Math. Res. Lett. **19** (2012), *no.* 02, 335–343 © International Press 2012

ISOMORPHISM CLASSES OF ELLIPTIC CURVES OVER A FINITE FIELD IN SOME THIN FAMILIES

Javier Cilleruelo, Igor E. Shparlinski and Ana Zumalacárregui

Abstract. For a prime p and a given square box, $\mathfrak{B}$, we consider all elliptic curves $E_{r,s} : Y^2 = X^3 + rX + s$ defined over a field $\mathbb{F}_p$ of p elements with coefficients $(r, s) \in \mathfrak{B}$. We obtain a nontrivial upper bound for the number of such curves which are isomorphic to a given one over $\mathbb{F}_p$, in terms of the size of $\mathfrak{B}$. We also give an optimal lower bound on the number of distinct isomorphic classes represented.

1. Background and notation

For a prime p we consider the family of elliptic curves $E_{a,b}$ given by a Weierstrass equation

$$E_{a,b}: \quad Y^2 = X^3 + aX + b$$

over the finite field $\mathbb{F}_p$ of p elements, where

$$(a, b) \in \mathbb{F}_p^2, \quad 4a^3 + 27b^2 \neq 0. \tag{1.1}$$

Recall that for a large enough prime, say $p > 3$, it is well known that every elliptic curve over $\mathbb{F}_p$ has a representation of this type, see [13] for a background on elliptic curves. Thus, from now on, curves are considered as parameterized by their coefficients.

Two curves $E_{r,s}$ and $E_{u,v}$ are isomorphic if for some $t \in \mathbb{F}_p^*$ we have

$$rt^4 \equiv u \pmod p \qquad \text{and} \qquad st^6 \equiv v \pmod p). \tag{1.2}$$

There are several works which count the number of curves $E_{r,s}$ isomorphic to a given curve $E_{a,b}$, with coefficients r, s lying in certain box $(r, s) \in [R + 1, R + K] \times [S + 1, S + L]$, see [2, 8]. In particular, for

$$KL \geq p^{3/2+\varepsilon} \qquad \text{and} \qquad \min\{K, L\} \geq p^{1/2+\varepsilon} \tag{1.3}$$

with some fixed $\varepsilon > 0$, using exponential sum techniques, Fouvry and Murty [8] have obtained an asymptotic formula for every pair (a, b) with (1.1). In [2], using bounds of multiplicative character sums, for almost all (a, b) with (1.1), this condition (1.3) has been relaxed to

$$KL \geq p^{1+\varepsilon} \qquad \text{and} \qquad \min\{K, L\} \geq p^{1/4+\varepsilon}.$$

Furthermore, it is shown in [2], that for

$$KL \geq p^{1+\varepsilon} \qquad \text{and} \qquad \min\{K, L\} \geq p^{1/4e^{1/2}+\varepsilon},$$

Received by the editors June 2, 2011.

one can get a lower bound with the right order of magnitude (again for almost all (a, b) with (1.1)). On average over p, such results are established for even smaller boxes, see [2].

Here we consider squared boxes, much smaller than the previous ones, given by

$$\mathfrak{B} = [R+1, R+M] \times [S+1, S+M] \subseteq \mathbb{F}_p \times \mathbb{F}_p, \tag{1.4}$$

for a prime p and some nonnegative integers R, S, M satisfying

$$R, S \geq 0, \ M \geq 1 \quad \text{and} \quad R+M, S+M < p. \tag{1.5}$$

We use $|\mathfrak{B}|$ to denote the area of $\mathfrak{B}$, that is,

$$|\mathfrak{B}| = M^2.$$

We are interested in understanding how isomorphism classes are distributed in such small boxes $\mathfrak{B}$. Among all curves $E_{r,s}$, parameterized by coefficients $(r, s) \in \mathfrak{B}$, we study, in first place, the number of isomorphism classes which are represented and, finally, the number of curves lying in a given isomorphism class.

