Bull. Aust. Math. Soc. **87** (2013), 527–528
doi:10.1017/S0004972712001062

CORRECTION TO 'SUM-PRODUCT ESTIMATES AND MULTIPLICATIVE ORDERS OF γ AND $\gamma + \gamma^{-1}$ IN FINITE FIELDS'

IGOR SHPARLINSKI

(Received 25 October 2012; accepted 29 October 2012; first published online 21 February 2013)

Unfortunately, the argument of the proof of [2, Theorem 1] contains a gap. (The author is grateful to Moubariz Garaev for pointing this out.) Here we present and prove a corrected statement.

Let p be a prime number and let $\mathbb{F}_p$ denote the finite field of p elements. We use $\operatorname{ord}\gamma$ to denote the multiplicative order of $\gamma \in \mathbb{F}_p$. For a fixed positive divisor $n \mid p-1$ we define $\Gamma_p(n)$ as the subgroup of $\mathbb{F}_p^*$ generated by the nonzero elements of the form $\gamma + \gamma^{-1}$ for $\gamma \in \mathbb{F}_p^*$ with $\operatorname{ord}\gamma \mid n$. Clearly $\#\Gamma_p(n) \ge (n-2)/2$. We now obtain a stronger bound.

THEOREM 1. *There is an absolute constant $c > 0$ such that for a prime p and a positive integer $2 \le n \le p^{1/2}$ with $n \mid p-1$,*

$$\#\Gamma_p(n) \ge c n^{12/11} (\log n)^{-4/11}.$$

PROOF. We define the sets

$$\mathcal{S} = \{\gamma \ : \ \operatorname{ord}\gamma \mid n, \gamma^2 \ne -1\} \quad \text{and} \quad \mathcal{A} = \{\gamma^2 + \gamma^{-2} \ : \ \gamma \in \mathcal{S}\}.$$

Thus, $n \ge \#\mathcal{S} \ge n-6$. Hence,

$$p^{1/2} \ge n \ge \#\mathcal{S} \ge \#\mathcal{A} \ge \frac{1}{4}\#\mathcal{S} \ge \frac{n-6}{4}. \tag{1}$$

Note that

$$\mathcal{A}^2 \subseteq \Gamma_p(n) \cup \{0\}. \tag{2}$$

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 we also have

$$2\mathcal{A} \subseteq \Gamma_p(n) \cup \{0\}. \tag{3}$$

Combining (2) and (3),

$$\#\Gamma_p(n) \geq \max\{\#(2\mathcal{A}), \#(\mathcal{A}^2)\} - 1.$$

By the version of the sum-product theorem which is due to Rudnev [1], there is an absolute constant $c_0 > 0$ such that

$$\max\{\#(2\mathcal{A}), \#(\mathcal{A}^2)\} \geq c_0(\#\mathcal{A})^{12/11}(\log \#\mathcal{A})^{-4/11},$$

provided that $\#\mathcal{A} < p^{1/2}$. Thus, recalling (1), we conclude the proof. □

References

[1] M. Rudnev, 'An improved sum-product inequality in fields of prime order', *Int. Math. Res. Not.* **2012** (2012), 3693–3705.

[2] I. E. Shparlinski, 'Sum-product estimates and multiplicative orders of γ and $\gamma + \gamma^{-1}$ in finite fields', *Bull. Aust. Math. Soc.* **85** (2012), 505–508.

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

https://doi.org/10.1017/S0004972712001062 Published online by Cambridge University Press