Michigan Math. J. 64 (2015), 655–672

Congruences with Intervals and Subgroups Modulo a Prime

Marc Munsch & Igor E. Shparlinski

Abstract. We obtain new results about the representation of almost all residues modulo a prime p by a product of a small integer and also an element of small multiplicative subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. These results are based on some ideas, and their modifications, of a recent work of Cilleruelo and Garaev (2014).

1. Introduction

It is well known that the progress on many classical and modern number-theoretic questions depends on the existence asymptotic formulas and good upper and lower bounds on the number of solutions to the congruences of the form

$$au \equiv x \pmod{m}, \tag{1}$$

where u runs through a multiplicative subgroup $\mathcal{G}$ of the group of units $\mathbb{Z}_m^*$ of the residue ring $\mathbb{Z}_m$ modulo an integers $m \geq 2$, and x runs through a set $\{A+1, \ldots, A+H\}$ of H consecutive integers; see [17] for an outline of such questions. In the special case where $m = p$ is a prime number and $\mathcal{G}$ is a group of squares, this is a celebrated question about the distribution of quadratic residues.

Recently, various modifications of the congruence (1) have been studied, such as congruences with elements from more general sets than subgroups on the left-hand side and also with products and ratios of variables from short intervals on the right-hand side; see [2; 3; 5; 6; 7; 8; 9; 10; 11; 12; 14; 18] and references therein. New applications of such congruences have also been found and include questions about

- nonvanishing of Fermat quotients [1],
- estimating fixed points of the discrete logarithm [2; 3],
- distribution of pseudopowers [4], and
- distribution of digits in reciprocals of primes [22].

Here we consider the congruence (1) in the special case where $m = p$ is prime. Furthermore, we are mostly interesting in the solvability of (1) for rather small intervals and subgroups.

Since we consider congruences modulo primes, it is convenient to use the language of finite fields.

Received December 8, 2014. Revision received May 13, 2015.

During the preparation of this work, M. Munsch was supported by a postdoctoral grant in CRM of Montreal under the supervision of Andrew Granville and Dimitris Koukoulopoulos, and I. E. Shparlinski was supported in part by the Australian Research Council Grant DP140100118.

For a prime p, we use $\mathbb{F}_p$ to denote the finite field of p elements, which we assume to be represented by the set $\{0, 1, \ldots, p-1\}$. We say that a set $\mathcal{I} \subseteq \mathbb{F}_p$ is an interval of length H if it contains H consecutive elements of $\mathbb{F}_p$, assuming that $p-1$ is followed by 0. Furthermore, we say that $\mathcal{I}$ is an initial interval if $\mathcal{I} = \{1, \ldots, H\}$ (we note that it is convenient to exclude 0 from initial intervals).

Furthermore, instead of subgroups, we consider a more general class sets, which also contain sets of N consecutive powers $\{g, \ldots, g^N\}$ of a fixed element $g \in \mathbb{F}_p^*$.

Namely, as usual, for a set $\mathcal{U} \subseteq \mathbb{F}_p$, we use $\mathcal{U}^{(m)}$ to denote its m-fold product set

$$\mathcal{U}^{(m)} = \{u_1 \cdots u_m : u_1, \ldots, u_m \in \mathcal{U}\}.$$

We say that $\mathcal{U} \subseteq \mathbb{F}_p^*$ is an *approximate subgroup* of $\mathbb{F}_p^*$ if

$$\#\mathcal{U}^{(2)} \le (\#\mathcal{U})^{1+o(1)}$$

as $\#\mathcal{U} \to \infty$.

Consequently, here we study the solvability of equations over $\mathbb{F}_p$ of the type

$$au = x, \quad u \in \mathcal{U}, x \in \mathcal{I}, \tag{2}$$

where $\mathcal{U} \subseteq \mathbb{F}_p^*$ is an approximate subgroup of $\mathbb{F}_p$, and $\mathcal{I} \subseteq \mathbb{F}_p^*$ is an interval.

It has been shown by Cilleruelo and Garaev [8] that for any $\varepsilon > 0$, there is $\delta > 0$ such that if $\mathcal{U} = \mathcal{G}$ is a subgroup of order $\#\mathcal{U} \ge p^{3/8}$ and $\mathcal{I}$ is an initial interval of length $\#\mathcal{I} \ge p^{5/8+\varepsilon}$, then (2) has a solution for all but at most $O(p^{1-\delta})$ values of $a \in \mathbb{F}_p$.

Here we show that the ideas of Cilleruelo and Garaev [8], combined with the approach of Garaev [10] to estimating character sums for almost all primes, allow us to obtain similar results for a wider range of sizes $\#\mathcal{U}$ and $\#\mathcal{I}$ (and also for approximate subgroups $\mathcal{U}$). Furthermore, we use some tools from additive combinatorics to establish a certain new result about subsets of approximate subgroups, which may be of independent interest.

