers that are not $\mathbb{Z}[\alpha]$-congruent have lower relative density at least $1/3$.*

6.2 Proof of the Theorem

For the proof of the theorem we borrow two statements from [14] and [15], respectively, that we state here as lemmas:

Lemma 5. *Let A be any subset of the prime numbers of positive relative upper density. Then A contains infinitely many arithmetic progressions of length l for all l.*

Lemma 6. *If R is a finitely generated integral domain of zero characteristic and l is an integer, then there exists a constant $A_l(R)$ such that every arithmetic progression in R having more than $A_l(R)$ elements contains an element which is not a sum of l units.*

Proof. Rational prime numbers p that remain inert in $\mathcal{O}_K$ have density $\varphi(d)/d$ in the set of prime numbers, as follows from the Chebotarev density theorem [30]. Let us denote by P'_K the set of prime numbers p that are inert in $\mathcal{O}_K$ and such that the equation

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

has a solution in $\mathcal{O}_K$ with $x \neq 0$. Thus, for $p \in P'_K$ holds

$$16\mathcal{O}_K(p\mathcal{O}_K)^2 = (x^2 - y)\mathcal{O}_K(x^2 + y)\mathcal{O}_K.$$

Since each ideal of $\mathcal{O}_K$ factorizes uniquely into prime ideals, we must have either

$$\begin{cases} (x^2 - y)\mathcal{O}_K = p\mathcal{O}_K I \\ (x^2 + y)\mathcal{O}_K = p\mathcal{O}_K I' \end{cases} \tag{6.2}$$

or

$$\begin{cases} (x^2 - y)\mathcal{O}_K = (p\mathcal{O}_K)^2 I \\ (x^2 + y)\mathcal{O}_K = I' \end{cases} \tag{6.3}$$

for some ideals $I, I' \subset \mathcal{O}_K$ that satisfy $II' = 16\mathcal{O}_K$. If (6.2) is the case, we deduce that

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

for some $r \in \mathcal{O}_K$ that divides 16. Thus,

$$2x^2 r = (r^2 + 16)p.$$

Let K' be the largest subfield of K such that the degree of the field extension $K'/\mathbb{Q}$ is odd. Denote $K'(i)$ by L. Observe that L is a cyclic extension of the field of rational numbers as well. Therefore, as it follows from the Chebotarev density theorem again, if $i \notin K$, rational prime numbers that remain inert in $\mathcal{O}_L$ have density $1/2$ among the prime numbers that remain inert in $\mathcal{O}_K$. Over $K(i)$ we can write

$$2r\mathcal{O}_{K(i)}(x\mathcal{O}_{K(i)})^2 = (r + i)\mathcal{O}_{K(i)}(r - i)\mathcal{O}_{K(i)}p\mathcal{O}_{K(i)}.$$

Let $\sigma \in Gal(K(i)/K)$ be the element of order two and denote by J the ideal $(r + i)\mathcal{O}_{K(i)}$. Let us intersect both sides of the equality with $\mathcal{O}_L$. Then the r.h.s. can be written as

$$(J \cap \mathcal{O}_L)\sigma(J \cap \mathcal{O}_L)p\mathcal{O}_L.$$

We thus can see that if p is a rational prime that remains inert in both K and L, the highest power of the prime ideal $p\mathcal{O}_L$ that divides the r.h.s. must be odd. On the other

hand, the highest power of any prime ideal, that is not a divisor of $2\mathcal{O}_L$, that divides the l.h.s. is even. Therefore all odd primes p that are in P'_K and are inert in L must satisfy (6.3). We deduce that for such p holds

