Bulletin of the Institute of Mathematics
Academia Sinica (New Series)
Vol. **9** (2014), No. 4, pp. 657-670

GENERATORS OF ELLIPTIC CURVES OVER FINITE FIELDS

IGOR E. SHPARLINSKI[1,a] AND JOSÉ FELIPE VOLOCH[2,b]

[1]Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia.
[a]E-mail: igor.shparlinski@unsw.edu.au
[2]Department of Mathematics, University of Texas, Austin, TX 78712, USA.
[b]E-mail: voloch@math.utexas.edu

Abstract

We prove estimates on character sums on the subset of points of an elliptic curve over $\mathbb{F}_{q^n}$ with x-coordinate of the form $\alpha + t$ where $t \in \mathbb{F}_q$ varies and fixed α is such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. We deduce that, for a suitable choice of α, this subset has a point of maximal order in $E(\mathbb{F}_{q^n})$. This provides a deterministic algorithm for finding a point of maximal order which for a very wide class of finite fields is faster than other available algorithms.

1. Introduction

As usual, for a prime power q we use $\mathbb{F}_q$ to denote the finite field of q elements. We study elliptic curves over extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$.

Let E be an elliptic curve given by an affine Weierstraß equation

$$y^2 = x^3 + ax^2 + bx + c$$

with some $a, b, c \in \mathbb{F}_{q^n}$ where q is assumed odd. We recall that the set of all points on E forms an abelian group with the "point at infinity" $\mathcal{O}$ as the neutral element (see [27] for background). Denoting by $E(\mathbb{F}_{q^n})$ the set of $\mathbb{F}_{q^n}$-rational points on E, we have

$$\#E(\mathbb{F}_{q^n}) \cong \mathbb{Z}/M \times \mathbb{Z}/L$$

Received November 25, 2013 and in revised form June 6, 2014.
AMS Subject Classification: Primary 11G20, 11Y16; Secondary 11T23.
Key words and phrases: Elliptic curves, generators, finite fields.

for for unique integers M and L with $L \mid M$ and $\#E(\mathbb{F}_{q^n}) = ML$. The number M is called the *exponent* of $E(\mathbb{F}_{q^n})$. Points $P \in E(\mathbb{F}_{q^n})$ of order M are called *points of maximum order*.

We recall, that the celebrated work of Schoof [23] provides an algorithm that computes $\#E(\mathbb{F}_{q^n})$ in deterministic polynomial time, see also [1] for more recent improvements (both theoretic and practical). Computing the group structure, that is, the numbers, M and L has also been considered in the literature and has turned out to be more difficult. In particular, a probabilistic algorithm of Miller [19] runs in expected polynomial time plus the time needed to factor $\gcd(\#E(\mathbb{F}_q), q-1)$, see also [4]. Furthermore, Friedlander, Pomerance and Shparlinski [12] have shown that for a sufficiently large prime p and for almost all elliptic curves E over $\mathbb{F}_p$, the factorisation part of the algorithm is in fact less time consuming than the rest of the computation (since $\gcd(\#E(\mathbb{F}_q), q-1)$ tends to be rather small). On the other hand, in some case this greatest common divisor is large and is difficult to factor.

The deterministic algorithm of [17] computes the group structure of any elliptic curve over $\mathbb{F}_q$ (and in fact produces two generators of the group of points) in exponential time $O(q^{1/2+o(1)})$ which is too slow for practical applications.

Here we show that, for high degree extensions $\mathbb{F}_{q^n}$ of finite fields $\mathbb{F}_q$, one can design a deterministic polynomial time algorithm, which generates a small set $\mathcal{G}$ of points on $E(\mathbb{F}_{q^n})$ such that at least one point $P \in \mathcal{G}$ is of maximum order. We remark that this is an elliptic curve analogue of the results of [7, 24, 25] (see also [26, Theorem 8]).