Clearly, the existence of an isomorphism between $E_{r,s}$ and $E_{u,v}$, see (1.2), implies that

$$r^3 v^2 \equiv u^3 s^2 \pmod p. \tag{1.6}$$

We denote by $T(\mathfrak{B})$ the number of solutions to (1.6) with $(r, s), (u, v) \in \mathfrak{B}$. Furthermore, for $\lambda \in \mathbb{F}_p$, we denote by $N_\lambda(\mathfrak{B})$ the number of solutions to the congruence

$$r^3 \equiv \lambda s^2 \pmod p, \quad (r, s) \in \mathfrak{B}.$$

We use the bounds of character sums detailed in Section 2 to obtain an upper bound on $T(\mathfrak{B})$. From this estimate we derive an almost optimal lower bound for the number $I(\mathfrak{B})$, of nonisomorphic curves with coefficients in $\mathfrak{B}$, of the form

$$I(\mathfrak{B}) \geq \min\left\{(1 + o(1))p, |\mathfrak{B}|^{1+o(1)}\right\}, \tag{1.7}$$

see Corollary 4.1 below for a more precise formulation.

Clearly, the bound (1.7) is quite tight as we have the trivial upper bound

$$I(\mathfrak{B}) \leq \min\{2p + O(1), |\mathfrak{B}|\},$$

since it is well known [12] that the number of isomorphism classes of elliptic curves in $\mathbb{F}_p$ is $2p + O(1)$.

Finally, we exploit the method of [5], based on the ideas of [4] (see also [15]), to obtain in Section 5 upper bounds on $N_\lambda(\mathfrak{B})$, which, in particular, imply upper bounds for the number of elliptic curves $E_{r,s}$ with coefficients $(r, s) \in \mathfrak{B}$ that fall in the same isomorphism class.

Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ are absolute. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$. Furthermore the notation $U = V^{o(1)}$ is equivalent to the statement that for every $\varepsilon > 0$ the inequality $U \leq c(\varepsilon)V^\varepsilon$ holds for some constant $c(\varepsilon) > 0$ that depends only on ε.

2. Character sums

Let $\mathcal{X}$ be the set of all multiplicative characters modulo p and let $\mathcal{X}^* = \mathcal{X} \setminus \{\chi_0\}$ be the set of nonprincipal characters.

We recall the Pólya–Vinogradov bound, see [11, Theorem 12.5].

Lemma 2.1. *For arbitrary integers W and Z, with $0 \le W < W+Z < p$, the bound*

$$\max_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right| \ll p^{1/2} \log p$$

holds.

We recall that Garaev and García [9], improving a result of Ayyad *et al.* [1] (see also [6]), have shown that for any integers W and Z

$$\sum_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \ll pZ^2 \left(\log p + \left(\log(Z^2/p) \right)^2 \right). \tag{2.1}$$

Note that for any fixed $\varepsilon > 0$, if $Z \ge p^{\varepsilon}$ the right-hand side of (2.1) is of the form $pZ^{2+o(1)}$. However for small values of Z, namely for $Z \ll (\log p)^{1/2}$, the bound (2.1) is trivial. We now combine (2.1) with a result of [4] to get the bound $pZ^{2+o(1)}$ for any Z.

Lemma 2.2. *For arbitrary integers W and Z, with $0 \le W < W+Z < p$, the bound*

$$\sum_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \ll pZ^{2+o(1)}$$

holds.

