PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 104, Number 1, September 1988

ELLIPTIC CURVES WITH NO RATIONAL POINTS

JIN NAKAGAWA AND KUNIAKI HORIE

(Communicated by Larry J. Goldstein)

ABSTRACT. The existence of infinitely many elliptic curves with no rational points except the origin ∞ is proved by refining a theorem of Davenport-Heilbronn. The existence of infinitely many quadratic fields with the Iwasawa invariant $\lambda_3 = 0$ is proved at the same time.

1. Introduction. One of the main purpose of this paper is to give a new proof of the existence of infinitely many elliptic curves over $\mathbf{Q}$ with trivial Mordell-Weil group. This fact is in principal well known. It is an immediate consequence of theorems which have been in the literature for several years. Indeed, let $E/\mathbf{Q}$ be an elliptic curve with complex multiplication by the ring of integers in an imaginary quadratic field K of class number one. By a theorem of Waldspurger, there exist infinitely many primitive quadratic characters χ such that $L(1, E^\chi) \neq 0$, where E^χ is the twist of E by χ. Then the Coates-Wiles theorem implies that $E^\chi(\mathbf{Q})$ is finite. If we choose E or K appropriately (for example, if we take the discriminant of $K < -8$), then the theory of complex multiplication shows that $E^\chi_{\mathrm{tors}}(\mathbf{Q}) = 0$, whence $E^\chi(\mathbf{Q}) = 0$.

In this paper, we use a completely different method to prove the above fact. The nonexistence of rational solutions of Diophantine equations $y^2 = x^3 + a$ ($a \neq 0$ is an integer) has been studied by Fueter, Brunner, Mordell and K.-L. Chang. They gave sufficient conditions for insolvabilities in terms of some invariants of the quadratic fields $\mathbf{Q}(\sqrt{a})$, $\mathbf{Q}(\sqrt{-3a})$ (see Mordell [**10**, Chapter 26]). The simplest condition among these is the one given by Fueter. Let k be an imaginary quadratic field and denote by Δ_k and h_k the discriminant of k and the class number of k respectively. He proved in [**6**] that if k satisfies the condition

$$(*) \qquad \Delta_k \equiv 2 \bmod 9, \quad \Delta_k \equiv 8 \text{ or } 12 \bmod 16, \quad 3 \nmid h_k,$$

then the elliptic curve $y^2 = x^3 + \Delta_k$ has no rational points except the origin ∞.

On the other hand, P. Hartung proved that there exist infinitely many imaginary quadratic fields with class numbers not divisible by 3. In his lecture at Osaka University in 1970, K. Iwasawa pointed out that if we extend Hartung's result with the condition $(*)$, then we have a proof of the existence of infinitely many elliptic curves defined over $\mathbf{Q}$ with no rational points except the origin ∞.

We shall extend Hartung's result with any congruence conditions on the discriminants by refining Davenport-Heilbronn [**4**, Theorem 3]. Let m, N be two positive

Received by the editors May 5, 1987 and, in revised form, July 28, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 10B10; 10B15; Secondary 12A25, 12A50.

Key words and phrases. Elliptic curve, rational point, Iwasawa invariant, class number.

integers satisfying the condition.

(**) If an odd prime number p is a common divisor of m and N, then $p^2 \mid N$ and $p^2 \nmid m$. Further if N is even, then (i) $4 \mid N$ and $m \equiv 1 \bmod 4$ or (ii) $16 \mid N$ and $m \equiv 8$ or $12 \bmod 16$.

For $x > 0$, denote by $N_2^+(x, m, N)$ (resp. $N_2^-(x, m, N)$) the number of real (resp. imaginary) quadratic fields k with $|\Delta_k| < x$ and $\Delta_k \equiv m \bmod N$. We also denote by $N_2^+(x)$ (resp. $N_2^-(x)$) the number of real (resp. imaginary) quadratic fields k with $|\Delta_k| < x$. For a quadratic field k, denote by $h_3^*(\Delta_k)$ the number of ideal classes of k whose cubes are principal. We shall prove the following theorem.