Throughout the paper, the implied constants in the symbols O and $\ll$ are absolute. We recall that the assertions $U = O(V)$ and $U \ll V$ are both equivalent to the inequality $|U| \le cV$ with some constant c.

2. Background on Exponential and Character Sums

Let $\mathcal{X}_q$ denote the set of all $\varphi(q)$ multiplicative characters modulo an integer $q \ge 2$, and let $\mathcal{X}_q^*$ be the set of primitive characters $\chi \in \mathcal{X}_q$, where $\varphi(q)$ to denotes the Euler function of q; we refer to [15] for a background on characters.

Let $\mathcal{A} = (a_n)_{n \in \mathbb{N}}$ be an arbitrary sequence of complex numbers. For an integer h and a character $\chi \in \mathcal{X}_q$, we consider the weighted character sums

$$S_q(\chi; h; \mathcal{A}) = \sum_{n=1}^{h} a_n \chi(n).$$

If $a_n = 1$ for all n, then we simply use the notation

$$S_q(\chi; h) = \sum_{n=1}^{h} \chi(n).$$

First, we recall that by the Pólya–Vinogradov (for $\nu = 1$) and Burgess (for $\nu \ge 2$) bounds (see [15, Thms. 12.5 and 12.6]) for an arbitrary integers $q \ge h \ge 1$, the bound

$$\max_{\chi \in \mathcal{X}_q \setminus \{\chi_0\}} |S_q(\chi; h)| \le h^{1-1/\nu} q^{(\nu+1)/4\nu^2 + o(1)} \tag{3}$$

holds with $\nu = 1, 2, 3$ for any q and with an arbitrary positive integer ν if q is cube-free.

It is well known that assuming the generalized Riemann hypothesis (GRH), we derive a "square-root cancellation" bound

$$\max_{\chi \in \mathcal{X}_q \setminus \{\chi_0\}} |S_q(\chi; h)| \le h^{1/2} q^{o(1)}, \tag{4}$$

which in particular is quoted in [19, Bound (13.2)]. Despite this, it seems to be difficult to find a proof of this bound; however, we can easily derive it from [13, Thm. 2].

Furthermore, we use the following well-known property of the Gauss sums:

$$\tau_q(\chi) = \sum_{v=1}^{q} \chi(v) e\left(\frac{v}{q}\right), \quad \chi \in \mathcal{X}_q;$$

see, for example, [15, eq. (3.12)].

LEMMA 1. *For any primitive multiplicative character $\chi \in \mathcal{X}_q^*$ and an integer b with $\gcd(b, q) = 1$, we have*

$$\chi(b)\tau_q(\overline{\chi}) = \sum_{\substack{v=1 \\ \gcd(v,q)=1}}^{q} \overline{\chi}(v) e\left(\frac{bv}{q}\right),$$

where $\overline{\chi}$ is the complex conjugate character to χ.

By [15, Lemma 3.1] we also have:

LEMMA 2. *For any $\chi \in \mathcal{X}_q^*$, we have*

$$|\tau_q(\chi)| = q^{1/2}.$$

We also recall the classical large sieve inequality, see [15, Thm. 7.11]:

LEMMA 3. *Let $a_1, \dots, a_T$ be an arbitrary sequence of complex numbers, and let*

$$A = \sum_{n=1}^{T} |a_n|^2 \quad \text{and} \quad T(u) = \sum_{n=1}^{T} a_n \exp(2\pi i n u).$$

Then, for an arbitrary integer $Q \geq 1$, we have

$$\sum_{q=1}^{Q} \sum_{\substack{v=1 \\ \gcd(v,q)=1}}^{q} \left| T\left(\frac{v}{q}\right) \right|^2 \ll (Q^2 + T)A.$$

3. Bounds of Character Sums for Almost All Moduli

Garaev [9], has obtained a series of improvements of the bound (3) that hold for almost all moduli integer $q \geq 1$. Namely, by [9, Thm. 10], for any $\delta < 1/4$, if h and Q tend to infinity in such a way that

$$\frac{\log h}{\sqrt{\log Q}} \to \infty,$$

then

$$\max_{\chi \in \mathcal{X}_q^*} \left| \sum_{n=1}^{h} \chi(n) \right| \leq h^{1-\delta}$$

for all but at most $Q^{4\delta} h^{(1-2\delta)\gamma + o(1)}$ moduli $q \leq Q$, where γ is the following fractional part:

$$\gamma = \left\{ \frac{2 \log Q}{\log h} \right\}. \tag{5}$$

Here we give some modifications of the bounds from [9] that are more convenient for our applications, in particular, the size of the exceptional set in [9, Thm. 10] of moduli $q \leq Q$, which depends on the fractional part γ.

