TOKYO J. MATH.
VOL. 31, NO. 1, 2008

Integral Points and the Rank of Elliptic Curves over Imaginary Quadratic Fields

Michitaka KOJIMA

Waseda University

(Communicated by Y. Yamada)

Abstract. One of Silverman's results gives a relationship between the number of integral points and the rank of elliptic curves over $\mathbf{Q}$. This paper generalizes this result for all imaginary quadratic fields.

1. Introduction

Let $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbf{Z}[x, y]$ be a homogeneous polynomial of degree 3 with non-zero discriminant. The discriminant is given by

$$\mathrm{disc}(f) = -27a^2d^2 - 4ac^3 + 18abcd - 4b^3d + b^2c^2 .$$

For each non-zero integer $m \in \mathbf{Z}$, let C_m be the projective curve

$$C_m : f(x, y) = mz^3 .$$

The curve C_m is non-singular, since $\mathrm{disc}(f) \neq 0$. Suppose that C_m has a $\mathbf{Q}$-rational point. Then C_m has a structure of an elliptic curve defined over $\mathbf{Q}$. It is well known that the set $C_m(\mathbf{Q})$ forms a finitely generated abelian group, and the order of its torsion part is bounded by 16. Namely the size of $C_m(\mathbf{Q})$ is measured by $\mathrm{rank}(C_m(\mathbf{Q}))$, the Mordell-Weil rank of $C_m(\mathbf{Q})$. On the other hand, Siegel proved the following fundamental result about the number of integral points:

THEOREM (Siegel [9] Ch. 9). *The number $N_f(m)$ of solutions $(x, y) \in \mathbf{Z}^2$ of the equation $f(x, y) = m$ is finite.*

The method developed by J. Silverman allows one to give an effective bound for $N_f(m)$ in terms of $\mathrm{rank}(C_m(\mathbf{Q}))$.

THEOREM (J. Silverman [6]). *There are constants κ and m_0, with κ absolute and m_0 depending on f, so that for all cube-free integers m satisfying $|m| > m_0$,*

$$N_f(m) < \kappa^{\mathrm{rank}(C_m(\mathbf{Q}))+1} .$$

Received October 2, 2006; revised December 1, 2006

One naturally asks if this result can be generalized for any number field. In the following, we formulate our problem.

Let K be a number field and let $f(x, y) \in o_K[x, y]$ be a homogeneous polynomial of degree 3 with distinct roots in $\bar{K}$. For each non-zero integer $\beta \in o_K$, let

$$N_f(\beta) = \#\{(x, y) \in o_K \times o_K \,|\, f(x, y) = \beta\} \tag{1}$$

and let C_β be the smooth curve

$$C_\beta : f(x, y) = \beta z^3 . \tag{2}$$

From Siegel's theorem, $N_f(\beta)$ is finite and if $N_f(\beta) > 0$, then C_β has a structure of an elliptic curve defined over K.

Now we state our problem. In view of Silverman's result and the main theorem of this paper, it may be called a conjecture.

CONJECTURE. *There are constants $\kappa > 0$, $M > 0$ with κ depending only on K and M depending on f such that, for all cube-free integers $\beta \in o_K$ (i.e., integers divisible by no cube of prime ideals of K) satisfying $H_K(\beta) \geq M$, we have*

$$N_f(\beta) < \kappa^{\operatorname{rank} C_\beta(K)+1} ,$$

where H_K is a height function (see section 2).

Our main result asserts that this conjecture is true for the case where K is an imaginary quadratic field.

THEOREM A. *The conjecture is true for the case where K is an arbitrary imaginary quadratic field.*

The proof of Theorem A consists of three steps. First, we give an upper bound for the height of the integral solutions to the equation $f(x, y) = \beta$ (Proposition B). Next, we look at the rational points on elliptic curves of the form

$$E_{\beta D} : y^2 = x^3 + \beta D$$

and prove a similar bound for the number of points whose height is bounded in a certain fashion (Proposition C). Finally we map the equation $f(x, y) = \beta$ to its Jacobian, which has a Weierstrass model of the form $E_{\beta D}$, and this allows us to combine the previous two steps to bound the number of integral solutions to the equation $f(x, y) = \beta$.