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

for some $r \in \mathcal{O}_K$ that divides 16. Thus,

$$2x^2 r = 16p^2 + r^2.$$

Let M be a field extension of K that is generated by elements of the form $\sqrt{r}$, where $r \in \mathcal{O}_K$ are divisors of 16. Up to multiplication by units, there are only finitely many such divisors. Let $r_1, ..., r_v$ be their representatives. The Dirichlet unit theorem [8], [9] tells also that the multiplicative group of units of $\mathcal{O}_K$ is finitely generated. Let $e_1, ..., e_s$ be its generators. Then $M = K(\sqrt{e_1}, ..., \sqrt{e_s}, \sqrt{r_1}, ..., \sqrt{r_v})$ is a finite extension of K. Over $\mathcal{O}_M$ one can write

$$(\sqrt{2r}x - 4p)(\sqrt{2r}x + 4p) = r^2.$$

Hence both $\sqrt{2r}x - 4p, \sqrt{2r}x + 4p$ are divisors of 16^2 in $\mathcal{O}_M$. Consequently, $8p$ is a sum of two divisors of 16^2. We will deduce that such primes must have density zero among the rational prime numbers. Let us assume, on the contrary, that they comprise a set of positive relative upper density. It follows then from the first lemma that there must exist arbitrarily long arithmetic progressions with terms that are sums of two divisors of 16^2 in $\mathcal{O}_M$. Let $r'_1, ...r'_l \in \mathcal{O}_M$ be the representatives of the divisors of 16^2 modulo the multiplicative group of units of $\mathcal{O}_M$. Then the ring $\mathcal{O}_M[1/r'_1, ..., 1/r'_l]$ is finitely generated. Furthermore, any term of an arithmetic progression as above is a sum of two units in this ring. This contradicts the second lemma. □

Chapter 7

On integer points on the hyperelliptic curves $x^{2n+1} - y^2 = 4$

"Determine all pairs (x, y) of integers such that

$$x^5 - y^2 = 4.$$"

The problem was proposed in [19]. The reader can find an elementary solution in the next issue. We offer a different solution that demonstrates how the basic knowledge of the ring of Gaussian integers may be employed in a Diophantine problem. This approach is well-known (e.g., see the survey article [7]) and dates back at least to [17]. In the second section we shortly discuss a more general problem.

7.1 On integer points on the hyperelliptic curve $x^5 - y^2 = 4$

Theorem 14. *There is no pair of integers (x, y) such that $x^5 - y^2 = 4$.*

Proof. Assume that there is such a pair (x, y). If x is even, then $x = 2x'$. We hence have

$$32x'^5 = y^2 + 4.$$

We see that y^2 must be divisible by 4. Thus $y = 2y'$. Therefore,

$$32x'^5 = 4y'^2 + 4 \Leftrightarrow 8x'^5 = y'^2 + 1.$$

Since the left hand side of the last equation is even, we see that y' must be odd. But then, the right hand side equals 2 modulo 4, while the left hand side equals 0 modulo 4. Thus x cannot be even. So x is odd.

We can write

$$x^5 = (y + 2i)(y - 2i)$$

over the ring of Gaussian integers $\mathbb{Z}[i]$. If there is a Gaussian prime $p \in \mathbb{Z}[i]$ such that $p|y + 2i, y - 2i$, then $p|y + 2i - (y - 2i) = 4i$. Thus p is a divisor of 2 and therefore is an associate of $1 + i$. Then, $1 + i|x^5$. Therefore, $\mathrm{Nm}(1 + i) = 2|\mathrm{Nm}(x^5) = x^{10}$. This, however, cannot happen since x is odd. Consequently, $y + 2i, y - 2i$ are coprime and, since their product is a 5-th power, they both must be associates of 5-th powers of some elements of $\mathbb{Z}[i]$. In particular,

$$e(y + 2i) = (k + li)^5 = \sum_{j=0}^{5} \binom{5}{j} k^{5-j}(li)^j = (k^5 - 10k^3l^2 + 5kl^4) + (5k^4l - 10k^2l^3 + l^5)i,$$

where $k, l \in \mathbb{Z}$ and $e \in \{\pm 1, \pm i\}$ is a unit. Therefore, either

$$2ie = k^5 - 10k^3l^2 + 5kl^4,$$

or

$$2ie = (5k^4l - 10k^2l^3 + l^5)i.$$

We claim that neither $k^5 - 10k^3l^2 + 5kl^4$, nor $5k^4l - 10k^2l^3 + l^5$ can be an associate of 2.

