Bull. Aust. Math. Soc. **88** (2013), 169–176
doi:10.1017/S0004972712000810

ELEMENTS OF LARGE ORDER IN PRIME FINITE FIELDS

MEI-CHU CHANG

(Received 8 August 2012; accepted 11 August 2012; first published online 16 October 2012)

Abstract

Given $f(x, y) \in \mathbb{Z}[x, y]$ with no common components with $x^a - y^b$ and $x^a y^b - 1$, we prove that for p sufficiently large, with $C(f)$ exceptions, the solutions $(x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ of $f(x, y) = 0$ satisfy $\operatorname{ord}(x) + \operatorname{ord}(y) > c(\log p/\log\log p)^{1/2}$, where c is a constant and $\operatorname{ord}(r)$ is the order of r in the multiplicative group $\overline{\mathbb{F}}_p^*$. Moreover, for most $p < N$, N being a large number, we prove that, with $C(f)$ exceptions, $\operatorname{ord}(x) + \operatorname{ord}(y) > p^{1/4+\epsilon(p)}$, where $\epsilon(p)$ is an arbitrary function tending to 0 when p goes to ∞.

2010 *Mathematics subject classification*: primary 11B75; secondary 11T22, 14G15, 11G20, 11T06, 11T30, 11T55, 11G99.

Keywords and phrases: multiplicative order, multiplicative group, finite fields, additive combinatorics.

1. Introduction

Given a finite field $\mathbb{F}_q$, it is a major problem to produce quickly a generator of its multiplicative group $\mathbb{F}_q^*$, and no deterministic polynomial-time algorithm seems to be known so far. Short of being able to produce primitive elements, one can settle for elements of large order. This question is also notoriously difficult and there is an extensive literature with various contributions. This note is mainly motivated by a paper of Voloch [V1] and earlier work of von zur Gathen and Shparlinski [GS, S1]. The main result in [V1] states roughly that if $F(x, y) \in \mathbb{F}_q[x, y]$ is absolutely irreducible and $F(x, 0)$ is not a monomial, given a solution $(a, b) \in \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$ of $F(x, y) = 0$ such that $d = [\mathbb{F}_q(a) : \mathbb{F}_q]$ is sufficiently large, then either a is of multiplicative order at least $d^{2-\epsilon}$ or b is of order at least $\exp(\delta(\log d)^2)$. In particular, considering the equation $y - x - 1 = 0$, it follows that either a or $a + 1$ is at least of order $d^{2-\epsilon}$. We recall the following general conjecture due to Poonen (see also [V1]).

Let A be a semiabelian variety defined over $\mathbb{F}_q$ and X a closed subvariety of A. Denote by Z the union of all translates of positive-dimensional semiabelian varieties over $\overline{\mathbb{F}}_q$ contained in X. Then, for every nonzero x in $(X - Z)(\overline{\mathbb{F}}_q)$, the order of x in $A(\overline{\mathbb{F}}_q)$ is at least $|\mathbb{F}_q(x)|^c$, for some constant $c > 0$.

Research partially financed by the National Science Foundation.

The conjecture (if true) is very strong, compared with the presently known results. In particular, those of [V1] (see also [V2]) appear as special cases, but are quantitatively much weaker. In this paper we pursue the same line of investigation but in a different direction. While the results of [V1] give lower bounds on the order of x in terms of its degree $[\mathbb{F}_q(x):\mathbb{F}_q]$, we are interested in large characteristic. Thus, fix a suitable $f(x,y)\in\mathbb{Z}[x,y]$, let p be a large prime and consider solutions $(x,y)\in\overline{\mathbb{F}}_p\times\overline{\mathbb{F}}_p$ of $f(x,y)=0$. What may be said about the orders of x and y? In particular, one can ask for a lower bound on $\min_{0<x<p-1}(\mathrm{ord}(x)+\mathrm{ord}(x+1))$ for $p\to\infty$. In this spirit, we should cite the result of Bugeaud, Corvaja, and Zannier [BCZ], according to which $(\mathrm{ord}(2)+\mathrm{ord}(3))/\log p\to\infty$ for $p\to\infty$. Although this seems a slight improvement over the obvious, the argument is deep and involves the subspace theorem in an ingenious way. It illustrates the difficulty of the problem, even in the restricted setting. Note that for large characteristic, one may also explore the above questions for 'most' p while expecting better results (see [EM]). In particular, we obtain the following results.