THEOREM 1. *Notation and assumptions being as above, we have*

$$\sum_{0<\Delta<x,\ \Delta\equiv m \bmod N} h_3^*(\Delta) \sim (\tfrac{4}{3})N_2^+(x, m, N) \qquad (x \to \infty),$$

$$\sum_{-x<\Delta<0,\ \Delta\equiv m \bmod N} h_3^*(\Delta) \sim 2N_2^-(x, m, N) \qquad (x \to \infty).$$

Using a trivial estimate, we immediately obtain the following theorem by Theorem 1 and Proposition 2 in the next section.

THEOREM 2.

$$\liminf_{x\to\infty}(\#\{\text{imag.quad.}f.k; |\Delta_k| < x, \ \textit{satisfying}\ (*)\}/x) \geq 1/16\pi^2.$$

In particular, there exist infinitely many elliptic curves defined by $y^2 = x^3 + a$ $(a \in \mathbf{Z})$ *with no rational points except the origin* ∞.

There is another application of Theorem 1. Let k be a quadratic field. For a prime number p, denote by $\lambda_p(k)$ the Iwasawa λ-invariant associated with the basic $\mathbf{Z}_p$-extension over k. It is well known that $\lambda_p(k) = 0$ if p is not decomposed in k and does not divide h_k. Hence for $p = 3$, $\lambda_3(k) = 0$ if $\Delta_k \not\equiv 1 \bmod 3$ and $3 \nmid h_k$. Using a trivial estimate, we immediately obtain the following theorem by Theorem 1 and Proposition 2 in the next section.

THEOREM 3.

$$\liminf_{x\to\infty}(\#\{\text{imag.quad.}f.k; |\Delta_k| > x, \ \lambda_3(k) = 0\}/N_2^-(x)) \geq 5/16,$$

$$\liminf_{x\to\infty}(\#\{\text{real quad.}f.k; |\Delta_k| < x, \ \lambda_3(k) = 0\}/N_2^+(x)) \geq 25/48.$$

In particular, there exist infinitely many imaginary (resp. real) quadratic fields k *with* $\lambda_3(k) = 0$.

REMARK. Actually, for any given prime number p, there exist infinitely many imaginary quadratic fields k with $\lambda_p(k) = 0$ (cf. [**9**]).

For hyperelliptic curves, we shall prove the following two results (we understand 'elliptic' is a special case of 'hyperelliptic').

THEOREM 4. *Let* n *be a positive integer divisible by* 3, 4, 5, 7, *or* 11. *Then there exist infinitely many hyperelliptic curves defined by* $Dy^2 = 4x^n - 1$ $(D \in \mathbf{Z})$ *with no rational points.*

THEOREM 5. *For any positive integer g, there exist infinitely many hyperelliptic curves of genus g defined over $\mathbf{Q}$ with no integral points.*

2. Proof of Theorem 1. We first summarize the main idea of the Davenport-Heilbronn proof. If $1, \omega, \nu$ is an integral basis of a cubic field K with discriminant Δ_k, then to each such field one may associate an irreducible, primitive, binary cubic form F_K by putting $F_K(x,y) = \Delta_K^{-1/2}\Delta^{1/2}(\omega x + \nu y)$, where $\Delta(\alpha)$ denotes the discriminant of α. This mapping is one-to-one between the set of cubic fields K such that the normal closure of K is unramified over the quadratic field $\mathbf{Q}(\Delta_K^{1/2})$ and a certain subset V of the classes of binary cubic forms with coefficients in $\mathbf{Z}$. Applying formulae for the class numbers of binary cubic forms, one obtains asymptotic formulae for the numbers of such cubic fields, which are written in terms of the 3-class numbers of quadratic fields by class field theory.

A crucial point is that the subset V is determined by infinitely many congruence conditions on the coefficients of F, and we see that the same argument works when we modify the congruence conditions at finitely many primes. Hence the problem is reduced to some local computations.

Let m, N be two positive integers. Denote by Φ_N the set of primitive binary cubic forms with coefficients in $\mathbf{Z}/N\mathbf{Z}$. Here "primitive" means that the coefficients generate the unit ideal $\mathbf{Z}/N\mathbf{Z}$. Put $\Phi_N(m) = \{f \in \Phi_N; D(f) = m \bmod N\}$, where $D = D(f) = 18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2$ is the discriminant of $f = ax^3 + bx^2y + cxy^2 + dy^3$. We see by checking the proof of [**4**, Theorem 3] that to prove Theorem 1, it suffices to prove the following two propositions.

