

# On the order of points on curves over finite fields

José Felipe Voloch

**Abstract:** We discuss the problem of constructing elements of multiplicative high order in finite fields of large degree over their prime field. We prove that for points on a plane curve, one of the coordinates has to have high order. We also discuss a conjecture of Poonen for subvarieties of semiabelian varieties for which our result is a weak special case. Finally, we look at some special cases where we obtain sharper bounds.

## 0. Introduction

We prove a theorem which gives information on the multiplicative orders of the coordinates of points on plane curves over finite fields. In the special case where the curve is given by  $x + y = 1$  our result is related to the main results of [GS] and [ASV], although the results there have stronger hypotheses and stronger conclusions, see section 5. Some of our arguments extend those of the aforementioned papers. Our result can also be viewed as a weak form a conjecture of Poonen in the case of two dimensional tori. We discuss Poonen's conjecture in section 4.

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.** *Let  $F(x, y) \in \mathbf{F}_q[x, y]$  be an absolutely irreducible polynomial such that  $F(x, 0)$  is not a monomial. Given  $\epsilon > 0$ , there exists  $\delta > 0$  such that, for  $d$  sufficiently large if  $a, b \in \bar{\mathbf{F}}_q^*$  satisfy  $F(a, b) = 0$  and  $d = [\mathbf{F}_q(a) : \mathbf{F}_q]$  and  $r$ , the multiplicative order of  $a$ , satisfies  $r < d^{2-\epsilon}$  then  $b$  has multiplicative order at least  $\exp(\delta(\log d)^2)$ .*

## 1. Elementary estimates

The following lemma is well-known and stated for convenience.

**Lemma 1.** For any  $\epsilon > 0$  we have that

$$\#\{1 \leq n \leq N \mid (n, r) = 1\} = N\phi(r)/r + O(r^\epsilon).$$

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

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

*Proof:* There are  $\phi(r)/d$  cosets of  $\langle q \rangle$  in  $(\mathbf{Z}/r)^*$ , so there exists a coset  $\Gamma_1$  of  $\langle q \rangle$  with

$$\#\{n \mid 1 \leq n \leq N, n \bmod r \in \Gamma_1\} \geq (d/\phi(r))\#\{n \mid 1 \leq n \leq N, (n, r) = 1\}.$$

For each  $n, 1 \leq n \leq N, n \bmod r \in \Gamma_1$  we can write  $n = un', (n', m) = 1$  and  $n'$  maximal. So  $u$  is divisible only by primes dividing  $m$  and, since  $u \leq n \leq N \leq d$ , there are  $O(d^\epsilon)$  possibilities for  $u$ , hence  $n'$  belongs to one of  $O(d^\epsilon)$  cosets of  $\langle q \rangle \subset (\mathbf{Z}/r)^*$  and select for  $\Gamma$  the coset among these cosets with the most values of  $n'$  obtained from the above  $n$ . Note also that each  $n'$  gives rise to at most  $O(d^\epsilon)$  values of  $n$ , again because this in an upper bound for the number of possible  $u$ 's.

It follows that

$$\#\{n \mid 1 \leq n \leq N, (n, m) = 1, n \bmod r \in \Gamma\} \gg (d/\phi(r))\#\{n \mid 1 \leq n \leq N, (n, r) = 1\}/d^{2\epsilon}$$

and lemma 2 now follows from lemma 1.

## 2. Some function fields

Let  $K$  be the function field of  $F(x, y) = 0$  (as in Section 0) contained in an algebraic closure of  $\mathbf{F}_q(x)$ . Within this algebraic closure, for each  $n, (n, p) = 1$ , select an  $n$ -th root of  $x, x^{1/n}$  and consider  $K_n = K(x^{1/n})$ . We now need to switch viewpoint as follows. Identify all the  $\mathbf{F}_q(x^{1/n})$  with  $\mathbf{F}_q(t)$  by sending  $x^{1/n}$  to  $t$  and embed the  $K_n$  in a fixed algebraic closure of  $\mathbf{F}_q(t)$  and denote the image of  $y \in K_n$  under this embedding by  $y_n$ ,

thus  $F(t^n, y_n) = 0$ . Let  $m$  be the degree of the divisor of zeros of  $x$  in  $K$ . If  $(n, mp) = 1$  then the extension  $K_n/K$  is separable of degree  $n$  and  $F(t^n, y)$  is absolutely irreducible. For those values of  $n$ , the divisor of zeros of  $y_n$  is supported at the places where  $t^n = \alpha$  where  $\alpha$  runs through the roots of  $F(x, 0) = 0$  in  $\bar{\mathbf{F}}_q$ . Note that, by hypothesis, one of these roots is nonzero.

**Lemma 3.** *The algebraic functions  $y_n, (n, pm) = 1$ , are multiplicatively independent.*

*Proof:* It is enough to show that if  $L$  is a function field containing the  $y_n, n \leq N, (n, pm) = 1$ , that the divisors of the  $y_n$  in  $L$  are  $\mathbf{Z}$ -linearly independent. This follows by induction on  $N$ , since if  $(N, p) = 1$ , not all the  $N$ -th roots of  $\alpha$  are  $n$ -th roots of  $\alpha$  for  $n < N$ , for  $\alpha \neq 0$ .

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  $z$  is non-constant. We have that  $\deg_{K_n} y_n \ll n$ .