The idea is to show that if $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ for some root α of an irreducible polynomial of degree n over $\mathbb{F}_q$, then one can find a point $P \in E(\mathbb{F}_{q^n})$ of maximum order with $x(P) = \alpha + t$ for some $t \in \mathbb{F}_q$, where as usual, we write every point $P \neq \mathcal{O}$ on E as $P = (x(P), y(P))$. In turn, this result is based on a new estimate of character sums over points P of an elliptic curve with x coordinates of the form $x(P) = \alpha + t$. These estimates are analogues of those of Carlitz [5] and Katz [16]. We note that if a finite field $\mathbb{F}_r$ is of the form $r = q^n$ with appropriate q and n, then the above argument immediately gives an explicit construction of a small set of points on $E(\mathbb{F}_r)$ which contains a point of an appropriate order. In the case that r is not of a suitable form (and thus $\mathbb{F}_r$ does not have a desired subfield), we use the same

approach as in [25]. More precisely, we first build an extension $\mathbb{F}_{r^m}$ which has a necessary subfield, apply our construction construction to $E(\mathbb{F}_{r^m})$ and then use the trace map to come back to points on $E(\mathbb{F}_r)$.

The setup is similar to Frey's Weil descent attack on the discrete logarithm problem on elliptic curves and related work on the index calculus on semi-abelian varieties, (see [2, 8, 9, 10, 13, 15] and references therein). Namely, there they consider a curve inside an abelian variety and use the set of rational points of the curve as a factor base for the index calculus algorithm. In initial works on this problem it simply has been assumed that the factor base generated the group or at least its reasonable "massive" subgroup (which is also quite enough for the index calculus applications). The first rigorous proof that this is so for curves embedded in their Jacobians, under suitable conditions, has been given in [29] and then reproved in [15] (see also [20, Theorem 4]). We also prove this in our setup, but we are actually proving a much stronger statement. Namely, when the group is cyclic, we prove that a single point from the curve is a generator (rather than just that the points on the curve is a generating set) and, in general, that there is a point on the curve with maximal order on the group. Our approach to prove this is based on bounds for character sums, which is a classical idea in number theory that dates back to Vinogradov [28], (see also [21, Chapter 2] for an outline of several related results).

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' are absolute (we recall that the notation $U \ll V$ is equivalent to $U = O(V)$).

2. Character Sum Bound

Denote by $R_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ the Weil restriction of scalars functor (see, for example, [11]) which, for a variety $X/\mathbb{F}_{q^n}$, gives a variety $R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(X)$ over $\mathbb{F}_q$. The choice of a basis for $\mathbb{F}_{q^n}/\mathbb{F}_q$ defines an isomorphism of varieties defined over $\mathbb{F}_q$, between $R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{A}^1)$ (where the affine line $\mathbb{A}^1$ is viewed as one-dimensional variety over $\mathbb{F}_{q^n}$) and $\mathbb{A}^n$ over $\mathbb{F}_q$.

Let α be such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. The basis $1, \alpha, \dots, \alpha^{n-1}$ then gives us an isomorphism as above and we consider the map of varieties over $\mathbb{F}_q$, $\mathbb{A}^1 \to R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{A}^1)$ given by $t \mapsto \alpha + t$.

This map, $t \mapsto \alpha + t$ extends to a map of projective varieties over $\mathbb{F}_q$:

$$\psi_\alpha : \mathbb{P}^1 \to R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{P}^1)$$

where $\mathbb{P}_1$ is a projective line over $\mathbb{F}_{q^n}$. We remark that, over $\mathbb{F}_{q^n}$, we have the isomorphism $R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{P}^1) \simeq (\mathbb{P}^1)^n$.

We denote $A = R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ and let $\pi : A \to R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{P}^1)$ be the map, defined over $\mathbb{F}_q$, induced by $x : E \to \mathbb{P}^1$. Let also $C_\alpha \subseteq A$ be the curve

$$C_\alpha = \pi^{-1}(\psi_\alpha(\mathbb{P}^1)). \tag{1}$$

The curve C_α is defined over $\mathbb{F}_q$. Over $\mathbb{F}_{q^n}$ the cover $C_\alpha \to \mathbb{P}^1$ is given by the system of equations

$$y_i^2 = h_i(t), \qquad i = 1, \dots, n,$$

where

$$h_i(T) = (T + \alpha^{(i)})^3 + a^{(i)}(T + \alpha^{(i)})^2 + b^{(i)}(T + \alpha^{(i)}) + c^{(i)} \in \mathbb{F}_{q^n}[T], \tag{2}$$

and we denote by $\gamma^{(i)}$, $i = 1, \dots, n$, the conjugates of $\gamma \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is, $\gamma^{(i)} = \gamma^{q^i}$. We also use $A(\mathbb{F}_q)$ and $C_\alpha(\mathbb{F}_q)$ to denote the set of $\mathbb{F}_q$-rational points on A and C_α respectively.

