*Bull. Aust. Math. Soc.* **85** (2012), 505–508
doi:10.1017/S0004972711002887

# SUM–PRODUCT ESTIMATES AND MULTIPLICATIVE ORDERS OF $\gamma$ AND $\gamma + \gamma^{-1}$ IN FINITE FIELDS

IGOR SHPARLINSKI

(Received 1 September 2011)

**Abstract**

Using a recent result on the sum–product problem, we estimate the number of elements $\gamma$ in a prime finite field such that both $\gamma$ and $\gamma + \gamma^{-1}$ are of small order.

2010 *Mathematics subject classification*: primary 11T30; secondary 11B30.
*Keywords and phrases*: multiplicative order, sum–product theorem.

## 1. Introduction

Let $\mathbb{F}_q$ denote the finite field of $q$ elements. Given a nonzero element $\alpha \in \mathbb{F}_q^*$, as usual we define its multiplicative order $\operatorname{ord} \alpha$ as the smallest positive integer $t$ with $\alpha^t = 1$.

In [2, Research problem 3.1], a question was posed about the possibility of finding $\operatorname{ord} (\gamma + \gamma^{-1})$ from the known value of $\operatorname{ord} \gamma$; see also [2, Research problem 5.1].

It was shown in [11] that no such algorithm can possibly exist and in fact $\operatorname{ord} \gamma$ and $\operatorname{ord} (\gamma + \gamma^{-1})$ are independent in the following sense: for a sufficiently large $q$ and any positive divisors $n$ and $m$ of $q - 1$, the number $W_p(m, n)$ of $\gamma \in \mathbb{F}_q^*$ with

$$\operatorname{ord} \gamma = n \quad \text{and} \quad \operatorname{ord} (\gamma + \gamma^{-1}) = m$$

satisfies the inequality

$$\left| W_p(m, n) - \frac{\varphi(m)\varphi(n)}{q-1} \right| < 2q^{1/2}\tau(m)\tau(n), \tag{1}$$

where, as usual, $\varphi(k)$ and $\tau(k)$ denote the Euler and divisor functions, respectively. See also [4]. In particular, using the well-known estimates

$$\tau(k) = k^{o(1)} \quad \text{and} \quad \varphi(k) = k^{1+o(1)} \tag{2}$$

(see [9, Theorems 317 and 328]), we conclude that, for any fixed $\varepsilon > 0$ and sufficiently large $q$, and for any positive divisors $n$ and $m$ of $q - 1$ with $nm \ge q^{3/2+\varepsilon}$, there exists $\gamma \in \mathbb{F}_q^*$ with

$$\operatorname{ord} \gamma = n \quad \text{and} \quad \operatorname{ord} (\gamma + \gamma^{-1}) = m.$$

Furthermore, it follows from [8] that for fields $\mathbb{F}_q$ of a fixed characteristic $p$, for any fixed $\varepsilon > 0$, at least one of the multiplicative orders ord $\gamma$ and ord $(\gamma + \gamma^{-1})$ is at least $c(p, \varepsilon)(\ln q)^{4/3-\varepsilon}$, where $c(p, \varepsilon) > 0$ depends only on $p$ and $\varepsilon$.

Several more results about the multiplicative orders of $\gamma$ and $\gamma + \gamma^{-1}$ are given in [1, 6, 7]. Orders of algebraically related finite field elements are investigated by Voloch [13, 14].

In this paper we study an associated question of estimating the cardinality $\#\Gamma_q(T)$ of the set

$$\Gamma_q(T) = \{\gamma \in \mathbb{F}_q : \text{ord } \gamma \le T \text{ and ord } (\gamma + \gamma^{-1}) \le T\}.$$

Since for every $t \mid q-1$ there are $\varphi(t)$ elements $\gamma \in \mathbb{F}_q$ of order $t$,

$$\#\Gamma_q(T) \le \sum_{\substack{t \le T \\ t \mid q-1}} \varphi(t) \le \sum_{\substack{t \le T \\ t \mid q-1}} t \le T\tau(q-1),$$

which implies the following trivial bound:

$$\#\Gamma_q(T) \le Tq^{o(1)}. \tag{3}$$

For large values of $T$ one derives from (1) that

$$\#\Gamma_q(T) \le \sum_{\substack{m \le T \\ m \mid q-1}} \sum_{\substack{n \le T \\ n \mid q-1}} W_p(m, n) = \frac{1}{q-1}\Bigg(\sum_{\substack{m \le T \\ m \mid q-1}} \varphi(m)\Bigg)^2 + O(q^{1/2+o(1)}).$$

Thus, using (2), we deduce

$$\#\Gamma_q(T) \le T^2 q^{-1+o(1)} + q^{1/2+o(1)}. \tag{4}$$

Although the question is also interesting for arbitrary finite fields $\mathbb{F}_q$, here we concentrate on the case of prime fields, that is, when $q = p$ is prime. This allows us to use a recent result of Rudnev [10] on the sum–product problem, see [3, 5, 10, 12] and references therein, which generally speaking does not hold in arbitrary finite fields. Furthermore, if $\mathbb{F}_r \subseteq \mathbb{F}_q$ then obviously $\#\Gamma_q(r-1) = r-1$. Thus without any other restrictions the trivial bound (3) is actually tied.

Here, we improve the bounds (3) and (4) for a prime $q = p$ and for values of $T$ that are not too large.