PROPOSITION 1. *Let m, N be two positive integers satisfying the condition $(**)$. Then we have*

$$\frac{\#\Phi_N(m)}{\#\Phi_N} = \varphi(N)^{-1}\prod_{p|N} q(p+1)^{-1}(1-p^{-2})^2(1-p^{-4})^{-1},$$

where p runs over all the prime divisors of N and $q = 4$ if $p = 2$, $q = p$ otherwise, and φ is the Euler function.

PROPOSITION 2. *Let m, N be as in Proposition 1. Then we have*

$$N_2^+(x,m,N) \sim N_2^-(x,m,N) \sim \left\{\varphi(N)^{-1}\prod_{p|N} q(p+1)^{-1}\right\} 3\pi^{-2}x \qquad (x \to \infty).$$

Proposition 2 is proved by a well-known method in analytic number theory (cf. Davenport-Heilbronn [**3**]). To prove Proposition 1, it suffices to prove it when N is a power of a prime number p.

LEMMA 1. *If $p \neq 2$ and $p \nmid m$, then $\#\Phi_p(m) = p(p^2-1)$.*

PROOF. Let $m, t \in (\mathbf{Z}/p\mathbf{Z})^*$ and put $n = mt^2$. Then the mapping $f(x,y) \mapsto t^{-1}f(tx,y)$ defines a bijection of $\Phi_p(m)$ onto $\Phi_p(n)$. On the other hand, for $f \in \Phi_p$ with $D(f) \neq 0$, $D(f)$ is a square in $\mathbf{Z}/p\mathbf{Z}$ if and only if f is irreducible or splits into three distinct linear factors. This follows from the fact that a finite extension of a finite field is a cyclic extension. By [**4**, Lemma 1], we have $\#\Phi_p(m)(p-1)/2 = p(p-1)(p^2-1)/2$.

For $f \in \Phi_N$, put $v(f) = (\partial D/\partial a, \partial D/\partial b, \partial D/\partial c, \partial D/\partial d) \in (\mathbf{Z}/N\mathbf{Z})^4$. Write 0 instead of $(0,0,0,0) \in (\mathbf{Z}/N\mathbf{Z})^4$. By a simple computation, we have

LEMMA 2. (i) *Let $p \neq 2$, $e \geq 2$ and $f \in \Phi_{p^e}$. Then $f \bmod p$ is the cube of a linear form if and only if $v(f) \equiv 0 \bmod p$. In particular, $v(f) \not\equiv 0 \bmod p$ if $D(f) \not\equiv 0 \bmod p^2$.*

(ii) *Let $e \geq 4$ and $f \in \Phi_{2^e}$. If $D(f) \equiv 1 \bmod 4$, then $v(f) \equiv 0 \bmod 2$ and $v(f) \not\equiv 0 \bmod 4$. If $D(f) \equiv 8$ or $12 \bmod 16$, then $v(f) \equiv 0 \bmod 4$ and $v(f) \not\equiv 0 \bmod 8$.*

By Lemmas 1 and 2, we have

LEMMA 3. (i) *Let $p \neq 2$, $e \geq 2$ and $m \in \mathbf{Z}/p^e\mathbf{Z}$, $m \not\equiv 0 \bmod p^2$. Then we have $\#\Phi_{p^e}(m) = p^{3e-2}(p^2-1)$.*

(ii) *Let $e \geq 4$ and $m \in \mathbf{Z}/2^e\mathbf{Z}$ with $m \equiv 1 \bmod 4$ or $m \equiv 8$ or $12 \bmod 16$. Then we have $\#\Phi_{2^e}(m) = 3 \cdot 2^{3e-1}$.*

Now Proposition 1 follows immediately from Lemma 3.

3. Proof of Theorems 4, 5. First we prove Theorem 5. Let g be a positive integer and put $n = 2g+1$. Let p be a prime divisor of n. Then there exist infinitely many imaginary quadratic fields K with $p \nmid h_K$ by Hartung [**8**]. Take such an imaginary quadratic field K and write $K = \mathbf{Q}(\sqrt{-D})$. Then the hyperelliptic curve $Dy^2 = 4x^n - 1$ has no integral points by Gross-Rohrlich [**7**, Theorem 5.3]. This completes the proof of Theorem 5.