We can simply estimate $\gamma \leq 1$ and still derive a nontrivial bound $O(Q^{4\delta} h^{1-2\delta})$ from [9, Thm. 10]. However, here we show that we can modify the argument of Garaev [9] and obtain a stronger bound than that corresponds to replacing γ with 1. We also show that the argument of [9], augmented by some standard techniques, can be used to estimate the largest values of sums $|S_q(\chi; h)|$ uniformly over all integers $h \leq H$ and $\chi \in \mathcal{X}_q^*$, which is important for some applications.

We now define γ by the analogue of (5) but with H instead of h, that is,

$$\gamma = \left\{ \frac{2 \log Q}{\log H} \right\}. \tag{6}$$

LEMMA 4. *Let H and Q be sufficiently large positive integer numbers with $Q \geq H \geq Q^{\varepsilon}$ for some fixed $\varepsilon > 0$, and let $\mathcal{A} = (a_n)_{n \in \mathbb{N}}$ be an arbitrary sequence of complex numbers with $|a_n| = 1$. Then, for any $\delta < 1/4$,*

$$\max_{\chi \in \mathcal{X}_q^*} \max_{h \leq H} |S_q(\chi; h; \mathcal{A})| \leq H^{1-\delta}$$

for all but at most $Q^{4\delta} H^{\vartheta + o(1)}$ moduli $q \leq Q$, where γ is given by (6), and $\vartheta = \min\{(1-2\delta)\gamma, 2\delta(1-\gamma)\}$.

Proof. As we have mentioned, we follow the ideas of Garaev [9, Thm. 3].

Without loss of generality we may assume that $H = 2M + 1$ is an odd integer. We also define the function $e(z) = \exp(2\pi i z)$. We recall that for any integer z, we have the orthogonality relation

$$\sum_{b=-M}^{M} e\left(\frac{bz}{H}\right) = \begin{cases} H & \text{if } z \equiv 0 \pmod{H}, \\ 0 & \text{if } z \not\equiv 0 \pmod{H}; \end{cases} \tag{7}$$

see [15, Sec. 3.1]. We also need the bound

$$\sum_{n=u+1}^{u+h} e\left(\frac{bn}{H}\right) \ll \frac{H}{|b|+1}, \tag{8}$$

which holds for any integers b, u, and $H \ge h \ge 1$ with $|b| \le H/2$; see [15, Bound (8.6)].

Now for each $q \le Q$, we fix $\chi_q \in \mathcal{X}_q^*$ and $h_q \le H$ with

$$|S_q(\chi_q; h_q; \mathcal{A})| = \max_{\chi \in \mathcal{X}_q^*} \max_{h \le H} |S_q(\chi; h; \mathcal{A})|.$$

Then using (7), we write

$$\begin{aligned} S_q(\chi_q; h_q; \mathcal{A}) &= \sum_{r=1}^{H} a_r \chi_q(r) \frac{1}{H} \sum_{n=1}^{h_q} \sum_{b=-M}^{M} e\left(\frac{b(r-n)}{H}\right) \\ &= \frac{1}{H} \sum_{b=-M}^{M} \sum_{n=1}^{h_q} e\left(-\frac{bn}{H}\right) \sum_{r=1}^{H} a_r \chi_q(r) e\left(\frac{br}{H}\right). \end{aligned}$$

Recalling (8), we see that

$$S_q(\chi_q; h_q; \mathcal{A}) \ll \sum_{b=-M}^{M} \frac{1}{|b|+1} \left| \sum_{r=1}^{H} a_r \chi_q(r) e\left(\frac{br}{H}\right) \right|.$$

Writing

$$|b| + 1 = (|b|+1)^{(2\nu-1)/2\nu} (|b|+1)^{1/2\nu}$$

and using the Hölder inequality, we derive

$$\sum_{q \le Q} |S_q(\chi_q; h_q; \mathcal{A})|^{2\nu} \ll (\log Q)^{2\nu-1} \sum_{b=-M}^{M} \frac{1}{|b|+1} U_b, \tag{9}$$

where

$$U_b = \sum_{q \le Q} \left| \sum_{r=1}^{H} a_r \chi_q(r) e\left(\frac{br}{H}\right) \right|^{2\nu}.$$

We now note that

$$\left(\sum_{r=1}^{H} a_r \chi_q(r) e\left(\frac{br}{H}\right) \right)^{\nu} = \sum_{n=1}^{T} \rho_b(n) \chi_q(n),$$

where $T = H^\nu$ and

$$\rho_b(n) = \sum_{\substack{r_1,\ldots,r_\nu=1\\ r_1\cdots r_\nu=n}}^{H} a_{r_1}\cdots a_{r_\nu} e\left(\frac{b(r_1+\cdots+r_\nu)}{H}\right).$$