2. The Size of Solutions

In this section we give an upper bound for the height of the integral solutions to the equation $f(x, y) = \beta$. Before stating our proposition, we set notations and review the definitions of the height functions briefly.

DEFINITIONS. Let M_K be a complete set of primes of K. For each $v \in M_K$, let $|\cdot|_v$ be the normalized valuation on K which belongs to v and let $n_v = [K_v : \mathbf{Q}_v]$ be the local degree at v, where a normalized valuation means that its restriction to $\mathbf{Q}$ is one of the normalized valuations on $\mathbf{Q}$. Let $P \in \mathbf{P}^N(K)$ be a point with homogeneous coordinates

$$P = [x_0, \dots, x_N], \quad x_i \in K .$$

The height of P (relative to K) is defined by

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \dots, |x_N|_v\}^{n_v} .$$

Further, the absolute height H and the absolute logarithmic height h of P are defined by

$$H(P) = H_K(P)^{1/[K:\mathbf{Q}]} \quad \textit{and} \quad h(P) = \log H(P) ,$$

respectively.

Also for each $x \in K$ the three types of heights of x are defined as follows

$$H_K(x) = H_K([x, 1]) , \quad H(x) = H([x, 1]) \quad \text{and} \quad h(x) = \log H(x) .$$

Finally, let E/K be an elliptic curve defined over K and let $g \in \bar{K}(E)$ be a non-constant even function. Then for each $P \in E(\bar{K})$ the absolute height H_g, the absolute logarithmic height h_g, and the canonical height $\hat{h}$ (relative to g) are defined by

$$H_g(P) = H(g(P)) , \quad h_g(P) = h(g(P)) \quad \text{and} \quad \hat{h}(P) = \frac{1}{\deg(g)} \lim_{n \to \infty} 4^{-n} h_g([2^n]P) ,$$

respectively.

Now we state our proposition.

PROPOSITION B. *Let K be an imaginary quadratic field and $f(x, y) \in o_K[x, y]$ a homogeneous polynomial of degree 3 with non-zero discriminant. Then there are constants $c > 0$ and $\gamma > 0$ with c depending only on K and γ depending on f so that for all non-zero integers $\beta \in o_K$ the integral solutions $(x, y) \in o_K \times o_K$ to the equation $f(x, y) = \beta$ satisfy*

$$H(x) , H(y) < \gamma H(\beta)^c .$$

PROOF. Write

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 (a, b, c, d \in o_K) .$$

We will prove that there are constants $c' > 0$ and $\gamma' > 0$ with c' depending only on K and γ' depending on f so that

$$x, y \in o_K , \ f(x, y) \neq 0 \Longrightarrow H(f(x, y)) > \gamma' \max(H(x), H(y))^{c'} . \tag{3}$$

Once this is done, substituting (3) for $f(x, y) = \beta$ gives the desired result. We consider several cases, and then taking the minimum of c' and γ' obtained by each case gives the desired inequality.

First, we consider the case $y = 0$. Then $f(x, y) = ax^3$. If $a = 0$, then $f(x, y) = 0$ and there is nothing to prove. If $a \neq 0$, then

$$H(f(x, y)) = |a|H(x)^3 (x \neq 0) .$$

Hence we can take $c' = 3$, $\gamma' < |a|$ to obtain the inequality (3). Similarly one can obtain the inequality in the case $x = 0$.