Proof. We can assume that $Z \le p^{1/4}$ since otherwise, as we have noticed before, the bound (2.1) implies the desired result. Now, using that for any integer z with $\gcd(z,p) = 1$, for the complex conjugated character $\overline{\chi}$ we have

$$\overline{\chi}(z) = \chi(z^{-1}),$$

we derive,

$$\sum_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \le \sum_{\chi \in \mathcal{X}} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 = \sum_{z_1,z_2,z_3,z_4=W+1}^{W+Z} \sum_{\chi \in \mathcal{X}} \chi(z_1 z_2 z_3^{-1} z_4^{-1}).$$

Thus, using the orthogonality of characters we obtain

$$\sum_{\chi \in \mathcal{X}^*} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \le pJ,$$

where J is number of solutions to the congruence

$$z_1 z_2 \equiv z_3 z_4 \pmod p, \quad z_1, z_2, z_3, z_4 \in [W+1, W+Z].$$

By [4, Theorem 1], for any $\lambda \not\equiv 0 \pmod p$ the congruence

$$z_1 z_2 \equiv \lambda \pmod p, \quad z_1, z_2 \in [W+1, W+Z]$$

has $Z^{o(1)}$ solutions, provided that $Z \le p^{1/4}$. Therefore $J \le Z^{2+o(1)}$ and the result follows. □

3. Small points on some hypersurfaces

For the number of points in very small boxes we can get a better bound by using the following estimate of Bombieri and Pila [3] on the number of integral points on polynomial curves.

Lemma 3.1. *Let $\mathcal{C}$ be an absolutely irreducible curve of degree $d \ge 2$ and $H \ge \exp(d^6)$. Then the number of integral points on $\mathcal{C}$ and inside of a square $[0, H] \times [0, H]$ does not exceed $H^{1/d} \exp(12\sqrt{d \log H \log\log H})$.*

For an integer a we used $\|a\|_p$ to denote the smallest by absolute value residue of a modulo p, that is

$$\|a\|_p = \min_{k \in \mathbb{Z}} |a - kp|.$$

By the Dirichlet pigeon-hole principle we easily obtain the following result.

Lemma 3.2. *For any real numbers $T_1, \ldots, T_s$ with*

$$p > T_1, \ldots, T_s \ge 1 \qquad \text{and} \qquad T_1 \cdots T_s > p^{s-1}$$

and any integers $a_1, \ldots, a_s$ there exists an integer t with $\gcd(t, p) = 1$ satisfying

$$\|a_i t\|_p \ll T_i, \quad i = 1, \ldots, s.$$

4. Bound on $T(\mathfrak{B})$

In fact we consider a more general quantity, that is for given positive integers i, j we bound the number $T_{i,j}(\mathfrak{B})$ of solutions to the equation

$$r^i v^j \equiv u^i s^j \pmod p \tag{4.1}$$

with $(r, s), (u, v) \in \mathfrak{B}$. Thus, in this setting, $T(\mathfrak{B}) = T_{3,2}(\mathfrak{B})$.

Theorem 4.1. *For any prime p and any box $\mathfrak{B}$ given by (1.4) and satisfying (1.5) we have,*

$$T_{i,j}(\mathfrak{B}) = d\frac{|\mathfrak{B}|^2}{p-1} + O\left(|\mathfrak{B}|p^{o(1)}\right)$$

as $|\mathfrak{B}| \to \infty$, where $d = \gcd(i, j, p-1)$.

Proof. Using the orthogonality of characters, we write the number of solutions to (4.1) with $(r, s), (u, v) \in \mathfrak{B}$ as

$$\begin{aligned} T_{i,j}(\mathfrak{B}) &= \sum_{r,u=R+1}^{R+M} \sum_{s,v=S+1}^{R+M} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \chi\left((r/u)^i (v/s)^j\right) \\ &= \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^2 \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2. \end{aligned}$$

The contribution to the above sum from d characters $\chi \in \mathcal{X}$ with $\chi^i = \chi^j = \chi_0$ is $dM^4/(p-1)$.

Using Lemma 2.1, we see that the contribution to the above sum from at most i characters $\chi \in \mathcal{X}$ with $\chi^i = \chi_0$ and $\chi^j \neq \chi_0$ is bounded by

$$\frac{M^2}{p-1} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i = \chi_0}} \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2 \ll M^2 (\log p)^2.$$

The contribution from the characters $\chi \in \mathcal{X}$ with $\chi^j = \chi_0$ and $\chi^i \neq \chi_0$ can be estimated similarly as $O\left(M^2 \log p\right)$.

