THESIS FOR THE DEGREE OF LICENTIATE OF PHILOSOPHY

Counting Rational Points on Genus One Curves

Manh Hung Tran

Division of Algebra and Geometry
Department of Mathematical Sciences
CHALMERS UNIVERSITY OF TECHNOLOGY
AND UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden, 2017

Counting rational points on genus one curves

MANH HUNG TRAN

Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg, Sweden
Phone: +46 (0)31 772 4997
Email: manhh@chalmers.se

Printed in Gothenburg, Sweden 2017

COUNTING RATIONAL POINTS ON GENUS ONE CURVES

Manh Hung Tran

Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg

ABSTRACT

This thesis contains two papers dealing with counting problems for curves of genus one. We obtain uniform upper bounds for the number of rational points of bounded height on such curves. The main tools to study these problems are descent and various refined versions of Heath-Brown's p-adic determinant method. In the first paper, we count rational points on smooth plane cubic curves. In the second paper, we count rational points on non-singular complete intersections of two quadrics. The methods are different for curves of small height and large height and descent is only used for curves of small height.

List of included papers

The following papers are included in this thesis:

I. Manh Hung Tran. *Counting Rational Points on Smooth Cubic Curves*. Submitted.

II. Manh Hung Tran. *Uniform Bounds for Rational Points on Complete Intersections of Two Quadric Surfaces*. Submitted.

Acknowledgments

First of all, I would like to thank my supervisor Per Salberger for introducing me to the topic of this thesis and giving me many important ideas and suggestions. I am very grateful to my assistant supervisor Dennis Eriksson for many useful conversations. I wish to thank the Department of Mathematical Sciences for the great support and letting me meet many wonderful colleagues and friends. I wish to thank my lovely wife Lien for her love and support.

Part A

Introduction

INTRODUCTION

Diophantine equations is one of the oldest areas in mathematics and one of the classical problems in this area is to study the density of solutions of such equations, i.e., the integral solutions of the equations of the form $F(x_0, x_1, ..., x_n) = 0$, where F is a polynomial in $\mathbb{Z}[x_0, x_1, ..., x_n]$. One of the most famous examples is the equation related to *Fermat's Last Theorem*:

$$x^n + y^n = z^n, \tag{1}$$

where n is a positive integer. Fermat conjectured in 1637 that if $n \geq 3$, (1) has no non-zero solution and this was proved by Andrew Wiles in 1995.

This problem can be viewed more geometrically since the equation $F = 0$ defines a hypersurface in the affine space $\mathbb{A}^{n+1}$. It means that integral solutions to Diophantine equations can be viewed as integral points on algebraic varieties. Moreover, if F is homogeneous, it defines a hypersurface in the projective space $\mathbb{P}^n$ and the non-zero primitive integer solutions of $F = 0$ correspond (up to sign) to rational points on this hypersurface. We are thus then interested in rational points on projective varieties.

Let us start with some basic examples in which F is a homogeneous polynomial in $\mathbb{Z}[x_0, x_1, x_2]$ defining a plane curve C in $\mathbb{P}^2$. The theory of plane curves has been studied for a long time by many mathematicians such as Fermat, Euler and Mordell and there are still many interesting open questions. In case deg $F = 1$, i.e., $F = a_0x_0+a_1x_1+a_2x_2$ for some integers a_0, a_1, a_2, then C is just a line in the plane. If say $a_2 \neq 0$, then its rational points can be represented by pairs of rational numbers $(x_0, x_1) \neq (0, 0)$ as $x_2 = -(a_0x_0 + a_1x_1)/a_2$. In case deg $F = 2$, then C is also rational and the solutions to $F = 0$ can be described by one parameter. For example, if $F = x_0^2 + x_1^2 - x_2^2$, then the rational solutions are of the form

$$(x_0, x_1, x_2) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}, 1\right),$$

where t is an arbitrary integer.