### 3. Proof of the main Theorem

With notation as in the statement of the theorem, let  $N = [d^{1-\epsilon}]$  and  $\Gamma = \gamma\langle q \rangle$  be the coset given by lemma 2. Choose an element  $c \in \bar{\mathbf{F}}_q$  such that  $a = c^\gamma$ . Note that  $c$  is also of multiplicative order  $r$ . If  $n \leq N, (n, q) = 1, n \bmod r \in \Gamma$  then  $n \equiv \gamma q^j \pmod{r}$  for some  $j$  and let  $J$  be the set of all such  $j$ . Thus, for  $j \in J, 0 = F(a, b)^{q^j} = F(a^{q^j}, b^{q^j})$  and  $a^{q^j} = c^{n_j}$ , where  $n_j \leq N, (n_j, q) = 1, n_j \bmod r \in \Gamma$  gives rise to  $j$ . It follows that there is a place of  $K_{n_j}$  above  $t = c$  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  $I \subset J, |I| \leq T$ . If  $b_I = b_{I'}$  for two distinct such subsets  $I, I'$ , 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  $L$ , compositum of the  $K_{n_j}, j \in I \cup I'$  above  $t = c$ , but, denoting by  $D$  the degree of  $F$ ,

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

which is smaller than  $d = [\mathbf{F}_q(c) : \mathbf{F}_q]$  for a suitably small choice of  $\eta$  and all  $d$  sufficiently large and that is not possible, unless  $z = 0$  and therefore the  $y_{n_j}, j \in I \cup I'$  are multiplicatively dependent. This contradicts lemma 3. It follows that there are at least  $\binom{|J|}{T}$  distinct powers of  $b$ . Now lemma 2 (with  $\epsilon/3$  instead of  $\epsilon$ ) gives that

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

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

#### 4. A conjecture of Poonen

**Conjecture (Poonen).** *Let  $A$  be a semiabelian variety defined over a finite field  $F_q$  and  $X$  a closed subvariety of  $A$ . Let  $Z$  be the union of all translates of positive-dimensional semiabelian varieties (over  $\bar{\mathbf{F}}_q$ ) contained in  $X$ . Then there exists a constant  $c > 0$  such that for every nonzero  $x$  in  $(X - Z)(\bar{\mathbf{F}}_q)$ , the order of  $x$  in  $A(\bar{\mathbf{F}}_q)$  is at least  $(\#\mathbf{F}_q(x))^c$ , where  $\mathbf{F}_q(x)$  is the field generated over  $\mathbf{F}_q$  by the coordinates of  $x$ .*

Our result corresponds to the special case  $A = \mathbf{G}_m \times \mathbf{G}_m$  but our bound is much weaker than the prediction of the conjecture. Our hypothesis that  $F(x, 0)$  is not a monomial is a bit stronger than requiring that  $X \neq Z$ , which would have been a more natural condition. Finally, our result is not symmetric in the  $x$  and  $y$  coordinates. A symmetric result would be that the order of  $(a, b)$  as in the theorem is at least  $d^{3/2-\epsilon}$ , which follows immediately from our theorem. However, it follows from the proof of Liardet's theorem (as e.g. given in [L]), that the order of  $(a, b)$  is at least  $d^2$ .

#### 5. Rational functions

In this section we discuss the special case where our plane curve can be described by  $y = R(x), R(x) \in \mathbf{F}_q(x)$ ,  $R(x)$  not a monomial. In this case, we can obtain much

better bounds. Indeed, following the proof of the theorem, we have that  $y_n = R(t^n)$  so  $K_n = \mathbf{F}_q(t)$  and we get the much smaller estimate  $\deg_L z \ll TDN$ . 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. In [GS] and [ASV] better estimates are obtained (essentially  $\delta = 1/2$ ) when  $R(x) = 1 - x$  and  $r = d + 1$

## 6. Gauss Periods

Let  $r$  be prime and  $a$  a primitive  $r$ -th root of unity in  $\bar{\mathbf{F}}_q$  of degree  $r - 1$  over  $\mathbf{F}_q$ . If  $H$  is a subgroup of  $\mathbf{Z}/r$  we define the Gauss period  $b = \sum_{h \in H} a^h$  and we'd like to estimate the order of  $b$  by the above methods. We need the following lemma proved in [BR].

**Lemma 4.** *There exists  $\gamma \in Z$  such that, for all  $h \in H$ , there exists  $u_h \equiv \gamma h \pmod{r}$ ,  $|u_h| \leq r^{1-1/\#H}$ .*

By choosing  $c$  with  $c^\gamma = a$  we can write  $b = \sum_{h \in H} c^{u_h}$ . We now use the same strategy as been used twice before and, as in the previous section, obtain the estimate  $\deg z \ll TDN$  with  $D \leq r^{1-1/\#H}$ . So we choose  $N = [r^{1/(2\#H)}]$  and lemma 2 yields  $J$  with  $\#J \gg r^{1/(2\#H)-\epsilon}$  and we can take  $T = \#J$  so we get that the order of  $b$  is at least  $2\#J$ , i.e.,  $2r^{1/(2\#H)-\epsilon}$ .

**Acknowledgements:** The author would like to thank Bjorn Poonen and Igor Shparlinski.

## References

- [ASV] O. Ahmadi, I. Shparlinski and J. F. Voloch, Multiplicative order of Gauss periods, preprint 2007.
- [BR] Brauer, Alfred; Reynolds, R. L., On a theorem of Aubry-Thue. Canadian J. Math. 3, (1951). 367–374.

[GS] J. von zur Gathen and I. E. Shparlinski, ‘Orders of Gauss periods in finite fields’,  
*Appl. Algebra in Engin., Commun. and Comp.*, **9** (1998), 15–24.

[L] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York 1983.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu