Bull. Aust. Math. Soc. **81** (2010), 425–429
doi:10.1017/S0004972709001075

ELEMENTS OF HIGH ORDER ON FINITE FIELDS FROM ELLIPTIC CURVES

JOSÉ FELIPE VOLOCH

(Received 3 June 2009)

Abstract

We discuss the problem of constructing elements of multiplicative high order in finite fields of large degree over their prime field. We obtain such elements by evaluating rational functions on elliptic curves, at points whose order is small with respect to their degree. We discuss several special cases, including an old construction of Wiedemann, giving the first nontrivial estimate for the order of the elements in this construction.

2000 *Mathematics subject classification*: primary 14G15; secondary 11G20, 11T06.
Keywords and phrases: finite fields, elliptic curves, multiplicative group.

1. Introduction

The multiplicative group of a finite field is cyclic. However, in general, there is no simple formula, or even a deterministic polynomial time algorithm, producing a generator for this group. The next best thing is to construct elements of large order in finite fields and this paper addresses this. Our main result can also be viewed as a weak form of a conjecture of Poonen which is discussed in [4].

We prove a theorem which gives information on the orders of the coordinates of points on a curve in $E \times \mathbf{G}_m$, where E is an elliptic curve defined over a finite field and $\mathbf{G}_m$ is the multiplicative group. This is analogous to the main theorem of [4] which concerns curves in $\mathbf{G}_m \times \mathbf{G}_m$ and some of our arguments extend those of that paper.

Throughout this paper, $\mathbf{F}_q$ is a field of q elements where q is a power of the prime p. Our main result is as follows.

THEOREM 1.1. *Let X be an absolutely irreducible curve in $E \times \mathbf{G}_m$, where E is an elliptic curve, with both X and E defined over $\mathbf{F}_q$. Assume that the projection of X to both factors is nonconstant. Given $\epsilon > 0$, there exists $\delta > 0$ and $d_0 \in \mathbf{Z}$ such that, if $(P, b) \in X$ satisfies*

(i) $d := [\mathbf{F}_q(P) : \mathbf{F}_q] > d_0$,

Research supported by NSA grant MDA904-H98230-09-1-0070.

(ii) *the group generated by* P *is invariant under the* $\mathbf{F}_q$*-Frobenius,*
(iii) *the order of* P*, say* r*, satisfies* $r < d^{3/2-\epsilon}$*,*

then b *has multiplicative order of at least* $\exp(\delta(\log d)^2)$.

We also obtain a much better lower bound (namely $\exp(d^\delta)$) for the multiplicative order of b when X is contained in the graph of a function $E \to \mathbf{P}^1$. (See Theorem 4.1.) This latter result is more relevant for applications that construct elements of high order in finite fields.

Note that our results apply only to certain finite fields, namely those generated (as a field) by a point on E of small order. In [4], we get the slightly better restriction $r < d^{2-\epsilon}$ due to the fact that multiplication by n has degree n on $\mathbf{G}_m$ and degree n^2 on E. On the positive side, the flexibility of choosing E expands the scope of applicability of the present results beyond those of [4]. We discuss some situations where the hypotheses of the theorem are fulfilled in Section 4. A result of Gao [3], using a different construction, produces elements of order at least $\exp(\delta(\log d)^2/\log\log d)$ in $\mathbf{F}_{q^d}$ for many (conjecturally all) values of d.

2. Preliminaries

We will use the following lemma from [4].