The first non-trivial case is thus when deg $F = 3$. Then C is of genus 1 if it is non-singular. The solutions to $F = 0$ can thus not be parametrized in the same way as before as C is no longer rational. In general, it is hard to know whether there are finitely or infinitely many rational points on C. It depends on the particular nature of the equation. But we will in this thesis focus on results which hold for general classes of curves. We shall therefore count the number of points inside large boxes and give upper bounds for the number

$$N(C,B) = \sharp\{P \in C(\mathbb{Q}) : \ H(P) \leq B\}$$

of rational points of height at most B on C. Here H is the naive height function $H(P) := \max\{|x_0|, |x_1|, |x_2|\}$ for $P = (x_0, x_1, x_2)$ with coprime integer values of x_0, x_1, x_2. The aim is to establish uniform estimates for $N(C,B)$ which do not depend on the polynomial F defining C.

The first important uniform upper bound for irreducible plane cubic curves was obtained by Heath-Brown [5] in 2002 as a special case of a more general result. He showed that

$$N(C,B) \ll_\varepsilon B^{2/3+\varepsilon}. \tag{2}$$

Here our notation $f \ll g$ means $f = O(g)$, i.e., there exists a positive constant M such that $|f| \leq Mg$. The implicit constant in (2) depends solely on ε.

The proof of (2) was based on his p-adic determinant method which is one of the few tools available for counting problems on varieties of low dimensions. We now give a description of the basic idea of this method by providing a sketch of the proof of (2).

1. The p-adic determinant method

We first divide all rational points of height at most B on C into congruence classes modulo some prime number p and then count points in each class. By the Hasse-Weil bound there are $p + O_d(\sqrt{p})$ $\mathbb{F}_p$-points on an irreducible plane curve of degree d. Since an irreducible cubic curve can have at most one singular point, we will only count non-singular points on $C(\mathbb{Q})$. Moreover, by a version of Siegel's lemma (see Theorem 4 of [5]), we can always assume that $||F|| \ll B^{30}$ and then any non-singular point on $C(\mathbb{Q})$ will be non-singular modulo p except for a small number of primes p. Here $||F||$ is the maximum modulus of the coefficients of $F(x_0, x_1, x_2) \in \mathbb{Z}[x_0, x_1, x_2]$.

For a given degree d, we first fix $3d$ monomials $\{F_j\}$, $1 \leq j \leq 3d$ of degree d, which are linearly independent on C. Our goal is now to prove that $\det(M) = 0$ for any $3d \times 3d$-matrix $M = (F_j(P_i))_{i,j}$, where $\{P_i\}$, $1 \leq i \leq 3d$ are rational points on C of height at most B, which reduce to the same non-singular $\mathbb{F}_p$-point for a prime p. The vanishing of $\det(M)$ for all such sets $\{P_i\}$ will guarantee the existence of a homogeneous polynomial G of degree d which does not vanish everywhere on C, but which vanishes at all $P \in C(\mathbb{Q})$ of height $H(P) \leq B$, which reduce to the given non-singular $\mathbb{F}_p$-point on the curve defined by $F(x_0, x_1, x_2) = 0 \pmod p$. By the theorem of Bézout, there are then at most $3d$ such points in $C(\mathbb{Q})$.

To show that $\det(M) = 0$, we first give an upper bound and then a factor of the integer $\det(M)$ which exceeds the bound. Since all the points are of height at most B, we get the following upper bound by using Hadamard's inequality:

$$|\det(M)| \leq (3d)^{\frac{3d}{2}} B^{3d^2}. \tag{3}$$

But we can also prove that $\det(M)$ is divisible by $p^{3d(3d-1)/2}$ by using the p-adic implicit function theorem and the fact that all $\{P_i\}$ reduce to the same non-singular $\mathbb{F}_p$-point. Hence as long as we only consider integral points which are non-singular (mod p) for a prime p with $p^{3d(3d-1)/2} > (3d)^{\frac{3d}{2}} B^{3d^2}$, then we get at most $3d$ points in each congruence class. We then obtain (2) by summing over all $O(p)$ congruence classes for such p.

