Isomorphism Classes of Elliptic Curves Over a Finite Field in Some Thin Families

Javier Cilleruelo
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM)
and
Departamento de Matemáticas, Universidad Autónoma de Madrid
Madrid, 28049, España
franciscojavier.cilleruelo@uam.es

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

Ana Zumalacárregui
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM)
and
Departamento de Matemáticas, Universidad Autónoma de Madrid
Madrid, 28049, España
ana.zumalacarregui@uam.es

Abstract

We give a non trivial upper bound for the number of elliptic curves $E_{r,s} : Y^2 = X^3 + rX + s$ with $(r, s) \in [R+1, R+M] \times [S+1, S+M]$ that are isomorphic to a given curve. We also give an almost optimal lower bound for the number of distinct isomorphic classes represented by elliptic curves $E_{r,s}$ with the coefficients r, s lying in a small box.

1 Background

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

$$(a,b) \in \mathbb{F}_p^2, \qquad 4a^3 + 27b^2 \neq 0. \tag{1}$$

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

$$rt^4 \equiv u \pmod p \qquad \text{and} \qquad st^6 \equiv v \pmod p. \tag{2}$$

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

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

with some fixed $\varepsilon > 0$, using the exponential sum technique, Fouvry and Murty [8] have obtained an asymptotic formula for every pair (a,b) with (1). In [2], using bounds of multiplicative character sum, for almost all (a,b) with (1), this condition (3) has been relaxed as

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

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

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

one can get a lower bound on the right order of magnitude (again for almost all (a,b) with (1)). On average over p, such results are established for even smaller boxes, see [2].

Here we consider much smaller boxes and obtain a lower bound on the number $I(R,S;M)$ of nonisomorphic curves $E_{r,s}$ with coefficients in r, s is a given box $(r,s) \in [R+1, R+M] \times [S+1, S+M]$.

Clearly, the congruences (2) imply that

$$r^3v^2 \equiv u^3s^2 \pmod p \tag{4}$$

So, given integers R, S and $M \geq 1$, we denote by $T(R,S;M)$ the number of solutions to (4) with

$$(r,s),(u,v) \in [R+1,R+M] \times [S+1,S+M].$$

Furthermore, for $\lambda \in \mathbb{F}_p$, we denote by $N_\lambda(R,S;M)$ the number of solutions to the congruence

$$r^3 \equiv \lambda s^2 \pmod p, \qquad (r,s) \in [R+1,R+M] \times [S+1,S+M].$$

We use the method of [5], that in turn is based on the ideas of [4] (see also [12]), to obtain an upper bound on $N_\lambda(R,S;M)$, which, in particular, implies an upper bound for the number of elliptic curves $E_{r,s}$ with coefficients $(r,s) \in [R+1,R+M] \times [S+1,S+M]$ that fall in the same isomorphism class.

We use the bounds of character sums to obtain an upper bound on $T(R,S;M)$ from which we derive an almost optimal lower bound $I(R,S;M)$.

Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ are absolute otherwise. 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 $c > 0$.

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. Garaev and García [9], improving a result of Ayyad, Cochrane and Zheng [1] (see also [6]), have shown that for any integers W and Z

$$\sum_{\chi \in \mathcal{X}_0} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \ll pZ^2 \left(\log p + \left(\log(Z^2/p) \right)^2 \right). \tag{5}$$

Note that for any fixed $\varepsilon > 0$, if $Z \geq p^\varepsilon$ the right hand side of (5) is of the form $pZ^{2+o(1)}$. However for small values of Z, namely for $Z \ll (\log p)^{1/2}$, the bound (5) is trivial. We now combine (5) with a result of [4] to get the bound $pZ^{2+o(1)}$ for any Z.

Lemma 1. *For arbitrary integers W and Z, with $0 \le W < W+Z < p$, the bound*

$$\sum_{\chi \in \mathcal{X}_0} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \ll p Z^{2+o(1)}$$

holds.

Proof. We can assume that $Z \le p^{1/4}$ since otherwise, as we have noticed, the bound (5) implies the desired result. Now, using that for z with $\gcd(z,p)=1$, for the complex conjugated character $\overline{\chi}$ we have

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

we derive,

$$\sum_{\chi \in \mathcal{X}_0} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \le \sum_{\chi \in \mathcal{X}} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 = \sum_{z_1,z_2,z_3,z_4=W+1}^{W+Z} \sum_{\chi \in \mathcal{X}} \chi(z_1 z_2 z_3^{-1} z_4^{-1})$$

Thus, using the orthogonality of characters we obtain

$$\sum_{\chi \in \mathcal{X}_0} \left| \sum_{z=W+1}^{W+Z} \chi(z) \right|^4 \le pJ$$

where J is number of solutions to the congruence

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

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

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

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

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 2. *Let $\mathcal{C}$ be an absolutely irreducible curve of degree $d \geq 2$ and $H \geq \exp(d^6)$. 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. *For any real numbers $T_1, \ldots, T_s$ with*

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

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

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

4 Bound on $N_\lambda(R, S; M)$

It is easy to see that for $\lambda \in \mathbb{F}_p^*$ the given curve is absolutely irreducible. So general bounds on the number of points on a curve in a given box (see, for example, [11]) immediately imply that

$$N_\lambda(R, S; M) = \frac{M^2}{p} + O\left(p^{1/2}(\log p)^2\right). \qquad (6)$$

We are now ready to derive an upper bound on $N_\lambda(R, S; M)$ for smaller values of M.