Using Lemma 1, we write

$$\left(\sum_{r=1}^{H} a_r \chi_q(r) e\left(\frac{br}{H}\right)\right)^\nu = \sum_{n=1}^{T} \rho_b(n) \frac{1}{\tau_q(\overline{\chi}_q)} \sum_{\substack{v=1\\ \gcd(v,q)=1}}^{q} \overline{\chi}_q(v) e\left(\frac{nv}{q}\right)$$

$$= \sum_{\substack{v=1\\ \gcd(v,q)=1}}^{q} \frac{\overline{\chi}_q(v)}{\tau_q(\overline{\chi}_q)} \sum_{n=1}^{T} \rho_b(n) e\left(\frac{nv}{q}\right).$$

Changing the order of summation, by Lemma 2 and the Cauchy inequality, we obtain

$$\left|\sum_{r=1}^{H} \chi_q(r) e\left(\frac{br}{H}\right)\right|^{2\nu} \le \sum_{\substack{v=1\\ \gcd(v,q)=1}}^{q} \left|\sum_{n=1}^{T} \rho_b(n) e\left(\frac{nv}{q}\right)\right|^2.$$

Therefore,

$$U_b \le \sum_{q\le Q} \sum_{\substack{v=1\\ \gcd(v,q)=1}}^{q} \left|\sum_{n=1}^{T} \rho_b(n) e\left(\frac{nv}{q}\right)\right|^2.$$

Recalling the well-known upper bound on the divisor function $d(n)$ (see [15, Bound (1.81)]), we conclude that

$$|\rho_b(n)| \le \sum_{\substack{r_1,\ldots,r_\nu=1\\ r_1\cdots r_\nu=n}}^{H} 1 \le (d(n))^\nu = n^{o(1)}$$

as $n \to \infty$. Thus,

$$\sum_{n=1}^{T} |\rho_b(n)|^2 \le T^{o(1)} \sum_{n=1}^{T} |\rho_b(n)| \le T^{o(1)} H^\nu = H^{\nu(1+o(1))}.$$

Hence, from Lemma 3 we now derive

$$U_b \le (Q^2+T) \sum_{n=1}^{T} |\rho_b(n)|^2 \le (Q^2+H^\nu) H^{\nu(1+o(1))},$$

which after substitution into (9) implies

$$\sum_{q\le Q} \max_{\chi\in\mathcal{X}_q^*} \max_{h\le H} |S_q(\chi; h; \mathcal{A})|^{2\nu} \le (Q^2+H^\nu) H^{\nu(1+o(1))}. \tag{10}$$

We now define the integer k by

$$k = \left\lfloor \frac{2\log Q}{\log H} \right\rfloor.$$

Note that

$$Q^2 = H^{k+\gamma}.$$

Using (10) with $\nu = k$ (so $\nu < 2/\varepsilon$ in particular), we see that

$$\sum_{q \le Q} \max_{\chi \in \mathcal{X}_q^*} \max_{h \le H} |S_q(\chi; h; \mathcal{A})|^{2k} \le Q^2 H^{k+o(1)}.$$

Hence, the desired bound holds for all but at most

$$\begin{aligned} Q^2 H^{k+o(1)} H^{-2k(1-\delta)} &= Q^2 H^{-k(1-2\delta)+o(1)} = H^{2k\delta+\gamma+o(1)} \\ &= Q^{4\delta} H^{(1-2\delta)\gamma+o(1)} \end{aligned} \tag{11}$$

moduli $q \le Q$ (which is essentially a bound of the same strength as that of [9, Thm. 10]).

Furthermore, using (10) with $\nu = k+1$, we see that

$$\sum_{q \le Q} \max_{\chi \in \mathcal{X}_q^*} \max_{h \le H} |S_q(\chi; h; \mathcal{A})|^{2(k+1)} \le H^{2(k+1)+o(1)}.$$

Hence, the desired bound holds for all but at most

$$H^{2(k+1)+o(1)} H^{-2(k+1)(1-\delta)} = H^{2(k+1)\delta+o(1)} = Q^{4\delta} H^{2\delta(1-\gamma)+o(1)} \tag{12}$$

moduli $q \le Q$.

