Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 26, 2020, No. 2, 47–52
DOI: 10.7546/nntdm.2020.26.2.47-52

On multiplicative order of elements in finite fields based on cyclotomic polynomials

Roman Popovych

Department of Specialized Computer Systems, Lviv Polytechnic National University
Bandery Str.,12, Lviv, 79013, Ukraine
e-mails: rombp07@gmail.com, roman.b.popovych@lpnu.ua

Received: 4 May 2019 **Revised:** 1 April 2020 **Accepted:** 8 April 2020

Abstract: We obtain explicit lower bound on multiplicative orders of all elements in finite field extensions generated by a root of unity. The bound does not depend on any unknown constant. The result of Ahmadi, Shparlinski and Voloch [1] is a consequence of our main result.

Keywords: Finite field, Multiplicative order, Lower bound, Partition.
2010 Mathematics Subject Classification: 11T30.

1 Introduction

The problem of constructing efficiently a primitive element for a given finite field is notoriously difficult in the computational theory of finite fields. That is why one considers less restrictive question: to find an element with large multiplicative order. It is sufficient in this case to obtain a lower bound on the order. Large order elements are needed in several applications. Such applications include but are not limited to cryptography, coding theory, pseudo random number generation and combinatorics. A review of obtained in this area results is provided in [9, Section 4.4]. The problem of such elements construction is considered both for general and for special finite fields (extensions based on cyclotomic, Kummer or Artin–Schreier polynomials, recursive extensions) [1, 3, 5, 8, 10–13]. For special finite fields, it is possible to construct elements which can be proved to have much larger orders.

A partition of an integer C is a sequence of such non-negative integers $u_1,...,u_C$ that $\sum_{j=1}^{C} ju_j = C$. $U(C,d)$ denotes the number of such partitions of C, for which $u_1,...,u_C \le d$, i.e. each part appears no more than d times. $Q(C,d)$ denotes the number of such partitions of C, for which $u_j = 0$ if $j \equiv 0 \bmod d$, that is each part is not divisible by d.

Let q be a power of a prime number p, and F_q be a finite field with q elements. We use F_q^* to denote the multiplicative group of F_q. Field extensions based on cyclotomic polynomials are considered in [1, 10, 12]. More precisely, the following extensions are constructed. Let $r \geq 3$ be a prime number coprime with q. Let q be a primitive root modulo r, that is the multiplicative order of q modulo r equals to $r-1$. Set $F_q(\theta) = F_{q^{r-1}} = F_q[x]/\Phi_r(x)$, where $\Phi_r(x) = x^{r-1} + x^{r-2} + ... + 1$ is the r-th cyclotomic polynomial and θ is the coset of x modulo $\Phi_r(x)$. It is clear that the equality $\theta^r = 1$ holds. The element $\theta + \theta^{-1} = \theta^{r-1} + \theta$ is called Gauss period of type $((r-1)/2,2)$.

The problem of finding lower bounds on the order of elements in the extensions based on cyclotomic polynomials was in particular considered in [1, 10, 11, 12]. Lower bound on the order of the Gauss period and some similar elements is given in [1, 10]. Voloch (see [12] and [9, Section 4.4]) gave lower bound on the orders for all elements in the extensions. He showed that, for $R(x) \in F_q[x]$, $R(x)$ not a monomial, $R(\theta)$ has the order at least $\exp(r^\delta)$ for some constant δ. In this paper, we prove Theorem 1 below that also gives explicit lower bound on multiplicative orders of all elements in the extensions. The obtained lower bound does not depend on any unknown constant. We also show that there are always elements of small order. The result from [1] is a consequence of our main result.

2 Main result

All lower bounds in Theorem 1 involve a notion of a partition, where each part appears no more than p – 1 times. We use for the proof of the theorem a modified technique from [10] that is in turn similar to that in [1]. Here $\lfloor a \rfloor$ denotes the nearest integer smaller than a.

