ACTA ARITHMETICA
XCII.4 (2000)

Corrigendum to the paper "The number of solutions of the Mordell equation"

(Acta Arith. 88 (1999), 173–179)

by

DIMITRIOS POULAKIS (Thessaloniki)

In Lemma 2 we produce an algebraic integer ξ which satisfies some conditions. For our purpose ξ must not be a rational integer. As Professors T. Wooley and M. Bennett pointed out to me this is not obvious by our arguments. So there is a gap in the proof. In this note we give a short proof of Lemma 2 by another method, which yields a significantly better estimate, and we considerably improve the estimates of our Theorems 1 and 2. For any positive integer a we write $\log^* a$ for $\max\{1, \log a\}$ and $\omega(a)$ for the number of its prime divisors.

LEMMA 2. *Let D be a rational integer with $|D| > 1$. Denote by $P(D)$ the product of distinct prime divisors p of D with $p > 3$. If D has no prime divisors > 3 put $P(D) = 1$. Then the number of cubic fields* (*up to isomorphism*) *of discriminant D is at most $225P(D)^{1/2} \log^* P(D)$.*

Proof. If D is a perfect square, then [1, Chapter 6, p. 333] implies that the number of cubic fields (up to isomorphism) of discriminant D is $\le 2^{\omega(D)-1}$. Suppose now that D is not a perfect square. Then $D = a(3^m b)^2$, where $a, b \in \mathbb{Z}$, b is not divisible by 3, a is square free and m a nonnegative integer. It follows from [4, Théorème 2.5] that the number of cubic fields (up to isomorphism) of discriminant D is $\le 2^{\omega(b)-1}9h$, where h is the class number of the quadratic field $\mathbb{Q}(\sqrt{-3a})$. By [2, pp. 620–625] we can take $|D| \ge 23$. Furthermore, [3] implies that $h < 5d^{1/2} \log^* d$, where d is the discriminant of $\mathbb{Q}(\sqrt{-3a})$. Combining the above estimates yields the lemma.

Using the above version of Lemma 2, we obtain the following improved version for Theorem 2.

THEOREM 2. *Let S be a finite set of rational primes with $2, 3 \in S$.*

2000 *Mathematics Subject Classification*: 11D25, 11G05.

Denote by $P(S)$ the product of primes p in S with $p > 3$. If $S = \{2, 3\}$, put $P(S) = 1$. Then the number of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$, with good reduction outside of S, is

$$< 10^{11\sharp S+23} P(S)^{1/2} \log^* P(S).$$

As a consequence of Theorem 2, we get the following improved version for Theorem 1.

THEOREM 1. *Let k be a nonzero rational integer. Denote by $P(k)$ the product of the prime divisors p of k with $p > 3$. If k has no prime divisors > 3, put $P(k) = 1$. Then the number of solutions $(x, y) \in \mathbb{Z}^2$ of the equation $y^2 = x^3 + k$ is*

$$< 10^{11\omega(k)+45} P(k)^{1/2} \log^* P(k).$$

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.

[2] H. Hasse, *Number Theory*, Springer, Berlin, 1980.

[3] A. F. Lavrik, *A remark on the Siegel–Brauer theorem concerning the parameters of algebraic number fields*, Mat. Zametki 8 (1970), 259–263 (in Russian); English transl.: Math. Notes 8 (1970), 615–617.

[4] J. Martinet et J. J. Payan, *Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne*, J. Reine Angew. Math. 228 (1967), 15–37.

Department of Mathematics
Aristotle University of Thessaloniki
54006 Thessaloniki, Greece
E-mail: poulakis@ccf.auth.gr

Received on 28.9.1999 (3692)