In this direction, Salberger [8] proved a slightly better estimate

$$N(C, B) \ll B^{2/3} \log B, \tag{4}$$

by using his global version of Heath-Brown's p-adic determinant method. He then considered congruences modulo all primes p where C is irreducible over $\mathbb{F}_p$.

The best known uniform bound for irreducible plane cubic curves was given by Walsh [10] using the global determinant method in [8]

$$N(C, B) \ll B^{2/3}. \tag{5}$$

We also observe that if $F(x_0, x_1, x_2) = x_0^3 - x_1^2 x_2$, then the solutions (m^2n, m^3, n^3) show that $N(C, B) \gg B^{2/3}$. But as this curve is singular, it may still be possible to find a sharper bound than (5) for non-singular plane cubic curves.

Remark: All the bounds (2), (4) and (5) are special cases of more general results for irreducible curves of arbitrary degree d in a fixed projective space. In that case the main term $B^{2/3}$ will then be replaced by $B^{2/d}$.

2. Elliptic curves

In this thesis we are interested in the case when the cubic curve C is non-singular. It is then a curve of genus 1. If we fix a rational point $\mathcal{O}$ on C, then we get a bijection between $C(\mathbb{Q})$ and $E(\mathbb{Q})$ for the Jacobian E of C, where P is sent to $P - \mathcal{O}$ in the group $E(\mathbb{Q})$. As E is an elliptic curve over $\mathbb{Q}$, we get by the Mordell-Weil theorem that $E(\mathbb{Q})$ is a finitely generated abelian group. More precisely,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r, \tag{6}$$

where $E(\mathbb{Q})_{\text{tors}}$ is the group of all elements of finite order of $E(\mathbb{Q})$ and r is called the rank of E. The group structure is such that $(P-\mathcal{O})+(Q-\mathcal{O})+(R-\mathcal{O}) = 0$ in $E(\mathbb{Q})$ if and only if $P, Q, R \in C(\mathbb{Q})$ are collinear.

The theory of elliptic curves has been studied for centuries. It is an area where many different branches of mathematics come together such as number theory, algebraic geometry and complex analysis. We will make essential use of the fact that the Jacobian $E =$Jac(C) of a genus 1 curve C is an elliptic curve. This makes it possible to use descent with unramified covers to study rational points on cubic curves. Since any rational point on the original cubic curve maybe lifted to a rational point on one of these new cubic curves, we can apply the determinant method to the new curves instead. This leads to sharper estimates which are not possible to obtain if we only use the determinant method. This is why we only consider *non-singular* cubic curves.

The main tools in this thesis are the determinant method and descent. We have already discussed the determinant method. It thus remains to discuss descent theory which plays an important role in the thesis. This theory was first developed to prove the Mordell-Weil theorem. We will therefore now provide a sketch of the proof of (6).

3. Mordell-Weil theorem and descent method

The theorem holds for general abelian varieties over number fields. But in this section we will only discuss the special case of elliptic curves over the rationals. The proof has two parts. The first part is the so called weak Mordell-Weil theorem which says that if E is an elliptic curve, then $E(\mathbb{Q})/mE(\mathbb{Q})$ is a finite abelian group for any positive integer m. To show this one uses Galois cohomology to find an injection of

$E(\mathbb{Q})/mE(\mathbb{Q})$ into a Selmer group which is known to be finite. This corresponds to a partition

$$E(\mathbb{Q}) = \bigcup_{\alpha} p_\alpha(C_\alpha(\mathbb{Q})) \tag{7}$$

for a finite set of unramified covers $p_\alpha : C_\alpha \to E$ of degree m^2.