Theorem 1. *Let q be a power of prime number p, $r \geq 3$ a prime number coprime with q, q a primitive root modulo r, θ generates the extension $F_q(\theta) = F_{q^{r-1}}$. Let $0 \leq e \leq r-1$, $1 \leq f \leq g \leq r-2$; w_g, w_f, w_0 belong to F_q^* and $c = \left\lfloor \frac{r-1}{g} \right\rfloor - 1$. Then element $\theta^e(\sum_{i=f}^{g} w_i\theta^i + w_0)$ has the multiplicative order at least $U(c, p-1)$.*

Proof. As q is primitive modulo r, for each $j = 1,...,c$, an integer α_j exists such that $q^{\alpha_j} \equiv j \bmod r$. The powers

$$\left(\theta^e(\sum_{i=f}^{g} w_i\theta^i + w_0)\right)^{q^{\alpha_j}} = \theta^{ej}(\sum_{i=f}^{g} w_i\theta^{ij} + w_0)$$

belong to the group generated by $\theta^e(\sum_{i=f}^{g} w_i\theta^i + w_0)$. Let S be the set of partitions $(u_1,...,u_c)$ of the integer c, where each part appears no more than $p-1$ times, that is

$\sum_{j=1}^{c} ju_j = c,\ 0 \le u_1,...,u_c \le p-1$. For every partition from S we construct the following product

$$\prod_{j=1}^{c}(\theta^{ej}(\sum_{i=f}^{g} w_i\theta^{ij} + w_0))^{u_j} = \theta^{e\sum_{j=1}^{c} ju_j} \prod_{j=1}^{c}(\sum_{i=f}^{g} w_i\theta^{ij} + w_0)^{u_j} = \theta^{ec}\prod_{j=1}^{c}(\sum_{i=f}^{g} w_i\theta^{ij} + w_0)^{u_j}$$

that also belongs to the group. We show that if two partitions from S are distinct, then the correspondent products do not coincide.

Assume that partitions $(u_1,...,u_c)$ and $(v_1,...,v_c)$ from S are distinct, and the correspondent products are equal:

$$\theta^{es}\prod_{j=1}^{c}(\sum_{i=f}^{g} w_i\theta^{ij} + w_0)^{u_j} = \theta^{es}\prod_{j=1}^{c}(\sum_{i=f}^{g} w_i\theta^{ij} + w_0)^{v_j} .$$

Since the polynomial $\Phi_r(x)$ is the characteristic polynomial of θ, we write

$$\prod_{j=1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{u_j} = \prod_{j=1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{v_j} (\bmod \Phi_r(x)).$$

As there are polynomials of degree $cg \le r-2 < \deg\Phi_r(x)$ on the left and on the right side of the equality, these polynomials are equal as polynomials over F_q, i.e.,

$$\prod_{j=1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{u_j} = \prod_{j=1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{v_j} . \tag{1}$$

Let k be the smallest integer for which $u_k \neq v_k$ and, say $u_k > v_k$. After removing common factors on both sides of (1), we obtain

$$(\sum_{i=f}^{g} w_i x^{ik} + w_0)^{u_k - v_k} \prod_{j=k+1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{u_j} = \prod_{j=k+1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{v_j} . \tag{2}$$

Denote the absolute term of the polynomial $\prod_{j=k+1}^{c}(\sum_{i=f}^{g} w_i x^{ij} + w_0)^{u_j}$ by b. Since $w_0 \neq 0$, then $b \neq 0$. Applying the multinomial formula to $(\sum_{i=f}^{g} w_i x^{ik} + w_0)^{u_k - v_k}$, we obtain that there is the term

$$(u_k - v_k) w_0^{u_k - v_k - 1} b w_f x^{fk}$$

on the left side of (2) with minimal non-zero power of x. Since $0 \le u_k, v_k \le p-1$, $u_k \neq v_k$, $w_0, w_f, b \neq 0$, the term is non-zero. And such term does not occur on the right side, which makes the identity (2) impossible. Hence, products, corresponding to distinct partitions, cannot be equal and the result follows. □

Consider the element $\theta+\theta^{-1}=\theta^{-1}(\theta^2+1)=\theta^{r-1}(\theta^2+1)$, that is the partial case $e=r-1$, $f=g=2$, $w_0=w_g=1$ of Theorem 1. Then we obtain the following corollary.

