Counting rational points on smooth cubic curves

(article starts on next page)

Counting rational points on smooth cubic curves

Manh Hung Tran

Department of Mathematical Sciences, Chalmers University of Technology, Sweden

A B S T R A C T

We use a global version of Heath-Brown's p-adic determinant method developed by Salberger to give upper bounds for the number of rational points of height at most B on non-singular cubic curves defined over $\mathbb{Q}$. The bounds are uniform in the sense that they only depend on the rank of the corresponding Jacobian.

© 2018 Elsevier Inc. All rights reserved.

1. Introduction

Let $F(X_0, X_1, X_2) \in \mathbb{Z}[X_0, X_1, X_2]$ be a non-singular cubic form, so that $F = 0$ defines a smooth plane cubic curve C in $\mathbb{P}^2$. We want to study the asymptotic behaviour of the counting function

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

with respect to the naive height function $H(P) := \max\{|x_0|, |x_1|, |x_2|\}$ for $P = [x_0, x_1, x_2]$ with co-prime integer values of x_0, x_1, x_2.

E-mail address: manhh@chalmers.se.

It is known that if the rank r of the Jacobian $\mathrm{Jac}(C)$ is positive, then we have

$$N(B) \sim c_F (\log B)^{r/2} \tag{1}$$

as $B \to \infty$. This result was shown by Néron. Moreover, if $r = 0$ then $N(B) \le 16$ by Mazur's theorem (see Mazur [5], Theorem 8) on torsion groups of elliptic curves. But (1) is not a uniform upper bound as the constant c_F depends on C. The aim of this paper is to give uniform upper bounds for $N(B)$ which only depend on the rank of $\mathrm{Jac}(C)$.

In this direction, Heath-Brown and Testa (see [4], Corollary 1.3) established the uniform bound

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

by using the p-adic determinant method developed by the first author (see [3]). In [4], they also used a result of David [1] about the successive minima of the quadratic form given by the canonical height pairing on $\mathrm{Jac}(C)$ to prove the sharper uniform bounds $N(B) \ll (\log B)^{1+r/2}$ for all r and $N(B) \ll (\log B)^{r/2}$ if r is sufficiently large.

We shall in this paper give a direct proof of the bound

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

based on the determinant method, which does not depend on any deep result about the canonical height pairing.

To do this, we follow the approach in [4] with descent. But we replace the p-adic determinant method by a global determinant method developed by Salberger [6]. The main result of this paper is the following

Theorem 1. *Let $F(X_0, X_1, X_2) \in \mathbb{Z}[X_0, X_1, X_2]$ be a non-singular cubic form, so that $F = 0$ defines a smooth plane cubic curve C. Let r be the rank of $\mathrm{Jac}(C)$. Then for any $B \ge 3$ and any positive integer m we have*

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

uniformly in C, with an implied constant independent of m.

This bound improves upon the estimate

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

in [4] (see Theorem 1.2). Taking $m = 1 + [\sqrt{\log B}]$ we immediately obtain the following result.

Corollary 2. *Under the conditions above we have*

$$N(B) \ll (\log B)^{2+r/2}$$

uniformly in C.

In the appendix we include for comparison a short account of the bounds for $N(B)$ that can be deduced from David's result.

2. The descent argument

We shall in this section recall the argument in [4], where the study of $N(B)$ is reduced to a counting problem for a biprojective curve.

Let $\psi : C \times C \to \mathrm{Jac}(C)$ be the morphism to the Jacobian of C defined by $\psi(P, Q) = [P] - [Q]$. Let m be a positive integer and define an equivalence relation on $C(\mathbb{Q})$ as follows: $P \sim_m Q$ if $\psi(P, Q) \in m(\mathrm{Jac}(C)(\mathbb{Q}))$. The number of equivalence classes is at most $16m^r$ by the theorems of Mazur and Mordell–Weil. There is therefore a class K such that

$$N(B) \ll m^r \sharp \{P \in K : H(P) \leq B\}.$$

If we fix a point R in K then for any other point P in K, there will be a further point Q in $C(\mathbb{Q})$ such that $[P] = m[Q] - (m-1)[R]$ in the divisor class group of C. We define the curve $X = X_R$ by

$$X_R := \{(P, Q) \in C \times C : [P] = m[Q] - (m-1)[R]\}$$

in $\mathbb{P}^2 \times \mathbb{P}^2$. Then $N(B) \ll m^r \sharp \mathcal{K}$, where

$$\mathcal{K} := \{(P, Q) \in X(\mathbb{Q}) : H(P) \leq B\}.$$

We have thus reduced the counting problem for C to a counting problem for a biprojective curve X in $\mathbb{P}^2 \times \mathbb{P}^2$. We shall also need the following lemma from [4] (see Lemma 2.1).