Next, we consider the case $y \neq 0$ and $H(x) \leq H(y)$. Let $\zeta_1, \zeta_2, \zeta_3 \in \mathbf{C}$ be distinct roots of $f(x, 1)$. Then

$$f(x, y) = ay^3 \left(\frac{x}{y} - \zeta_1\right)\left(\frac{x}{y} - \zeta_1\right)\left(\frac{x}{y} - \zeta_1\right) . \tag{4}$$

Let $\Delta = \min\{|\zeta_i - \zeta_j| \ |i \neq j\}$. If $\left|\frac{x}{y} - \zeta_i\right| > \frac{\Delta}{2}$ for all $i = 1, 2, 3$, then from (4)

$$H(f(x, y)) = |f(x, y)| > |a|\left(\frac{\Delta}{2}\right)^3 H(y)^3 .$$

So taking $c' = 3$, $\gamma' = |a|\left(\frac{\Delta}{2}\right)^3$ gives the desired inequality.

In the following, we consider the case $\left|\frac{x}{y} - \zeta_{i_0}\right| \leq \frac{\Delta}{2}$ for some i_0. Note that if $i \neq i_0$ then $\left|\frac{x}{y} - \zeta_i\right| \geq \frac{\Delta}{2}$, since it follows from the triangular inequality that

$$\left|\frac{x}{y} - \zeta_i\right| \geq \left|\zeta_{i_0} - \zeta_i\right| - \left|\zeta_{i_0} - \frac{x}{y}\right| \geq \Delta - \frac{\Delta}{2} = \frac{\Delta}{2} .$$

Hence

$$H(f(x, y)) = |f(x, y)| \geq |a|\left(\frac{\Delta}{2}\right)^2 |y|^3 \left|\frac{x}{y} - \zeta_{i_0}\right| . \tag{5}$$

We will find the lower bound for $\left|\frac{x}{y} - \zeta_{i_0}\right|$. Write $K = \mathbf{Q}(\omega)$ ($\omega = \sqrt{-m}$, $m \in \mathbf{N}$) and $\frac{x}{y} = c + d\omega$ ($c, d \in \mathbf{Q}$). We can also write

$$\zeta_{i_0} = c_{i_0} + d_{i_0}\omega \ (c_{i_0}, d_{i_0} \in \mathbf{R}) ,$$

since $1, \omega \in \mathbf{C}$ are linearly independent over $\mathbf{R}$. One can easily see that $c_{i_0}, d_{i_0} \in \bar{\mathbf{Q}}$. Then

$$\left|\frac{x}{y} - \zeta_{i_0}\right| = \sqrt{(c - c_{i_0})^2 + m(d - d_{i_0})^2} \geq \max\{|c - c_{i_0}|, |d - d_{i_0}|\} . \tag{6}$$

If $c = c_{i_0}, d = d_{i_0}$, then $f(x, y) = 0$ and there is nothing to consider. So assume that $c \neq c_{i_0}$ or $d \neq d_{i_0}$. We consider the former case. One can deal similarly with the later case. Fix a number ε such that $0 < \varepsilon < 1$ ($\varepsilon = 1/2$). Then Roth's theorem (see [3] or [9] Ch. 9) says that for all but finitely many $c \in \mathbf{Q}$

$$|c - c_{i_0}| > H(c)^{-(2+\varepsilon)} .$$

Hence, there is a sufficiently small $\gamma_{i_0} > 0$ such that for all $c \in \mathbf{Q}$ different from c_{i_0}

$$|c - c_{i_0}| > \gamma_{i_0} H(c)^{-(2+\varepsilon)} . \tag{7}$$

Substituting (6) into (7) implies

$$\left| \frac{x}{y} - \zeta_{i_0} \right| > \gamma_{i_0} H(c)^{-(2+\varepsilon)} . \tag{8}$$

On the other hand

$$H(c) = H\left(\frac{1}{2}\left(\frac{x}{y} + \overline{\left(\frac{x}{y}\right)}\right)\right) \leq \gamma' H\left(\frac{x}{y}\right) \leq \gamma' \max\{H(x)\, , H(y)\} = \gamma' H(y)\, , \tag{9}$$

where $\gamma' = H(\frac{1}{2}) \cdot 4$. (Note that $H(\alpha) = H(\bar{\alpha})$ for $\alpha \in K$.) Substituting (8) into (9) implies

$$\left| \frac{x}{y} - \zeta_{i_0} \right| > \gamma'_{i_0} H(y)^{-(2+\varepsilon)} . \tag{10}$$

Finally, substitution (5) into (10) yields

$$H(f(x, y)) \geq |a| \left(\frac{\Delta}{2}\right)^2 \gamma'_{i_0} H(y)^{1-\varepsilon} .$$

This is the desired result. One can deal similarly with the remaining case $x \neq 0$, $H(x) \geq H(y)$.