Theorem 1. *If the polynomials $h_1, \dots, h_n$ given by (2) are pairwise relatively prime then, for any non-trivial character χ of $A(\mathbb{F}_q)$, we have*

$$\sum_{P \in C_\alpha(\mathbb{F}_q)} \chi(P) \ll n 2^n q^{1/2}.$$

Proof. If $h_1, \dots, h_n$ are pairwise relatively prime, then the cover $C_\alpha \to \mathbb{P}^1$ has geometric Galois group $(\mathbb{Z}/2)^n$, as the polynomials $h_1, \dots, h_n$ are independent modulo squares. It follows that C_α is absolutely irreducible under these conditions. Furthermore, the zeros of each h_i and the point at infinity have 2^{n-1} pre-images in C_α all with ramification index 2. We check this at infinity, the other cases are similar and easier. On the curve given by $y_1^2 = h_1(t)$, the function $u = t/y_1$ is a local parameter at the unique point at infinity and $t = u^{-2} + \dots$ there. So infinity is ramified with ramification index 2 on the cover of this curve to $\mathbb{P}^1$. For each of 2^{n-1} choices of sign,

there is a solution to $y_i^2 = h_i(t)$, $i > 1$, in power series in u of the form $y_i = \pm u^{-3} + \ldots$, which give the 2^{n-1} pre-images of infinity in C_α. It follows from the Hurwitz formula that the genus of (the normalization of) C_α is $2^{n-1}(3n-1)+1$.

If we prove that χ induces a non-trivial character on the divisor class group of C_α with trivial conductor, the bound on the theorem follows from this and the Weil bound (see, for example, [17]).

Let J be the Jacobian of (the normalization of) C_α. The inclusion $C_\alpha \to A$ induces $f_* : J \to A$, $f^* : A \to J$ with $f_* \circ f^* = [2^{n-1}]$ on A (see [8, Theorem 1]). If χ has odd order, it automatically follows from this that $\chi \circ f_*$ is non-trivial.

We show that our condition on χ is satisfied if $q^{1/2} \gg n2^n$. Note that the bound in the theorem is trivial otherwise. To handle the case of general χ, it is enough to consider the case of characters of order two. As $A(\mathbb{F}_q) \simeq E(\mathbb{F}_{q^n})$, the set of characters of order two has zero, one or three elements and corresponds to maps $E(\mathbb{F}_{q^n}) \to \mathbb{F}_{q^n}^*/(\mathbb{F}_{q^n}^*)^2, (x,y) \mapsto (x-\beta) \bmod (\mathbb{F}_{q^n}^*)^2$, where β is a root of $x^3 + ax^2 + bx + c$ in $\mathbb{F}_{q^n}$.

It is enough to show that there exists $t \in \mathbb{F}_q$ with $t + \alpha - \beta$ not a square in $\mathbb{F}_{q^n}$ and such that $t + \alpha$ lifts to a point P in C_α, since we have $\chi(P) \neq 1$ by construction. We must show that the cover of C_α given by the additional equation $y^2 = k(t)$ has an affine point with $y \neq 0$, where

$$k(t) = c \prod_{i=0}^{n-1} (t + (\alpha - \beta)^{q^i})$$

and c is not a square in $\mathbb{F}_q$. The condition that the h_i are pairwise relatively prime implies that $k(t)$ has distinct roots and this cover is an unramified double cover of C_α. Thus it has genus $O(n2^n)$, so a point as required exists by the Weil bound if $q^{1/2} \gg n2^n$. As noted above, this suffices. □

Remark 2. The curve C_α is not always absolutely irreducible. Here is an example

$$q = n = 3, \qquad E : y^2 = x^3 - x, \qquad \alpha^3 - \alpha = -1.$$

Then $h_1 = h_2$ and $C_\alpha(\mathbb{F}_3) = \{\mathcal{O}\}$, so some condition on α is needed.

