TAIWANESE JOURNAL OF MATHEMATICS
Vol. 17, No. 2, pp. 621-628, April 2013
DOI: 10.11650/tjm.17.2013.2307
This paper is available online at http://journal.taiwanmathsoc.org.tw

ORDER OF GAUSS PERIODS IN LARGE CHARACTERISTIC

Mei-Chu Chang

Abstract. Let p be the characteristic of $\mathbb{F}_q$ and let q be a primitive root modulo a prime $r = 2n + 1$. Let $\beta \in \mathbb{F}_{q^{2n}}$ be a primitive rth root of unity. We prove that the multiplicative order of the Gauss period $\beta + \beta^{-1}$ is at least $(\log p)^{c \log n}$ for some $c > 0$. This improves the bound obtained by Ahmadi, Shparlinski and Voloch when p is very large compared with n. We also obtain bounds for "most" p.

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 [8]. This note is mainly motivated by the paper [1] and earlier work of von zur Gathen and Shparlinski [6, 9] related to the orders of Gauss periods. In [1], the following is proven.

Theorem ASV. *Let p be the characteristic of $\mathbb{F}_q$ and let q be a primitive root modulo a prime $r = 2n + 1$. Let $\beta \in \mathbb{F}_{q^{2n}}$ be a primitive rth root of unity. Then the Gauss period*

$$\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^n} \tag{1.1}$$

has multiplicative order L_n satisfying the lower bound

$$L_n > \exp\left(\left(\pi\sqrt{\frac{2(p-1)}{3p}} + o(1)\right)\sqrt{n}\right) \tag{1.2}$$

Received March 14, 2012, accepted September 10, 2012.
Communicated by Wen-Ching Li.
2010 *Mathematics Subject Classification*: Primary 11B75; Secondary 11T22, 14G15, 11G20, 11T06, 11T30, 11T55, 11G99.
Key words and phrases: Multiplicative order, Multiplicative group, Finite fields, Additive combinatorics.
Research partially financed by the National Science Foundation.

as $n \to \infty$ and the bound (1.2) *is uniform in q.*

(For a further improvement on (1.2), see [7].)

This estimate is unsatisfactory if for instance we would fix a large n and let $p \to \infty$. We will prove the following

Theorem 1'. *Under the assumption of Theorem ASV, assuming $n > n_0$ for some constant n_0, we have*

$$L_n > \left[\frac{\log p}{5n(\log n)^2}\right]^{12^{-7}\log n}. \tag{1.3}$$

Theorem 1' combined with Theorem ASV and Theorem 3 in [2] give the following.

Theorem 1. *Under the assumption of Theorem ASV, and either $n > 1$ or $\left(\frac{-3}{p}\right) = -1$, we have*

$$L_n > (\log p)^{c \log n}$$

for some constant $c > 0$.

If $n \leq n_0$,we invoke Theorem 3 in [2] and its proof, which provides explicitly the exceptional cases. (See also Remark 1.2 below.) In fact, [2] gives the following lower bound

$$\operatorname{ord}(x) + \operatorname{ord}(x + x^{-1}) > c\Big(\frac{\log p}{\log\log p}\Big)^{1/2}, \tag{1.4}$$

if $x \in \overline{\mathbb{F}}_p$ and $\operatorname{ord}(x) \neq 3, 6$.

Remark 1.1. Under the assumption of Theorem ASV, we have $\Phi_r(\beta) = 0$ (Φ_r being the r-cyclotomic polynomial). Hence $[\mathbb{F}_p(\beta) : \mathbb{F}_p] \leq r - 1 = 2n$ and $\operatorname{ord}(\beta + \beta^{-1}) < p^{2n}$. Thus, we cannot expect a lower bound on L_n in terms of $q = p^k$.

Remark 1.2. We see that the assumption $n > n_0$ is necessary. Let $n = 1$, $r = 3$, and $p = q \equiv 2 \pmod 3$. Take $\beta \in \overline{\mathbb{F}}_p$ satisfying $\beta^2 + \beta + 1 = 0$. Then $\alpha = \beta + \beta^{-1}$ satisfies $\alpha^2 = 1$ and has order 2.

In a more general context, we should also refer to the work of Voloch [10].

The main result in [10] 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 $\exp\big(\delta(\log d)^2\big)$. In particular, considering the equation $y - x - \frac{1}{x} = 0$, it follows that either a or $a + \frac{1}{a}$ is at least of order $d^{2-\epsilon}$. We recall the following general conjecture due to Poonen (See also [10].)