3. The Equation $y^2 = x^3 + \beta D$

In this section we study the rational points on the elliptic curve $E_{\beta D} : y^2 = x^3 + \beta D$ as β varies, and prove a result similar to Theorem A for the number of points whose height is bounded by an expression of the form $ch(\beta) + \gamma$.

PROPOSITION C. *Let $D(\neq 0) \in o_K$, $c > 0$, and $\gamma \in \mathbf{R}$ be given and K is an imaginary quadratic field. Then there are constants c_1, c_2, c_3 depending only on K and a constant $M > 0$ depending on D, c, γ such that for all sixth-power-free integers β satisfying $H_K(\beta) \geq M$,*

$$\#\{P \in E_{\beta D}(K) | h_x(P) < c\, h(\beta) + \gamma\} < c_1(c_2\sqrt{c + c_3} + 1)^{\operatorname{rank} E_{\beta D}(K)} .$$

In the following, we will use $c_1, c_2, \cdots$ to denote positive constants depending only on K, and $\gamma_1, \gamma_2, \cdots$ to denote constants which may depend on D and γ. Before proving Proposition C, we first collect a number of preliminary results.

LEMMA 1. $\#(E_{\beta D}(K))_{tor} \leq c_4$.

PROOF. Merel [1] shows for an arbitrary number field K, there is a constant c depending only on $[K : \mathbf{Q}]$ such that for all elliptic curves E/K

$$\#E(K)_{tor} \leq c \,.$$

LEMMA 2. *Let E be an elliptic curve defined over a number field K. Then the canonical height $\hat{h}$ has the following properties.*

i) $\hat{h}(P) \geq 0$ *for all* $P \in E(K)$. *Moreover* $\hat{h}(P) = 0$ *if and only if* $P \in E(K)_{tor}$.

ii) $\hat{h}(P)$ *depends only on the coset* $P + E(K)_{tor}$.

Thus there is a natural map

$$\hat{h} : E(K)/E(K)_{tor} \to \mathbf{R}\,,$$

and this is a positive definite quadratic form on the lattice $E(K)/E(K)_{tor}$.

PROOF. See in the monograph of Silverman [9, Theorem 9.3 and Remark 9.4 in Ch.VIII].

LEMMA 3. *Let $\beta \in o_K$ be a non-zero integer and P be a point on $E_{\beta D}(K)$. Then*

$$|2\hat{h}(P) - h_x(P)| < c_5 h(\beta) + \gamma_1 \,.$$

PROOF. See Chap. VIII Exercise 8.18(b) in [9] or[11].

LEMMA 4. *Let $\beta \in o_K$ be a non-zero integer and P be a non-torsion point on $E_{\beta D}(K)$. Then*

$$\hat{h}(P) > c_6 \log N_K(\mathfrak{D}_{E_{\beta D}/K})\,,$$

where $\mathfrak{D}_{E_{\beta D}/K}$ is the minimal discriminant of $E_{\beta D}/K$ and $N_K(\mathfrak{D}_{E_{\beta D}/K})$ is the absolute norm of $\mathfrak{D}_{E_{\beta D}/K}$.

PROOF. There is a conjecture by Serge Lang, which asserts for any elliptic curve E defined over a number field K and a non-torsion point $P \in E(K)$

$$\hat{h}(P) > c_1 \log N_K(\mathfrak{D}_{E/K}) + c_2\,,$$

where c_1, c_2 are positive constants depending only on K. This conjecture is true for elliptic curves with integral j-invariant. (See [8] or [10].) Since the j-invariant of $E_{\beta D}$ is 0, this completes the proof.