Using an elliptic curve of the same equation but now $q = n = p > 3$, p prime, $\alpha^p - \alpha = c$, where c is a non-square in $\mathbb{F}_p$, we get an example where C_α is absolutely irreducible and, yet, we still have $C_\alpha(\mathbb{F}_p) = \{\mathcal{O}\}$. The reason this time is that $\mathrm{Norm}_{\mathbb{F}_{p^p}/\mathbb{F}_p}((t+\alpha)^3 - (t+\alpha)) = c^3$, $t \in \mathbb{F}_p$, so $E(\mathbb{F}_{p^p})$ has no point with x-coordinate $t + \alpha, t \in \mathbb{F}_p$.

3. Construction

We always assume that we are given an element $\vartheta \in \mathbb{F}_{q^n}$ with $\mathbb{F}_q(\vartheta) = \mathbb{F}_{q^n}$.

Theorem 3. *For any $\varepsilon > 0$, sufficiently large prime power q, and integer n with*

$$n \le \left(\frac{1}{2\log 2} - \varepsilon\right)\log q$$

and any set $\mathcal{R} \subset \mathbb{F}_q$ of size $\#\mathcal{R} = 9n+1$ there is $r \in \mathcal{R}$ such that for $\alpha = r\vartheta$ there is $P \in C_\alpha(\mathbb{F}_q)$ of maximum order as an element of $A(\mathbb{F}_q)$.

Proof. For $\alpha \in \mathbb{F}_{q^n}$ we denote by N_α^* the number of points $P \in C_\alpha(\mathbb{F}_q)$ of maximum order M as an element of $A(\mathbb{F}_q)$. Furthermore, for $d \mid M$, we also use $L_{\alpha,d}$ to denote the number of points of order dividing M/d.

Then, using the inclusion-exclusion principle, we see that for any integer $k \ge 1$, the following inequality holds:

$$N_\alpha^* \ge \#C_\alpha(\mathbb{F}_q) + \sum_{\nu=1}^{2k+1} \sum_{\substack{d \mid M \\ \omega(d)=\nu}} \mu(d) L_{\alpha,d}. \tag{3}$$

where $\omega(d)$ and $\mu(d)$ denote the number of distinct prime factors and the Möbius function of d, respectively.

Let $\mathcal{X}_d$ be the set of characters χ of $A(\mathbb{F}_q)$ of order dividing d; that is, such that $\chi^d = \chi_0$, where χ_0 is the principal character. By the orthogonality property of characters,

$$\frac{1}{\#\mathcal{X}_d} \sum_{\chi \in \mathcal{X}_d} \chi(P) = \begin{cases} 1, & \text{if } P = dQ \text{ for some } Q \in A(\mathbb{F}_q), \\ 0, & \text{otherwise.} \end{cases}$$

we write

$$L_{\alpha,d} = \frac{1}{\#\mathcal{X}_d} \sum_{\chi \in \mathcal{X}_d} \sum_{P \in C_\alpha(\mathbb{F}_q)} \chi(P).$$

Separating the contribution of the principal character, we derive

$$\left| L_{\alpha,d} - \frac{1}{\#\mathcal{X}_d} \#C_\alpha(\mathbb{F}_q) \right| \le \frac{1}{\#\mathcal{X}_d} \sum_{\substack{\chi \in \mathcal{X}_d \\ \chi \ne \chi_0}} \left| \sum_{P \in C_\alpha(\mathbb{F}_q)} \chi(P) \right|. \tag{4}$$

To apply Theorem 1 to the character sums in (4) we need to find α such that the polynomials $h_1, \dots, h_n$ given by (2) are pairwise relatively prime. If $\beta_j, j = 1, 2, 3$ are the roots of $x^3 + ax^2 + bx + c$, this leads us to the condition on α that

$$\alpha^{(i)} - \alpha \ne \beta_j^{(i)} - \beta_k, \qquad 1 \le i < n,\ j, k = 1, 2, 3,$$

(recall that $\alpha^{(n)} = \alpha^{q^n} = \alpha$).

