BULL. AUSTRAL. MATH. SOC. 14H52, 11T23, 94A60
VOL. 66 (2002) [353–358]

AVERAGE NORMALISATIONS OF ELLIPTIC CURVES

WILLIAM D. BANKS AND IGOR E. SHPARLINSKI

Ciet, Quisquater, and Sica have recently shown that every elliptic curve E over a finite field $\mathbb{F}_p$ is isomorphic to a curve $y^2 = x^3 + ax + b$ with a and b of size $O(p^{3/4})$. In this paper, we show that almost all elliptic curves satisfy the stronger bound $O(p^{2/3})$. The problem is motivated by cryptographic considerations.

1. INTRODUCTION

Let $p > 3$ be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements, which we identify with the set $\{0, 1, 2, \ldots, p-1\}$. For any $a, b \in \mathbb{F}_p$ with $4a^3 + 27b^2 \neq 0$, let $E(a, b)$ be the elliptic curve over $\mathbb{F}_p$ given by the equation $y^2 = x^3 + ax + b$. Since every elliptic curve E is isomorphic to some $E(a, b)$, the invariant

$$\mu(E) = \min\big\{ \max\{a, b\} \,\big|\, a, b \in \mathbb{F}_p,\ E(a, b) \cong E \big\},$$

is a positive integer that is well-defined on isomorphism classes of elliptic curves over $\mathbb{F}_p$.

For many cryptographic applications, or when performing other calculations on elliptic curves where efficiency is an issue, it is often desirable to work with curves $E \cong E(a, b)$ where the coefficients a and b are very small relative to the prime p. Since every elliptic curve E is isomorphic to some $E(a, b)$ with $0 \leqslant a, b \leqslant \mu(E)$, this leads naturally to the problem of estimating the size of $\mu(E)$. This question has been recently considered in [2], where it is shown that $\mu(E) = O(p^{3/4})$ for all elliptic curves E over $\mathbb{F}_p$, with an effectively computable constant. A very similar result has also been obtained in [4]. In this paper, we shall show that for a "randomly chosen" elliptic curve E, one can improve this to $\mu(E) = O(p^{2/3})$; for a precise statement, see Theorem 1 in Section 3 below.

As in [2], we use exponential sums, but our scheme is somewhat different. For example, our proof does not use the Weil bound and can therefore be extended to "elliptic curves" over arbitrary residue rings. In our estimates, we give explicit constants which hold for any prime $p > 2^{35}$. By using more sophisticated techniques and better (known)

Received 10th September, 2001
The authors want to thank Francesco Pappalardi for useful discussions. The first author would also like to thank Macquarie University for its hospitality during the preparation of this paper. Work supported in part by NSF grant DMS-0070628 (W. Banks) and by ARC grant A00000184 (I. Shparlinski).

bounds, one can easily both improve the constants and lower the limit 2^{35}; this is particularly true for primes in certain congruence classes modulo 4 or 6. In any case, the condition $p > 2^{35}$ is irrelevant for most cryptographic applications, since primes used in such constructions are typically several hundred bits long.

2. General Estimates

Throughout this section, let $p > 3$ be a fixed prime number, and define $\mathbf{e}(x) = e^{2\pi i x/p}$ for all $x \in \mathbb{F}_p$. Then

$$p^{-1} \sum_{\lambda \in \mathbb{F}_p} \mathbf{e}(\lambda x) = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{if } x \in \mathbb{F}_p^*. \end{cases} \tag{1}$$

Lemma 1. *For every integer $n > 2$ and all $a \in \mathbb{F}_p^*$, the following inequality holds:*

$$\left| \sum_{u \in \mathbb{F}_p} \mathbf{e}(au^n) \right| \leqslant \big(\gcd(n, p-1) - 1\big) p^{1/2}.$$

Proof: See [7, Exercise 11b in Chapter VI]. □

Lemma 2. *For every positive integer h, the following inequality holds:*

$$\sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{\nu=0}^{h-1} \mathbf{e}(\lambda \nu) \right| \leqslant p \ln p.$$