Therefore

$$T_{i,j}(R,S;M) = d\frac{M^4}{p-1} + O(M^2(\log p)^2 + W), \tag{4.2}$$

where

$$W = \frac{1}{(p-1)^2} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^2 \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2 .$$

Using the Cauchy inequality, we derive

$$W^2 \leq \frac{1}{(p-1)^2} \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \times \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^4 . \tag{4.3}$$

When χ runs through $\mathcal{X}$ the power χ^h represents any other character in $\mathcal{X}$ no more that h times. Thus

$$\sum_{\substack{\chi \in \mathcal{X} \\ \chi^i,\, \chi^j \neq \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \ll \sum_{\chi \in \mathcal{X}^*} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4$$

and similarly for the second double sums over s.

Combining the above bounds with inequality (4.3), applying Lemma 2.2, and then using (4.2), we conclude the proof. □

Corollary 4.1. *For any prime p and any box $\mathfrak{B}$ given by* (1.4) *and satisfying* (1.5) *we have,*

$$I(\mathfrak{B}) \geq \min\left\{p(1 + O(|\mathfrak{B}|^{-1+o(1)}p)), |\mathfrak{B}|p^{o(1)}\right\}$$

as $|\mathfrak{B}| \to \infty$.

Proof. Let $\Gamma = \{r^3/s^2 : \ (r,s) \in \mathfrak{B}\}$, we recall that

$$N_\lambda(\mathfrak{B}) = |\{(r,s) \in \mathfrak{B} \, : \, r^3/s^2 = \lambda\}|.$$

Using the Cauchy inequality we derive

$$|\mathfrak{B}|^2 = \left(\sum_{\lambda \in \Gamma} N_\lambda(\mathfrak{B})) \right)^2 \leq |\Gamma| \sum_\lambda N_\lambda^2(\mathfrak{B}) \leq I(\mathfrak{B})\, T_{3,2}(\mathfrak{B}).$$

We conclude the proof by estimating $T_{3,2}(\mathfrak{B})$ with Theorem 4.1. □

It is easy to see that the error term of Theorem 4.1 and thus the second term of Corollary 4.1 can be replaced with $|B|^{1+o(1)}$.

5. Bound on $N_\lambda(\mathfrak{B})$

It is easy to see that for $\lambda \in \mathbb{F}_p^*$ the curve $X^3 = \lambda Y^2$ is absolutely irreducible. So general bounds on the number of points on a curve in a given box (see, for example, [14]) immediately imply that

$$N_\lambda(\mathfrak{B}) = \frac{|\mathfrak{B}|}{p} + O\left(p^{1/2}(\log p)^2\right), \tag{5.1}$$

which gives a trivial upper bound when $|\mathfrak{B}| \ll p^{1/2}\log p$.

We are now ready to derive a nontrivial upper bound on $N_\lambda(\mathfrak{B})$ for smaller values of M.

Lemma 5.1. *For any prime p, any box $\mathfrak{B}$, given by* (1.4) *and with $1 \le |\mathfrak{B}| \le p^{2/9}$, satisfying* (1.5) *and $\lambda \in \mathbb{F}_p^*$ we have*

$$N_\lambda(\mathfrak{B}) \le |\mathfrak{B}|^{1/6+o(1)}$$

as $|B| \to \infty$.