THEOREM 1.1. *Let $f(x,y)\in\mathbb{Z}[x,y]$. Assume that the zero set of f has no common components with that of x^a-y^b or x^ay^b-1 for any $a,b\in\mathbb{Z}^+$. Then there is a constant $C(f)$, depending only on f, such that, for a sufficiently large prime p, for all but at most $C(f)$ solutions $(x,y)\in\overline{\mathbb{F}}_p\times\overline{\mathbb{F}}_p$ of*

$$f(x,y)=0, \tag{1.1}$$

we have

$$\mathrm{ord}(x)+\mathrm{ord}(y)>c\Big(\frac{\log p}{\log\log p}\Big)^{1/2}, \tag{1.2}$$

where c is a constant and $\mathrm{ord}(r)$ is the order of r in the multiplicative group $\overline{\mathbb{F}}_p^*$.

Theorem 1.1 can be improved for almost all p as follows.

THEOREM 1.2. *Let $f(x,y)\in\mathbb{Z}[x,y]$. Assume that the zero set of f has no common components with that of x^a-y^b or x^ay^b-1 for any $a,b\in\mathbb{Z}^+$. Then there is a constant $C(f)$, depending only on f, such that, for a set of primes p of relative density 1, for all but at most $C(f)$ solutions $(x,y)\in\overline{\mathbb{F}}_p\times\overline{\mathbb{F}}_p$ of*

$$f(x,y)=0,$$

we have

$$\mathrm{ord}(x)+\mathrm{ord}(y)>p^{1/4+\epsilon(p)}, \tag{1.3}$$

where $\epsilon(p)$ is an arbitrary function tending to 0 when p goes to ∞.

Our arguments are based on elimination theory combined with a finiteness result of torsion points on irreducible curves, conjectured by Lang and proved by Ihara, Serre and Tate. (See [L1, L2] and Ailon and Rudnick [AR] for other applications of this result in a similar vein.) The formulation appears in Lemma 2.3(a) below. For the reader's convenience, we include a proof based on the finiteness of solutions

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press

of linear equations in roots of unity. (See Theorem CJ in the next section.) On the quantitative side, more precise statements appear in Corvaja and Zannier [CZ], but these refinements are not essential for our modest purpose. In our detailed presentation, we aim to illustrate the use of the subspace theorem and its consequences for problems in finite fields. They may have other applications and the above results are likely to have extensions to more variables.

In special cases, the above results can be made more precise.

THEOREM 1.3. *Let $F(x) = x + 1$ or $F(x) = x + (1/x)$.*

(i) *Let p be prime and $(-3/p) = -1$, where $(-3/p)$ is a Legendre symbol. Then for all $x \in \mathbb{F}_p$, (1.2) holds.*

(ii) *For a set of primes $p < N$ of relative density 1 such that $(-3/p) = -1$, all $x \in \mathbb{F}_p$ satisfy (1.3).*

This theorem should be compared with the 'large order' results due to von zur Gathen and Shparlinski [GS] and Voloch [V1].

We conclude this section with some notation and conventions.

(1) Let $f, f_\alpha \in \mathbb{C}[x_1, \dots, x_n]$.
$V(f) = \{(x_1, \dots, x_n) \in \mathbb{C}^n : f(x_1, \dots, x_n) = 0\}$.
$V(\{f_\alpha\}_\alpha) = \bigcap_\alpha V(f_\alpha)$.

(2) $\epsilon(x)$ is an arbitrary function tending to 0 when x goes to ∞.