The second part of the descent is to use the height function defined at the beginning. It can be seen that if a finite set A of elements of $E(\mathbb{Q})$ can be found, such that they generate the group $E(\mathbb{Q})/mE(\mathbb{Q})$, then the finite set $A \cup B$ will generate $E(\mathbb{Q})$, where $B \subset E(\mathbb{Q})$ is the finite set of elements of a given bounded height. Hence, $E(\mathbb{Q})$ is finitely generated. The method is called descent since it can be viewed as a modern more general version of Fermat's method of infinite descent.

A basic feature of the descent process is that for any rational point P and positive integer m, we have that $H(mP) \approx m^2 H(P)$. From (7), we thus get that the study of $N(E, B)$ essentially reduces to the study of $\sum_\alpha N(C_\alpha, B/m)$ for a finite set of unramified covers $p_\alpha : C_\alpha \to E$ of degree m^2. This leads to better estimates since we are now working with points of smaller height. This was first used by Ellenberg and Venkatesh [4] and by Heath-Brown and Testa [6] and it will play an important role in this thesis.

4. A survey of results

Ellenberg and Venkatesh [4] proved the following bound for smooth plane cubic curves

$$N(C, B) \ll_\varepsilon B^{2/3-1/450+\varepsilon} \tag{8}$$

by combining the p-adic determinant method with descent theory. Their method was then refined by Heath-Brown and Testa [6] by a clever use of the p-adic determinant method for biprojective curves. They got in this way the sharper estimate

$$N(C, B) \ll_\varepsilon B^{2/3-1/110+\varepsilon}. \tag{9}$$

The proof of (9) is divided into three steps. The first step is to partition $C(\mathbb{Q})$ into equivalence classes by means of descent where each class is of the form $p_\alpha(C_\alpha(\mathbb{Q}))$ for some unramified cover $p_\alpha : C_\alpha \to C$. The second step is to embed each C_α in $\mathbb{P}^2 \times \mathbb{P}^2$ and reduce to the counting problem for a biprojective curve in $\mathbb{P}^2 \times \mathbb{P}^2$ in order to avoid the comparisons with canonical heights on $\mathrm{Jac}(C)$ used in [4]. The last step is to apply the p-adic determinant method for this biprojective curve. This is more complicated than for the projective plane curves in Section 1. But the fundamental idea is the same.

The best known result is the following proved by Salberger in his unpublished work

$$N(C,B) \ll_{\varepsilon} B^{2/3-1/84+\varepsilon}. \tag{10}$$

A striking feature of [6] is that Heath-Brown and Testa also proved the following bound for any positive integer m

$$N(C,B) \ll m^{r+2}\left(B^{\frac{2}{3m^2}} + \log B\right)\log B, \tag{11}$$

with an implied constant independent of m, where r is the rank of $\mathrm{Jac}(C)$. Taking $m = 1 + [\sqrt{\log B}]$ they obtain that

$$N(C,B) \ll (\log B)^{3+r/2}. \tag{12}$$

5. Paper I: Counting rational points on smooth cubic curves

In Paper I, we follow the approach of [6] closely except that we replace the p-adic determinant method by the global determinant method of Salberger. This gives the following improvements of (11) and (12):

$$N(C,B) \ll m^{r}\left(B^{\frac{2}{3m^2}} + m^2\right)\log B, \tag{13}$$

and

$$N(C,B) \ll (\log B)^{2+r/2}. \tag{14}$$

The bounds are uniform in the sense that the implicit constants only depend on the rank r of the corresponding Jacobian.

In the appendix of Paper I we also include an even better estimate (see Theorem 9), which is obtained by a re-examination of the argument in [6]. This is based on a deep result of David [3] about successive minima for the quadratic form corresponding to the canonical height on $\mathrm{Jac}(C)$. These estimates should be compared with the classical result of Néron:

$$N(C,B) \sim c_F(\log B)^{r/2}, \tag{15}$$

where c_F is a constant depending on F. But the proof of that result gives very little information about the error terms and no uniform bounds for $N(C,B)$.