Proof. We have to estimate the number of solutions to

$$(R+x)^3 \equiv \lambda(S+y)^2 \pmod p,$$

with $1 \le x, y \le M$, which is equivalent to the congruence

$$x^3 + 3Rx^2 + 3R^2x - \lambda y^2 - 2\lambda Sy \equiv \lambda S^2 - R^3 \pmod p. \tag{5.2}$$

For any $T \le p^{1/4}/M^{1/2}$, we can apply Lemma 3.2 to

$$a_1 = 1, \quad a_2 = 3R, \quad a_3 = 3R^2, \quad a_4 = -\lambda, \quad a_5 = -2\lambda S$$

and

$$T_1 = T^4M^2, \quad T_2 = T_4 = p/(TM), \quad T_3 = T_5 = p/T,$$

and conclude that there exits $|t| \le T^4M^2$ with $\gcd(t,p) = 1$ such that

$$\|3Rt\|_p \le p/(TM), \quad \|\lambda t\|_p \le p/(TM), \quad \|3R^2t\|_p \le p/T, \quad \|2\lambda St\|_p \le p/T.$$

Thus, by multiplying both sides of the congruence (5.2) by t, we can replace the congruence (5.2) with the following equation over $\mathbb{Z}$:

$$A_1x^3 + A_2x^2 + A_3x + A_4y^2 + A_5y + A_6 = pz, \tag{5.3}$$

where

$$|A_1| \le T^4M^2, \quad |A_2|, |A_4| \le p/(TM), \quad |A_3|, |A_5| \le p/T, \quad |A_6| \le p/2.$$

Since, for $0 \le x, y \le M$, the left hand side of equation (5.3) is bounded by $T^4M^5 + 4pM/T + p/2$, it follows that

$$|z| \ll \frac{T^4M^5}{p} + \frac{4M}{T} + 1.$$

The choice $T \sim p^{1/5}/M^{4/5}$ leads us to the bound

$$|z| \ll M^{9/5}p^{-1/5} + 1 \ll 1$$

provided that $M = |\mathfrak{B}|^{1/2} \le p^{1/9}$.

We note that the polynomial $A_1X^3 + A_2X^2 + A_3X + A_4Y^2 + A_5Y + A_6$ on left-hand side of (5.3) is absolutely irreducible. Indeed, it is obtained from $X^3 - \lambda Y^2$ (which is an absolutely irreducible polynomial) by a nontrivial modulo p affine transformation. Therefore, for every integer z, the polynomial $A_1X^3 + A_2X^2 + A_3X + A_4Y^2 + A_5Y + A_6 - pz$ is also absolutely irreducible (as its reduction modulo p is absolutely irreducible modulo p).

Thus, for each z in the previous range, equation (5.3) corresponds to an absolutely irreducible curve of degree 3 which, by Lemma 3.1, has at most $M^{1/3+o(1)}$ points lying in $[0, M]^2$. Therefore, the number of solutions in the original equation is bounded by $M^{1/3+o(1)} = |\mathfrak{B}|^{1/6+o(1)}$. □

The family of curves $E_{r,s}$ with $(r, s) = (t^2, t^3)$, $1 \le t \le |\mathfrak{B}|^{1/6}$, shows that the exponent $1/6$ in the bound of Lemma 5.1 cannot be improved, which means that we cannot obtain a general bound stronger than $N_\lambda(\mathfrak{B}) = O(|\mathfrak{B}|^{1/6})$.

Clearly the argument used in the proof of Lemma 5.1 works for large values of $|\mathfrak{B}|$. In particular, for $|\mathfrak{B}| > p^{2/9}$, it leads to the bound $N_\lambda(\mathfrak{B}) \ll |\mathfrak{B}|^{16/15+o(1)}p^{-1/5}$ which is nontrivial for $|\mathfrak{B}| \le p^{6/17}$.

However, using a modification of this argument we can obtain a stronger bound which is nontrivial for $p^{2/9} < |\mathfrak{B}| \le p^{2/5}$:

Lemma 5.2. *For any prime p, any box $\mathfrak{B}$, given by* (1.4) *with $p^{2/9} < |\mathfrak{B}| \le p^{2/5}$, satisfying* (1.5) *and $\lambda \in \mathbb{F}_p^*$ we have*

$$N_\lambda(\mathfrak{B}) \le |\mathfrak{B}|^{11/12+o(1)}p^{-1/6}$$

as $|\mathfrak{B}| \to \infty$.