(3) A solution to the equation $\sum_{i=1}^n a_i x_i = 1$ is *nondegenerate* if $\sum_{i \in I} a_i x_i \neq 0$ for any $I \subset \{1, \dots, n\}$.

(4) $U = \{\text{roots of unity}\}$.
$\phi(m) =$ the Euler's totient function.
$\Phi_m =$ the mth cyclotomic polynomial, of degree $\phi(m)$.

2. The proofs

We will use the following result from elimination theory [CLO].

LEMMA 2.1. *Let $f(x, y) \in \mathbb{Z}[x, y]$, $P_1(x) \in \mathbb{Z}[x]$, $P_2(y) \in \mathbb{Z}[y]$ such that*

$$V(f, P_1, P_2) = \emptyset.$$

Write $d_0 = \deg f$, $d_1 = \deg P_1$, $d_2 = \deg P_2$ and let H be a bound on the coefficients of f, P_1, P_2. Then there exist $a \in \mathbb{Z} \setminus \{0\}$ and $g_0, g_1, g_2 \in \mathbb{Z}[x, y]$ such that:

(i) $a = g_0(x, y)f(x, y) + g_1(x, y)P_1(x) + g_2(x, y)P_2(y)$;

(ii) $|a| < [(d_0 + d_1 + d_2)^2 H]^{d_0 d_1 + d_1 d_2 + d_2 d_0}$.

PROOF. The argument is standard and we include it for the sake of completeness.

Let A be an integral domain. Given $u(x), v(x) \in A[x]$, we denote by $\mathrm{Res}_x(u, v) \in A$ the determinant of the Sylvester matrix of u and v. Recall that there are polynomials $U(x), V(x) \in A[x]$ such that

$$\mathrm{Res}_x(u, v) = U(x)u(x) + V(x)v(x).$$

Also, $\mathrm{Res}_x(u, v) = 0$ if and only if $\gcd(u, v) \neq 1$.

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press

Take $A = \mathbb{Z}[y]$. It follows that

$$r(y) = \mathrm{Res}_x(f(x,y), P_1(x)) = U(x,y)f(x,y) + V(x,y)P_1(x)$$

for some $U, V \in \mathbb{Z}[x,y]$.

Next, we apply elimination theory to the polynomials $r(y), P_2(y) \in \mathbb{Z}[y]$ and have

$$\begin{aligned} a &= \mathrm{Res}_y(r, P_2) = R(y)r(y) + W(y)P_2(y) \\ &= R(y)U(x,y)f(x,y) + R(y)V(x,y)P_1(x) + W(y)P_2(y). \end{aligned}$$

Clearly, $a \neq 0$. Otherwise, for some y_0, $r(y_0) = P_2(y_0) = 0$. Then $f(x,y_0)$ and $P_1(x)$ also have a common root x_0. Hence $(x_0, y_0) \in V(f, P_1, P_2)$. This is a contradiction.

It remains to evaluate a. Clearly, $r(y)$ is of degree at most d_0d_1 with coefficients bounded by $(d_0+d_1)!\binom{d_0}{d_1}H^{d_0+d_1} < (d_0+d_1)!\, d_0^{d_1} H^{d_0+d_1}$ and hence

$$\begin{aligned} |a| &< (d_0d_1 + d_2)!H^{d_0d_1}[(d_0+d_1)!\, d_0^{d_1} H^{d_0+d_1}]^{d_2} \\ &< (d_0d_1 + d_2)!(d_0(d_0+d_1)H)^{(d_0+d_1)d_2} H^{d_0d_1}, \end{aligned}$$

so the proof is complete. □

Remark 2.2. In our application, $f(x,y)$ will be a fixed polynomial; since d_0 is a constant, the bound (ii) turns out to be better than the estimate obtained from the quantitative Nullstellensatz theorem in [KPS].

We also need the following version of a theorem of Conway and Jones about linear equations in roots of unity. (See [CJ, E] for further reference and [DZ, E, Sc] for results of this type over $\mathbb{C}$.)

Theorem CJ. *Let $a_1, \ldots, a_n \in \mathbb{C} \setminus \{0\}$. Then the number of nondegenerate solutions in U of the equation*

$$a_i\xi_1 + \cdots + a_n\xi_n = 1$$

is at most $O(\exp(cn^{3/2}(\log n)^{1/2}))$.

From the theorem above, one can easily deduce the following corollary.

Corollary CJ. *Consider the linear equation*

$$a_1\xi_1 + \cdots + a_n\xi_n = 0, \quad a_i \in \mathbb{Z} \setminus \{0\} \tag{2.1}$$

with solutions $\xi_i \in U$. Then there exists a subset $\mathcal{U}$ of U^n with $|\mathcal{U}| \leq O(\exp(cn^{3/2}(\log n)^{1/2}))$ such that for any $\xi = (\xi_1, \ldots, \xi_n) \in U^n$ satisfying (2.1), there is a partition $\{1, \ldots, n\} = \bigcup_\alpha I_\alpha$ with $|I_\alpha| \geq 2$ and there is $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathcal{U}$ such that

$$\frac{\xi_i}{\xi_j} = \frac{\zeta_i}{\zeta_j}, \quad \forall \alpha \text{ and } \forall\, i, j \in I_\alpha.$$

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press

From the foregoing, we derive a further result.

LEMMA 2.3. *Let $f(x, y) \in \mathbb{Z}[x, y]$. Assume that $V(f)$ has no common components with $V(x^a - y^b)$ and $V(x^a y^b - 1)$ for any $a, b \in \mathbb{Z}^+$. Then:*

(a) $|V(f) \bigcap U^2| < C(f)$;

(b) *there exists $K(f) \in \mathbb{Z}^+$ such that, for any cyclotomic polynomials Φ_k, Φ_ℓ with*

$$\max\{k, \ell\} \geq K(f),$$

we have

$$V(f, \Phi_k(x), \Phi_\ell(y)) = \emptyset. \tag{2.2}$$

PROOF OF LEMMA 2.3(a). Let $f(x, y) = \sum_{k,\ell} a_{k,\ell} x^k y^\ell$. Setting $\xi_{k,\ell} = x^k y^\ell$, we obtain the equation

$$\sum_{k,\ell} a_{k,\ell} \xi_{k,\ell} = 0 \tag{2.3}$$

to which we apply Corollary CJ. Hence, there is $\mathcal{U}$, with $|\mathcal{U}| \leq C(\deg f)$, consisting of triples $\zeta = (\zeta_{k,\ell})$, $\zeta_{k,\ell} \in U$, such that, for any $\xi = (\xi_{k,\ell})$ with $\xi_{k,\ell} \in U$ satisfying (2.3), there is a partition I_α of the indices and some $\zeta \in \mathcal{U}$ such that

$$\frac{\xi_{k,\ell}}{\xi_{k',\ell'}} = \frac{\zeta_{k,\ell}}{\zeta_{k',\ell'}}, \quad \forall \alpha \text{ and } \forall (k, \ell), (k', \ell') \in I_\alpha.$$

Hence

$$x^{k-k'} y^{\ell-\ell'} = \zeta_{k,\ell} \overline{\zeta_{k',\ell'}}.$$

If there exist α, α' and $(k_1, \ell_1), (k_2, \ell_2) \in I_\alpha$, $(k_3, \ell_3), (k_4, \ell_4) \in I_{\alpha'}$ such that

$$\frac{k_1 - k_2}{\ell_1 - \ell_2} \neq \frac{k_3 - k_4}{\ell_3 - \ell_4},$$

then x, y are determined. Therefore, we assume that

$$\dim\langle (k_1 - k_2, \ell_1 - \ell_2) : (k_1, \ell_1), (k_2, \ell_2) \in I_\alpha \text{ for some } \alpha \rangle \leq 1. \tag{2.4}$$

For each α, we take some $(k_\alpha, \ell_\alpha) \in I_\alpha$. Rewrite f as

$$f(x, y) = \sum_\alpha x^{k_\alpha} y^{\ell_\alpha} \sum_{(k,\ell) \in I_\alpha} a_{k,\ell} x^{k-k_\alpha} y^{\ell-\ell_\alpha}, \tag{2.5}$$

where, by (2.4)

$$(k - k_\alpha, \ell - \ell_\alpha) = c_{k,\ell}(e, f) \tag{2.6}$$

for some $(e.f) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

Moreover, we may assume that there is some $(x_0, y_0) \in U^2$ satisfying

$$\sum_{(k,\ell) \in I_\alpha} a_{k,\ell} x_0^k y_0^\ell = 0 \quad \text{for all } \alpha \tag{2.7}$$

(since otherwise, we would not have to consider the partition $\{I_\alpha\}$).

It follows from (2.5)–(2.7) that the curve $V(x - x_0 t^f) \cap V(y - y_0 t^{-e})$ is contained in $V(f)$, contradicting our assumption on $V(f)$. □

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press

Proof of Lemma 2.3(b). Clearly, from part (a), we may conclude that there is an integer $M = M(f)$ such that

$$V(f) \cap U^2 \subset V(x^M - 1, y^M - 1).$$

Also,

$$V(f, \Phi_k(x), \Phi_\ell(y)) \subset V(f) \cap U^2.$$

Hence, if $V(f, \Phi_k(x), \Phi_\ell(y)) \neq \emptyset$, then $\Phi_k(x) | x^M - 1$ and $\Phi_\ell(y) | y^M - 1$, which are impossible assuming $K > M$. □

Combining Lemma 2.1 with Lemma 2.3(b) gives the following result.

Lemma 2.4. *Let $f(x, y) \in \mathbb{Z}[x, y]$. Assume that $V(f)$ has no common components with $V(x^a - y^b)$ and $V(x^a y^b - 1)$ for any $a, b \in \mathbb{Z}^+$. Let $K(f) \in \mathbb{Z}^+$ be given by Lemma 2.3(b) and let Φ_k and Φ_ℓ be cyclotomic polynomials with* $\max\{k, \ell\} \geq K(f)$.

Then there exist $a \in \mathbb{Z}^+$ and $g_0, g_1, g_2 \in \mathbb{Z}[x, y]$ such that:

(i) $a = g_0(x, y) f(x, y) + g_1(x, y)\Phi_k(x) + g_2(x, y)\Phi_\ell(y)$;
(ii) $\log a < c\, d^2 \log d$, *where* $d = \max\{\phi(k), \phi(\ell)\}$.

Proof of Theorem 1.1. Let $K = K(f)$ be given by Lemma 2.4, and let

$$\mathcal{E} = \{\rho \in \overline{\mathbb{F}}_p : \exists\, \Phi_m \text{ with } m \leq K \text{ and } \Phi_m(\rho) = 0\}.$$

Thus

$$|\mathcal{E}| < K^2 < C(f).$$

We claim that (1.2) holds, except possibly for those $(x, y) \in \overline{\mathbb{F}}_p$ in $\mathcal{E} \times \mathcal{E}$. Let $(x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ satisfy (1.1) and $(x, y) \notin \mathcal{E} \times \mathcal{E}$. Let $k = \operatorname{ord}(x)$ and $\ell = \operatorname{ord}(y)$. Then $\Phi_k(x) \equiv 0 \pmod p$ and $\Phi_\ell(y) \equiv 0 \pmod p$. Since $(x, y) \notin \mathcal{E} \times \mathcal{E}$, we have $\max\{k, \ell\} > K$. Lemma 2.4(i) gives

$$a \neq 0 \quad \text{and} \quad a \equiv 0 \pmod p$$

by the foregoing. It follows from Lemma 2.4(ii) that

$$\log p \leq \log a < c(\phi(k)^2 \log \phi(k) + \phi(\ell)^2 \log \phi(\ell)) < c(k^2 + \ell^2) \log(k + \ell)$$

and hence (1.2) holds. □

Proof of Theorem 1.2. Let N be a large integer and $M = [N^{1/4-\epsilon}]$. Let $K = K(f)$ be given by Lemma 2.4. For any k, ℓ satisfying $K < \max\{k, \ell\} < M$, we apply Lemma 2.4 to Φ_k and Φ_ℓ. Lemma 2.4(i) gives

$$a_{k,\ell} = g_{0,k,\ell}(x, y) f(x, y) + g_{1,k,\ell}(x, y)\Phi_k(x) + g_{2,k,\ell}(x, y)\Phi_\ell(y) \tag{2.8}$$

with $a_{k,\ell} \in \mathbb{Z}^+$, $a_{k,\ell} < M^{cM^2}$ and $g_{0,k,\ell}, g_{1,k,\ell}, g_{2,k,\ell} \in \mathbb{Z}[x, y]$.

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press

Define

$$a = \prod_{\substack{k,\ell \\ K<\max\{k,\ell\}<M}} a_{k,\ell} \in \mathbb{Z},$$

which satisfies

$$a < M^{cM^4}. \tag{2.9}$$

We will repeat the argument for Theorem 1.1.

Given prime p, let $\mathcal{E}_p = \mathcal{E}$ as defined in the proof of Theorem 1.1. Assume that $(x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \setminus \mathcal{E}_p \times \mathcal{E}_p$ and $f(x, y) = 0$. Let $k = \operatorname{ord}(x)$, $\ell = \operatorname{ord}(y)$. Assume that $k, \ell < M$. It follows from (2.8) that $a_{k,\ell} \equiv 0 \pmod{p}$ and hence $p \mid a$. Since $\omega(a) \le cM^4 < N^{1-\epsilon}$ by (2.9), for most primes $p < N$ and any $(x, y) \in \overline{\mathbb{F}}_p$ satisfying $f(x, y) = 0$, we have $\operatorname{ord}(x) + \operatorname{ord}(y) > M = N^{1/5-\epsilon} > p^{1/5-\epsilon}$.

Combining this last statement with the following theorem by Erdős and Murty (see [EM, Theorem 2]), we conclude the proof of Theorem 1.2. □

Theorem EM. *Let $\delta > 0$ be fixed and $\epsilon(x)$ be an an arbitrary function tending to 0 when x goes to ∞. Then the number of primes $p \le x$ such that $p - 1$ has a divisor in $(x^{\delta}, x^{\delta+\epsilon(x)})$ is $o(x/\log x)$.*

Proof of Theorem 1.3. We note that if x and $x + 1 \in U$, then x satisfies

$$x^2 + x + 1 = 0. \tag{2.10}$$

Indeed, let $x = \cos\theta + i \sin\theta$ and $x + 1 = \cos\gamma + i \sin\gamma$. Then $\cos\theta = -1 + \cos\gamma$. On the other hand, from $\sin\theta = \sin\gamma$, we have $\cos\theta = \pm\cos\gamma$. Hence $\cos\theta = -\frac{1}{2}$ and $x = e^{\frac{2}{3}\pi i}$ is a cubic root of unity.

Therefore, we have (2.2) for $\max\{k, \ell\} > 3$. Combining with Lemma 2.1, we have Lemma 2.4.