LEMMA 2.1. *Fix integers* m, $a \geq 2$ *and real* $\epsilon > 0$. *If* $r \geq 2$, $(r, ma) = 1$ *is an integer and* d *is the order of* $a \bmod r$*, then, given* $N < d$*, there is a coset* Γ *of* $\langle a \rangle \subset (\mathbf{Z}/r)^*$ *with*

$$\#\{n \mid 1 \leq n \leq N, (n, m) = 1, n \bmod r \in \Gamma\} \gg Nd^{1-\epsilon}/r - r^\epsilon.$$

The following construction is going to be very similar to that in [4] but here it will be useful to take a more geometric approach. We begin by embedding $\mathbf{G}_m$ in $\mathbf{P}^1$ and replacing X by its closure in $E \times \mathbf{P}^1$; all curves considered below will be projective. We retain the choice of a coordinate y in $\mathbf{P}^1$, corresponding to the natural coordinate in $\mathbf{G}_m$.

We have the projection $X \to E$ and we denote its degree by D. Also, for any positive integer n, we have the map $[n] : E \to E$ given by multiplication by n. We consider the curve X_n obtained by taking the fiber product of these two maps (for any given n). So X_n is the locus of points (P, y) such that $(nP, y) \in X$. If we regard the function y on X_n as an algebraic function of P, we can view y as an element of a fixed algebraic closure of $F_q(E)$ and we denote this element by y_n.

If $(n, Dp) = 1$ then the map $X_n \to X$ is separable of degree n^2 and X_n is absolutely irreducible. For those values of n, the divisor of zeros of y_n is supported at the points of X_n above the points R on E with $nR = Q$, where Q runs through the points on E below the zeros of y_1 on X.

LEMMA 2.2. *The algebraic functions* y_n, $(n, Dp) = 1$*, are multiplicatively independent.*

https://doi.org/10.1017/S0004972709001075 Published online by Cambridge University Press

PROOF. It is enough to show that, if L is a function field containing the y_n, for $n \le N$, $(n, Dp) = 1$, then the divisors of the y_n in L are $\mathbf{Z}$-linearly independent. We prove this by induction on N. Let k be the largest order (in the group law of E) among the points of E below the zeros of y_1 on X. Among the points of E below the zeros of y_N there is a point of order kN which cannot be below a zero of y_n, for $n < N$. □

For a function field $L/\mathbf{F}_q$ and an element z of L, denote by $\deg_L z$ the degree of the divisor of zeros of z in L, which is also $[L : \mathbf{F}_q(z)]$ if z in nonconstant. We have that $\deg_{K_n} y_n \ll n^2$, where $K_n = \mathbf{F}_q(X_n)$.

3. Proof of the main theorem

Let F denote the $\mathbf{F}_q$-Frobenius map on all varieties over $\mathbf{F}_q$ appearing in what follows. With the notation as in the statement of the theorem, let $F(P) = aP$, for $a \in \mathbf{Z}$, $(a, r) = 1$ and $N = [d^{1/2-\epsilon}]$, and let $\Gamma = \gamma\langle a\rangle$ be the coset given by Lemma 2.1. Choose a point $C \in E$ of order r such that $P = \gamma C$. If $n \le N$ and $(n, q) = 1$, where $n \bmod r \in \Gamma$, then $n \equiv \gamma a^j \bmod r$ for some j. Let J be the set of all such j. Thus, for $j \in J$,

$$F^j(P, b) = (F^j(P), b^{q^j}) = (a^j P, b^{q^j})$$

and $a^j P = n_j C$, where $n_j \le N$, $(n_j, q) = 1$ and $n_j \bmod r \in \Gamma$ give rise to j. It follows that there is a point of X_{n_j} above $C \in E$ where y_{n_j} takes the value b^{q^j}. Let $T = [\eta \log d]$, where $\eta > 0$ will be chosen later. If $I \subset J$, let $b_I = \prod_{j\in I} b^{q^j}$.

