

Multiplicative Order of Gauss Periods

OMRAN AHMADI

Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario, M5S 3G4, Canada
oahmadid@comm.utoronto.ca

IGOR E. SHPARLINSKI

Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

JOSÉ FELIPE VOLOCH

Department of Mathematics
University of Texas
Austin TX 78712 USA
voloch@math.utexas.edu

Abstract

We obtain a lower bound on the multiplicative order of Gauss periods which generate normal bases over finite fields. This bound improves the previous bound of J. von zur Gathen and I. E. Shparlinski.

1 Introduction

For a prime power q we use \mathbb{F}_q to denote the finite field with q elements.

Normal bases are a very useful notion in the theory of finite fields,, see [5, 16, 17] for the definition, basic properties and references. One of the most interesting constructions of normal bases come from *Gauss periods*, see [7, 8, 9, 10, 11, 12, 13] and references therein. In particular, Gauss periods of type $(n, 2)$ are of special interest, which can be defined as follows.

Let $r = 2n + 1$ be a prime number coprime with q and $\beta \in \mathbb{F}_{q^{2n}}$ be a primitive r th root of unity. Then the element

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

is called a Gauss period of type $(n, 2)$. The Gauss period of type $(n, 2)$ can be defined for composite r too, see [7], however we do not consider them in this paper (neither we study Gauss period of type (n, k) for $k \neq 2$).

It is well-known that the minimal polynomial of β over \mathbb{F}_q is of degree t , where t is the multiplicative order of q modulo r . Thus $t|2n$.

It is also well known that α given by (1), generates a normal basis of \mathbb{F}_{q^n} if and only if $\gcd(2n/t, n) = 1$, which, therefore, is possible if and only if

- $t = 2n = r - 1$, that is, q is a primitive root modulo r ;
- $t = n = (r - 1)/2$ and n is odd, that is, q generates the subgroup of quadratic residues modulo $r \equiv 3 \pmod{4}$

In one direction this follows from [5, Lemma 5.4 and Theorem 5.5] and in the other direction it follows by examining the proof of these results see also [1] and [3].

It is shown [11] that in the first case, that is, for $t = r - 1$, α is of multiplicative order

$$L_n \geq 2^{\sqrt{2n} + O(1)}, \tag{2}$$

see also [12]. This gives an explicit example of finite field elements of exponentially large order. Here we use some new arguments to improve the bound (2).

Recent results of Q. Cheng [6] give polynomial time constructions of elements of large order for certain values of (q, n) . Our construction seems to apply to different sets of pairs (q, n) and complement the results of [6]. Furthermore it is interesting to establish tighter bounds on the size of the multiplicative order of such classical objects as Gauss periods of type $(n, 2)$, especially of those which generate normal bases.

Let $P(s, v)$ be the number of integer partitions of an integer s where each part appears no more than v times, that is, the number of solutions to the equation

$$\sum_{j=1}^s u_j j = s$$

in non-negative integers $u_1, \dots, u_s \leq v$.

Theorem 1. *Let p be the characteristic of \mathbb{F}_q and let q be a primitive root modulo a prime $r = 2n + 1$. Then the multiplicative order L_n of α , given by (1), satisfies the bound*

$$L_n \geq P(n - 1, p - 1).$$

Now we can use some standard estimates to derive an asymptotic lower bound on L_n .

Corollary 2. *Let p be the characteristic of \mathbb{F}_q and let q be a primitive root modulo a prime $r = 2n + 1$. Then, uniformly over q , the multiplicative order L_n of α , given by (1), satisfies the bound*

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

as $n \rightarrow \infty$.

Note that when in the worst case (when $p = 2$) $\exp \left(\pi \sqrt{2/6} \right) = 6.1337 \dots$ while $\exp \left(\pi \sqrt{2/3} \right) = 13.0019 \dots$ (which corresponds to $p \rightarrow \infty$). On the other hand, we have $2^{\sqrt{2}} = 2.6651 \dots$

2 Proof of Theorem 1

Let us consider the set

$$\mathfrak{B} = \left\{ (u_1, \dots, u_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1} \mid \sum_{j=1}^{n-1} u_j j = n - 1, u_1, \dots, u_{n-1} \leq p - 1 \right\}.$$

Now, for $j = 1, 2, \dots, n - 1$ we define an integer z_j by $q^{z_j} \equiv j \pmod{r}$, $0 \leq z_j < r$ (which is possible since q is a primitive root modulo r).