The bounds (11) and (12) yield the result. □

Covering the interval $[1, H]$ by $O(\log H)$ dyadic intervals of the form $[H_0/2, H_0]$ and using that

$$\min\{(1-2\delta)\gamma, 2\delta(1-\gamma)\} \le 2\delta(1-2\delta),$$

we obtain the following:

COROLLARY 5. *Let H and Q be sufficient large positive integer numbers with $Q \ge H \ge Q^\varepsilon$ for some fixed $\varepsilon > 0$, and let $\mathcal{A} = (a_n)_{n \in \mathbb{N}}$ be an arbitrary sequence of complex numbers with $|a_n| = 1$. Then, for any $\delta < 1/4$,*

$$\max_{\chi \in \mathcal{X}_q^*} |S_q(\chi; h; \mathcal{A})| \le h^{1-\delta}$$

for all $h \le H$ and for all but at most $Q^{4\delta} H^{2\delta(1-2\delta)+o(1)}$ moduli $q \le Q$.

For the traditional character sums, that is, when $a_n = 1$, we also have the following result.

COROLLARY 6. *Let Q be a sufficiently large positive integer number. For any fixed $\varepsilon > 0$ and $3/14 > \delta > 0$, there is some $\xi > 0$ such that*

$$\max_{\chi \in \mathcal{X}_q^*} |S_q(\chi; h)| \le h^{1-\delta}$$

for all $h \in [Q^\varepsilon, Q]$ and for all but at most $Q^{1-\xi}$ moduli $q \le Q$.

Proof. Clearly, it suffices to consider only $q \in [Q/2, Q]$. Let us fix some positive δ with $(3-\sqrt{7})/2 < \delta < 3/14$. Simple calculus shows that there is some $\alpha > 1/2$ such that

$$4\delta + 2\alpha\delta(1-2\delta) < 1 \quad \text{and} \quad 4\delta + (2-3\alpha)(1-2\delta) < 1.$$

We now note that with the previous parameters, Corollary 5, used with $H = \lceil Q^{\alpha} \rceil$, implies that it remains to establish the results only for the values of $h \in [Q^{\alpha}, Q]$.

Furthermore, by the Pólya–Vinogradov bound (that is, by (3) taken with $\nu = 1$) we have

$$\max_{\chi \in \mathcal{X}_q^*} |S_q(\chi; h)| \le h^{1-\delta}$$

for any $h \ge Q^{1/2(1-\delta)}$ and $q \le Q$.

Therefore, we only need to consider the values of h in the interval $[Q^{\alpha}, Q^{1/2(1-\delta)}]$, which we can cover by $O(\log Q)$ dyadic intervals $[H/2, H]$. Now, for $H \in [Q^{\alpha}, Q^{1/2(1-\delta)}]$, we have

$$3 < 4(1-\delta) \le \frac{2\log Q}{\log H} \le 2\alpha^{-1} < 4.$$

Hence, writing $H = Q^{\beta}$, for the parameter γ given by (6), we have

$$\gamma = 2\beta^{-1} - 3.$$

Recalling Lemma 4, we see that it remains to check that

$$4\delta + \beta \min\{(2\beta^{-1} - 3)(1-2\delta), 2(4 - 2\beta^{-1})\delta\} < 1$$

for every $\beta \in [\alpha, 1/2(1-\delta)]$. We now have the following elementary estimates:

$$\begin{aligned} 4\delta + \beta &\min\{(2\beta^{-1} - 3)(1-2\delta), 2(4 - 2\beta^{-1})\delta\} \\ &= 4\delta + \beta(2\beta^{-1} - 3)(1-2\delta) = 4\delta + (2-3\beta)(1-2\delta) \\ &\le 4\delta + (2-3\alpha)(1-2\delta) < 1, \end{aligned}$$

and the result follows. □

4. Background from Additive Combinatorics

We use standard notation of additive combinatorics, including sumsets $\mathcal{A} + \mathcal{B} = \{a+b : a \in \mathcal{A}, b \in \mathcal{B}\}$ and k-folded sumsets $k\mathcal{A} = \{a_1 + \cdots + a_k : a_1, \ldots, a_k \in \mathcal{A}\}$, assuming that $\mathcal{A}$ and $\mathcal{B}$ are subsets of some Abelian group $\mathcal{G}$.

We first recall the *Plünnecke inequality;* see [23, Cor. 6.29].

LEMMA 7. *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are subsets of some Abelian group $\mathcal{G}$ and that $\#(\mathcal{A} + \mathcal{B}) \le K\#\mathcal{A}$ for some $K \ge 1$. Then for any nonnegative integers k and m, we have*

$$\#(k\mathcal{B} - m\mathcal{B}) \le K^{k+m}\#\mathcal{A}.$$

We now have the following obvious consequence of Lemma 7.