Corollary 2 [1, theorem 1]**.** *Let q be a power of prime number p, $r\geq 3$ a prime number coprime with q, q a primitive root modulo r, θ generates the extension $F_q(\theta)=F_{q^{r-1}}$. Then Gauss period $\theta+\theta^{-1}$ has the multiplicative order at least* $U\left(\frac{r-1}{2}-1,p-1\right)$.

Corollary 3. *Let q be a power of prime number p, $r\geq 3$ a prime number coprime with q, q a primitive root modulo r, θ generates the extension $F_q(\theta)=F_{q^{r-1}}$. Let $1\leq f\leq g\leq r-2$; w_f, w_g, w_0 belong to F_q^*,* $c=\left\lfloor\frac{r-1}{g}\right\rfloor-1$ and $T(\theta)=\sum_{i=f}^{g}w_i\theta^i+w_0$. *Then $\theta^iT(\theta^j)$ for $0\leq i,j\leq r-1$ has the multiplicative order at least $U(c,p-1)$.*

Proof. According to [6, Theorem 2.18], the conjugates of an element from the group $F_{q^{r-1}}^*$ with respect to any subfield of $F_{q^{r-1}}$ have the same order in $F_{q^{r-1}}^*$. Clearly, all conjugates of $\theta^eT(\theta)$ with respect to $F_{q^{r-1}}$ are obtained by substitution $\theta\to\theta^j$ for some $0\leq j\leq r-1$ and have the form $\theta^{ej}T(\theta^j)$. Then the result follows from Theorem 1. □

Remark 4. As a consequence of Theorem 1, most of elements of the form $R(\theta)$, where $R(x)\in F_q[x]$, $R(x)$ not a monomial, have the large order. However, consider element $R(\theta)=\theta^{(r-1)/2+1}+\theta^{(r-1)/2}+1$. Since *c* = 0, we cannot assert, using Theorem 1, that the $R(\theta)$ is of large order. But if we put $j=(r-1)/2$ and rewrite $R(\theta)=\theta^{-j}(\theta^{2j}+\theta^j+1)$, then, according to Corollary 3, the order of $R(\theta)$ is at least $U\left(\frac{r-1}{2}-1,p-1\right)$.

Remark 5. It is known [4, exercise 2.3.10] that finite cyclic group of order *n* has a unique subgroup of order *m* for every positive divisor *m* of *n*, hence there are $\varphi(m)$ elements of order *m*. Since $q^{(r-1)/2}-1$ and $q^{(r-1)/2}+1$are even, we have that 8 divides the order $q^{r-1}-1$ of $F_{q^n}^*$. Therefore, there are always elements of small order in $F_{q^n}^*$: 2 elements of order 4 and 4 elements of order 8. If 4 does not divide $q-1$, then these elements does not belong to F_q^*.

Explicit lower bounds on the orders of elements in terms of *p* and *c* (which depends on *r* and *g*) are of special interest in applications. That is why we use below some known estimates from [2, 7] and Corollary 1 to derive such bound on the multiplicative order of the examined elements. We consider the most interesting case when *c* is large comparatively to *p*. The following corollary holds in this case.

Corollary 6. *Let q be a power of prime number p,* $r \geq 3$ *a prime number coprime with q, q a primitive root modulo r, θ generates the extension* $F_q(\theta) = F_{q^{r-1}}$. *Let* $1 \leq f \leq g \leq r-2$; *w*$_g$, *w*$_f$, *w*$_0$ *belong to* F_q^*, $c = \left\lfloor \frac{r-1}{g} \right\rfloor - 1$ *and* $T(\theta) = \sum_{i=f}^{g} w_i \theta^i + w_0$. *If* $c \geq p^2$, *then* $\theta^i T(\theta^j)$ *for* $0 \leq i, j \leq r-1$ *has the multiplicative order larger than*

$$\left(\frac{p(p-1)}{160c}\right)^{\sqrt{p}} \exp\left(\pi\sqrt{\frac{2}{3}(1-\frac{1}{p})c}\right).$$