Similarly, for part (ii), if x and $x + (1/x) \in U$, then x satisfies either (2.10) or

$$x^2 - x + 1 = 0. \tag{2.11}$$

If $(-3/p) = -1$, then (2.10), (2.11) have no solutions (mod p). The rest of the argument is the same as that for part (i). □

Remark 2.5. If $(-3/p) = 1$, then (2.10) has a solution and $y = x + 1$ satisfies $y^2 - y + 1 \equiv 0 \pmod{p}$. Hence

$$\operatorname{ord}(x) = 6, \quad \operatorname{ord}(x + 1) = 3.$$

Remark 2.6. According to a result in [S2], there are at least $p^{1/2}$ elements $x \in F_p$ with

$$\operatorname{ord}(x) + \operatorname{ord}(x + x^{-1}) < p^{3/4+\epsilon},$$

if $p - 1$ has a divisor $d \in [p^{3/4+\epsilon/2}, p^{3/4+\epsilon}]$. (By a result of Ford [F], there is a positive proportion of such primes.) The same proof works if $x + x^{-1}$ is replaced by a nonmonomial rational function F.

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press

Acknowledgements

The author would like to thank J. Bourgain and I. Shparlinski for communications, particularly for bringing to the author's attention [EM] and Poonen's conjecture, resulting in the current version of this paper. The author is grateful to I. Shparlinski for his comments on earlier versions, the referee for comments and the Mathematics Department of the University of California at Berkeley for hospitality.

References

[AR] N. Ailon and Z. Rudnick, 'Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$', *Acta Arith.* **113** (2004), 31–38.

[BCZ] Y. Bugeaud, P. Corvaja and U. Zannier, 'An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$', *Math. Z.* **243**(1) (2003), 79–84.

[CJ] J. H. Conway and A. J. Jones, 'Trigonometric diophantine equations (on vanishing sums of roots of unity)', *Acta Arith.* **30** (1976), 229–240.

[CZ] P. Corvaja and U. Zannier, 'On the maximal order of a torsion point on a curve in $\mathbb{G}_m^n$', *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Math. Appl.* **19**(1) (2008), 73–78.

[CLO] D. A. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms* (Springer, New York, 1992).

[DZ] R. Dvornicich and U. Zannier, 'On sums of roots of unity', *Monatsh. Math.* **129**(2) (2000), 97–108.

[EM] P. Erdős and M. R. Murty, 'On the order of $a \pmod p$', *Proc. 5th Canadian Number Theory Association Conf.* (American Mathematical Society, Providence, RI, 1999), pp. 87–97.

[E] J.-H. Evertse, 'The number of solutions of linear equations in roots of unity', *Acta Arith.* **89** (1999), 45–51.

[F] K. Ford, 'The distribution of integers with a divisor in a given interval', *Ann. of Math.* (2) **168** (2008), 367–433.

[GS] J. von zur Gathen and I. Shparlinski, 'Gauss periods in finite fields', *Proc. 5th Conference of Finite Fields and their Applications*, Augsburg, 1999 (Springer, Berlin, 2001), pp. 162–177.

[KPS] T. Krick, L. M. Pardo and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.* **109**(3) (2001), 521–598.

[L1] S. Lang, 'Division points on curves', *Annali di Matematica pura ed applicata* (IV), Vol. LXX, (1965), 229–234.

[L2] S. Lang, *Fundamentals of Diophantine Geometry* (Springer, New York, 1983), pp. 200–207.

[Sc] H. P. Schlickewei, 'Equations in roots of unity', *Acta Arith.* **76** (1996), 99–108.

[S1] I. Shparlinski, 'Additive combinatorics over finite fields: new results and applications', *Proc. RICAM-Workshop on Finite Fields and their Applications: Character Sums and Polynomials* (De Gruyter), to appear.

[S2] I. Shparlinski, 'On the multiplicative orders of γ and $\gamma + \gamma^{-1}$ over finite fields', *Finite Fields Appl.* **7** (2001), 327–331.

[V1] J. F. Voloch, 'On the order of points on curves over finite fields', *Integers* **7** (2007), A49.

[V2] J. F. Voloch, 'Elements of high order on finite fields from elliptic curves', *Bull. Aust. Math. Soc.* **81** (2010), 425–429.

MEI-CHU CHANG, Department of Mathematics, University of California, Riverside, USA
e-mail: mcc@math.ucr.edu

https://doi.org/10.1017/S0004972712000810 Published online by Cambridge University Press