Lemma 4. *For any integers $p^{1/9} \geq M \geq 1$, $R \geq 0$, $S \geq 0$ with $R + M, S + M < p$ and $\lambda \in \mathbb{F}_p^*$ we have*

$$N_\lambda(R, S; M) \leq M^{1/3+o(1)}$$

as $M \to \infty$.

Proof. We have to estimate the number of solutions of the congruence

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

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

$$x^3 + 3Rx^2 + 3R^2x - \lambda y^2 - 2\lambda Sy \equiv \lambda S^2 - R^3 \pmod p. \tag{7}$$

By Lemma 3, for any $T \le p^{1/4}/M^{1/2}$ there exits $|t| \le T^4M^2$ such that

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

We now multiply both sides of the congruence (7) by t, replace the congruence with the following equation over $\mathbb{Z}$:

$$A_1x^3 + A_2x^2 + A_3x + A_4y^2 + A_5y + A_6 = pz, \tag{8}$$

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 the equation (8) is bounded by $T^4M^5 + 4pM/T + p/2$, we see that

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

We choose $T \sim p^{1/5}/M^{4/5}$ which leads to the bound $|z| \ll M^{9/5}p^{-1/5} + 1$.

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 (8) is absolutely irreducible. Indeed, it is obtained from $X^3 - \lambda Y^2$ (which, as it is easy to see, is absolutely irreducible) by a nontrivial modulo p affine transformation. Therefore, for every integers 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 is absolutely irreducible modulo p).

Now, for each z, we have an absolutely irreducible curve of degree 3 corresponding to the equation (8) and we apply Lemma 2 to derive that the number of points in $[0, M]^2$ is $\ll M^{1/3+o(1)}$.

Thus, the number of solutions in the original equation is bounded by $\left(M^{9/5}p^{-1/5} + 1\right) M^{1/3+o(1)}$. Recalling that $M \le p^{1/9}$, thus $M^{9/5}p^{-1/5} + 1 \ll 1$ we conclude the proof. $\square$

The example of the curves $E_{r,s}$ with $(r, s) = (m^2, m^3)$, $1 \le m \le M^{1/3}$, shows that the exponent 1/3 in the bound of Lemma 4 cannot be improved.

Clearly the argument used in the proof of Lemma 4 works for large values of M. In particular, for $M > p^{1/9}$ it leads to the bound $N_\lambda(R, S; M) \ll M^{32/15+o(1)}p^{-1/5}$ which is nontrivial for $M \le p^{3/17}$.

However, using a modification of this argument we can obtain a stronger bound which is nontrivial for $p^{1/9} < M \le p^{1/5}$:

Lemma 5. *For any integers $p^{1/5} \ge M \ge p^{1/9}$, $R \ge 0$, $S \ge 0$ with $R+M, S+M < p$ and $\lambda \in \mathbb{F}_p^*$ we have*

$$N_\lambda(R, S; M) \le M^{11/6+o(1)}p^{-1/6}$$

as $M \to \infty$.

Proof. Let $K = \lfloor p^{1/6}/M^{1/2} \rfloor$ and observe that $1 \le K \le M$ when $p^{1/9} < M$. Next, we cover the square $[R+1, R+M] \times [S+1, S+M]$ by $J = O(M/K)$ rectangles of the form $[R_j+1, R_j+K] \times [S+1, S+M]$, $j = 1, \dots, J$. Then, the equation in each rectangle can be written as

$$x^3 + 3R_jx^2 + 3R_j^2x - \lambda y^2 - 2\lambda Sy \equiv \lambda S^2 - R_j^3 \pmod p. \tag{9}$$

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

To estimate the number of solutions of (9), 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 again Lemma 3. Hence, as in the proof of Lemma 4, we obtain an equivalent equation over $\mathbb{Z}$:

$$A_1x^3 + A_2x^2 + A_3x + A_4y^2 + A_5y + A_6 = pz, \tag{10}$$

with $|A_i| \le T_i$ for $i = 1, \dots, 5$ and $|A_6| \le p/2$. The left hand side of (10) is bounded by

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

Thus, z can take at most 11 values. As we have seen in the proof of Lemma 4, the polynomial on the left hand side of (10) is absolutely irreducible. Therefore, Lemma 2 implies that for each value of z, the equation (10) has at most $M^{1/3+o(1)}$ solutions. Summing up all the solutions we have finally that the original congruence has

$$(M/N)M^{1/3+o(1)} = M^{11/6+o(1)}p^{-1/6}$$

solutions. □

Combining the bounds (6) with Lemmas 4 and 5, we obtain:

Theorem 6. *For any integers $M \geq 1$, $R \geq 0$, $S \geq 0$ with $R+M, S+M < p$, we have,*

$$N_\lambda(R,S;M) \ll M^{o(1)} \begin{cases} M^{1/3}, & \text{if } M < p^{1/9}, \\ M^{11/6}p^{-1/6}, & \text{if } p^{1/9} \leq M < p^{1/5}, \\ p^{1/2}, & \text{if } p^{1/2} \leq M < p^{3/4}, \\ M^2p^{-1}, & \text{if } p^{3/4} \leq M < p, \end{cases}$$

as $M \to \infty$

We note that unfortunately in the range $p^{1/5} \leq M < p^{1/2}$ we do not have any nontrivial estimates.

5 Bound on $T(R,S;M)$

In fact we consider a more general quantity. Given positive integers i, j let $T_{i,j}(R,S;M)$ denote the number of solutions of the equation

$$r^i v^j \equiv u^i s^j \pmod p \tag{11}$$

with

$$(r,s),(u,v) \in [R+1,R+M] \times [S+1,S+M].$$

Thus, $T(R,S;M) = T_{3,2}(R,S;M)$.

Theorem 7. *For any integers $M \geq 1$, $R \geq 0$, $S \geq 0$ with $R+M, S+M < p$, we have,*

$$T_{i,j}(R,S;M) \ll \frac{M^4}{p} + M^{2+o(1)}$$

as $M \to \infty$.

Proof. Using the orthogonality of characters, we write the the number of solutions to (11) with

$$(r, s), (u, v) \in [R + 1, R + M] \times [S + 1, S + M].$$

as

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

Thus by the Cauchy inequality

$$T_{i,j}(R, S; M)^2 \le \frac{1}{(p-1)^2} \sum_{\chi \in \mathcal{X}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \times \sum_{\chi \in \mathcal{X}} \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^4. \qquad (12)$$

We estimate the contribution to the first sums from at most i characters χ with $\chi^i = \chi_0$ trivially as iM^4 getting

$$\sum_{\chi \in \mathcal{X}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \le iM^4 + \sum_{\substack{\chi \in \mathcal{X} \\ \chi^i \ne \chi_0}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^4 \le iM^4 + i \sum_{\chi \in \mathcal{X}^*} \left| \sum_{r=R+1}^{R+M} \chi(r) \right|^4.$$

Substituting the above bounds in the inequality (12) (similarly for j) and then using Lemma 1 we conclude the proof. $\square$

Corollary 8. *For any integers $M \ge 1$, $R \ge 0$, $S \ge 0$ with $R+M, S+M < p$, we have,*

$$I(R, S; M) \gg \min\left\{p, M^{2-o(1)}\right\}$$

as $M \to \infty$

Proof. Let

$$\Gamma = \{r^3/s^2 : \ r \in [R+1, R+M], \ s \in [S+1, S+M]\}$$

and let

$$f(\lambda) = |\{(r, s) \in [R+1, R+M] \times [S+1, S+M] : \ r^3/s^2 = \lambda\}|.$$

Using the Cauchy inequality we derive

$$M^4 = \left(\sum_{\lambda \in \Gamma} f(\lambda) \right)^2 \leq |\Gamma| \sum_{\lambda} f^2(\lambda) \leq I(R, S; M) T_{3,2}(R, S; M).$$

Using Theorem 7 we conclude the proof. □

Clearly the bound of Corollary 8 is quite tight as we have the trivial upper bound

$$I(R, S; M) \leq \min \left\{ p, M^2 \right\}.$$

6 Comments and Open Problems

Note that Theorem 7 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 (6) also holds for such rectangles).

As we have mentioned the exponent $1/3$ in the bound of Lemma 4 cannot be improved, however the range $M \leq p^{1/9}$ can possibly be extended. As the first step towards this, the following question has to be answered:

Problem 1. *Let E be an elliptic curve over $\mathbb{Z}$ 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 4 we do not have any nontrivial bounds on $N_\lambda(R, S; M)$ for $p^{1/5} \leq M < p^{1/2}$. It is certainly interesting to close this gap.

Problem 2. *Is it true that $N_\lambda(R, S; M) = o(M)$ for all $M = o(p)$?*

Finally, it is also natural to expect that the term $M^{o(1)}$ can be removed from the bound of Corollary 8.

Problem 3. *Is it true that $I(R, S; M) \gg \min \{p, M^2\}$?*

Acknowledgement

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 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. and Func. Anal.* (to appear).

[5] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Preprint*, 2011, 1–18.

[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. Notices* **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] 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.

[12] A. Zumalacárregui, 'Concentration of points on modular quadratic forms', *Inter. J. Number Theory*, (to appear).