Proof. Let $K = \lfloor p^{1/6}/M^{1/2} \rfloor$ and observe that we have $1 \le K \le M$ when $p^{2/9} < |\mathfrak{B}| = M^2$. Also observe that one could cover $\mathfrak{B}$ with $J = O(M/K)$ rectangles of the form $[R_j + 1, R_j + K] \times [S + 1, S + M]$, $j = 1, \ldots, J$. Then, the equation in each rectangle can be written as

$$x^3 + 3R_jx^2 + 3R_j^2x - \lambda y^2 - 2\lambda Sy \equiv \lambda S^2 - R_j^3 \pmod p \tag{5.4}$$

with $1 \le x \le K$ and $1 \le y \le M$.

To estimate the number of solutions to (5.4), we set

$$T_1 = p^{1/2}M^{3/2}, \quad T_2 = p^{2/3}M, \quad T_3 = p^{5/6}M^{1/2}, \quad T_4 = p/M^2, \quad T_5 = p/M.$$

and apply, once more, Lemma 3.2 where a_i are the coefficients of x, y in (5.4). Hence, as in the proof of Lemma 5.1, we obtain an equivalent equation over $\mathbb{Z}$:

$$A_1x^3 + A_2x^2 + A_3x + A_4y^2 + A_5y + A_6 = pz, \tag{5.5}$$

where $|A_i| \le T_i$ for $i = 1, \ldots, 5$ and $|A_6| \le p/2$. The left-hand side of (5.5) is bounded by

$$\begin{aligned} &|A_1K^3 + A_2K^2 + A_3K + A_4M^2 + A_5M + A_6| \\ &\le p^{1/2}M^{3/2}\left(\frac{p^{1/6}}{M^{1/2}}\right)^3 + p^{2/3}M\left(\frac{p^{1/6}}{M^{1/2}}\right)^2 + p^{5/6}M^{1/2}\frac{p^{1/6}}{M^{1/2}} \\ &\quad + \frac{p}{M^2}M^2 + \frac{p}{M^2}M + p/2 \\ &= 5.5p. \end{aligned}$$

Thus, z can take at most 11 values. As we have seen in the proof of Lemma 5.1, the polynomial on the left-hand side of (5.5) is absolutely irreducible. Therefore, Lemma 3.1 implies that, for each value of z, equation (5.5) has at most $M^{1/3+o(1)}$ solutions. Summing over all rectangles we finally obtain that the original congruence has at most

$$(M/K)M^{1/3+o(1)} = M^{11/6+o(1)}p^{-1/6} = |\mathfrak{B}|^{11/12+o(1)}p^{-1/6}$$

solutions. □

Combining (5.1) with Lemmas 5.1 and 5.2, we obtain:

Theorem 5.1. *For any prime p, box $\mathfrak{B}$ given by* (1.4) *and satisfying* (1.5) *and $\lambda \in \mathbb{F}_p^*$ we have,*

$$N_\lambda(\mathfrak{B}) \ll |\mathfrak{B}|^{o(1)} \begin{cases} |\mathfrak{B}|^{1/6}, & \text{if } |\mathfrak{B}| < p^{2/9}, \\ |\mathfrak{B}|^{11/12}p^{-1/6}, & \text{if } p^{2/9} \le |\mathfrak{B}| < p^{2/5}, \\ p^{1/2}, & \text{if } p \le |\mathfrak{B}| < p^{3/2}, \\ |\mathfrak{B}|p^{-1}, & \text{if } p^{3/2} \le |\mathfrak{B}| < p^2, \end{cases}$$

as $|\mathfrak{B}| \to \infty$.

We note that unfortunately in the range $p^{2/5} \le |\mathfrak{B}| < p$ we could not find any nontrivial estimate.