6. Counting rational points on curves of genus g

Although the thesis is only devoted to curves of genus one, it is illuminating to give an overview of the density of rational points on an arbitrary non-singular curve C of genus g in $\mathbb{P}^n$. We will here use the notation $N(C,B)$ for the number of points $P \in C(\mathbb{Q})$ with $H(P) \leq B$, where the height function H is then defined by $H(P) := \max\{x_0, ..., x_n\}$ for $P = (x_0, ..., x_n)$ with coprime integer values of $x_0, ..., x_n$. There are three cases:

+) If $g(C) = 0$: either C has no rational point or $C \cong \mathbb{P}^1$. In the latter case, C is called a rational curve and that $N(C,B) \sim_C B^{2/d}$, where d is the degree of C. Thus the best possible result is $N(C,B) \ll_d B^{2/d}$ shown by Walsh [10].
+) If $g(C) = 1$: either C has no rational point or C is an elliptic curve and its rational points form a finitely generated abelian group by Mordell-Weil theorem. Then by Néron, $N(C,B) \sim_C (\log B)^{r/2}$, where r is the rank of the Jacobian $\text{Jac}(C)$.
+) if $g(C) \geq 2$: according to Mordell's conjecture, now Faltings's Theorem, C has only a finite number of rational points, i.e., $N(C,B) = O_C(1)$. The best known *uniform* bound is due to Ellenberg-Venkatesh [4]. They showed that $N(C,B) \ll_d B^{2/d-\delta}$, where δ is a small constant depending only on d, which they do not specify.

The asymptotic behaviour is similar over any number field if we normalize the heights correctly. Here the genus 0 case is very easy. So the first non-trivial case is when $g(C) = 1$. Apart from smooth plane cubic curves, there is also an important class of genus one curves given by non-singular complete intersections of two quadrics in $\mathbb{P}^3$. The counting problem for that class is discussed in the second paper.

7. Paper II: Uniform bounds for rational points on complete intersections of two quadric surfaces

In Paper II, we study the density of rational points on quartic curves in $\mathbb{P}^3$. In [5], Heath-Brown proved that

$$N(C,B) \ll_\varepsilon B^{2/d+\varepsilon} \tag{16}$$

for arbitrary irreducible space curves over $\mathbb{Q}$ of degree d by means of his p-adic determinant method. Salberger [8] showed a slightly better uniform bound by using his global determinant method

$$N(C,B) \ll B^{2/d} \log B, \tag{17}$$

which was then improved by Walsh [10] to

$$N(C,B) \ll B^{2/d}. \tag{18}$$

So in the case where $d=4$, it is known that $N(C,B) \ll B^{1/2}$.

In Paper II, we consider non-singular quartic curves C in $\mathbb{P}^3$ given by complete intersections of two quadrics. As C is of genus 1, the Jacobian $\mathrm{Jac}(C)$ is again an elliptic curve and we can apply descent theory. We will therefore use the same basic dichotomy as in two articles [4] of Ellenberg and Venkatesh and [6] of Heath-Brown and Testa:
+) For curves of small height we use descent (see (7)) and the determinant method for unramified covers of C. To sum over the descent classes we will also need upper estimates for the rank of $\mathrm{Jac}(C)$ in terms of its discriminant.
+) For curves of large height we use a refinement of the determinant method where we find extra factors in the determinant which come from the coefficients of the quadratic forms defining C.

One difficulty is that we first need to define a height function on a parameter variety of such quartic curves. This is much easier for cubic curves where the height function can be defined by the maximum modulus of coefficients of the polynomial F defining C. Unfortunately the author has not been able to prove the main estimate (25) for general non-singular complete intersections of two quadrics in $\mathbb{P}^3$. So we will only consider the case where C is given by a complete intersection of two simultaneously diagonal quadratic forms.

We first use descent and the global determinant method to prove the following bound for any positive integer m:

$$N(C,B) \ll m^r \left(B^{\frac{1}{2m^2}} + m^2\right) \log B. \tag{19}$$

Taking $m = 1 + [\sqrt{\log B}]$ we obtain

$$N(C, B) \ll (\log B)^{2+r/2}, \tag{20}$$

where r is the rank of Jac(C). These results should be compared with (13) and (14) for cubic curves.