Observe that it is enough to show the first, as the other follows by renaming k by l and vice versa. If

$$k^5 - 10k^3l^2 + 5kl^4 = k(k^4 - 10k^2l^2 + 5l^4) = \pm 2,$$

then $k|2$. Thus $k = \pm 1$ or $k = \pm 2$. In the first case,

$$k^4 - 10k^2l^2 + 5l^4 = 1 - 10l^2 + 5l^4 = \pm 2.$$

One can verify that for $l^2 = 0, 1$ this is not the case, while for $l^2 \geq 4, 1 - 10l^2 + 5l^4 \geq 1 - l^2(10 - 20) > 2$. Hence the first case cannot happen.

In the second case,

$$k^4 - 10k^2l^2 + 5l^4 = 16 - 40l^2 + 5l^4 = \pm 1.$$

By checking values of $l^2 = 0, 1, 4$ and seeing that when $l^2 \geq 9$, holds $16 - 40l^2 + 5l^4 \geq 16 - l^2(40 - 45) > 1$, one concludes that this case cannot happen as well. We conclude that the equation $x^5 - y^2 = 4$ cannot have integer solutions.

□

7.2 On integer points on curves $x^{2n+1} - y^2 = 4$.

This approach allows us to say a bit more:

Theorem 15. *For $n \geq 0$, the equation $x^{2n+1} - y^2 = 4$ has a solution in integers (x, y) precisely when the equation*

$$y + 2i = \pm(l + 2i)^{2n+1}$$

has a solution in integers (y, l).

Proof. First, observe that if (x, y) is a solution, then, in the same manner as above, x must be odd and $y + 2i, y - 2i$ therefore have to be coprime. Hence $y + 2i, y - 2i$ both have to

be associates of $2n+1$-th powers of Gaussian integers. Thus,

$$e(y+2i) = (k+li)^{2n+1},$$

where $k, l \in \mathbb{Z}$ are integers and $e \in \{\pm 1, \pm i\}$ is a unit. By the binomial expansion, we have

$$e(y+2i) = \sum_{j=0}^{2n+1} \binom{2n+1}{j} k^{2n+1-j}(li)^j.$$

The real and imaginary parts of the binomial expansion are

$$\sum_{j=0}^{n} \binom{2n+1}{2j} k^{2n+1-2j}(li)^{2j}, \sum_{j=0}^{n} \binom{2n+1}{2j+1} k^{2n-2j}(li)^{2j},$$

respectively. One of them must equal ± 2. Up to renaming k by l and vice versa, we may assume that it is the first one. Then $k|2$, and thus either $k = \pm 1$ or $k = \pm 2$. We will show that $k = \pm 1$ is not possible. Say, $k = \pm 1$. Then

$$\pm 2 = \sum_{j=0}^{n} \binom{2n+1}{2j} k^{2n+1-2j}(li)^{2j} = \sum_{j=0}^{n} \binom{2n+1}{2j} (-l^2)^j.$$

By observing that the first summand of the binomial expansion is equal to 1 and subtracting it from both sides we obtain

$$\sum_{j=1}^{n} \binom{2n+1}{2j} (-l^2)^j \in \{-3, 1\}.$$

Thus $l^2|3$ and therefore $l = \pm 1$. Hence the complex number $k + li$ has norm equal to 2. We can see that the norm of $(k+li)^{2n+1}$ is an even number, while the norm of $e(y+2i)$ is odd. Therefore, the equality $e(y+2i) = (k+li)^{2n+1}$ is not possible. Hence $k = \pm 1$ is not possible. Thus $k = \pm 2$. Then we have $e(y+2i) = (\pm 2 + li)^{2n+1}$. By multiplying both sides by a unit we thus obtain

$$y + 2i = e(l+2i)^{2n+1},$$

where e denotes a unit again. Since y is odd, l must be odd too. Then $(l+2i)^{2n+1}$ has an odd real part and an even imaginary part. Since after multiplication by e the real part must equal y and thus remain odd, we conclude that $e = \pm 1$. Therefore

$$y + 2i = \pm(l + 2i)^{2n+1}.$$

Conversely, say that

$$y + 2i = \pm(l + 2i)^{2n+1}$$

holds for integers (y, l). By multiplying both sides of the equality by their conjugates we obtain

$$y^2 + 4 = (l^2 + 4)^{2n+1}.$$

Thus $(x, y) = (l^2 + 4, y)$ is a solution. □

The equation $y+2i = \pm(l+2i)^{2n+1}$ can be interpreted geometrically. It may be interesting to ask whether n for which it has an integer solution could be arbitrarily large. It turns out that the answer is known to be negative. In fact, for $n \geq 2$ the corresponding equation has no integer solutions. The result follows from the work of T. Nagell [21], as referenced to in [6]. Very generally, a conjecture of S. S. Pillai states that each positive integer occurs at most finitely many times as a difference of two perfect powers (see e.g., [32]).

