Canad. Math. Bull. Vol. **50** (3), 2007 pp. 409–417

# Discriminants of Complex Multiplication Fields of Elliptic Curves over Finite Fields

Florian Luca and Igor E. Shparlinski

*Abstract.* We show that, for most of the elliptic curves $\mathbf{E}$ over a prime finite field $\mathbb{F}_p$ of $p$ elements, the discriminant $D(\mathbf{E})$ of the quadratic number field containing the endomorphism ring of $\mathbf{E}$ over $\mathbb{F}_p$ is sufficiently large. We also obtain an asymptotic formula for the number of distinct quadratic number fields generated by the endomorphism rings of all elliptic curves over $\mathbb{F}_p$.

## 1 Introduction

Let $p > 3$ be prime and let $\mathbb{F}_p$ be the field of $p$ elements.

Throughout this paper, the implied constants in the symbols '$O$', '$\ll$' and '$\gg$' are absolute. We recall that $A \ll B$ and $B \gg A$ are both equivalent to $A = O(B)$.

Let $\mathbf{E}$ be an elliptic curve over $\mathbb{F}_p$ given by an affine *Weierstrass equation* of the form

$$y^2 = x^3 + ax + b, \tag{1}$$

with coefficients $a, b \in \mathbb{F}_p$, such that $4a^3 + 27b^2 \neq 0$. In particular, there are $W_p = p^2 + O(p)$ distinct elliptic curves over $\mathbb{F}_p$.

We recall that the set $\mathbf{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points on any elliptic curve $\mathbf{E}$ forms an Abelian group (with a point at infinity as the identity element). Moreover, if we define the *trace* of $\mathbf{E}$ as $t(\mathbf{E}) = p+1-\#\mathbf{E}(\mathbb{F}_p)$, then the *Hasse–Weil* bound asserts that

$$|t(\mathbf{E})| \le 2p^{1/2}, \tag{2}$$

(see [11] for this and some other general properties of elliptic curves).

We recall that the polynomial $X^2 - t(\mathbf{E})X + p$ is called the *characteristic polynomial* of $\mathbf{E}$ and plays an important role in the description of various properties of $\mathbf{E}$. For example, it is also the characteristic polynomial of the Frobenius automorphism on $\mathbf{E}$, that is, the $p$-th power automorphism. Adjoining its roots to $\mathbb{Q}$ we get a quadratic field $\mathbb{K}_{\mathbf{E}}$ containing the ring of endomorphisms of $\mathbf{E}$ over $\mathbb{F}_p$, which is called the *complex multiplication field of* $\mathbf{E}$. Furthermore, writing $t(\mathbf{E})^2 - 4p = -d(\mathbf{E})^2 D(\mathbf{E})$ with some integers $d(\mathbf{E})$ and $D(\mathbf{E})$, where $D(\mathbf{E})$ is square-free, we see that one of $-D(\mathbf{E})$ or $-4D(\mathbf{E})$ is the discriminant of $\mathbb{K}_{\mathbf{E}} = \mathbb{Q}\left(\sqrt{-D(\mathbf{E})}\right)$ (see [11]), and as such is a natural object to study. It is clear from (2) that $D(\mathbf{E})$ is non-negative. We shall also

Received by the editors April 15, 2005; revised January 19, 2006.

Research of the first author was supported in part by grants SEP-CONACYT 46755, PAPIIT IN104505 and a Guggenheim Fellowship and that of the second author by ARC grant DP0211459.

AMS subject classification: 11G20, 11N32, 11R11.

assume that $d(\mathbf{E})$ is non-negative. In the situation when the curve $\mathbf{E}$ is defined over $\mathbb{Q}$ and one considers the reductions of $\mathbf{E}$ modulo a prime $p$ which varies, the parameter $d(\mathbf{E})$ has been studied in [2], while the complex quadratic field $\mathbb{K}_{\mathbf{E}}$ has been studied in [3].