THEOREM 1. *Let $p$ be prime. Then, for any fixed $\varepsilon > 0$ and $T \le p^{11/20-\varepsilon}$,*

$$\#\Gamma_p(T) \le T^{10/11} p^{o(1)}.$$

Note that for $T > p^{11/20-\varepsilon}$ the bound (4) already also gives a nontrivial estimate on $\#\Gamma_p(T)$.

https://doi.org/10.1017/S0004972711002887 Published online by Cambridge University Press

## 2. Sum–product problem

Let $\mathbb{F}_p$ denote the finite field of $p$ elements. For a set $\mathcal{A} \subseteq \mathbb{F}_p^*$ we define the sum and product sets

$$2\mathcal{A} = \{a_1 + a_2 : a_1, a_2 \in \mathcal{A}\} \quad \text{and} \quad \mathcal{A}^2 = \{a_1 a_2 : a_1, a_2 \in \mathcal{A}\}.$$

Rudnev [10], improving the previous result of Bourgain and Garaev [3], proved the following estimate.

LEMMA 2. *Let $p$ be prime. Then, for an arbitrary set $\mathcal{A} \subseteq \mathbb{F}_p$ with $\#\mathcal{A} \le p^{1/2}$,*

$$\max\{\#(2\mathcal{A}), \#(\mathcal{A}^2)\} \ge c\frac{(\#\mathcal{A})^{11/10}}{(\log \#\mathcal{A})^{4/11}}$$

*for some absolute constant $c > 0$.*

## 3. Proof of Theorem 1

We see from (2) that for some $m, n \le T$ there is a set

$$\mathcal{R} = \{\gamma \ : \ \gamma \in \Gamma_q(T), \ \operatorname{ord}\gamma = m, \ \operatorname{ord}(\gamma+\gamma^{-1}) = n\}$$

and also

$$\#\mathcal{R} = \#\Gamma_p(T)p^{o(1)}. \tag{5}$$

Removing, if necessary, some elements from $\mathcal{R}$ we obtain a set $\mathcal{S} \subseteq \mathcal{R}$ with

$$\#\mathcal{S} = \min\{\#\mathcal{R}, \lfloor p^{1/2} \rfloor\}.$$

We now define

$$\mathcal{A} = \{\gamma^2 + \gamma^{-2} : \gamma \in \mathcal{S}\} \quad \text{and} \quad \mathcal{B} = \{\gamma + \gamma^{-1} : \gamma \in \mathcal{S}\}.$$

Clearly

$$\#\mathcal{A} \ge \frac{\#\mathcal{S}}{4}.$$

From the identity

$$(\rho+\rho^{-1})(\sigma+\sigma^{-1}) = \rho\sigma + \rho^{-1}\sigma^{-1} + \rho\sigma^{-1} + \rho^{-1}\sigma,$$

we conclude that

$$\mathcal{A}^2 \subseteq 2\mathcal{A}. \tag{6}$$

Now let us take $\alpha, \beta \in \mathcal{S}$. Then

$$\alpha^2 + \alpha^{-2} + \beta^2 + \beta^{-2} = (\alpha\beta + \alpha^{-1}\beta^{-1})(\alpha\beta^{-1} + \alpha^{-1}\beta).$$

Therefore

$$2\mathcal{A} \subseteq \mathcal{B}^2. \tag{7}$$

Combining (6) and (7),

$$\#(\mathcal{B}^2) \ge \#(2\mathcal{A}) = \max\{\#(2\mathcal{A}), \#(\mathcal{A}^2)\}.$$

https://doi.org/10.1017/S0004972711002887 Published online by Cambridge University Press

Now, using Lemma 2 and the inequality (6),

$$\#(\mathcal{B}^2) \ge (\#\mathcal{S})^{11/10} p^{o(1)}. \tag{8}$$

On the other hand, recalling the definition of $\mathcal{R}$,

$$\#(\mathcal{B}^2) \le \varphi(n) \le n \le T,$$

which, together with (5) and (8), implies

$$T \ge \min\{(\#\Gamma_p(T))^{11/10}, p^{11/20}\} p^{o(1)}.$$

From the condition on $T$ we see that $\min\{(\#\Gamma_p(T))^{11/10}, p^{11/20}\} = p^{11/20}$ is impossible, which concludes the proof.

## References


[1] O. Ahmadi, I. Shparlinski and J. F. Voloch, 'Multiplicative order of Gauss periods', *Int. J. Number Theory* **6** (2010), 877–882.

[2] I. F. Blake, S. Gao, A. J. Menezes, R. Mullin, S. Vanstone and T. Yaghoobian, *Applications of Finite Fields* (Kluwer Academic Press, Dordrecht, 1993).

[3] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambridge Philos Soc.* **146** (2008), 1–21.

[4] S. D. Cohen, 'The orders of related elements of a finite field', *Ramanujan J.* **7** (2003), 169–183.

[5] M. Z. Garaev, 'Sums and products of sets and estimates for rational trigonometric sums in fields of prime order', *Russian Math. Surveys* **65** (2010), 599–658.

[6] J. von zur Gathen and I. Shparlinski, 'Orders of Gauss periods in finite fields', *Appl. Algebra Engrg. Comm. Comput.* **9** (1998), 15–24.

[7] J. von zur Gathen and I. Shparlinski, 'Constructing elements of large order in finite fields and Gauss periods', *Proc. the 13th Symp. on Appl. Algebra, Algebraic Algorithms, and Error-Correcting Codes, Honolulu, HI, 1999*, Lecture Notes in Computer Science, 1719 (Springer, Berlin, 1999), pp. 404–497.

[8] 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.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 1979).

[10] M. Rudnev, 'An improved sum-product inequality in fields of prime order', Preprint, 2010. arXiv:1011.2738.

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

[12] T. Tao, 'The sum-product phenomenon in arbitrary rings', *Contrib. Discrete Math.* **4** (2009), 59–82.

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

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


IGOR SHPARLINSKI, Department of Computing, Macquarie University,
NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au

https://doi.org/10.1017/S0004972711002887 Published online by Cambridge University Press