Lemma 3. *Let C be a smooth plane cubic curve defined by a primitive form F with $\|F\| \ll B^{30}$, and R be a point in $C(\mathbb{Q})$. There exists an absolute constant A with the following property. Suppose that (P, Q) is a point in $X_R(\mathbb{Q})$ and that $B \geq 3$. Then if $H(P), H(R) \leq B$ we have $H(Q) \leq B^A$.*

3. The global determinant method

We shall in this section apply Salberger's global determinant method in [6] to X and consider congruences between integral points on X modulo all primes of good reduction for C and X. It is a refinement of the p-adic determinant method used in [3] and [4].

We will label the points in $\mathcal{K}$ as (P_j, Q_j) for $1 \leq j \leq N$, say, and fix integers $a, b \geq 1$. Let I_1 be the vector space of all bihomogeneous forms in $(x_0, x_1, x_2; y_0, y_1, y_2)$ of bidegree (a, b) with coefficients in $\mathbb{Q}$ and I_2 be the subspace of such forms which vanish on X. Since the monomials

$$x_0^{e_0} x_1^{e_1} x_2^{e_2} y_0^{f_0} y_1^{f_1} y_2^{f_2}$$

with

$$e_0 + e_1 + e_2 = a \text{ and } f_0 + f_1 + f_2 = b$$

form a basis for I_1, there is a subset of monomials $\{F_1, ..., F_s\}$ whose corresponding cosets form a basis for I_1/I_2. As in [4] (see Lemma 3.1), if $\frac{1}{a} + \frac{m^2}{b} < 3$, then $s = 3(m^2 a + b)$. Thus we shall always assume that $a \geq 1$ and $b \geq m^2$ to make sure that $s = 3(m^2 a + b)$. Consider the $N \times s$ matrix

$$M = \begin{pmatrix} F_1(P_1, Q_1) & F_2(P_1, Q_1) & \dots & F_s(P_1, Q_1) \\ F_1(P_2, Q_2) & F_2(P_2, Q_2) & \dots & F_s(P_2, Q_2) \\ \vdots & \vdots & \dots & \vdots \\ F_1(P_N, Q_N) & F_2(P_N, Q_N) & \dots & F_s(P_N, Q_N) \end{pmatrix}.$$

If we can choose a and b such that $\mathrm{rank}(M) < s$, then there is a non-zero column vector $\underline{c}$ such that $M\underline{c} = \underline{0}$. This will produce a bihomogeneous form G, say, of bidegree (a, b) such that $G(P_j, Q_j) = 0$ for all $1 \leq j \leq N$. Hence all points in $\mathcal{K}$ will lie on the variety $Y \subset \mathbb{P}^2 \times \mathbb{P}^2$ given by $G = 0$, while the irreducible curve X does not lie on Y. Thus

$$N \leq \sharp(X \cap Y) \leq 3(m^2 a + b) \tag{4}$$

by the Bézout-type argument in [4] (see Lemma 5.1).

In order to show that $\mathrm{rank}(M) < s$, we may clearly suppose that $N \geq s$. We will show that each $s \times s$ minor $\det(\Delta)$ of M vanishes. Without loss of generality, let Δ be the $s \times s$ matrix formed by the first s rows of M.

$$\Delta = \begin{pmatrix} F_1(P_1, Q_1) & F_2(P_1, Q_1) & \dots & F_s(P_1, Q_1) \\ F_1(P_2, Q_2) & F_2(P_2, Q_2) & \dots & F_s(P_2, Q_2) \\ \vdots & \vdots & \dots & \vdots \\ F_1(P_s, Q_s) & F_2(P_s, Q_s) & \dots & F_s(P_s, Q_s) \end{pmatrix}.$$

The idea is now to give an upper bound for $\det(\Delta)$ which is smaller than a certain integral factor of $\det(\Delta)$. To do this, we first recall a result from [3] (see Theorem 4).