Recall that $\mathbb{F}_q(\vartheta) = \mathbb{F}_{q^n}$, implies that $\vartheta^{(i)} - \vartheta \ne 0$ for $1 \le i < n$. Consider $\alpha = r\vartheta$ with $r \in \mathbb{F}_q^*$. Then $\alpha^{(i)} - \alpha = r(\vartheta^{(i)} - \vartheta)$. If $\#\mathcal{R} > 9n$, by inspection of $9n + 1$ values of $r \in \mathcal{R}$ we can find at least one with

$$r \ne (\beta_j^{(i)} - \beta_k)/(\vartheta^{(i)} - \vartheta), \qquad 1 \le i < n,\ j, k = 1, 2, 3.$$

With this r, for $\alpha = r\vartheta$ we apply Theorem 1 and derive from (4)

$$\left| L_{\alpha,d} - \frac{1}{\#\mathcal{X}_d} \#C_\alpha(\mathbb{F}_q) \right| \ll n 2^n q^{1/2}.$$

Hence, after the substitution of the above inequality in (3), we obtain

$$N_\alpha^* \ge \#C_\alpha(\mathbb{F}_q) \Big(1 + \sum_{\nu=1}^{2k+1} \sum_{\substack{d \mid M \\ \omega(d) = \nu}} \frac{\mu(d)}{\#\mathcal{X}_d} \Big) + O(\omega(M)^{2k+1} n 2^n q^{1/2}).$$

Finally, we rewrite this as

$$N_\alpha^* \ge \#C_\alpha(\mathbb{F}_q)\rho + O(\Delta \#C_\alpha(\mathbb{F}_q) + \omega(M)^{2k+1} n 2^n q^{1/2}), \tag{5}$$

where

$$\rho = \sum_{d|M} \frac{\mu(d)}{\#\mathcal{X}_d}$$

and

$$\Delta = \left| \sum_{\nu \ge 2k+2} \sum_{\substack{d|M \\ \omega(d)=\nu}} \frac{\mu(d)}{\#\mathcal{X}_d} \right|.$$

Using the same inclusion-exclusion principle, to count the number N^* of points of order M on the whole curve $E(\mathbb{F}_{q^n})$, we derive

$$N^* = \rho \# E(\mathbb{F}_{q^n}).$$

Now it follows that

$$\rho \ge \frac{\varphi(M)}{M}, \tag{6}$$

with equality unless $L = M$, where $\varphi(M)$ is the Euler function.

We now concentrate on Δ. Since, for $d \mid M$, we have $\#\mathcal{X}_d \ge d$, we derive

$$\Delta \le \sum_{\nu \ge 2k+2} \sum_{\substack{d|M \\ \omega(d)=\nu}} \frac{1}{d} \le \sum_{\nu \ge 2k} \frac{1}{\nu!} \sigma(M)^\nu,$$

where

$$\sigma(M) = \sum_{\substack{\ell|M \\ \ell \text{ prime}}} \frac{1}{\ell}.$$

We now assume that

$$k \ge e\sigma(M). \tag{7}$$

Then, by the well-known inequality

$$\nu! \ge (\nu/e)^\nu,$$

we have

$$\sum_{\nu \ge 2k+2} \frac{1}{\nu!} \sigma(M)^\nu \le \sum_{\nu \ge 2k+2} \Big(\frac{e\sigma(M)}{\nu} \Big)^\nu \le \sum_{\nu \ge 2k+2} 2^{-\nu} = 2^{-2k+1}.$$

Recalling (5) and (6) we now infer

$$N_\alpha^* \ge \#C_\alpha(\mathbb{F}_q)\frac{\varphi(M)}{M} + O(\#C_\alpha(\mathbb{F}_q)2^{-2k} + \omega(M)^{2k+1}n2^nq^{1/2}).$$