Here, we look at the dual situation of studying $D(\mathbf{E})$ when $p$ is fixed, but the curve $\mathbf{E}$ varies. Understanding the size of $D(\mathbf{E})$ is of intrinsic interest and has also turned out to have some cryptographic applications. For example, it appears in some bounds of [9], and thus affects in a significant way the complexity of the algorithm for analyzing the discrete logarithm problem in the group of points of isogenous elliptic curves over a prime field described there. Our current results show that unfortunately this parameter tends to be large. It is also well known that given $p$ and $t$, the complexity of constructing a curve $\mathbf{E}$ over $\mathbb{F}_p$ with a given value of $t(\mathbf{E}) = t$ depends exponentially on the size of $D(\mathbf{E})$ (see [1, §18.1]).

It follows immediately from (2) that $d(\mathbf{E}) < 2p^{1/2}$.

For a positive real number $\delta > 0$, we denote by $N_p(\delta)$ the number of elliptic curves $\mathbf{E}$ over $\mathbb{F}_p$ having $d(\mathbf{E}) > \delta$ and let

$$\eta_p(\delta) = \frac{N_p(\delta)}{W_p}$$

be the density of such curves in the set of all such curves over $\mathbb{F}_p$. In this paper, we obtain an upper bound on $\eta_p(\delta)$ which is nontrivial for $\delta \geq (\log p)^2$.

## 2 Main Results

***Theorem 1*** *For any positive $\delta \ll p^{1/6}(\log p)^{1/3}(\log\log p)^{-2/3}$, the bound*

$$\eta_p(\delta) \ll \frac{(\log p)^2}{\delta}$$

*holds.*

The arguments from [10, §1] used in the analysis of the Kronecker class numbers and in counting isomorphisms and automorphisms of elliptic curves, immediately show that for any positive integer $t$, the number $W_p(t)$ of elliptic curves $\mathbf{E}$ given by (1) with $a, b \in \mathbb{F}_p$ such that $t(\mathbf{E}) = t$ is

$$W_p(t) \ll \left(\frac{d}{\varphi(d)}\right)^2 p^{3/2}\log p, \tag{3}$$

where $d$ is the largest positive integer with $d^2 | t^2 - 4p$.

Since, by (3), we clearly have $d(\mathbf{E})^2 D(\mathbf{E}) = 4p - t(\mathbf{E})^2 = p^{1+o(1)}$ for all but $o(p^2)$ elliptic curves (1) over $\mathbb{F}_p$, we conclude from Theorem 1 that $D(\mathbf{E}) = p^{1+o(1)}$ for all but $o(p^2)$ curves over $\mathbb{F}_p$.

We also obtain an asymptotic formula for the number $G_p$ of all possible complex multiplication fields generated by all possible elliptic curves over $\mathbb{F}_p$.

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

By the classical results of Deuring [5], for each $t$ with $|t| \le 2p^{1/2}$ there is an elliptic curve over $\mathbb{F}_p$ with $t(\mathbf{E}) = t$. Therefore $G_p$ is equal to the number of distinct fields of the form $\mathbb{Q}\big(\sqrt{t^2 - 4p}\big)$ for some integer $t$ with $0 \le t \le 2p^{1/2}$.

The question of estimating the number $F_f(T)$ of distinct fields of the form $\mathbb{Q}\big(\sqrt{f(t)}\big)$, $t = 0, \dots, T-1$, for a given quadratic polynomial $f(X) \in \mathbb{Z}[X]$, has been considered in [4]. In fact, under the *ABC*-conjecture, the case of arbitrary polynomials has also been studied in [4]. However, the results of [4] cannot be applied directly to estimating $G_p$ since they are not uniform in terms of the coefficients of $f$. Here, in the case of quadratic polynomials, we extend and improve the corresponding result of [4]. Namely, we make it uniform and also improve the error term of the asymptotic formula for $F_f(T)$ [4, Theorem 1B] from $O(T/\log T)$ to $T^{2/3+o(1)}$. Our result is the following.