6. Comments and open problems

Observe that Theorem 4.1 can be easily extended to coefficients (r, s) that belong to rectangles $[R+1, R+K] \times [S+1, S+L]$ rather than squares (the bound (5.1) also holds for such rectangles).

As we have mentioned the exponent $1/6$ in the bound of Lemma 5.1 cannot be improved, however, the range $|\mathfrak{B}| \le p^{2/9}$ can possibly be extended. As the first step towards this, the following question has to be answered:

Problem 6.1. *Let E be an elliptic given by a Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \ a_i \in \mathbb{Z},$$

such that all the coefficients are $M^{o(1)}$. Is it true that the number of integer points $(x, y) \in [0, M] \times [0, M]$ on E is $M^{o(1)}$?

We refer to [7, 10] for some bounds on the number of points on elliptic curves in boxes.

As we have noticed in Section 5 we have not found nontrivial bounds on $N_\lambda(\mathfrak{B})$ for $p^{2/5} \le |\mathfrak{B}| < p$. It is certainly interesting to close this gap.

Problem 6.2. *Is it true that $N_\lambda(\mathfrak{B}) = o(|\mathfrak{B}|^{1/2})$ for all $|\mathfrak{B}| = o(p^2)$?*

Finally, it is also natural to expect that the term $|\mathfrak{B}|^{o(1)}$ can be removed from the result obtained in Corollary 4.1.

Problem 6.3. *Is it true that $I(\mathfrak{B}) \gg \min\{p, |\mathfrak{B}|\}$?*

Acknowledgment

The authors are grateful to Moubariz Garaev and Joe Silverman for their comments.

This work started during a very pleasant visit by I. S. to the Universidad Autónoma de Madrid; the support and hospitality of this institution are gratefully acknowledged.

During the preparation of this paper, J.C. was supported by grant MTM 2008-03880 of MICINN (Spain), I.S. was supported in part by ARC grant DP1092835 (Australia) and by NRF grant CRP2-2007-03 (Singapore), and A.Z. was supported by Departamento de Matemáticas, UAM (Spain).

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, *The congruence* $x_1x_2 \equiv x_3x_4 \pmod p$*, the equation* $x_1x_2 = x_3x_4$ *and the mean value of character sums*, J. Number Theory **59** (1996), 398–413.

[2] W. D. Banks and I. E. Shparlinski, *Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. **173** (2009), 253–277.

[3] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.

[4] J. Cilleruelo and M. Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications*, Geom. Funct. Anal. **21** (2011), 892–904.

[5] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I.E. Shparlinski, *On the concentration of points of polynomial maps and applications*, Math. Z., to appear.

[6] T. Cochrane and S. Sih, *The congruence* $x_1x_2 \equiv x_3x_4 \pmod p$ *and mean values of character sums*, J. Number Theory **130** (2010), 767–785.

[7] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **2007** (2007), article ID rnm002, 1–18.

[8] É. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), 81–104.

[9] M. Z. Garaev and V. Garcia, *The equation* $x_1x_2 = x_3x_4 + \lambda$ *in fields of prime order and applications*, J. Number Theory **128** (2008), 2520–2537.

[10] H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc. **19** (2006), 527–550.

[11] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[12] H. W. Lenstra, *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987), 649–673.

[13] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 2009.

[14] M. Vâjâitu and A. Zaharescu, *Distribution of values of rational maps on the* $\mathbb{F}_p$*-points on an affine curve*, Monatsh. Math. **136** (2002), 81–86.

[15] A. Zumalacárregui, *Concentration of points on modular quadratic forms*, Internat. J. Number Theory **7** (2011), 1835–1839.

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid 28049, España

E-mail address: `franciscojavier.cilleruelo@uam.es`

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: `igor.shparlinski@mq.edu.au`

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid 28049, España

E-mail address: `ana.zumalacarregui@uam.es`