LEMMA 5. *For all sixth-power-free integers $\beta \in o_K$,*

$$\log N_K(\mathfrak{D}_{E_{\beta D}/K}) > c_7 h(\beta) - \gamma_2 \,.$$

PROOF. We use the fact that β is sixth-power-free. The discriminant of the Weierstrass model

$$E_{\beta D} : y^2 = x^3 + \beta D$$

is $\Delta = -16 \cdot 27(\beta D)^2$. Since β is sixth-power-free, this model is already minimal for all but primes which divide $6D$. Write $(\beta) = \mathfrak{b}\mathfrak{b}'$ as a product of two ideals with $(\mathfrak{b}, 6D) = 1$ and $\mathfrak{b}'$ contains only primes dividing $6D$ as prime divisors. Then

$$\mathfrak{b}^2 | \mathfrak{D}_{E_{\beta D}/K} \, , \, \mathfrak{b}' | (6D)^5 \, .$$

Note that since $\mathfrak{b}'$ is sixth-power-free, any exponent in the factorization of the ideal $\mathfrak{b}'$ as a product of prime ideal of K is at most 5. Hence,

$$\begin{aligned} \log N_K(\mathfrak{D}_{E_{\beta D}/K}) &\geq \log N_K(\mathfrak{b}^2) \\ &= 2 \log N_K(\mathfrak{b}) \\ &= 2 \log N_K(\beta/\mathfrak{b}') \\ &= 2(\log N_K(\beta) - \log N_K(\mathfrak{b}')) \\ &\geq 2 \log N_K(\beta) - 10 \log N_K(6D) \\ &= 4h(\beta) - 10 \log N_K(6D) \, . \end{aligned}$$

LEMMA 6. *Let Λ be a lattice of rank r with a positive definite quadratic form Q. Let*

$$A = \min\{Q(\lambda) | \lambda \in \Lambda \, , \, \lambda \neq 0\} \, .$$

Then for all positive constants B

$$\#\{\lambda \in \Lambda | Q(\lambda) \leq B\} \leq (2\sqrt{B/A} + 1)^r \, .$$

PROOF. Let N be the least integer greater than $2\sqrt{B/A}$. We will prove that the natural map

$$\{\lambda \in \Lambda | Q(\lambda) \leq B\} \to \Lambda / N\Lambda$$

$$\lambda \mapsto \lambda + N\Lambda$$

is injective. Suppose that it is not injective. Choose $\lambda_1, \lambda_2 \in \Lambda$ $(Q(\lambda_i) \leq B (i = 1, 2) \, , \, \lambda_1 \neq \lambda_2)$ such that

$$\lambda_1 + N\Lambda = \lambda_2 + N\Lambda \, .$$

Then there is an element $\mu \in \Lambda$ $(\neq 0)$ such that $\lambda_1 - \lambda_2 = N\mu$.

Hence,

$$\begin{aligned} 0 < Q(\mu) = Q(\lambda_1 - \lambda_2)/N^2 &\leq (Q(\lambda_1) + Q(\lambda_2) + 2\sqrt{Q(\lambda_1)Q(\lambda_2)})/N^2 \\ &= (\sqrt{Q(\lambda_1)} + \sqrt{Q(\lambda_2)})^2/N^2 \\ &\leq (\sqrt{B} + \sqrt{B})^2/N^2 = 4B/N^2 < A \, . \end{aligned}$$

This contradicts the definition of A. Thus the map is injective. Then

$$\#\{\lambda \in \Lambda | Q(\lambda) \leq B\} \leq \#\Lambda/N\Lambda = N^r \leq (2\sqrt{B/A} + 1)^r \, .$$

PROOF OF PROPOSITION C. Let $\beta \in o_K$ be a sixth-power-free integer. We use Lemma 3, Lemma 2, and Lemma 1 successively.