***Theorem 2*** *Let $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$, $a \ne 0$, be a quadratic polynomial without multiple roots. Let $d_f = \gcd(a, b, c)$. For an integer $T \ge 1$ we define*

$$M_f(T) = \max_{t=0,\dots,T-1} |f(t)|$$

*and*

$$U_f(T) = \#\{(t_1, t_2) : 0 \le t_1 < t_2 \le T-1, f(t_1) = f(t_2)\}.$$

*Then the bound*

$$F_f(T) = T + O((d_f^{2/3}T^{2/3} + d_f^{1/3}M_f(T)^{1/3})M_f(T)^{o(1)} + U_f(T))$$

*holds as $T \to \infty$.*

In principle, for the proof of Theorem 2 we follow the same approach as in [4] together with some new arguments.

Clearly, if the polynomial $f$ is fixed, then $M_f(T) = O(T^2)$, $U_f(T) = O(1)$ and $d_f = O(1)$, and the error term in Theorem 2 becomes $T^{2/3+o(1)}$, which improves the error term $O(T/\log T)$ given in [4, Theorem 1B].

Obviously, using Theorem 2 for $f(X) = X^2 - 4p$ and $T = \lceil 2p^{1/2} \rceil$ (thus, $M_f(T) = O(p)$, $U_f(T) = 0$ and $d_f = 1$ in this case), we derive the following.

***Corollary 3*** *The bound $G_p = 2p^{1/2} + O(p^{1/3+o(1)})$ holds as $p \to \infty$.*

It is clear that $U_f(T)$ can be estimated directly. For example, if $f(t_1) = f(t_2)$ and $0 \le t_1 < t_2$, then $a(t_1 + t_2) = -b$. In particular, $U_f(T) = 0$ if $a \not| b$, or $b/a \ge 0$. Otherwise, for each positive divisor $d$ of $b/a$, there are at most $d$ pairs $(t_1, t_2)$. Thus, $U_f(T) \le \sigma(|b/a|)$ where, as usual, $\sigma(k)$ is the sum of positive divisors of the integer $k \ge 1$. We recall that $\sigma(k) = O(k \log\log(k+1))$ (see [6, Theorem 323]). In particular, denoting $H_f = \max\{|a|, |b|, |c|\}$, and estimating

$$d_f = O(H_f), \quad M_f(T) = O(H_f T^2), \quad U_f(T) \le H_f^{1+o(1)},$$

we derive from Theorem 2 that the bound

$$F_f(T) = T + O(H_f^{2/3}T^{2/3+o(1)} + H_f(T)^{1+o(1)})$$

holds as $T \to \infty$.

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

## 3 Proof of Theorem 1

As usual, we use $\varphi(k)$ to denote the Euler function of $k$.

We see from (3) that the inequality

$$N_p(\delta) \ll p^{3/2} T_p(\delta) \log p \tag{4}$$

holds, where

$$T_p(\delta) = \sum_{\delta<d} \sum_{\substack{|t|<2p^{1/2} \\ t^2 \equiv 4p \pmod{d^2}}} \frac{d^2}{\varphi(d)^2}.$$

It is clear that the inner sum is void for $d > 2p^{1/2}$. We now fix some $\mu \geq 2$ to be determined later, and we split $T_p(\delta)$ into sums $T_{p,1}(\delta)$ and $T_{p,2}(\delta)$ over the range $d \leq 2p^{1/2}/\mu$, and over the range $d > 2p^{1/2}/\mu$, respectively.

Let $\rho(n)$ denote the number of solutions to the congruence $t^2 \equiv 4p \pmod{n}$, where $0 \leq t < n$. This function $\rho(n)$ can be studied directly, but we simply use the famous Nagell–Ore theorem (see [7] for its strongest known form). It immediately implies that $\rho(n) \ll 2^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime divisors of $n$.

Hence, for the first sums, we have

$$\begin{aligned} T_{p,1}(\delta) &= \sum_{\delta<d\leq 2p^{1/2}/\mu} \sum_{\substack{|t|<2p^{1/2} \\ t^2 \equiv 4p \pmod{d^2}}} \frac{d^2}{\varphi(d)^2} \\ &\leq \sum_{\delta<d\leq 2p^{1/2}/\mu} \left(\frac{4p^{1/2}}{d^2} + 1\right) \frac{d^2 \rho(d^2)}{\varphi(d)^2} \qquad (5) \\ &\ll \sum_{\delta<d\leq 2p^{1/2}/\mu} \left(\frac{p^{1/2}}{d^2} + 1\right) \frac{d^2 2^{\omega(d)}}{\varphi(d)^2} \\ &= p^{1/2} \sum_{\delta<d\leq 2p^{1/2}/\mu} \frac{2^{\omega(d)}}{\varphi(d)^2} + \sum_{\delta<d\leq 2p^{1/2}/\mu} \frac{d^2 2^{\omega(d)}}{\varphi(d)^2}. \qquad (6) \end{aligned}$$