Bibliography

[1] M. Bhargava, B. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, arXiv:1208.1007v1 (2012).

[2] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, arXiv:1006.1002 (2010).

[3] L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10**(1), 1-35 (1997).

[4] V. Chandrasekar, *The congruent number problem*, Resonance **3**(8), 33-45 (1998).

[5] K. Česnavičius, `http://mathoverflow.net/questions/87455/irreducibility-of-compositions-of-polynomials`.

[6] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$, Acta Arithmetica **65**, 367-381 (1993).

[7] K. Conrad, *Examples of Mordell's equation*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/mordelleqn1.pdf`.

[8] P. G. Lejeune Dirichlet, *Werke* (Ed. by L. Kronecker) **1** 639-644 (1889).

[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., p. 98, Springer-Verlag, Berlin-Heidelberg (2004).

[10] H. Davenport, D. J. Lewis, A. Schinzel, *Quadratic Diophantine equations with a parameter*, Acta Arithmetica **11**, 353-358 (1966).

[11] A. Dubickas, personal communication.

[12] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Mathematicae **73**(3), 349-366 (1983).

[13] E. Girondo, G. Gonzalez-Diez, E. Gonzalez-Jimenez, R. Steuding, J. Steuding, *Right triangles with algebraic sides and elliptic curves over number fields*, Math. Slovaca **59**(3), 299-306 (2009).

[14] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167**(2), 481-547 (2008).

[15] M. Jarden, W. Narkiewicz, *On sums of Units*, Monatsh. Math. **150**(4), 327-332 (2006).

[16] T. Jedrzejak, *Congruent numbers over real number fields*, Colloquium Mathematicum **128**(2), 179-186 (2012).

[17] V. A. Lebesque, *Sur l'impossibilité en nobres entiers de l'équation* $x^m = y^2 + 1$, Nouvelles annales de mathématiques **9**, 178-181 (1850).

[18] D. J. Lewis, A. Schinzel, *Quadratic diophantine equations with parameters*, Acta Arithmetica **37**, 134-141 (1980).

[19] Mathematical Excalibur **15**(2), Problem 353 (2010).

[20] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, arXiv:0904.3709v3 (2010).

[21] T. Nagell, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Nova Acta Regiae Soc. Sci. Upsaliensis, Ser. IV **16**(2) (1955).

[22] G. Pólya, G. Szegő, *Problems and Theorems in Analysis, Vol. II* (Part Eight, Problem 266), p. 356, Springer, Berlin-Heidelberg-New York (1976).

[23] B. Poonen, M. Stoll, *Chabauty's method proves that most odd degree hyperelliptic curves have only one rational point*, arXiv:1302.0061v1 (2013).

[24] B. Poonen, *Curves over every global field violating the local-global principle*, J. of Mathematical Sciences **171**(6), 782-785 (2010).

[25] A. Schinzel, *Polynomials with special regard to reducibility* (p. 298), Cambridge University Press (2000).

[26] A. Schinzel, *Selected topics on polynomials*, (p. 202), University of Michgan Press (1982).

[27] M. Stoll, *How to Solve a Diophantine Equation*, arXiv:1002.4344 (2010).

[28] M. Stoll, *On the average number of rational points on curves of genus 2*, arXiv:0902.4165v1 (2009).

[29] M. Tada, *Congruent numbers over real quadratic fields*, Hiroshima Math. J. **31**(2), 331-343 (2001).

[30] N. Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95**, 191-228 (1925).

[31] J. B. Tunnell, *A Classical Diophantine problem and Modular Forms of Weight 3/2*, Inventiones Mathematicae **72**, 323-334 (1983).

[32] M. Waldschmidt, *Perfect Powers: Pillai's works and their developments*, arXiv:0908.4031v1 (2009).

[33] A. Zinevičius, *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).