COROLLARY 8. *For any fixed integer $m \ge 1$ and approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$, we have*

$$\#\mathcal{U}^{(m)} \le (\#\mathcal{U})^{1+o(1)}.$$

Suppose that $\mathcal{A} \subseteq \mathcal{G}$ and $\mathcal{B} \subseteq \mathcal{H}$ are subsets of Abelian groups $\mathcal{G}$ and $\mathcal{H}$, respectively. A map $\psi : \mathcal{A} \to \mathcal{B}$ is called *Freiman k-homomorphism* if whenever

$$a_1 + \cdots + a_k = a_{k+1} + \cdots + a_{2k}$$

for some $a_1, \ldots, a_{2k}$, then we also have

$$\psi(a_1) + \cdots + \psi(a_k) = \psi(a_{k+1}) + \cdots + \psi(a_{2k}).$$

If ψ has an inverse that is also a Freiman k-homomorphism, then we say that ψ is a *Freiman k-isomorphism* and also that $\mathcal{A}$ and $\mathcal{B}$ are *Freiman k-isomorphic*.

We note that if $\mathcal{G}$ is a torsion-free group, then considering $a_1 = \cdots = a_k = a$ and $a_{k+1} = \cdots = a_{2k} = b$ for some $a, b \in \mathcal{A}$, we derive that any Freiman k-isomorphism is an injection.

We need the following result of Ruzsa [21, Thm. 2.3.5], which is known as the *modelling lemma* (see also [20, Thm. 2] for the case $\mathcal{G} = \mathbb{Z}$, which is fully sufficient for our purposes).

LEMMA 9. *Suppose that $\mathcal{A} \subseteq \mathcal{G}$ is a finite nonempty subset of a torsion-free Abelian group $\mathcal{G}$. Then for all integers $k \ge 2$ and $q \ge |k\mathcal{A} - k\mathcal{A}|$, there is a set $\mathcal{B} \subseteq \mathcal{A}$ with $\#\mathcal{B} \ge \#\mathcal{A}/k$ such that $\mathcal{B}$ is Freiman k-isomorphic to a subset of $\mathbb{Z}/q\mathbb{Z}$.*

We now use Lemma 9 to show that sets with a small doubling contain subsets of a given cardinality and also with small doubling. We present it in a more general and explicit form than we need for applications since we think that it may be of independent interest.

LEMMA 10. *Suppose that $\mathcal{A} \subseteq \mathcal{G}$ is a finite nonempty subset of a torsion-free Abelian group $\mathcal{G}$ of cardinality $N = \#\mathcal{A}$ such that for some $L \ge 1$, we have $\#(2\mathcal{A}) \le LN$. Then for any positive integer $M \le N$, there is a set $\mathcal{C} \subseteq \mathcal{A}$ with*

$$\#\mathcal{C} = M \quad \text{and} \quad \#(2\mathcal{C}) \le 10L^4M.$$

Proof. If $M \ge N/2$, then we simply take C to be any subset of $\mathcal{A}$ of cardinality M. Then

$$\#(2\mathcal{C}) \le \#(2\mathcal{A}) \le LN \le 2LM.$$

Now assume that $M \le N/2$. First, we note that applying Lemma 7, we derive $\#(2\mathcal{A} - 2\mathcal{A}) \le KN$, where $K = L^4$.

Let

$$\mathcal{B} \subseteq \mathcal{A} \quad \text{and} \quad KN \le q \le 2KN$$

be as in Lemma 9 (applied with $k = 2$), and let ψ be the corresponding Freiman 2-isomorphism. We consider the set $\mathcal{X} = \psi(\mathcal{B}) \subseteq \mathbb{Z}/q\mathbb{Z}$. As we have noticed, ψ is an injection, so

$$\#\mathcal{X} = \#\mathcal{B} \ge \frac{N}{2} \ge M.$$

By a simple averaging argument, for any integer $R \geq 1$, there is a subset $\mathcal{Y} \subseteq \mathbb{Z}/q\mathbb{Z}$ of R consecutive residue classes modulo q, that is, of $\{r, \ldots, r+R-1\}$ for some $r \in \mathbb{Z}$, such that

$$\#(\mathcal{X} \cap \mathcal{Y}) \geq \frac{\#\mathcal{X} \cdot \#\mathcal{Y}}{q} = \frac{R}{q}\#\mathcal{X}.$$

We now take

$$R = \left\lceil \frac{qM}{\#\mathcal{X}} \right\rceil$$

to guarantee $\#(\mathcal{X} \cap \mathcal{Y}) \geq M$. We now collect arbitrary M elements of $\mathcal{X} \cap \mathcal{Y}$ in one set $\mathcal{Z}$ and define

$$\mathcal{C} = \psi^{-1}(\mathcal{Z}).$$

We clearly have $\#\mathcal{C} = \#\mathcal{Z} = M$ and also, by the property of Freiman 2-isomorphisms,

$$\#(2\mathcal{C}) = \#(2\mathcal{Z}) \leq \#(2\mathcal{Y}) \leq 2\#\mathcal{Y} = 2R$$