Proof: See [7, Exercise 11c in Chapter III]. □

Lemma 3. *For all $b \in \mathbb{F}_p^*$, $d \in \mathbb{F}_p$, and $1 \leqslant h \leqslant p$, let*

$$\mathcal{U}_{b,d,h} = \{u \in \mathbb{F}_p^* \mid 0 \leqslant bu^6 + d < h\}.$$

Then

$$\big|\#\mathcal{U}_{b,d,h} - h\big| < 6p^{1/2} \ln p.$$

Proof: Using (1), we have

$$\begin{aligned} \#\mathcal{U}_{b,d,h} &= \sum_{u \in \mathbb{F}_p^*} \sum_{\nu=0}^{h-1} p^{-1} \sum_{\lambda \in \mathbb{F}_p} \mathbf{e}\big(\lambda(bu^6 + d - \nu)\big) \\ &= h(1 - p^{-1}) + p^{-1} \sum_{\lambda \in \mathbb{F}_p^*} \mathbf{e}(\lambda d) \sum_{u \in \mathbb{F}_p^*} \mathbf{e}(\lambda b u^6) \sum_{\nu=0}^{h-1} \mathbf{e}(-\lambda \nu) \end{aligned}$$

Since $1 \leqslant h \leqslant p$, it follows that

$$\big|\#\mathcal{U}_{b,d,h} - h\big| \leqslant 1 + p^{-1} \sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{u \in \mathbb{F}_p^*} \mathbf{e}(\lambda b u^6) \right| \left| \sum_{\nu=0}^{h-1} \mathbf{e}(\lambda \nu) \right|. \tag{2}$$

https://doi.org/10.1017/S0004972700040211 Published online by Cambridge University Press

By Lemma 1, we have for all $\lambda \in \mathbb{F}_p^*$:

$$\left|\sum_{u\in\mathbb{F}_p^*} \mathbf{e}(\lambda b u^6)\right| \leqslant 1 + \left|\sum_{u\in\mathbb{F}_p} \mathbf{e}(\lambda b u^6)\right| \leqslant 1 + 5p^{1/2}.$$

Using this inequality in (2) and applying Lemma 2, we have

$$\left|\#\mathcal{U}_{b,d,h} - h\right| \leqslant 1 + p^{-1}(1 + 5p^{1/2})(p \ln p) < 6p^{1/2} \ln p,$$

and the lemma is proved. □

LEMMA 4. *For all $a, b \in \mathbb{F}_p^*$, $c, d \in \mathbb{F}_p$, and $1 \leqslant h \leqslant p$, let*

$$\mathcal{V}_{a,b,c,d,h} = \{u \in \mathbb{F}_p^* \mid 0 \leqslant au^4 + c,\ bu^6 + d < h\}.$$

If c, d and h are fixed, then for any $0 < \delta < 1$, $\mathcal{V}_{a,b,c,d,h}$ is empty for fewer than $\delta p(p-1)$ pairs $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ provided that $p > 2^{35}$ and $h \geqslant 4\delta^{-2/3}p^{2/3}$.

PROOF: Let $b \in \mathbb{F}_p^*$, and note that for every $a \in \mathbb{F}_p^*$,

$$\mathcal{V}_{a,b,c,d,h} = \{u \in \mathcal{U}_{b,d,h} \mid 0 \leqslant au^4 + c < h\},$$

where $\mathcal{U}_{b,d,h}$ is defined as in Lemma 3. Put $k = \lfloor h/2 \rfloor$, and let $\mathcal{N}_{a,b,c,d,h}$ be the number of solutions to the relation $au^4 + c = k + \nu_1 - \nu_2$ with $u \in \mathcal{U}_{b,d,h}$ and $0 \leqslant \nu_1, \nu_2 < k$. Clearly, $\mathcal{N}_{a,b,c,d,h} > 0$ implies that $\mathcal{V}_{a,b,c,d,h}$ is non-empty.