Lemma 4. *For a plane cubic curve C defined by a primitive integral form F, either $N(B) \leq 9$ or $\|F\| \ll B^{30}$.*

Thus from now on, we may and shall always suppose that $\|F\| \ll B^{30}$. It is not difficult to see that every entry in Δ has modulus at most $B^a B^{Ab}$, where A is the absolute constant in Lemma 3. Since Δ is an $s \times s$ matrix, we get that

$$\log|\det(\Delta)| \le s\log s + s\log B^{a+Ab}. \tag{5}$$

Now we find a factor of $\det(\Delta)$ of the form p^{N_p}, where p is a prime of good reduction for C. In order to do that, we divide Δ into blocks such that elements in each block have the same reduction modulo p.

Let p be a prime number and Q^* be a point on $C(\mathbb{F}_p)$. Then we define the set

$$S(Q^*, p, \Delta) = \{(P_j, Q_j) : 1 \le j \le s, \ \overline{Q_j} = Q^*\},$$

where $\overline{Q_j}$ denotes the reduction from $C(\mathbb{Q})$ to $C(\mathbb{F}_p)$. Suppose $\sharp S(Q^*, p, \Delta) = E$. We consider any $E \times E$ sub-matrix Δ^* of Δ corresponding to $S(Q^*, p, \Delta)$ and recall a result from [4] (see Lemma 4.2). Note that our set $S(Q^*, p, \Delta)$ has fewer elements than the set $S(Q'; p, B)$ defined at the beginning of Section 3 in [4] but the proof still works.

Lemma 5. *If p is a prime of good reduction for C, then $p^{E(E-1)/2}$ divides $\det(\Delta^*)$.*

From this lemma we obtain a factor of $\det(\Delta)$ of the form p^{N_p} by means of Laplace expansion. Moreover, we can do the same argument for all primes of good reduction for C and then obtain a very large factor of $\det(\Delta)$. That is the idea of the global determinant method in [6].

Lemma 6. *Let p be a prime of good reduction for C. There exists a non-negative integer $N_p \ge \frac{s^2}{2n_p} + O(s)$ such that $p^{N_p}|\det(\Delta)$, where n_p is the number of $\mathbb{F}_p$-points on $C(\mathbb{F}_p)$.*

Proof. Let P be a point on $C(\mathbb{F}_p)$ and s_P be the number of elements in $S(P, p, \Delta)$. Then by Lemma 5, there exists an integer $N_P = s_P(s_P - 1)/2$ such that $p^{N_P}|\det(\Delta^*)$ for each $s_P \times s_P$ sub-matrix Δ^* of Δ corresponding to $S(P, p, \Delta)$.

If we apply this to all points on $C(\mathbb{F}_p)$ and use Laplace expansion, then we get that $p^{N_p}|\det(\Delta)$ for

$$N_p = \sum_P N_P = \frac{1}{2}\sum_P s_P{}^2 - \frac{s}{2} \ge \frac{s^2}{2n_p} + O(s)$$

in case C has good reduction at p. This completes the proof of Lemma 6.

We now give a bound for the product of primes of bad reduction for C. Since $\|F\| \ll B^{30}$, the discriminant D_F of F will satisfy $\log|D_F| \ll \log B$. Thus $\log \Pi_C \ll \log B$, where Π_C is the product of all primes of bad reduction for C. We have therefore the following bound.

Lemma 7. *Suppose that $\|F\| \ll B^{30}$. The product Π_C of all primes of bad reduction for C satisfies $\log \Pi_C = O(\log B)$.*

We need one more lemma from [6] (see Lemma 1.10).

Lemma 8. *Let $\Pi > 1$ be an integer and p run over all prime factors of Π. Then*

$$\sum_{p|\Pi} \frac{\log p}{p} \leq \log \log \Pi + 2.$$

Proof. We may and shall assume that Π is a square-free. Let l be a positive integer such that $l \leq \Pi$ and $v_p(n)$ be the highest integer such that $p^{v_p(n)}|n$. We then have (see Tenenbaum [7], pp. 13–14)

$$l \sum_{p|\Pi} \frac{\log p}{p} - \sum_{p|\Pi} \log p \leq \sum_{p|\Pi} v_p(l!)\log p$$

$$\leq \sum_{p \leq \Pi} v_p(l!)\log p = \log l! \leq l\log l,$$

$$\Rightarrow \sum_{p|\Pi} \frac{\log p}{p} \leq \log l + \frac{1}{l} \sum_{p|\Pi} \log p \leq \log l + (1/l)\log \Pi.$$

To obtain the assertion, let $l = [\log \Pi]$ for $\Pi > 2$.