(since $\mathcal{Y}$ consists of consecutive residue classes). Furthermore, we have

$$R \leq \left\lceil \frac{qM}{\#\mathcal{X}} \right\rceil \leq \left\lceil \frac{2qM}{N} \right\rceil \leq \lceil 4KM \rceil = \lceil 4L^4 M \rceil \leq 5L^4 M,$$

which concludes the proof. □

We now see that Lemma 10 implies that an approximate subgroup of $\mathbb{F}_p^*$ contains subsets of any size that behave as approximate subgroups.

LEMMA 11. *For any approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$ and for any integer $M \leq \#\mathcal{U}$, there is a subset $\mathcal{V} \subseteq \mathcal{U}$ such that $\#\mathcal{V} = M$ and*

$$\#\mathcal{V}^{(2)} \leq \#\mathcal{V}(\#\mathcal{U})^{o(1)}.$$

Proof. We fix a primitive root g of $\mathbb{F}_p^*$ and define the set

$$\mathcal{A} = \{a \in \{0, \ldots, p-2\} : g^a \in \mathcal{U}\}.$$

We consider $\mathcal{A}$ as the set of integers. Since $0 \leq a + b \leq 2p - 4$, at most two elements from $2A$ correspond to the same element in $\mathcal{U}^{(2)}$. So, we conclude that

$$\#(2A) \leq 2\#(\mathcal{U}^{(2)}).$$

The result now follows immediately from Lemma 10. □

We note that in our applications of Lemma 11 the sets $\mathcal{U}$ and $\mathcal{V}$ are of comparable cardinalities, so $(\#\mathcal{U})^{o(1)} = (\#\mathcal{V})^{o(1)}$, and thus $\mathcal{V}$ is also an approximate subgroup.

5. Some Equation over $\mathbb{F}_p$ with Variables from Intervals and Subgroups

We easily verify that Corollary 8 allows us to obtain the following slight variation of [8, Thm. 1], where instead of the sets $\mathcal{U} \subseteq \mathbb{F}_p$ with $\#\mathcal{U}^{(2)} \le 10\#\mathcal{U}$, we use approximate subgroups. The proof then goes through without any changes.

LEMMA 12. *Let an initial interval $\mathcal{I} \subseteq \mathbb{F}_p$ of length H and an approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$ of size N satisfy*

$$H^k N < p \quad \text{and} \quad N \le p^{k/(2k+1)}$$

for some fixed integer $k \ge 1$. Then the number J of solutions of the equation over $\mathbb{F}_p$

$$x_1 = x_2 u, \quad u \in \mathcal{U}, x_1, x_2 \in \mathcal{I},$$

satisfies

$$J \le H N^{o(1)}.$$

Accordingly, we also have the following version of [8, Cor. 1].

COROLLARY 13. *Let an initial interval $\mathcal{I} \subseteq \mathbb{F}_p$ of length H and an approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$ of size N satisfy*

$$H^k N < p \quad \text{and} \quad N \le p^{k/(2k+1)}$$

for some fixed integer $k \ge 1$. Then the number K of solutions of the equation over $\mathbb{F}_p$

$$x_1 u_1 = x_2 u_2, \quad u_1, u_2 \in \mathcal{U}, x_1, x_2 \in \mathcal{I},$$

satisfies

$$K \le H N^{1+o(1)}.$$

We now prove the following direct extension of [8, Lemma 7]:

LEMMA 14. *Let an initial interval $\mathcal{I} \subseteq \mathbb{F}_p$ of length H and an approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$ of size N satisfy*

$$H \le N/2, \qquad H^k N < p, \qquad N \le p^{k/(2k+1)}$$

for some fixed integer $k \ge 1$, and let $\mathcal{Q}$ be the set of primes $q \in [N/2, N]$. Then the number S of solutions of the equation over $\mathbb{F}_p$

$$q_1 u_1 x_1 = q_2 u_2 x_2, \quad q_i \in Q, u_i \in \mathcal{U}, x_i \in \mathcal{I}, i = 1, 2,$$

satisfies

$$S \le H N^{2+o(1)}.$$

Proof. We have $S = S_1 + S_2$, where S_1 is the number of solutions with the additional condition $q_1 = q_2$, and S_2 is the number of solutions with $q_1 \ne q_2$.