Using (1), we have

$$\begin{aligned}\mathcal{N}_{a,b,c,d,h} &= \sum_{u\in\mathcal{U}_{b,d,h}} \sum_{\nu_1,\nu_2=0}^{k-1} p^{-1} \sum_{\lambda\in\mathbb{F}_p} \mathbf{e}\big(\lambda(au^4 + c - k - \nu_1 + \nu_2)\big) \\ &= \#\mathcal{U}_{b,d,h}\cdot k^2 p^{-1} + p^{-1} \sum_{\lambda\in\mathbb{F}_p^*} \mathbf{e}\big(\lambda(c-k)\big) \sum_{u\in\mathcal{U}_{b,d,h}} \mathbf{e}(\lambda a u^4) \left|\sum_{\nu=0}^{k-1} \mathbf{e}(\lambda\nu)\right|^2.\end{aligned}$$

Thus,

$$\left|\mathcal{N}_{a,b,c,d,h} - \#\mathcal{U}_{b,d,h}\cdot k^2 p^{-1}\right| \leqslant p^{-1} \sum_{\lambda\in\mathbb{F}_p^*} \left|\sum_{u\in\mathcal{U}_{b,d,h}} \mathbf{e}(\lambda a u^4)\right| \left|\sum_{\nu=0}^{k-1} \mathbf{e}(\lambda\nu)\right|^2$$

Summing over all $a \in \mathbb{F}_p^*$, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_p^*} \left|\mathcal{N}_{a,b,c,d,h} - \#\mathcal{U}_{b,d,h}\cdot k^2 p^{-1}\right| &\leqslant p^{-1} \sum_{\lambda\in\mathbb{F}_p^*} \sum_{a\in\mathbb{F}_p^*} \left|\sum_{u\in\mathcal{U}_{b,d,h}} \mathbf{e}(\lambda a u^4)\right| \left|\sum_{\nu=0}^{k-1} \mathbf{e}(\lambda\nu)\right|^2 \\ &= p^{-1} \sum_{a\in\mathbb{F}_p^*} \left|\sum_{u\in\mathcal{U}_{b,d,h}} \mathbf{e}(au^4)\right| \cdot \sum_{\lambda\in\mathbb{F}_p^*} \left|\sum_{\nu=0}^{k-1} \mathbf{e}(\lambda\nu)\right|^2.\end{aligned}$$

https://doi.org/10.1017/S0004972700040211 Published online by Cambridge University Press

Using the Cauchy inequality, we estimate

$$\begin{aligned}\Big(\sum_{a\in\mathbb{F}_p^*}\Big|\sum_{u\in\mathcal{U}_{b,d,h}}\mathbf{e}(au^4)\Big|\Big)^2 &< p\sum_{a\in\mathbb{F}_p}\Big|\sum_{u\in\mathcal{U}_{b,d,h}}\mathbf{e}(au^4)\Big|^2\\ &= p\sum_{a\in\mathbb{F}_p}\sum_{u_1,u_2\in\mathcal{U}_{b,d,h}}\mathbf{e}\big(a(u_1^4-u_2^4)\big)\\ &= p^2\sum_{u_1,u_2\in\mathcal{U}_{b,d,h}}p^{-1}\sum_{a\in\mathbb{F}_p}\mathbf{e}\big(a(u_1^4-u_2^4)\big)\\ &= p^2\,\#\{u_1,u_2\in\mathcal{U}_{b,d,h}\mid u_1^4=u_2^4\}\\ &\leqslant 4p^2\#\mathcal{U}_{b,d,h}.\end{aligned}$$

Also,

$$\begin{aligned}\sum_{\lambda\in\mathbb{F}_p^*}\Big|\sum_{\nu=0}^{k-1}\mathbf{e}(\lambda\nu)\Big|^2 &< \sum_{\lambda\in\mathbb{F}_p}\Big|\sum_{\nu=0}^{k-1}\mathbf{e}(\lambda\nu)\Big|^2\\ &= \sum_{\lambda\in\mathbb{F}_p}\sum_{\nu_1,\nu_2=0}^{k-1}\mathbf{e}\big(\lambda(\nu_1-\nu_2)\big)\\ &= p\sum_{\nu_1,\nu_2=0}^{k-1}p^{-1}\sum_{\lambda\in\mathbb{F}_p}\mathbf{e}\big(\lambda(\nu_1-\nu_2)\big)=pk.\end{aligned}$$