We now recall the Wirsing theorem [12], which can be formulated as follows. Assume that a real-valued multiplicative function $f(d)$ satisfies the following conditions:

- For every positive integer $d$ we have $f(d) \geq 0$.
- There exist positive constants $c_1$ and $c_2$ with $c_2 < 2$ such that for every prime $\ell$ we have $f(\ell^\nu) \leq c_1 c_2^\nu$, $\nu = 2, 3, \ldots$.
- There exists a constant $\tau > 0$ such that

$$\sum_{\ell \leq x} f(\ell) = (\tau + o(1)) \frac{x}{\log x},$$

where the sum is taken over primes $\ell \leq x$.

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

Then the estimate

$$\sum_{d\le x} f(d) = \Big(\frac{1}{e^{\gamma\tau}\Gamma(\tau)} + o(1)\Big)\frac{x}{\log x}\prod_{\ell\le x}\sum_{\nu=0}^{\infty}\frac{f(\ell^\nu)}{\ell^\nu}$$

holds as $x \to \infty$, where $\gamma$ is the Euler constant, and the $\Gamma$-function is defined by $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\,dt$.

It is clear that

$$f(d) = \frac{d^2 2^{\omega(d)}}{\varphi(d)^2}$$

is a multiplicative function and also that

$$\sum_{\ell\le x} f(\ell) = 2\sum_{\ell\le x}\frac{\ell^2}{(\ell-1)^2} = (2+o(1))\,\frac{x}{\log x}.$$

Thus, $f(d)$ satisfies the conditions of the Wirsing theorem with $\tau = 2$, and we derive

$$\begin{aligned}\sum_{d\le x} f(d) &= \Big(\frac{1}{e^{2\gamma}\Gamma(2)} + o(1)\Big)\frac{x}{\log x}\prod_{\ell\le x}\Big(1 + 2\sum_{\nu=1}^{\infty}\frac{\ell^{2\nu}}{\ell^{3\nu-2}(\ell-1)^2}\Big)\\ &= \Big(\frac{1}{e^{2\gamma}\Gamma(2)} + o(1)\Big)\frac{x}{\log x}\prod_{\ell\le x}\Big(1 + 2\frac{\ell^2}{(\ell-1)^2}\sum_{\nu=1}^{\infty}\frac{1}{\ell^\nu}\Big)\\ &= \Big(\frac{1}{e^{2\gamma}\Gamma(2)} + o(1)\Big)\frac{x}{\log x}\prod_{\ell\le x}\Big(1 + 2\frac{\ell^2}{(\ell-1)^3}\Big).\end{aligned}$$

By the Mertens theorem,

$$\begin{aligned}\sum_{\ell\le x}\log\Big(1 + 2\frac{\ell^2}{(\ell-1)^3}\Big) &= 2\sum_{\ell\le x}\Big(\frac{\ell^2}{(\ell-1)^3} + O\Big(\frac{\ell^4}{(\ell-1)^6}\Big)\Big)\\ &= \sum_{\ell\le x}\frac{1}{\ell} + O\Big(\sum_{\ell\le x}\ell^{-2})\Big)\\ &= 2\log\log x + O(1),\end{aligned}$$

therefore

$$\sum_{d\le x}\frac{d^2 2^{\omega(d)}}{\varphi(d)^2} = \sum_{d\le x} f(d) \ll x\log x. \tag{7}$$

By partial summation, it also implies that

$$\sum_{y\le d\le x}\frac{2^{\omega(d)}}{\varphi(d)^2} = \sum_{y\le d\le x}\frac{f(d)}{d^2} \ll \frac{\log x}{y} \tag{8}$$