Let A be a semiabelian variety defined over $\mathbb{F}_q$ and X a closed subvariety of A. Denote 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* $\left|\mathbb{F}_q(x)\right|^c$, *for some constant* $c > 0$.

The conjecture (if true) is very strong, compared with the presently known results. In particular, those of [1, 6, 10] and [11] appear as special cases, but are quantitatively much weaker.

In this paper we pursue the same line of investigation as in [2], considering large characteristic p. Using the same method of proving Theorem 1', we also establish Theorem 2 and Theorem 3 below. The following statement gives a lower bound on L_n for 'most p'.

Theorem 2. *For most primes p, under the assumption of Theorem ASV, we have the lower bound*

$$L_n > p^{1-\frac{C}{\log n}} \tag{1.5}$$

for some constant c.

The following remark has the same flavor as Theorem 2 and is a consequence of Voloch's result [10].

Remark 2.1. Let q be fixed. For most primes ℓ, the following holds.
Let $\beta \in \overline{\mathbb{F}}_q$ *satisfy* $\Phi_\ell(\beta) = 0$. *Then* $\operatorname{ord}(\beta + \beta^{-1}) > \exp(\ell^\delta)$, *where* $\delta > 0$ *is some constant.*

Note that instead of $\beta+\beta^{-1}$, we may consider any polynomial $f(x) \in \mathbb{F}_q[x]$, which is not a monomial polynomial.

The next result is an extension of Theorem 3 in [2].

Theorem 3. *Let p be the characteristic of* $\mathbb{F}_q$ *and let* $\beta \in \overline{\mathbb{F}}_q$, $[\mathbb{F}_q(\beta) : \mathbb{F}_q] = n$ *with* $n > c$ *for some constant c. Then*

$$\operatorname{ord}(\beta) + \operatorname{ord}\Big(\beta + \frac{1}{\beta}\Big) > \big(\log p\big)^{1-\frac{C}{\log n}} \big(\log\log p \ \log n\big)^{-1}. \tag{1.6}$$

Remark 3.1. A similar statement (with essentially identical proof) holds for $\beta + 1$ instead of $\beta + \frac{1}{\beta}$.

Notations.

Let $g(x) = \sum_i a_i x^i \in \mathbb{C}[x]$. The *height* of g is $\operatorname{ht}(g) = \max_i |a_i|$.
$[1, n] = \{1, \cdots, n\}$.
$U = \{$ roots of unity $\}$.
$\phi(m) =$ the Euler's totient function.
$\Phi_m =$ the mth cyclotomic polynomial.
$\operatorname{ord}(x) =$ the order of x in the multiplicative group $\overline{\mathbb{F}}_p^*$.
$\overline{\mathbb{F}}_p =$ the algebraic closure of $\mathbb{F}_p$.

2. The Proofs

The following statement depends on the subspace theorem by Evertse, Schlickewei, and Schmidt [5].

Lemma 1. *Let r be sufficiently large and let $\xi_1, \cdots, \xi_r \in \mathbb{C}^*$ be r distinct roots of unity. Then there is a subset $I \subset [1, r]$ satisfying*
(i). $|I| > 12^{-7} \log r$,
(ii). *the elements $\xi_s + \xi_s^{-1}$, $s \in I$ are multiplicatively independent.*

Proof. Denote $\eta_s = \xi_s + \xi_s^{-1}$ and let $\{\eta_s\}_{s\in I} \subset \{\eta_s\}_{s\in[1,r]}$ be a maximal subset of multiplicative independent elements. Let $r_1 = |I|$, $H_0 < \langle \mathbb{C}^*, \cdot \rangle$ be the multiplicative group generated by $\{\eta_s\}_{s\in I}$, and

$$H_1 = \{z \in \mathbb{C}^* : z^m \in H_0 \text{ for some } m \in \mathbb{Z}_+\}.$$