4. Proof of Theorem 1

We now use the lemmas in Section 3 to prove that $\det(\Delta)$ vanishes if s is large enough. Let Π_C be the product of all primes p of bad reduction for C. Then

$$\sum_{p|\Pi_C} \frac{\log p}{p} \leq \log \log B + O(1) \tag{6}$$

by Lemma 7 and Lemma 8. We apply Lemma 6 to the primes $p \leq s$ of good reduction for C and write $\sum\limits_{p \leq s}^{*}$ for a sum over these primes. We then obtain a positive factor T of $\det(\Delta)$ which is relatively prime to Π_C such that

$$\log T \geq \frac{s^2}{2} \sum_{p \leq s}^{*} \frac{\log p}{n_p} + O(s) \sum_{p \leq s}^{*} \log p.$$

The last term is $O(s^2)$ since $\sum_{p \leq s} \log p = O(s)$ (see [7], p. 31). Also,

$$\frac{\log p}{n_p} \geq \frac{\log p}{p} - \frac{(n_p - p)\log p}{p^2}.$$

Moreover, it is well-known that if p is a prime of good reduction for C, then $n_p = p + O(\sqrt{p})$. Thus we conclude that

$$\frac{\log p}{n_p} \geq \frac{\log p}{p} + O\left(\frac{\log p}{p^{3/2}}\right)$$

for all primes p of good reduction for C. Therefore,

$$\sideset{}{^*}\sum_{p \leq s} \frac{\log p}{n_p} \geq \sideset{}{^*}\sum_{p \leq s} \frac{\log p}{p} + O(1)$$

and then

$$\log T \geq \frac{s^2}{2} \sideset{}{^*}\sum_{p \leq s} \frac{\log p}{p} + O(s^2).$$

But by (6),

$$\sum_{p \leq s} \frac{\log p}{p} - \sideset{}{^*}\sum_{p \leq s} \frac{\log p}{p} \leq \log \log B + O(1)$$

and $\sum_{p \leq s} \dfrac{\log p}{p} = \log s + O(1)$ (see [7], p. 14). Hence,

$$\log T \geq \frac{s^2}{2} \log \left(\frac{s}{\log B}\right) + O(s^2). \tag{7}$$

Thus from (5) and (7) we obtain

$$\log \left(\frac{|\det(\Delta)|}{T}\right) \leq s\log s + s\log B^{a+Ab} - \frac{s^2}{2}\log\left(\frac{s}{\log B}\right) + O(s^2)$$

$$= \frac{s^2}{2}\left(\log B^{\frac{2(a+Ab)}{s}} - \log\left(\frac{s}{\log B}\right)\right) + O(s^2).$$

There is therefore an absolute constant $u \geq 1$ such that

$$\log\left(\frac{|\det(\Delta)|}{T}\right) \leq \frac{s^2}{2}\left(\log B^{\frac{2(a+Ab)}{s}} - \log\left(\frac{s}{u\log B}\right)\right).$$

If

$$s > uB^{\frac{2(a+Ab)}{s}} \log B \tag{8}$$

we have in particular that $\log\left(\frac{|\det(\Delta)|}{T}\right) < 0$ and hence $\det(\Delta) = 0$ as $\frac{|\det(\Delta)|}{T} \in \mathbb{Z}_{\geq 0}$.