For every partition $\mathcal{U} = (u_1, \dots, u_{n-1}) \in \mathfrak{P}$ we put

$$Q_{\mathcal{U}} = \sum_{j=1}^{n-1} u_j q^{z_j}.$$

We now consider the powers

$$\alpha^{Q_{\mathcal{U}}} = \prod_{j=1}^{n-1} \alpha^{u_j q^{z_j}} = \prod_{j=1}^{n-1} (\beta + \beta^{-1})^{u_j q^{z_j}} = \prod_{j=1}^{n-1} (\beta^{q^{z_j}} + \beta^{-q^{z_j}})^{u_j}$$

taken for all $\mathcal{U} \in \mathfrak{P}$. Since $\beta^r = 1$, we have

$$\alpha^{Q_{\mathcal{U}}} = \prod_{j=1}^{n-1} (\beta^j + \beta^{-j})^{u_j} = \beta^{-(n-1)} \prod_{j=1}^{n-1} (\beta^{2j} + 1)^{u_j}. \quad (3)$$

Clearly it suffices to show that for two distinct partitions $\mathcal{U}, \mathcal{V} \in \mathfrak{P}$ we have $\alpha^{Q_{\mathcal{U}}} \neq \alpha^{Q_{\mathcal{V}}}$.

We now assume that there are two distinct partitions

$$\mathcal{U} = (u_1, \dots, u_{n-1}), \quad \mathcal{V} = (v_1, \dots, v_{n-1}) \in \mathfrak{P}$$

with

$$\alpha^{Q_{\mathcal{U}}} = \alpha^{Q_{\mathcal{V}}}. \quad (4)$$

By (3) we conclude that

$$\prod_{j=1}^{n-1} (\beta^{2j} + 1)^{u_j} = \prod_{j=1}^{n-1} (\beta^{2j} + 1)^{v_j}.$$

Since the characteristic polynomial of β is the r -th cyclotomic polynomial $\Phi_r(X)$, we obtain polynomial divisibility

$$\Phi_r(X) \mid U(X) - V(X) \quad (5)$$

where

$$U(X) = \prod_{j=1}^{n-1} (X^{2j} + 1)^{u_j}, \quad V(X) = \prod_{j=1}^{n-1} (X^{2j} + 1)^{v_j},$$

are polynomials of degree $2(n-1) < 2n = r-1 = \deg \Phi_r(X)$. Hence (5) implies that $U(X) = V(X)$. After removing common factors, the identity

$$\prod_{j=1}^{n-1} (X^{2j} + 1)^{u_j} = \prod_{j=1}^{n-1} (X^{2j} + 1)^{v_j}$$

leads to the relation

$$\prod_{h \in \mathcal{H}} (X^{2h} + 1)^{y_h} = \prod_{k \in \mathcal{K}} (X^{2k} + 1)^{z_k} \quad (6)$$

for two disjoint sets $\mathcal{H}, \mathcal{K} \in \{1, \dots, n-1\}$ and some positive integers y_h , $h \in \mathcal{H}$, and z_k , $k \in \mathcal{K}$. Since It is now clear that since

$$\gcd \left(\prod_{h \in \mathcal{H}} y_h \prod_{k \in \mathcal{K}} z_k, p \right) = 1,$$

the term X^{2f} where f is the smallest element of $\mathcal{H} \cup \mathcal{K}$ occurs only on one side of (6), which makes this identity impossible.

Therefore (4) cannot hold and the result follows.

3 Proof of Corollary 2

Unfortunately, a uniform with respect to v lower bound on $P(s, v)$ does not seem to be in the literature. However, by [2, Corollary 1.3] we have

$$P(s, v) = Q(s, v+1)$$

where $Q(s, d)$ is the number of integer partitions of an integer s where each part is not divisible by d , that is, the number of solutions to the equation

$$\sum_{j=1}^s u_j j = s$$

in non-negative integers u_1, \dots, u_s such that $u_j = 0$ for $j \equiv 0 \pmod{d}$, $j = 1, \dots, s$.

By [14, Corollary 7.2], applied to a set $\{1, \dots, (\ell-1)/2\}$ for a fixed prime ℓ (thus $r = (\ell-1)/2$) implies that

$$Q(s, \ell) \geq \exp \left(\left(\pi \sqrt{\frac{2(\ell-1)}{3\ell}} + o(1) \right) \sqrt{s} \right). \quad (7)$$

Therefore there is a function $\lambda(s) \rightarrow \infty$ as $s \rightarrow \infty$, such that (7) holds uniformly over all primes $\ell \leq \lambda(s)$.