Hence $H_1 < \mathbb{C}^*$ is a multiplicative group of rank r_1. By maximality and that $1 \in H_0$,

$$H_1 \supset \ \ U \cup \{\eta_s\}_{s\in[1,r]}.$$

Therefore, for each $s = 1, \cdots, r$,

$$1 + \xi_s^2 = \xi_s z_s \quad \text{for some } z_s \in H_1 \downarrow \tag{2.1}$$

implying that the unit equation

$$x_1 - x_2 = 1, \ \ x_1, x_2 \in H_1 \tag{2.2}$$

has at least $\left[\frac{r}{2}\right]$ solutions. On the other hand, according to Theorem 1 in [5], the number of solutions of (2.2) maybe uniformly bounded in terms of the rank of H_1, specifically by

$$\exp\left(12^6(2r_1 + 1)\right). \tag{2.3}$$

It follows that $r_1 > 12^{-7} \log r$. ■

Lemma 2. *Let $P_1(x), P_2(x) \in \mathbb{Z}[x]$ be polynomials of degrees d_1, d_2 and heights H_1, H_2 respectively. Then their resultant* $\mathrm{Res}(P_1, P_2)$ *satisfies the bound*

$$|\mathrm{Res}(P_1, P_2)| \le \sqrt{d_1 + 1}^{\,d_2} \sqrt{d_2 + 1}^{\,d_1} H_1^{d_2} H_2^{d_1}. \tag{2.4}$$

Proof. The resultant of P_1 and P_2 is the determinant of the Sylvester matrix of the two polynomials. Viewing the determinant as the volume and bounding it by the product of lengths of the row vectors give (2.4). ■

We will need the following notation for the next lemma.

Given a pair of nonempty disjoint sets $I_1, I_2 \subset [1, r]$, and a set of exponents $\widetilde{k} = \{k_s\}_{s\in I_1\cup I_2}$, we denote

$$P_{I_1,I_2,\widetilde{k}}(x) = \prod_{s\in I_2} x^{s\,k_s} \prod_{s\in I_1} (x^{2s}+1)^{k_s} - \prod_{s\in I_1} x^{s\,k_s} \prod_{s\in I_2} (x^{2s}+1)^{k_s}. \tag{2.5}$$

Lemma 3. *Let r be a prime and $\Phi_r \in \mathbb{Z}[x]$ be the rth cyclotomic polynomial. Let*

$$r_1 = [12^{-7} \log r].$$

Then there exists $I \subset [1, r-1]$ with $|I| = r_1$ such that for any pair of nonempty disjoint sets $I_1, I_2 \subset I$ and any set of exponents $\widetilde{k} = \{k_s\}_{s\in I_1\cup I_2}$, we have polynomials $\Psi(x), Q(x) \in \mathbb{Z}[x]$:

(a). $A = \Phi_r(x)\Psi(x) + P_{I_1,I_2,\widetilde{k}}(x)Q(x) \in \mathbb{Z}\setminus\{0\}$.

(b). $\log A < r(\log r)^2\, K$, *where* $K = \max_s k_s$.

Proof.

Let $z \in \mathbb{C}$ be a root of Φ_r. Applying Lemma 1 to the distinct roots of unity $z, z^2, \cdots, z^{r-1}$, we obtain $I \subset [1, r]$ with $|I| = r_1$ and $\{z^s + z^{-s}\}_{s\in I}$ is a multiplicatively independent set. Hence for any $I_1, I_2 \subset I$ and $\{k_s\}_{s\in I_1\cup I_2}$,

$$\prod_{s\in I_1} (z^s + z^{-s})^{k_s} \neq \prod_{s\in I_2} (z^s + z^{-s})^{k_s}.$$

Namely, $P_{I_1,I_2,\widetilde{k}}(z) \neq 0$.

Since $\Phi_r(x)$ is irreducible, $\gcd(\Phi_r, P_{I_1,I_2,\widetilde{k}}) = 1$ and $\mathrm{Res}(\Phi_r, P_{I_1,I_2,\widetilde{k}}) \neq 0$. Part (a) follows by letting $A = \mathrm{Res}(\Phi_r, P_{I_1,I_2,\widetilde{k}})$. (See [3].)

Next, apply Lemma 2, taking $d_1 \leq 2rr_1K$, $H_1 \leq 2^{Kr_1}$, $d_2 = \phi(r)$, $H_2 = 1$ to get Part (b) with $\log A < 2rr_1(\log r)K < r(\log r)^2\, K$. ∎

Proof of Theorem 1'. Let $I \subset [1, r-1]$ with $|I| = r_1 = [12^{-7} \log r]$ be given by Lemma 3. Denote

$$K = \left[\frac{\log p}{5n(\log n)^2}\right]. \tag{2.6}$$

We may assume $K > 1$, since otherwise there is nothing to prove.