It follows easily from the Prime Number Theorem that

$$\sigma(M) \le \log\log\log M + O(1).$$

We now set

$$k = \left\lfloor \sqrt{\log\log M} + C \right\rfloor,$$

where the constant C is chosen to satisfy (7). It is also obvious that that $\omega(M) = O(\log M)$. Thus with the above choice of parameters we have

$$\omega(M)^{2k+1} = q^{o(1)}$$

as $q \to \infty$, which yields

$$N_\alpha^* \ge \#C_\alpha(\mathbb{F}_q)\frac{\varphi(M)}{M} + O(e^{-\sqrt{\log\log M}}\#C_\alpha(\mathbb{F}_q) + n2^nq^{1/2+o(1)}). \quad (8)$$

As we have seen in the proof of Theorem 1, C_α is an absolutely irreducible curve of genus $O(n2^n)$. So, from the Weil bound we derive

$$\#C_\alpha(\mathbb{F}_q) = q + O(n2^nq^{1/2}).$$

Using this bound together the well-known estimate of the Euler function

$$\frac{M}{\varphi(M)} \ll \log\log M \quad (9)$$

as $M \to \infty$, see [14, Theorem 328], we now conclude from (8) that $N_\alpha^* > 0$ under the conditions of the theorem. □

In particular, we see that if $r = p^k$ for a prime $p \ge 3$ and the integer $k \to \infty$ then for an elliptic curve E over $\mathbb{F}_r$, in polynomial time, one can find a set of $r^{o(1)}$ points $P \in E(\mathbb{F}_r)$ such that at least one of them is of maximum order, provided that k contains a divisor n in an appropriate range.

We now show that in fact a similar set can be constructed over any finite field of small characteristic. First we need the following auxiliary statement.

Lemma 1. *The trace map* $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} : A(\mathbb{F}_{q^k}) \to A(\mathbb{F}_q)$ *sending a point to the sum of its* $\mathbb{F}_{q^k}/\mathbb{F}_q$*-conjugates, is surjective.*

Proof. Consider first the map $A(\mathbb{F}_{q^k}) \to A(\mathbb{F}_{q^k})$ given by $P \mapsto \mathrm{Fr}(P) - P$, where Fr is the $\mathbb{F}_q$-Frobenius and let G denote its image. Since the kernel of this map is visibly $A(\mathbb{F}_q)$, we have $\#G = \#A(\mathbb{F}_{q^k})/\#A(\mathbb{F}_q)$. We abbreviate $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ and note that $\mathrm{Tr} = \sum_{j=0}^{k-1} \mathrm{Fr}^j$.

We now show that G is the kernel of Tr and cardinality considerations then implies the result. It is clear that G is contained in the kernel of Tr. Let now $P \in A(\mathbb{F}_{q^k})$, $\mathrm{Tr}(P) = \mathcal{O}$. By a result of Lang [18], there exists $Q \in A(\overline{\mathbb{F}}_q)$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$, with $\mathrm{Fr}(Q) - Q = P$. Now

$$\mathcal{O} = \mathrm{Tr}(P) = \mathrm{Tr}(\mathrm{Fr}(Q) - Q) = \mathrm{Fr}^k(Q) - Q,$$

therefore $Q \in A(\mathbb{F}_{q^k})$ and $P \in G$. □

Theorem 4. *For any fixed* $\varepsilon > 0$ *and sufficiently large prime power* $r = p^n$ *where* p *is prime and* $n \geq 1$ *is an integer for an elliptic curve* E *over* $\mathbb{F}_r$*, in time* $O(p2^{(2+\varepsilon)n})$*, one can compute a set of* $O(p2^{(2+\varepsilon)n})$ *points* $Q \in E(\mathbb{F}_r)$ *such that at least one of them is of maximum order.*

Proof. Fix some small $\varepsilon > 0$ and choose m as the smallest positive integer satisfying the inequality

$$n \leq \Big(\frac{1}{2\log 2} - \varepsilon/2\Big) m \log p. \tag{10}$$

We see from the definition of m that

$$\Big(\frac{1}{2\log 2} - \varepsilon/2\Big)(m-1)\log p < n.$$

Thus

$$p^{m-1} \leq 2^{2n/(1-\varepsilon\log 2)} \leq 2^{(2+\varepsilon)n}, \tag{11}$$