We now claim that the b_I are distinct for distinct $I \subset J$, where $|I| \le T$. If $b_I = b_{I'}$ for two distinct such subsets I and I', then the algebraic function $z = (\prod_{j\in I} y_{n_j}/\prod_{j\in I'} y_{n_j}) - 1$ vanishes at a place of the field L, the compositum of the K_{n_j}, for $j \in I \cup I'$ above $C \in E$,

$$\deg_L z \le \sum_{j\in I\cup I'} \deg_L y_{n_j} = \sum_{j\in I\cup I'} [L : K_{n_j}] \deg_{K_{n_j}} y_{n_j} \ll TD^{2T}N^2,$$

which is smaller than $d = [\mathbf{F}_q(C) : \mathbf{F}_q]$ for a suitably small choice of η and all d sufficiently large; this is not possible unless $z = 0$ and therefore the y_{n_j}, for $j \in I \cup I'$ are multiplicatively dependent. This contradicts Lemma 2.2. It follows that there are at least $\binom{|J|}{T}$ distinct powers of b. Now Lemma 2.1 (with $\epsilon/3$ instead of ϵ) gives that

$$|J| \gg d^{3/2-\epsilon/3}/r - r^{\epsilon/3} \gg d^{2\epsilon/3} - (d^{3/2-\epsilon})^{\epsilon/3} \gg d^{2\epsilon/3},$$

hence $\binom{|J|}{T} \ge (|J|/T - 1)^T \gg \exp(\delta(\log d)^2)$, for some suitably small $\delta > 0$, proving the theorem.

4. Rational maps

In this section we discuss the special case where our curve X is an open subset of the graph of $y : E \to \mathbf{P}^1$. In this case, we can obtain much better bounds. Indeed,

https://doi.org/10.1017/S0004972709001075 Published online by Cambridge University Press

following the proof of the theorem, we have that $y_n = y \circ [n]$ so $K_n = \mathbf{F}_q(E)$ and we get the much smaller estimate $\deg_L z \ll TDN^2$. We can therefore choose a much larger value of T, say $T = [d^\eta]$, for some small $\eta > 0$ and the proof of the theorem yields that b has multiplicative order at least $\exp(d^\delta)$ with the same notation and assumptions. More precisely, we have the following theorem.

THEOREM 4.1. *Let E be an elliptic curve and y a nonconstant function on E, with both y and E defined over $\mathbf{F}_q$. Given $\epsilon > 0$, there exist $\delta > 0$ and $d_0 \in \mathbf{Z}$ such that, if $P \in E$ satisfies*

(i) $d := [\mathbf{F}_q(P) : \mathbf{F}_q] > d_0$,
(ii) *the group generated by P is invariant under the $\mathbf{F}_q$-Frobenius,*
(iii) *the order of P, say r, satisfies $r < d^{3/2-\epsilon}$,*

then $y(P)$ has multiplicative order at least $\exp(d^\delta)$.

We now explore a couple of special cases of Theorem 4.1. We begin by taking E to be a supersingular elliptic curve such that F acts by multiplication by a on E, where $a = \pm\sqrt{q}$, for q a square. Under these assumptions, the condition that the group generated by P is invariant under F is automatic and the only condition to be checked is $r < d^{3/2-\epsilon}$. Note that $E(\mathbf{F}_{q^d}) \cong (\mathbf{Z}/(\sqrt{q}^d \pm 1))^2$ and that d is the order of a mod r. The condition on r and d is essentially the condition that q has large order mod r. This case is very similar to that of $\mathbf{G}_m$ treated in [4].

Now, consider the case when E is an ordinary elliptic curve and $r = p^k$, where p is the characteristic of $\mathbf{F}_q$. Since $E[p^k]$ is cyclic, again the condition that the group generated by P is invariant under F is automatic and the only condition to be checked is $r < d^{3/2-\epsilon}$. Note that $d = sp^{k-k_0}$ for some fixed k_0, s and all k large. So the inequality $r < d^{3/2-\epsilon}$ is satisfied for large k and the conclusion of the theorem holds.