Now taking ℓ as the largest prime with

$$\ell \leq \min\{p, \lambda(n-1)\}$$

we obtain

$$P(n-1, p-1) \geq P(n-1, \ell-1) = Q(n-1, \ell).$$

Applying (7) we obtain the desired estimate. Indeed, if $\ell = p$ this is obvious. If $\ell \leq \lambda(n-1) < p$ then by the prime number theorem $\ell \sim \lambda(n-1)$ as $n \rightarrow \infty$. Therefore,

$$\frac{\ell-1}{\ell} = 1 + O(1/\lambda(n-1)) \quad \text{and} \quad \frac{p-1}{p} = 1 + O(1/\lambda(n-1)).$$

4 Remarks

It seems to be natural to use the approach of [4, 21], based on the polynomial *ABC*-theorem, see [18], in order to obtain good bounds on L_n . In fact this is possible indeed, however it seems to lead to a result which is slightly weaker than the bound of Theorem 1. In fact, instead of the set \mathfrak{P} one seems to need to consider sets of the shape

$$\mathfrak{R}_s(N) = \left\{ (u_1, \dots, u_s) \in \mathbb{Z}_{\geq 0}^{n-1} \mid \sum_{j=1}^s u_j j = N \right\}$$

with $s \sim \alpha n^{1/2}$ and $N = \beta n$, where α and β are positive constants (which are to be optimised). We remark that an asymptotic formula for $\#\mathfrak{R}_s(N)$ is given by a result of G. Szekeres [19, 20]. Using this approach we have been able to get a stronger bound than (2) but marginally weaker than that of Theorem 1. Still, it seems quite plausible that a use of the polynomial *ABC*-theorem may lead to stronger bounds. We pose this as an open question.

Acknowledgements

The authors are very gratefully to George Andrews for providing several crucial references.

This work was initiated during very pleasant visits by I. S. to Department of Combinatorics & Optimization of the University of Waterloo the Department of Mathematics of the University of Texas; the hospitality, support and stimulating research atmosphere of these institutions are gratefully acknowledged. During the preparation of this paper, I. S. was supported in part by ARC grant DP0556431.

References

- [1] O. Ahmadi, D. Hankerson, and A. Menezes, ‘Software implementation of arithmetic in \mathbb{F}_{3^m} ’, *Proc. International Workshop on the Arithmetic of Finite Fields (WAIFI 2007)*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, to appear.
- [2] G. E. Andrews, *The theory of partitions*, Addison-Wesley, 1976.
- [3] D. Ash, I. Blake, and S. Vanstone, ‘Low complexity normal bases’, *Discrete Applied Mathematics*, **25** (1989), 191–210.
- [4] D. J. Bernstein, ‘Sharper ABC-based bounds for congruent polynomials’, *J. Théorie des Nombres Bordeaux*, **17** (2005), 721–725.
- [5] I. F. Blake, X.H. Gao, A. J. Menezes, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Applications of finite fields*, Kluwer Acad. Publ., 1993.
- [6] Q. Cheng, ‘On the construction of finite field elements of large order’, *Finite Fields and Their Appl.*, **11** (2005), 358–366.
- [7] S. Feisel, J. von zur Gathen and A. Shokrollahi, ‘Normal bases via general Gauss periods’, *Math. Comp.*, **68** (1999), 271–290.
- [8] S. Gao, J. von zur Gathen and D. Panario, ‘Gauss periods: Orders and cryptographical applications’, *Math. Comp.*, **67** (1998), 343–352.
- [9] J. von zur Gathen and M. J. Nöcker, ‘Fast arithmetic with general Gauss periods’, *Theor. Comput. Sci.*, **315**, (2004), 419–452.
- [10] J. von zur Gathen and M. J. Nöcker, ‘Polynomial and normal bases for finite fields’, *J. Cryptology*, **18** (2005), 337–355.

- [11] 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.
- [12] J. von zur Gathen and I. E. Shparlinski, ‘Constructing elements of large order in finite fields’, *Lecture Notes in Computer Science*, vol. **1719**, Springer-Verlag, Berlin, 1999, 404–409.
- [13] J. von zur Gathen and I. E. Shparlinski, ‘Gauss periods in finite fields’, *Proc. 5th Conference of Finite Fields and their Applications*, Augsburg, 1999, Springer-Verlag, Berlin, 2001, 162–177.
- [14] P. Hagsis, ‘A problem on partitions with a prime modulus $p \geq 3$ ’, *Trans. Amer. Math. Soc.*, **102** (1962), 30–62.
- [15] G. H. Hardy and E. M. Wright, *An Introduction to the theory of numbers*, The Clarendon Press, Oxford University Press, New York, 1979.
- [16] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
- [17] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, 1999.
- [18] N. Snyder, ‘An alternate proof of Mason’s theorem’, *Elemente der Mathematik*, **55** (2000), 93–94.
- [19] G. Szekeres, ‘An asymptotic formula in the theory of partitions’, *Quart. J. Math.*, **2** (1951), 85–108.
- [20] G. Szekeres, ‘Some asymptotic formulae in the theory of partitions (II)’, *Quart. J. Math.*, **4** (1953), 96–111.
- [21] J. F. Voloch, ‘On some subgroups of the multiplicative group of finite rings’, *J. Théorie des Nombres Bordeaux*, **16** (2004), 233–239.