Consequently,

$$\sum_{a\in\mathbb{F}_p^*}\big|\mathcal{N}_{a,b,c,d,h}-\#\mathcal{U}_{b,d,h}\cdot k^2p^{-1}\big|<2pk(\#\mathcal{U}_{b,d,h})^{1/2}. \tag{3}$$

Now let $\mathcal{B}_\delta$ be the set of elements $a\in\mathbb{F}_p^*$ such that

$$\big|\mathcal{N}_{a,b,c,d,h}-\#\mathcal{U}_{b,d,h}\cdot k^2p^{-1}\big|\geqslant 2\delta^{-1}k(\#\mathcal{U}_{b,d,h})^{1/2}.$$

From (3), it follows that $\#\mathcal{B}_\delta<\delta p$. On the other hand, for all $a\in\mathbb{F}_p^*\backslash\mathcal{B}_\delta$, we have

$$\mathcal{N}_{a,b,c,d,h}>\#\mathcal{U}_{b,d,h}\cdot k^2p^{-1}-2\delta^{-1}k(\#\mathcal{U}_{b,d,h})^{1/2},$$

hence $\mathcal{N}_{a,b,c,d,h}>0$ (and $\mathcal{V}_{a,b,c,d,h}$ is non-empty) provided that

$$\#\mathcal{U}_{b,d,h}\geqslant 4\delta^{-2}k^{-2}p^2. \tag{4}$$

Since h is an integer, we have

$$k=\lfloor h/2\rfloor\geqslant(h-1)/2\geqslant 2\delta^{-2/3}p^{2/3}-1/2>3^{1/2}\delta^{-2/3}p^{2/3}.$$

Hence the right hand side of (4) is less than

$$4\delta^{-2}(3^{1/2}\delta^{-2/3}p^{2/3})^{-2}p^2=(4/3)\delta^{-2/3}p^{2/3}\leqslant h/3.$$

On the other hand, by Lemma 3, the left hand side of (4) is greater than $h-6p^{1/2}\ln p$, and this is at least $h/3$ provided that $h\geqslant 9p^{1/2}\ln p$. Since $\delta<1$, this condition holds whenever $4p^{2/3}\geqslant 9p^{1/2}\ln p$, hence for all primes $p>2^{35}$. The result now follows. □

https://doi.org/10.1017/S0004972700040211 Published online by Cambridge University Press

3. Main Result

We are now able to prove our main result.

We say that an elliptic curve E is *typical* if $E \cong E(a,b)$ with $a, b \in \mathbb{F}_p^*$; otherwise (that is, if $ab = 0$) we say that E is *atypical*. It is well-known that there are precisely $(2p-4)$ distinct isomorphism classes of typical elliptic curves over $\mathbb{F}_p$, while the number of atypical isomorphism classes is

$$\gcd(4, p-1) + \gcd(6, p-1) \leqslant 10.$$

Theorem 1. *If $p > 2^{35}$, then for any $0 < \delta < 1$, the bound $\mu(E) > 4\delta^{-2/3}p^{2/3}$ holds for fewer than $2\delta p$ distinct isomorphism classes of typical elliptic curves.*

Proof: The isomorphism classes of typical elliptic curves over $\mathbb{F}_p$, collectively denoted here by Λ, are in bijection with the set

$$\mathcal{S} = \left\{(a,b) \in \mathbb{F}_p^* \times \mathbb{F}_p^* \mid 4a^3 + 27b^2 \neq 0\right\}$$

modulo the equivalence relation on $\mathcal{S}$ defined by: $(a,b) \sim (a',b')$ if and only if $a' = au^4$ and $b' = bu^6$ for some $u \in \mathbb{F}_p^*$. The correspondence between $\mathcal{S}/\sim$ and Λ is given by $(a,b) \leftrightarrow E(a,b)$.