provided that ε is sufficiently small. We now put $q = p^m$, and construct an irreducible polynomial of degree n over $\mathbb{F}_q$ (which can be done deterministically in time $p^{1/2}(mn)^{O(1)} = p^{1/2}n^{O(1)}$, see [24]). Thus for any root ϑ of the polynomial we have $\mathbb{F}_q(\vartheta) = \mathbb{F}_{q^n} = \mathbb{F}_{p^{mn}}$. We can consider the abelian variety $A = R_{\mathbb{F}_{q^n}/\mathbb{F}_q}(E)$ as before. However, we note that, since E is defined

over $\mathbb{F}_r$, we have that A is defined over $\mathbb{F}_p$ and that it is independent of way the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is represented. We also consider, as before, the curve C_α defined over $\mathbb{F}_q$, for a suitable choice of α as afforded by Theorem 3. Unlike A, C_α does not necessarily descend to $\mathbb{F}_p$, but we only consider it over $\mathbb{F}_q$. We now examine the set of points

$$\mathcal{Q}_\alpha = \{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} P \ : \ P \in C_\alpha(\mathbb{F}_q)\}$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ is the $\mathbb{F}_q/\mathbb{F}_p$-trace as in Lemma 1.

Clearly $\mathcal{Q}_\alpha \subseteq A(\mathbb{F}_p) \simeq E(\mathbb{F}_r)$. Furthermore, recalling (11), we derive

$$\#\mathcal{Q}_\alpha \ll q \le p^m \le p2^{(2+\varepsilon)n}.$$

We also remark that finding points on an elliptic curve with a given x-coordinate involves taking square roots. Using an algorithm of [26] one can find a quadratic nonresidue of $\mathbb{F}_{q^n} = \mathbb{F}_{p^{mn}}$ in time

$$p^{1/2}(mn\log p)^{O(1)} = p^{1/2}(n\log p)^{O(1)}$$

(as the set of [26] contains a primitive root it also contains a quadratic nonresidue and that property can be tested in polynomial time). After this, using the Tonelli-Shanks algorithm (see [3, Sections 7.1 and 7.2]) one can extract square roots in polynomial time.

So it remains to show that $\mathcal{Q}_\alpha$ contains a point of maximum order. First we notice that the exponent M of $E(\mathbb{F}_r)$ is a divisor of the exponent of $E(\mathbb{F}_{q^n}) = E(\mathbb{F}_{r^m})$.

Furthermore, in the notation of the proof of Theorem 3, for any non-trivial character χ of $A(\mathbb{F}_q)$ we have

$$\sum_{P\in C_\alpha(\mathbb{F}_q)} \chi(\mathrm{Tr}\, P) \ll n2^n q^{1/2}. \tag{12}$$

Indeed we only need to notice that $P \mapsto \chi(\mathrm{Tr}\, P)$ is a non-trivial character of $A(\mathbb{F}_q)$. and this follows from Lemma 1.

Using the bound (12) in the same way as Theorem 1 is used in the proof of Theorem 3 (and noting that (10) is essentially equivalent to the condition of Theorem 3) we conclude the proof, provided that r is large enough. □

4. Comments

We note that the result of Theorem 4, in wide range of p and n gives a much faster deterministic algorithm and a much smaller set containing a point of maximum order on $E(\mathbb{F}_r)$ than that of [17].

On the other hand, it has an exponential dependence on n, while its finite field analogues [24, 25, 26] depend on n polynomially. The reason is the exponential factor 2^n in the bound of Theorem 1, which in turn comes from the evaluation of the genus of C_α and seems to be unavoidable.

On the other hand, one can try to get an analogue of Theorem 1 for incomplete sums (in the style of [22]) and then reduce the dependence on p in Theorem 4 from linear to $p^{1/2}$ (as it is done in [26, Theorem 8] in the case of primitive roots of finite fields).

Finally, we notice that actually identifying a point of maximum order in any set requires computing and factoring the cardinality of $E(\mathbb{F}_r)$, we refer to [1] and [6] for a description of the state-of-art in both areas.

Acknowledgments

The authors would like to thank the referees for a careful reading of the manuscript and several useful comments.