We now suppose that C is given by a complete intersection of two simultaneously diagonal quadratic forms $q = a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ and $r = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 + b_3x_3^2$ with integral coefficients. Then C is smooth if and only if all six minors $d_{ij} = a_ib_j - a_jb_i \neq 0$, $0 \leq i < j \leq 3$. These six minors will satisfy a quadratic Plücker relation. So C is parametrized by a rational point P on a quadric in $\mathbb{P}^5$ with coordinates given by those six minors. We now define the height $H(C)$ of C to be the height of P in $\mathbb{P}^5$. We have thus

$$H(C) := \max_{0 \leq i < j \leq 3}(|d_{ij}|) / \gcd_{0 \leq i < j \leq 3}(d_{ij}).$$

Then we use a refinement of Heath-Brown's p-adic determinant method to prove that

$$N(C, B) \ll_\varepsilon B^{1/2+\varepsilon}/H(C)^{1/8} + B^\varepsilon. \tag{21}$$

This bound is an analog of the bound

$$N(C, B) \ll_\varepsilon B^{2/3+\varepsilon}/H(C)^{1/9} + B^\varepsilon$$

in [4] for plane cubic curves.

We now use a standard 2-descent argument as in Brumer - Kramer [2] to bound the rank r of Jac(C) in terms of its discriminant D. One can prove that for any $c > 1/(2\log 2)$ we have

$$r < c \log|D| + \mathrm{O}_\varepsilon(1).$$

This is discussed by Ellenberg and Venkatesh [4, p. 2177]. In (19), if we take $m = 2$ then

$$N(C, B) \ll 2^r B^{1/8} \log B \ll_\varepsilon |D|^{1/2+\varepsilon} B^{1/8} \log B. \tag{22}$$

The discriminant D of Jac(C) can be computed by means of the formulas in [1, Sections

3.1 and 3.3]. This gives

$$D = 2^{-8} \prod_{0 \le i \ne j \le 3} (a_i b_j - a_j b_i).$$

We can here reduce to the case where (q, r) is a *primitive* pair with $\gcd_{0 \le i < j \le 3}(a_i b_j - a_j b_i) = 1$, in which case we prove that

$$|D| \le H(C)^{12}. \tag{23}$$

From (22) and (23) we obtain that

$$N(C, B) \ll_\varepsilon H(C)^{6+\varepsilon} B^{1/8} \log B. \tag{24}$$

Comparing (21) with (24) we see that the worst case is that in which $H(C) = B^{3/49}$. We then obtain the main result of this paper: Let C be a non-singular complete intersection of two simultaneously diagonal quadrics in $\mathbb{P}^3$. Then

$$N(C, B) \ll_\varepsilon B^{1/2 - 3/392 + \varepsilon}. \tag{25}$$

References

[1] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum and A. R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90**, 2001, no. 2, 304-315.

[2] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44**, 1977, no.4, 715-743.

[3] S. David, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory **64**,

[4] J. Ellenberg and A. Venkatesh, *On uniform bounds for rational points on nonrational curves*, Int. Math. Res. Not. **35**, 2005, 2163-2181.

[5] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Ann. of Math. (2) **155**, 2002, 553-595.

[6] D. R. Heath-Brown, D. Testa, *Counting rational points on cubic curves*, Sci. China Math., **53**, 2010, No. 9, 2259-2268.

[7] P. Salberger, *On the density of rational and integral points on algebraic varieties*, J. Reine Angew. Math. **606**, 2007, 123-147.

[8] P. Salberger, *Counting rational points on projective varieties*, preprint.

[9] J. P. Serre, *Lectures on the Mordell-Weil theorem.*

[10] M. N. Walsh, *Bounded rational points on curves*, Int. Math. Re. Notices **14**, 2015, 5644-5658.