Claim. The K^{r_1} elements

$$\alpha^{\sum_{t\in I} h_t q^t}, \quad 0 \leq h_t < K \tag{2.7}$$

are distinct in $\mathbb{F}_{q^n}$.

Proof of Claim. Write

$$\alpha^{\sum_{t\in I} h_t q^t} = \prod_{t\in I} \left(\beta^{q^t} + \beta^{-q^t}\right)^{h_t}. \tag{2.8}$$

Since $q \in \mathbb{Z}$ is primitive $\pmod r$, the set of the least nonnegative residues of $\{q^t \pmod r) : 1 \le t \le r-1\}$ is $\{1, \cdots, r-1\}$. Let $\widetilde{I}$ (respectively, $\{k_s\}_s$) be the set corresponding to I (resp. $\{h_t\}_t$) under this identification. Then

$$\alpha^{\sum_{t\in I} h_t q^t} = \prod_{s\in \widetilde{I}} \left(\beta^{s} + \beta^{-s}\right)^{k_s}. \tag{2.9}$$

Thus, if the claim is false, then there exist $I_1, I_2 \subset \widetilde{I}$ and $\widetilde{k} = \{k_s\}_{s\in I_1\cup I_2}$ such that

$$P_{I_1,I_2,\widetilde{k}}(\beta) = 0 \quad \text{in } \overline{\mathbb{F}}_q \tag{2.10}$$

with $P_{I_1,I_2,\widetilde{k}}$ defined as in (2.5).

Apply Lemma 3. The right hand side of Part (a) vanishes in $\overline{\mathbb{F}}_q$. Therefore, $A \equiv 0 \pmod p$. Hence $|A| \ge p$ contradicting to Part (b) and (2.6).

The claim implies that α has order at least K^{r_1}. $\square$

Proof of Theorem 2. We start by observing that in view of (1.2), we may assume $n < (\log p)^2$.

Take P large and fix $n < (\log P)^2$. Let r_1 be given by Lemma 3. (Note that $r = 2n + 1$.) Take

$$K = \frac{1}{r}\left(\frac{P}{(\log P)^7}\right)^{\frac{1}{r_1+1}}. \tag{2.11}$$

Let

$$A = A_n = \prod_{\substack{I_1\cap I_2=\emptyset, |I_1|+|I_2|\le r_1 \\ \widetilde{k}=\{k_s\}_{s\in I_1\cup I_2}, k_s<K}} \operatorname{Res}(\Phi_r, P_{I_1,I_2,\widetilde{k}}) \in \mathbb{Z}\setminus\{0\}, \tag{2.12}$$

where $\prod$ is over non-vanishing resultants.

By Lemma 3 Part (b),

$$|A| < e^{r(\log r)^2 K\, K^{r_1}\, r^{r_1}} = e^{P/(\log P)^5}. \tag{2.13}$$

(The last inequality is by (2.11) and that $r \le (\log P)^2$.)

Let $\mathcal{E}_n$ be the set of prime divisors of A_n. Then $|\mathcal{E}_n| \lesssim P/(\log P)^6$. Also, for $p \notin \mathcal{E}_n$, we have $(p, A_n) = 1$.

Let

$$\mathcal{E} = \bigcup_{n<(\log P)^2} \mathcal{E}_n.$$

Then

$$|\mathcal{E}| < \frac{P}{(\log P)^4}.$$

Let $p < P$, $p \notin \mathcal{E}$. We repeat the argument in the proof of Theorem 1 and have

$$\mathrm{ord}(\alpha) > K^{r_1} > P^{1-\frac{1}{r_1+1}}(\log P)^{-\log\log P} > P^{1-\frac{C}{\log n}} > p^{1-\frac{C}{\log n}}. \qquad \blacksquare$$

Proof of Remark 2.1. Let $d = [\mathbb{F}_q(\beta) : \mathbb{F}_q]$. Since ℓ is prime and $\Phi_\ell(\beta) = 0$, we have $\mathrm{ord}(\beta) = \ell$ and hence $q^d \equiv 1 \pmod{\ell}$. According to the result of Erdös-Murty [4] (see Theorem EM below), for most ℓ, $\mathrm{ord}_\ell(q) > \ell^{1/2+\epsilon(\ell)}$, where $\epsilon(\ell) \to 0$ as $\ell \to \infty$. Hence $d > \ell^{1/2+\epsilon(\ell)}$, i.e. $d^{2-\epsilon(\ell)} > \ell$. Voloch's result ([10], section 5) implies $\mathrm{ord}(\beta + \beta^{-1}) > \exp(d^{\delta'}) > \exp(\ell^\delta)$. $\blacksquare$