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

for all real numbers $1 < y < x$. Therefore, applying estimate (7) with $x = 2p^{1/2}/\mu$, estimate (8) with $x = 2p^{1/2}/\mu$ and $y = \delta$, and using (5), we get

$$T_{p,1}(\delta) \ll p^{1/2}\left(\delta^{-1} + \mu^{-1}\right)\log p. \tag{9}$$

For the second sum, using the well-known bound

$$\frac{d}{\phi(d)} \ll \log\log d \ll \log\log p \tag{10}$$

(see [6, Theorem 328]), we deduce

$$\begin{aligned} T_{p,2}(\delta) &\ll (\log\log p)^2 \sum_{2p^{1/2}/\mu < d \le 2p^{1/2}} \sum_{\substack{|t|<2p^{1/2} \\ t^2 \equiv 4p \pmod{d^2}}} 1 \\ &\ll (\log\log p)^2 \sum_{0<m<\mu^2} R(m), \end{aligned}$$

where $R(m)$ is the number of solutions in positive integers $t$ and $d$ to the *norm form equation* $t^2 + md^2 = 4p$. The above equation can be rewritten as

$$\left(\frac{t + \iota\sqrt{m}d}{2}\right)\left(\frac{t - \iota\sqrt{m}d}{2}\right) = p,$$

where $\iota = \sqrt{-1}$. Because $p$ is prime, we conclude $R(m)$ is at most the number of units of the quadratic order $\mathbb{Z}[\iota\sqrt{m}]$. This order has always two units $\pm 1$ except when $m = 1$ when it has four units $\pm 1, \pm\iota$. In fact, $R(m) > 0$ if and only if $-m$ is a quadratic residue modulo $p$ and one of the (hence, both) prime ideals in the ring of integers $\mathcal{O}_{\mathbb{K}_m}$ of the quadratic field $\mathbb{K}_m = \mathbb{Q}[\sqrt{-m}]$ sitting above $p$ is principal and belongs to the order $\mathbb{Z}[(1 + \iota\sqrt{m})/2]$. The last condition above, namely that the prime ideal dividing $p$ belongs to the order $\mathbb{Z}[(1 + \iota\sqrt{m})/2]$, is not needed when $m$ is squarefree as in this case the above order is the full ring of integers $\mathcal{O}_{\mathbb{K}_m}$. Thus,

$$T_{p,2}(\delta) \le 4(\mu^2 + 3)(\log\log p)^2. \tag{11}$$

We now choose $\mu = p^{1/6}(\log p)^{1/3}(\log\log p)^{-2/3}$ to balance the estimates (9) and (11), and finish the proof. ∎

## 4 Proof of Theorem 2

Our next proof is the proof of Theorem 2 which improves the error term in the asymptotic formula of Theorem 1B of [4]. It also makes it uniform, which we need for applications to the polynomial $f(X) = X^2 - 4p$.

We assume that $T$ is sufficiently large and let

$$y = (d_f T)^{2/3} \quad \text{and} \quad z = \left(M_f(T)/d_f\right)^{1/3}.$$

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

Let $L_f(y,T)$ be the number of $t \in \{0,\dots,T-1\}$, such that $m^2 | f(t)$ for some integer $m \geq y$. Since $f$ does not have multiple roots, for every $m$ there are at most $\gcd(d_f, m^2)m^{o(1)} \leq d_f m^{o(1)}$ roots to the congruence $f(t) \equiv 0 \pmod{m^2}$, $t = 0,\dots,m^2-1$ (see [7]). Therefore the contribution to $L_f(y,T)$ coming from $m \in [y,z]$ is at most

$$d_f \sum_{y \leq m \leq z} m^{o(1)} \Big( \frac{T}{m^2} + 1 \Big) \leq d_f (T y^{-1+o(1)} + z^{1+o(1)}). \tag{12}$$

We now estimate the contribution to $L_f(y,T)$ from $m > z$. We note that for each such $m$, we have

$$f(t) = m^2 k \tag{13}$$

with some integer $k$ such that $|k| \leq M_f(T) z^{-2}$.

From (13), we derive

$$(2at+b)^2 - \Delta = m^2 ak, \tag{14}$$

where $\Delta = b^2 - 4ac \neq 0$. For each integer $k$, we denote the number of integer solutions $(t,m)$ of (14) by $Q_f(k)$.