Now we prove Theorem 4. It suffices to prove the theorem for $n = 3, 4, 5, 7$, or 11. The proof is divided into three cases.

Case 1. $n = 5, 7$, or 11. There exist infinitely many imaginary quadratic fields K with $n \nmid h_K$ by [**8**]. Take such an imaginary quadratic field K and write $K = \mathbf{Q}(\sqrt{-D})$. Then the hyperelliptic curve $Dy^2 = 4x^n - 1$ has no rational points by [**7**, Theorem 5.2].

Case 2. $n = 3$. By Theorem 1, there exist infinitely many imaginary quadratic fields K with $\Delta_K \equiv 2 \bmod 3$ and $3 \nmid h_K$. Take such an imaginary quadratic field K and write $K = \mathbf{Q}(\sqrt{-D})$. Suppose $Dy_0^2 = 4x_0^3 - 1$ for some rational numbers x_0, y_0. Put $\alpha = (1+\sqrt{-D})/2$. Then we have $\alpha + \alpha' = 1$ and $\alpha\alpha' = x_0^3$, where α' is the conjugate of α. Hence the principal ideal (α) is the cube of an ideal in K. Since $3 \nmid h_K$ and every unit of K is the cube of a unit, we have $\alpha = \beta^3$ for some $\beta \in K$. Hence $\beta^3 + \beta'^3 = 1$. By Fueter [**5**], this is impossible.

Case 3. $n = 4$. There exist infinitely many prime numbers p with $p \equiv 7 \bmod 8$ by Dirichlet's prime number theorem in arithmetic progressions. Take such a prime number p and put $K = \mathbf{Q}(\sqrt{-p})$. Suppose $py_0^2 = 4x_0^4 - 1$ for some rational numbers x_0, y_0. Put $\alpha = (1+\sqrt{-p})/2$. Then we have $\alpha + \alpha' = 1$ and $\alpha\alpha' = x_0^4$. Hence the principal ideal (α) is the 4th power of an ideal in K. By Gauss' genus theory, h_K is odd. Since the units are ± 1, $\alpha = \pm\beta^4$ for some $\beta \in K$. Hence we have $\beta^4 + \beta'^4 = \pm 1$. By Aigner [**1**] and Nagell [**11**], this is impossible.

ACKNOWLEDGEMENT. The authors are grateful to the referee for valuable comments.

REFERENCES

1. A. Aigner, *Über die Möglichkeit von* $x^4 + y^4 = z^4$ *in quadratischen Körpern*, Jber. Deutsch. Math. Verein. **43** (1934), 226–229.
2. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.
3. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, Bull. London Math. Soc. **1** (1969), 345–348.
4. ——, *On the density of discriminants of cubic fields.* II, Proc. Roy. Soc. London Ser. A **322** (1971), 405–420.
5. R. Fueter, *Die Diophantische Gleichung* $\xi^3 + \eta^3 + \varsigma^3 = 0$, Sitzungsberichte Heidelberg Akad. Wiss. **25**. Abh. (1913), 25 pp.
6. ——, *Über kubische diophantische Gleichungen*, Comment. Math. Helv. **2** (1930), 69–89.
7. B. Gross and D. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201–220.
8. P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by* 3, J. Number Theory **6** (1974), 276–278.
9. K. Horie, *A note on basic Iwasawa* λ*-invariants of imaginary quadratic fields*, Invent. Math. **88** (1987), 31–38.
10. L. J. Mordell, *Diophantine equations*, Academic Press, New York, 1969.
11. T. Nagell, *Sur la résolubilite de l'équation* $x^2 + y^2 + z^2 = 0$ *dans un corps quadratique*, Acta Arith. **21** (1972), 35–43.
12. J. L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. **60** (1981), 375–484.

DEPARTMENT OF MATHEMATICS, JOETSU UNIVERSITY OF EDUCATION, JOETSU 943, JAPAN (Current address of Jin Nakagawa)

DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY, SETAGAYA-KU, TOKYO 158, JAPAN

Current address (Kuniaki Horie): Department of Mathematics, Kyoyobu, Yamaguchi University, Yamaguchi 753, Japan