Remember that $s = 3(m^2a + b)$ if $a \geq 1$ and $b \geq m^2$. We now choose $b = m^2$ and

$$a = 1 + \left[\frac{uB^{\frac{2}{3m^2}} \log B}{m^2} + A \log B \right].$$

Then

$$uB^{\frac{2(a+Ab)}{s}} \log B = uB^{\frac{2(a+Am^2)}{3m^2(a+1)}} \log B$$

$$< uB^{\frac{2}{3m^2}} B^{\frac{2A}{3a}} \log B < s.$$

Thus (8) holds and hence $\det(\Delta) = 0$. Then $\mathrm{rank}(M) < s$ such that there is a bihomogeneous form in $\mathbb{Q}[x_0, x_1, x_2, y_0, y_1, y_2]$ which vanishes at all $(P_j, Q_j) \in X(\mathbb{Q})$, $1 \leq j \leq N$, with $H(P_j) \leq B$ but not everywhere on X. Hence (see (4))

$$N \leq 3(m^2a + b) \ll \left(B^{\frac{2}{3m^2}} + m^2 \right) \log B$$

$$\Rightarrow N(B) \ll m^r \left(B^{\frac{2}{3m^2}} + m^2 \right) \log B.$$

This completes the proof of Theorem 1.

Acknowledgment

Appendix A

In this appendix we record the following more precise version of a result in [4].

Theorem 9. *Let C be any smooth plane cubic curve and r be the rank of Jac(C). Let $m_l = \frac{l^2 - 4l - 4}{8l^2 + 8l}$ for $l \geq 1$. Then*

$$N(B) \ll \begin{cases} (\log B)^{-(m_1 + \ldots + m_r) + r/2}, & \text{if } 1 \leq r < 16; \\ (\log B)^{r/2}, & \text{if } r \geq 16, \end{cases}$$

with an absolute implied constant. In particular, $N(B) \ll (\log B)^{1+r/2}$ for all r.

Proof. The proof is just a careful re-examination of the argument of Heath-Brown and Testa [4]. This argument is based on a result of David [1] about successive minima for the quadratic form Q corresponding to the canonical height on Jac(C). As in [4] (see (11)),

$$N(B) \ll \prod_{j \leq r} \max\left\{1, 4\frac{\sqrt{c\log B}}{M_j}\right\}, \tag{9}$$

where c is an absolute constant and M_j, $j = 1, ..., r$ are successive minima of $\sqrt{Q}$.

We now recall Corollary 1.6 from [1], which shows that if D is the discriminant of $\mathrm{Jac}(C)$ then for all $l \leq r$, $M_l \gg (\log|D|)^{m_l}$, where $m_l = \frac{l^2 - 4l - 4}{8l^2 + 8l}$. Note that David's result refers to the successive minima for Q, while we have given the corresponding results for $\sqrt{Q}$.

In Lemma 4 we saw that $\|F\| \ll B^{30}$ if $N(B) > 9$. There is, therefore, in that case an absolute constant k such that

$$\max\left\{1, 4\frac{\sqrt{c\log B}}{M_j}\right\} \leq k(\log B)^{1/2}(\log|D|)^{-m_j}$$

for $j = 1, ..., r$ since $|m_j| < 1/2$ and $\log|D| \ll \log B$. Hence, if $N(B) > 9$, then from (9) we obtain

$$N(B) \ll k^r(\log B)^{r/2}(\log|D|)^{-(m_1+...+m_r)}. \tag{10}$$

If $1 \leq r < 16$, then $-(m_1 + ... + m_r) > 0$ and the assertion holds. If $r \geq 16$, let $D_0 = \exp(k^{1/m_{16}})$. Then $k(\log|D|)^{-m_j} \leq 1$ for $j > 16$ and $|D| \geq D_0$. Hence

$$N(B) \ll (\log B)^{r/2}(\log|D|)^{-(m_1+...+m_{16})} \ll (\log B)^{r/2}$$

as $-(m_1 + ... + m_{16}) < 0$. When $|D| \leq D_0$ the rank r is bounded and we get the same assertion by (10).

So in any case, $N(B) \ll (\log B)^{r/2}$, if $r \geq 16$. It should thereby be noted that Elkies (see [2]) has shown that there exist elliptic curves of rank $r \geq 28$.

References

[1] S. David, Points de petite hauteur sur les courbes elliptiques, J. Number Theory 64 (1997) 104–129.
[2] N.D. Elkies, $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, May 2006, Number Theory Listserver.
[3] D.R. Heath-Brown, The density of rational points on curves and surfaces, Ann. of Math. (2) 155 (2002) 553–595.
[4] D.R. Heath-Brown, D. Testa, Counting rational points on cubic curves, Sci. China Math. 53 (9) (2010) 2259–2268.
[5] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977) 33–186.
[6] P. Salberger, Counting rational points on projective varieties, preprint.
[7] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, Cambridge University Press, 1995.