$$\begin{aligned}
&\#\{P \in E_{\beta D}(K) | h_x(P) < c\,h(\beta) + \gamma\} \\
&\quad \leq \#\left\{P \in E_{\beta D}(K) | \hat{h}(P) < \frac{1}{2}\big(c + c_5\big)h(\beta) + \gamma_3\right\} \\
&\quad = \#(E_{\beta D}(K)_{tor}) \cdot \#\left\{\bar{P} \in E_{\beta D}(K)/E_{\beta D}(K)_{tor} | \hat{h}(P) < \frac{1}{2}\big(c + c_5\big)h(\beta) + \gamma_3\right\} \\
&\quad \leq c_4 \cdot \#\left\{\bar{P} \in E_{\beta D}(K)/E_{\beta D}(K)_{tor} | \hat{h}(P) < \frac{1}{2}\big(c + c_5\big)h(\beta) + \gamma_3\right\}.
\end{aligned}$$

On the other hand, if $\bar{P}(\neq \bar{0}) \in E_{\beta D}(K)/E_{\beta D}(K)_{tor}$, then it follows from Lemmas 4 and 5 that

$$\hat{h}(\bar{P}) > c_6 \log N_K(\mathfrak{D}_{E_{\beta D}/K}) > c_6(c_7 h(\beta) - \gamma 2) = c_8 h(\beta) - \gamma_4 .$$

Now apply Lemma 6 to the lattice $\Lambda = E_{\beta D}(K)/E_{\beta D}(K)_{tor}$ and the positive definite quadratic form $Q = \hat{h}$, with

$$A > c_8 h(\beta) - \gamma_4$$

and

$$B = \frac{1}{2}(c + c_5)h(\beta) + \gamma_3 .$$

This yields

$$\#\{P \in E_{\beta D}(K) | h_x(P) < c\,h(\beta) + \gamma\} < c_4 \left(2\sqrt{\frac{\frac{1}{2}(c + c_5)h(\beta) + \gamma_3}{c_8 h(\beta) - \gamma_4}} + 1\right)^{\operatorname{rank} E_{\beta D}(K)} .$$

Now if $H_K(\beta)$ is arbitrarily large, then $h(\beta)$ becomes large. Thus

$$\frac{\frac{1}{2}(c + c_5)h(\beta) + \gamma_3}{c_8 h(\beta) - \gamma_4} \to \frac{\frac{1}{2}(c + c_5)}{c_8} .$$

Hence, there is a sufficiently large constant M depending on D and γ such that for all sixth-power-free integers $\beta \in o_K$ such that $H_K(\beta) \geq M$

$$\frac{\frac{1}{2}(c + c_5)h(\beta) + \gamma_3}{c_8 h(\beta) - \gamma_4} < \frac{c + c_5}{c_8} .$$

Then we have

$$\#\{P \in E_{\beta D}(K) | h_x(P) < c\,h(\beta) + \gamma\} < c_4 \left(2\sqrt{\frac{c + c_5}{c_8}} + 1\right)^{\operatorname{rank} E_{\beta D}(K)} .$$

This is the desired result if we set $c_1 = c_4$, $c_2 = \sqrt{\frac{2}{c_8}}$, $c_3 = c_5$.

4. Proof of Main Theorem

THEOREM A. *Let K be an arbitrary imaginary quadratic field and let $N_f(\beta)$ and C_β be the same as in Section 1. (For the definitions of these, see Section 1 (1), (2) respectively.) Then there are constants $\kappa > 0$, $M > 0$ with κ depending only on K and M depending on f, such that for all cube-free integers $\beta \in o_K$ satisfying $H_K(\beta) \geq M$, we have*

$$N_f(\beta) < \kappa^{\operatorname{rank} C_\beta(K)+1} .$$

PROOF. As before, $c, c_1, c_2, \ldots$ will denote constants depending only on K, and $\gamma, \gamma_1, \gamma_2, \cdots$ will be constants depending on f. Write