If $-ak < 0$, we then rewrite (14) as

$$\big(2at + b - m\sqrt{-ak}\big)\big(2at + b + m\sqrt{-ak}\big) = \Delta. \tag{15}$$

For every fixed $k$, the above equation has $Q_f(k) = |\Delta|^{o(1)}$ integer solutions $(t,m)$ (corresponding to integer ideal divisors of $\Delta$ in the complex quadratic order $\mathbb{Z}[\iota\sqrt{ak}]$).

If $-ak > 0$ and a perfect square, then (15) has again at most $Q_f(k) = |\Delta|^{o(1)}$ solutions $(t,m)$ corresponding to integral divisors of $\Delta$.

Finally, if $-ak > 0$ is not a perfect square, then the equation (15) is a *Pell* equation. For every fixed $k$, this equation has

$$Q_f(k) \leq |\Delta|^{o(1)} \frac{\log(\max\{T,|a|,|b|\})}{\log|\varepsilon_k|} \ll |\Delta|^{o(1)} \log(\max\{T,|a|,|b|\})$$

integer solutions $(t,m)$ (corresponding to generators of principal ideal divisors of $\Delta$ in the quadratic order $\mathbb{Z}[\sqrt{-ak}]$ multiplied by some power of the fundamental unit $\varepsilon_k$ in $\mathbb{Q}[\sqrt{-ak}]$ which satisfies $|\varepsilon_k| \geq \log(1+\sqrt{5}/2)$). Expressing the coefficients $a$, $b$ and $c$ via $f(1)$, $f(2)$, $f(3)$, one concludes that

$$\max\{|a|,|b|,|c|\} \ll \max\{|f(1)|,|f(2)|,|f(3)|\} \leq M_f(T). \tag{16}$$

Therefore $|\Delta| \ll M_f(T)^2 T^{o(1)}$. Thus the total contribution to $L_f(y,T)$ coming from $m > z$ is at most

$$\sum_{k \leq M_f(T) z^{-2}} Q_f(k) \leq M_f(T)^{1+o(1)} T^{o(1)} z^{-2}. \tag{17}$$

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

Combining (12) and (17), we obtain

$$L_f(y,T) \le d_f T y^{-1+o(1)} + d_f z^{1+o(1)} + M_f(T)^{1+o(1)} T^{o(1)} z^{-2}$$
$$= d_f T y^{-1+o(1)} + M_f(T)^{1/3+o(1)} T^{o(1)} d_f^{2/3+o(1)}.$$

Let $R_f(y,T)$ be the number of pairs of integers $(t_1,t_2)$ with $0 \le t_1 < t_2 < T-1$, and such that

$$f(t_1)/m_1^2 = f(t_2)/m_2^2 \tag{18}$$

for some distinct positive integers $m_1, m_2 \le y$.

It is now easy to check that the arguments of [4, §5] together with (16) give the uniform bound $R_f(y,T) \le y^2 M_f(T)^{o(1)}$. Indeed, as in [4], we let $\Delta = 4ac - b^2$ and note that if $(t_1,t_2)$ is a solution to (18), then one can easily verify that

$$(m_2 r_1 - m_1 r_2)(m_2 r_1 + m_1 r_2) = \Delta(m_1^2 - m_2^2),$$

where $r_1 = 2at_1 + b$, $r_2 = 2at_2 + b$. Thus, for every fixed $y \ge m_1 > m_2 > 0$, there are at most $\tau(\Delta(m_1^2 - m_2^2))$ solutions, where $\tau(k)$ is the number of positive divisors of the integer $k \ge 1$. Recalling that $\tau(k) = k^{o(1)}$ (see [6, Theorem 317]), and summing up over all the possible choices of $0 < m_2 < m_1 \le y$, we obtain the above bound on $R_f(y,T)$.