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 $p \leq x$ such that $p-1$ has divisor in $(x^\delta, x^{\delta+\epsilon(x)})$ is $o(\frac{x}{\log x})$.*

Proof of Theorem 3. Let $J \subset [0, r-1]$ be the set of the least nonnegative residues modulo r of $1, q, q^2, \cdots, q^{n-1}$. Our assumption implies that $|J| = n$. Denote

$$K = \left[\frac{\log p}{r \log r \log n}\right]. \tag{2.14}$$

Let $z \in \mathbb{C}$ be a root of Φ_r. Applying Lemmas 1 and 3 on $\{z^s : s \in J\}$, we obtain $I \subset J$ with $r_1 = |I| = [12^{-7}\log n]$ such that $P_{I_1,I_2,\widetilde{k}}(z) \neq 0$ for any $P_{I_1,I_2,\widetilde{k}}$, where $I_1, I_2, \overline{k}$ and $P_{I_1,I_2,\widetilde{k}}$ are as in (2.5).

Since $\deg(P_{I_1,I_2,\widetilde{k}}) \leq rK\log n$ and $\mathrm{ht}(P_{I_1,I_2,\widetilde{k}}) \leq 2^{K\log n}$, by Lemma 2, we have

$$\mathrm{Res}(\Phi_r, P_{I_1,I_2,\widetilde{k}}) < r^{rK\log n} < p.$$

The last inequality is by (2.14). The argument for Theorem 1' gives

$$\mathrm{ord}(\alpha) > K^{r_1} > \left(\frac{\log p}{r\log r\log n}\right)^{c\log n}.$$

If $r = \mathrm{ord}(\beta) < \big(\log p\big)^{1-\frac{1}{c\log n}}\big(\log n\big)^{-1}$, then $\log r < \log\log p$ and hence

$$\mathrm{ord}(\alpha) > \frac{\log p}{(\log\log p)^{c\log n}} > \big(\log p\big)^{1-\frac{1}{c\log n}}\big(\log\log p\ \log n\big)^{-1}. \qquad \blacksquare$$

ACKNOWLEDGMENT

The author would like to thank I. Shparlinski and the referee for helpful comments which improve the theorems. The author would also like to thank K. Bibak for pointing out an error in a reference and the Mathematics Department of University of California at Berkeley for hospitality.

REFERENCES

1. O. Ahmadi, I. Shparlinski and J. F. Voloch, Multiplicative Order of Gauss Periods, *Int. J. Number. Theory*, **6** (2010), 877-882.
2. M.-C. Chang, Elements of large order in prime finite fields, *Bull. Aust. Math. Soc.*, to appear.
3. D. A. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.
4. P. Erdős and M. R. Murty, *On the order of a* $\pmod p$, Number theory (Ottawa, 1996), 87-97, CRM Proc. Lecture Notes, 19.
5. J.-H. Evertse, H. Schlickewei and W. Schmidt, Linear equations in variables which lie in a multiplicative group, *Annals Math.*, **155** (2002), 807-836.
6. J. von zur Gathen and I. Shparlinski, *Gauss periods in finite fields*, Proc. 5th Conference of Finite Fields and their Applications, Augsburg, 1999, Springer-Verlag, Berlin, 2001, pp. 162-177.
7. R. Popovych, Elements of high order in finite fields of the form $\mathbb{F}_q[x]/\Phi_r(x)$, *Finite Fields Appl.*, **18** (2012), 700-710.
8. I. Shparlinski, Additive combinatorics over finite fields: New results and applications, in: *Proc. RICAM-Workshop on Finite Fields and Their Applications: Character Sums and Polynomials*, De Gruyter, (to appear).
9. I. Shparlinski, On the multiplicative orders of γ and $\gamma + \gamma^{-1}$ over finite fields, *Finite Fields Appl.*, **7** (2001), 327-331.
10. J. F. Voloch, On the order of points on curves over finite fields, *Integers*, **7** (2007), A49.
11. 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, U.S.A.
E-mail: mcc@math.ucr.edu