In [5], Wiedemann introduced the elements of $\bar{\mathbf{F}}_2$, defined inductively, as $a_0 = 1$ and a_n a root of $x^2 + a_{n-1}x + 1$, for $n > 0$. He showed that $\mathbf{F}_{2^{2^n}} = \mathbf{F}_2(a_n)$ and conjectured that a_n has order $2^{2^{n-1}} + 1$ for all n. Note that, as a_n has $\mathbf{F}_{2^{2^n}}/\mathbf{F}_{2^{2^{n-1}}}$-norm 1, its order cannot be larger. Let $E/\mathbf{F}_2$ be the elliptic curve $y^2 + xy = x^3 + 1$. We will now show how to obtain Wiedemann's elements from the construction of the preceding paragraph. We will show that a_n is the x-coordinate of a point of order 2^n of E. It then follows that a_n has order at least $\exp(2^{\delta n})$, for some $\delta > 0$. Note that multiplication by 2 on E factors as FV, where V is the Verschiebung and a simple calculation shows that the x-coordinate of $V(x, y)$ is $(x^2 + 1)/x$. If P_n are defined inductively by $P_0 = (1, 0)$ and $V(P_{n+1}) = P_n$, then the x-coordinate of P_n is easily seen to satisfy the same equation as a_n, so we can take $a_n = x(P_n)$.

Wiedemann's construction is an example of an iterative construction of finite fields. Other examples can be found in [2] and the references therein and also in [1], where the multiplicative order of elements thus obtained is estimated. When considering points of order s^n on an elliptic curve for fixed s and varying n, other examples of iterative constructions can be found to which we can apply the theorems of this paper. We thus

https://doi.org/10.1017/S0004972709001075 Published online by Cambridge University Press

obtain many examples of iterative constructions of finite fields together with estimates for their multiplicative order which are much better than those previously obtained.

5. Generalizations

It is possible to remove the condition that $\langle P \rangle$ is F-invariant from the statement of our theorems at the expense of a much weaker bound. This requires an analogue of Lemma 2.1 with $\mathbf{Z}[F]$ instead of $\mathbf{Z}$. It is also possible to state a similar theorem with the roles of E and $\mathbf{G}_m$ reversed or with $\mathbf{G}_m$ replaced by another elliptic curve, and a proof along the lines of this paper will provide estimates. The technique seems to be able to prove results about points on a curve inside $A \times B$ where A, B are semi-abelian varieties. The use of degrees prevents the argument from being extended from a curve to an arbitrary subvariety of $A \times B$. However, Poonen's conjecture (stated in [4]) would imply that the main hypothesis of such a theorem (namely, that the order of one of the coordinates is small) could not be satisfied unless $\dim A = \dim B = 1$. Therefore, we do not pursue such a generalization so as to avoid proving a potentially vacuous theorem.

Acknowledgement

We would like to thank the referee for the many helpful comments and for catching an inaccuracy in an earlier version of this paper.

References

[1] J. F. Burkhart, N. J. Calkin, S. Gao, J. C. Hyde-Volpe, K. James, H. Maharaj, S. Manber, J. Ruiz and E. Smith, 'Finite field elements of high order arising from modular curves', *Des. Codes Cryptogr.* **51**(3) (2009), 301–314.
[2] S. D. Cohen, 'The explicit construction of irreducible polynomials over finite fields', *Des. Codes Cryptogr.* **2**(2) (1992), 169–174.
[3] S. Gao, 'Elements of provable high orders in finite fields', *Proc. Amer. Math. Soc.* **127** (1999), 1615–1623.
[4] J. F. Voloch, 'On the order of points on curves over finite fields', *Integers* **7** (2007), A49.
[5] D. Wiedemann, 'An iterated quadratic extension of GF(2)', *Fibonacci Quart.* **26** (1988), 290–295.

JOSÉ FELIPE VOLOCH, Department of Mathematics, University of Texas, Austin, TX 78712, USA
e-mail: voloch@math.utexas.edu

https://doi.org/10.1017/S0004972709001075 Published online by Cambridge University Press