Proof. According to [2, Corollary 1.3], the following equality is true:

$$U(n, d-1) = Q(n, d). \tag{3}$$

It follows from Corollary 1 and Equality (3) that the multiplicative order *L* of $\theta^i T(\theta^j)$ satisfies the bound $L \geq U(c, p-1) = Q(c, p)$. According to [7, Theorem 5.1], the following inequality holds for *d* > 1 and $n \geq d^2$:

$$Q(n,d) > \left(\frac{d(d-1)}{160n}\right)^{\sqrt{d}} \exp\left(\pi\sqrt{\frac{2}{3}(1-\frac{1}{d})n}\right). \tag{4}$$

Inequality (4) implies the result. □

Remark 7. The considered above extensions exist for infinitely many *r* under the assumption that the Artin's conjecture holds for *q*. Artin's conjecture on primitive roots states that a given integer *q* which is neither a perfect square nor −1 is a primitive root modulo infinitely many primes *r*. For example, we give below some computed pairs *q*, *r*.

$q = 3,\ \ r = 401$	$q = 5,\ \ r = 257$	$q = 11, r = 419$
$q = 11,\ r = 1009$	$q = 3,\ \ r = 65537$	

Note that $2^{16} + 1 = 65537$ is the largest known prime Fermat number.

Example. Elements of the form $\theta + w_0$, where *w*$_0$ is any nonzero element from F_q, have the order larger than

$$L = \left(\frac{p(p-1)}{160(r-2)}\right)^{\sqrt{p}} \exp\left(\pi\sqrt{\frac{2}{3}\left(1-\frac{1}{p}\right)(r-2)}\right).$$

We provide a few numerical examples of the bound *L*. Recall that the number of elements in the multiplicative group $F_{q^{r-1}}^*$ equals $q^{r-1} - 1$. We have chosen to take logarithms to base 2 of numbers $q^{r-1} - 1$ and *L* because of their size. Results for some pairs *q*, *r* (*q* = *p*) are given in the following table.

No.	*q*	*r*	**log**$_2$**(**q^{r-1} **– 1)**	**log**$_2$$L$
1	3	401	633.98	37.18
2	5	257	594.41	28.27
3	11	419	1446.04	41.39
4	11	1009	3487.1	77.09
5	3	65537	103872.1	737.6

Acknowledgements

The author would like to thank Felipe Voloch and the referees for useful comments.

References

[1] Ahmadi, O., Shparlinski, I. E., & Voloch, J. F. (2010). Multiplicative order of Gauss periods, *Intern. J. Number Theory*, 6 (4), 877–882.

[2] Andrews, G.E. (1976). *The Theory of Partitions*, Addison–Wesley, Reading.

[3] Cheng, Q. (2005). On the construction of finite field elements of large order, *Finite Fields Appl.*, 11 (3), 358–366.

[4] Ehrlich, G. (1991). *Fundamental Concepts of Abstract Algebra*, PWS-Kent Publ., Boston.

[5] Gao, S. (1999). Elements of provable high orders in finite fields, *Proc. Amer. Math. Soc.*, 127 (6), 1615–1623.

[6] Lidl, R., & Niederreiter, H. (1997). *Finite Fields*, Cambridge University Press.

[7] Maroti, A. (2003). On elementary lower bounds for the partition function, *Integers*, 3, A10.

[8] Martinez, F. E. B., & Reis, L. (2016). Elements of high order in Artin–Schreier extensions of finite fields F_q, *Finite Fields Appl.*, 41, 24–33.

[9] Mullen, G. L., & Panario, D. (2013). *Handbook of Finite Fields*, CRC Press, Boca Raton.

[10] Popovych, R. (2012). Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$, *Finite Fields Appl.*, 18 (4), 700–710.

[11] Popovych, R. (2013). Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$, *Finite Fields Appl.*, 19 (1), 86–92.

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

[13] Voloch, J. F. (2010). Elements of high order on finite fields from elliptic curves, *Bull. Aust. Math. Soc.*, 81 (3), 425–429.