In the notation of Lemma 4, take $c = d = 0$, let $0 < \delta < 1$, and put $h = \lfloor 4\delta^{-2/3}p^{2/3} \rfloor + 1$. Observe that

$$\#\mathcal{V}_{a,b,c,d,h} = \#\mathcal{V}_{a',b',c,d,h}$$

for all $(a,b), (a',b') \in \mathcal{S}$ with $(a,b) \sim (a',b')$. Thus, the function F given by

$$F(E) = \#\mathcal{V}_{a,b,c,d,h}, \qquad \text{if } E \cong E(a,b),$$

is well-defined on Λ. Note that $F(E) \neq 0$ implies $\mu(E) \leqslant h - 1 \leqslant 4\delta^{-2/3}p^{2/3}$.

Now by Lemma 4, $\mathcal{V}_{a,b,c,d,h}$ is empty for fewer than $\delta p(p-1)$ elements of $\mathcal{S} \subset \mathbb{F}_p^* \times \mathbb{F}_p^*$. Since every equivalence class in $\mathcal{S}$ contains precisely $(p-1)/2$ elements, $F(E) = 0$ for fewer than $2\delta p$ classes $E \in \Lambda$. ∎

4. Remarks

It is easy to see that for any $\gamma > 16^{1/3} = 2.519\ldots$ and all sufficiently large p (depending on γ), the bound $\mu(E) > \gamma\delta^{-2/3}p^{2/3}$ holds for fewer than $2\delta p$ distinct isomorphism classes of typical elliptic curves.

One can also identify $\mathbb{F}_p$ with the set $\{0, \pm 1, \pm 2, \ldots, \pm(p-1)/2\}$ and define

$$\mu_0(E) = \min\left\{\max\{|a|, |b|\} \mid a, b \in \mathbb{F}_p,\ E(a,b) \cong E\right\}.$$

Then the result of Theorem 1 extends to $\mu_0(E)$ with slightly better values for the constants.

https://doi.org/10.1017/S0004972700040211 Published online by Cambridge University Press

The arguments of [2] show that the bounds $\mu(E) = o(p^{1/2})$ and $\mu_0(E) = o(p^{1/2})$ cannot be valid for almost all typical elliptic curves. It would be very interesting to narrow the gap between this lower bound of order $p^{1/2}$ and our upper bound of order $p^{2/3}$.

We also remark that in the case of atypical curves much stronger results can be obtained with the help of character sums. Indeed, the Burgess bound on character sums implies that $\mu(E) = O(p^{1/4})$. In fact, using the results of [3] or [5] one can easily derive that for such curves $\mu(E) = O(p^{1/4-c})$ for some non-negative $c > 0$. Also, from the bound of multiplicative character sums in Chapter 13 of [6], which holds under the assumption of the Extended Riemann Hypothesis, one can derive that $\mu(E) = o(\psi(p)\log^2 p)$ for any function $\psi(p) \to \infty$.

Finally, it would be very interesting to see whether our arguments could be combined with the methods of [4] to improve the error term in the asymptotic formula given in [4]. We recall that the results of [4] are also based on studying "small" representatives in the same family of curves that we consider in this paper. Although the obvious attack on this question fails, we hope that by further developing our arguments, such a goal might be attained.

References

[1] D.A. Burgess, 'The distribution of quadratic residues and non-residues', *Mathematika* **4** (1957), 106–112.

[2] M. Ciet, J.-J. Quisquater and F. Sica, 'Elliptic curve normalization', in *Crypto Group Technical Report Series CG-2001/2* (Univ. Catholique de Louvain, Belgium, 2001), **pp.** 1–13.

[3] P.D.T.A. Elliott,, 'Some remarks about multiplicative functions of modulus $\leqslant 1$', in *Analytic Number Theory*, Progr. Math. **85** (Birkhäuser, Boston, MA, 1990), **pp.** 159–164.

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

[5] A. Hildebrand, 'A note on Burgess' character sum estimate', *C. R. Math. Rep. Acad. Sci. Canada* **8** (1986), 35–37.

[6] H.L. Montgomery, *Topics in multiplicative number theory*, Lect. Notes in Math. **227** (Spinger-Verlag, Berlin, 1971).

[7] I.M. Vinogradov, *Elements of number theory* (Dover Publ., New York, 1954).

Department of Mathematics
University of Missouri
Columbia, MO 65211
United States of America
e-mail: bbanks@math.missouri.edu

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