Clearly, $F_f(T) = T + O(L_f(y,T) + R_f(y,T) + U_f(y,T))$. Since $f(t)$ takes every value at most twice and each of them is divisible by $d_f$, it is obvious that $M_f(T) \gg d_f T$. Therefore the terms with $d_f^{o(1)}$ and $T^{o(1)}$ can be replaced with $M_f(T)^{o(1)}$. Thus, recalling our choice of $y$, we finish the proof. ∎

## 5 Remarks

It is easy to see that Theorem 1 is non-trivial starting from the values of $\delta$ of order $(\log p)^2$. Using, the bound (10) in our treatment of $T_{p,1}(\delta)$ in the proof of Theorem 1 together with (3), one can get a shorter proof of a slightly weaker version of Theorem 1 with an extra factor of $(\log\log p)^2$ on the right-hand side. Accordingly, the non-triviality range would be slightly shorter.

On the other hand, for larger values of $\delta$ than those allowed in Theorem 1, one can simply use the fact that $\eta_p(\delta)$ is monotonically increasing getting

$$\eta_p(\delta) \ll p^{-1/6}(\log p)^{5/3}$$

for $\delta > p^{1/6}(\log p)^{1/3}$.

It is easy to see that $\rho(n) \ne 0$ only if $p$ is a quadratic residue modulo $\ell$ for all prime divisors $\ell | n$. It appears that the results on the distribution of such primes $\ell$ implied by the extended Riemann hypothesis (the unconditional results do not seem to be enough), combined with the Brun sieve, can be used to improve our bounds. Furthermore, using that the extended Riemann hypothesis implies the bound

$$L(1,\chi_D) \ll \log\log(D+1)$$

https://doi.org/10.4153/CMB-2007-039-2 Published online by Cambridge University Press

on $L$-functions $L(s, \chi_D)$, where $\chi_D$ is the quadratic character of conductor $D \geq 2$ (see [8, §22.6]), one can replace $\log p$ by $\log\log p$ in (3). Both these improvements should lead to the disappearance of $\log p$ from our bounds, at the cost of the appearance of some power of $\log\log p$.

One can also consider this question "on average" over $p$, which should also allow stronger bounds.

Finally, it is natural to expect that $\eta_p(\delta) \to 0$ as $\delta \to \infty$ as $p \to \infty$. However, neither the bound of Theorem 1 nor its possible improvements outlined above seem to lead to such a statement, which we pose as an open question.

**Acknowledgements** We thank the referee for suggestions which improved the quality of this paper.

## References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice.* CRC Press, 2005.
[2] A. Cojocaru and W. Duke, *Reductions of an elliptic curve and their Tate-Shafarevich groups.* Math. Ann. **329**(2004), no. 3, 513–534.
[3] A. Cojocaru, E. Fouvry and M. R. Murty, *The square sieve and the Lang-Trotter conjecture.* Canad. J. Math. **57**(2005), no. 6, 1155–1178.
[4] P. Cutter, A. Granville and T. J. Tucker, *The number of fields generated by the square root of values of a given polynomial.* Canad. Math. Bull. **46**(2003), no. 1, 71–79.
[5] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hansischen Univ. **14**(1941), 197–272.
[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* Fifth edition. Oxford University Press, New York, 1979.
[7] M. N. Huxley, *A note on polynomial congruences.* In: Recent Progress in Analytic Number Theory, Vol.1, Academic Press, London, 1981, pp. 193–196.
[8] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications 53, American Mathematical Society, Providence, RI, 2004.
[9] D. Jao, S. D. Miller and R. Venkatesan, *Ramanujan graphs and the random reducibility of discrete log on isogenous elliptic curves.*Preprint (available from `http://arxiv.org/abs/math.NT/0411378`), 2004.
[10] H. W. Lenstra, Jr., *Factoring integers with elliptic curves.* Annals of Math. **126**(1987), no. 3, 649–673.
[11] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer-Verlag, Berlin, 1995.
[12] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen.* Math. Ann. **143**(1961), 75–102.

*Instituto de Matemáticas*
*Universidad Nacional Autónoma de México*
*C.P. 58089, Morelia, Michoacán*
*México*
*e-mail: fluca@matmor.unam.mx*

*Department of Computing*
*Macquarie University*
*Sydney, NSW 2109*
*Australia*
*e-mail: igor@ics.mq.edu.au*