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 (a, b, c, d \in o_K) .$$

The discriminant of the polynomial f is given by

$$D = \operatorname{disc}(f) = -27a^2d^2 - 4ac^3 + 18abcd - 4b^3d + b^2c^2 .$$

Let J_β be the Jacobian of C_β. (For the definition of C_β, see Section 1 (2).) Then J_β has a model

$$J_\beta : y^2z = x^3 - 432\beta^2Dz^3 .$$

We have a map of degree 3, defined over K, given by

$$\phi : C_\beta \to J_\beta$$

$$[x, y, z] \mapsto [-4zG(x, y), 4H(x, y), z^3] ,$$

where $G(x, y)$ and $H(x, y)$ are the covariant polynomials of f of degree 2 and 3, respectively. They are given by

$$\begin{aligned} G(x, y) &= (3ac - b^2)x^2 + (9ad - bc)xy + (3bd - c^2)y^2 \\ H(x, y) &= (27a^2d - 9abc + 2b^3)x^3 - 3(6ac^2 - b^2c - 9abd)x^2y \\ &\quad +3(6b^2d - bc^2 - 9acd)xy^2 - (27ad^2 - 9bcd + 2c^3)y^3 . \end{aligned}$$

(For the derivation of these formulas, see [4, pp. 175–178].)

Let $(x, y) \in o_K \times o_K$ be a solution of $f(x, y) = \beta$. Then from Proposition B

$$H(x), H(y) < \gamma_1 H(\beta)^{c_4} .$$

Thus

$$h_x(\phi([x, y, 1])) = h(-4G(x, y)) = \log H(-4G(x, y)) < 2c_4h(\beta) + \gamma_2 .$$

Now we apply Proposition C with $(\beta, D, c, \gamma) = (\beta^2, -432D, 2c_4, \gamma_2)$. (Note that β is cube-free, so that β^2 is sixth-power-free as required in Proposition C.) We obtain an upper bound

$$\#\{P \in J_\beta(K) | h_x(P) < 2c_4 h(\beta) + \gamma_2\} < c_1(c_2\sqrt{2c_4 + c_3} + 1)^{\operatorname{rank} J_\beta(K)}$$

for sufficiently large $H_K(\beta)$. Since $\deg(\phi) = 3$ and $\operatorname{rank}(J_\beta(K)) = \operatorname{rank}(C_\beta(K))$,

for all cube-free integers β whose height $H_K(\beta)$ is sufficiently large, we obtain

$$N_f(\beta) < 3c_1(c_2\sqrt{2c_4 + c_3} + 1)^{\operatorname{rank}(J_\beta(K))} \le \kappa^{\operatorname{rank}(C_\beta(K))+1},$$

where $\kappa = \max(3c_1, c_2\sqrt{2c_4 + c_3} + 1)$ is a constant depending only on K.

References

[1] MEREL, L., Bounds for the torsion of elliptic curves over number fields, Invent. Math. **124** (1996), 437–449.

[2] LANG, S., *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, 1978.

[3] LANG, S., *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.

[4] SALMON, G., *Lessons Introductory to the Modern Higher Algebra*, 3rd ed., Cambridge:Hodges, Foster, and Co. 1876.

[5] SILVERMAN, J., Computing Heights on Elliptic Curves, Math. Comp. **51** (1988), 339–358.

[6] SILVERMAN, J., Integer Points and the Rank of Thue Elliptic Curves, Invent. Math. **66** (1982), 395–404.

[7] SILVERMAN, J., Integer points on curves of genus 1, J. London Math. Soc. **28** (1983), 1–7.

[8] SILVERMAN, J., Lower bound for the canonical height on elliptic curves, Duke Math.J. **48** (1981), 633–648.

[9] SILVERMAN, J., *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[10] SILVERMAN, J., The canonical height and integral points on elliptic curves, Invent. Math. **93** (1988), 419–450.

[11] SILVERMAN, J., The difference between the Weil height and the canonical height on elliptic curves, Math. Comp. **55** (1990), 723–743.

Present Address:
DEPARTMENT OF MATHEMATICS,
SCHOOL OF FUNDAMENTAL SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
TOKYO, JAPAN.