The first author was supported by ARC Grant DP130100237. The second author would like to thank Macquarie University and the University of Canterbury for their hospitality during the period in which this paper was written and the NSA for its support through Grant MDA904-H98230-09-1-0070.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and Hyperelliptic Curve Crytography: Theory and Practice*, CRC Press, 2005.

2. L. M. Adleman, J. DeMarrais and M.-D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, *Lect. Notes in Comp. Sci.*, **877**, Springer-Verlag, Berlin, 1994, 28-40.

3. E. Bach and J. Shallit, *Algorithmic Number Theory*, MIT Press, 1996.

4. I. F. Blake, V. K. Murty and G. Xu, Refinements of Miller's algorithm for computing the Weil/Tate pairing, *J. Algorithms*, **58** (2006), 134-149.

5. L. Carlitz, Distribution of primitive roots in a finite field, *Quart. J. Math. Oxford*, **4** (1953), 4-10.

6. R. Crandall and C. Pomerance, *Prime numbers: A Computational Perspective*, Springer-Verlag, Berlin, 2005.

7. H. Davenport, On primitive roots in finite fields, *Quart. J. Math.* (Oxford Ser.), **8** (1937), 308-312.

8. C. Diem, The GHS Attack in odd characteristic, *J. Ramanujan Math. Soc.*, **18** (2003), 1-32.

9. C. Diem, On the discrete logarithm problem in elliptic curves, *Compos. Math.*, **147** (2011), 75-104.

10. C. Diem, The GHS Attack in odd characteristic. II, Preprint, 2011.

11. C. Diem and N. Naumann, On the structure of the Weil restriction of Abelian varieties, *J. Ramanujan Math. Soc.*, **18** (2003), 153-174.

12. J. B. Friedlander, C. Pomerance and I. E. Shparlinski, Finding the group structure of elliptic curves over finite fields, *Bull. Aust. Math. Soc.*, **72** (2005), 251-263.

13. P. Gaudry, F. Hess, and N. Smart, Constructive and destructive facets of Weil descent, *J. Cryptology*, **15**, (2002), 19-46.

14. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, Oxford, 1979.

15. F. Hess, Computing relations in divisor class groups of algebraic curves over finite fields, Preprint, 2005.

16. N. M. Katz, An estimate for character sums, *J. Amer. Math. Soc.*, **2** (1989), 197-200.

17. D. R. Kohel and I. E. Shparlinski, Exponential sums and group generators for elliptic curves over finite fields, *Lect. Notes in Comp. Sci.*, **1838** Springer-Verlag, Berlin, 2000, 395-404.

18. S. Lang, Algebraic groups over finite fields, *Amer. J. Math.*, **78** (1956), 555-563.

19. V. S. Miller, The Weil pairing, and its efficient calculation, *J. Cryptology*, **17** (2004), 235-261.

20. V. Müller, A. Stein and C. Thiel, Computing discrete logarithms in real quadratic congruence function fields of large genus, *Math. of Comp.*, **68** (1999), 807-822.

21. W. Narkiewicz, *Classical problems in number theory*, Polish Sci. Publ., Warszawa, 1986.

22. G. I. Perel'muter and I. Shparlinski, On the distribution of primitive roots in finite fields, *Uspechi Matem. Nauk*, **45**, no.1 (1990), 185-186 (in Russian).

23. R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. of Comp.*, **44** (1985), 483-494.

24. V. Shoup, Searching for primitive roots in finite fields, *Math. Comp.*, **58** (1992), 369-380.

25. I. Shparlinski, On primitive elements in finite fields and on elliptic curves, *Matem. Sbornik*, **181** (1990), 1196-1206 (in Russian).

26. I. Shparlinski, Approximate constructions in finite fields, *Proc. 3rd Conf. on Finite Fields and Appl., Glasgow, 1995*, London Math. Soc., Lect. Note Series, 1996, v.233, 313-332.

27. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 1995.

28. I. M. Vinogradov, Sur la distribution des r'esidus et des non r'esidus des puissances, *Zurnal Fiz.-Mat. Obšč. Univ. Perm = J. Phys.-Math. Soc., Perm Univ.*, **1** (1918), 94-98.

29. J. F. Voloch, 'Jacobians of curves over finite fields', *Rocky Mountain J. Math.*, **30** (2000), 755-759.