To estimate S_1, we observe that we can apply Corollary 13 and derive

$$S_1 \le H N^{2+o(1)}. \tag{13}$$

It remains to estimate S_2. We fix x_2, u_1, u_2 such that for $\lambda = u_2 x_2/u_1$, we have

$$S_2 \le HN^2 T_2, \tag{14}$$

where T_2 is the number of solutions of the equation

$$\frac{q_1 x_1}{q_2} = \lambda, \quad q_1, q_2 \in Q, q_1 \ne q_2, x_1 \in \mathcal{I}.$$

From $H < N/2$ we deduce that $\gcd(q_1 x_1, q_2) = 1$. Since $N^2 H < p$, from [8, Lemma 3] we derive that $x_1 q_1$ and q_1 are uniquely determined. Since $x_1 < q_1$, the value $x_1 q_1$ uniquely determines x_1 and q_1. Hence, $T_2 \le 1$, which, together with (14), implies

$$S_2 \le HN^2. \tag{15}$$

Combining (13) and (15), we conclude the proof. □

6. Products of Intervals and Subgroups

Following the standard notation, we use

$$\mathcal{A} \cdot \mathcal{B} = \{ab : a \in \mathcal{A}, b \in \mathcal{B}\}$$

to denote the product set of two sets $\mathcal{A}, \mathcal{B} \in \mathbb{F}_p$.

We say that a certain property holds for almost all primes p if it fails for $o(Q/\log Q)$ primes $p \le Q$ as $x \to \infty$.

Here we are interested in the cardinality of the set $\mathcal{I} \cdot \mathcal{U}$ for an initial interval $\mathcal{I} \subseteq \mathbb{F}_p$ and an approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$. In particular, for almost all primes p, we extend [8, Thm. 3] to a wider range of $\#\mathcal{I}$ and $\#\mathcal{U}$.

THEOREM 15. *For any fixed α with $1/3 \le \alpha < 1/2$ and $\kappa > 0$, for almost all primes p, for any initial interval $\mathcal{I} \subseteq \mathbb{F}_p$ of length H, and any approximate subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$ of size N that satisfy*

$$H > p^{1-\alpha+\kappa} \quad \text{and} \quad N \ge p^{\alpha},$$

we have

$$\#(\mathcal{I} \cdot \mathcal{U}) = p + O(p^{1-\eta}),$$

where

$$\eta = \frac{3\kappa}{7(1+\kappa)}.$$

Proof. Let Q be a sufficiently large positive integer. It is clear that it suffices to establish the desired result for all but $o(Q/\log Q)$ primes p in the dyadic interval $p \in [Q/2, Q]$. Using Corollary 6 with some fixed positive $\varepsilon < 1 - 2\alpha$ and $\delta < 3/14$, we see that we can remove $o(Q/\log Q)$ primes $p \in [Q/2, Q]$ such that for remaining primes p, we have

$$\max_{\chi \in \mathcal{X}_p^*} \left| \sum_{n=1}^{h} \chi(n) \right| \le h^{1-\delta} \tag{16}$$

for every integer

$$h \in [p^{\varepsilon}, p], \tag{17}$$

provided that Q is large enough.

We now always assume that p is such that (16) holds.

We now set

$$m = \lceil \kappa^{-1} \rceil, \qquad \ell = \lfloor p^{1/m} \rfloor, \qquad M = \lfloor p^{\alpha} \rfloor, \qquad h = \lfloor 0.4 p^{1-2\alpha} \rfloor.$$

By Lemma 11 we can choose a subset $\mathcal{V} \subseteq \mathcal{U}$ such that

$$\#\mathcal{V} = M \quad \text{and} \quad \#\mathcal{V}^{(2)} \le \#\mathcal{V} p^{o(1)} = (\#\mathcal{V})^{1+o(1)}.$$

Let $\mathcal{Q}$ be the set of primes $q \in [M/2, M]$.

We verify that

$$h\ell M \le 0.4 p^{1-2\alpha} \times p^{1/m} \times p^{\alpha} = 0.4 p^{1-\alpha+1/m} \le H$$

since $1/m < \kappa$. Hence, it suffices to prove that for some $\rho > 0$ that depends only on α, κ, and ε, there are at most $O(p^{1-\rho})$ values of $\lambda \in \mathbb{F}_p^*$ for which the equation over $\mathbb{F}_p$

$$qvxz = \lambda \tag{18}$$

has no solution in $q \in \mathcal{Q}$, $v \in \mathcal{V}$ and positive integers $x \le h$, $z \le \ell$.

Let $\Lambda \subset \mathbb{F}_p^*$ be the set of these elements λ, and let $L = \#\Lambda$.

We use the orthogonality of characters $\chi \in \mathcal{X}_p$ to express the number of solutions to (18) for $\lambda \in \Lambda$ via the following character sums:

$$\frac{1}{p-1} \sum_{\lambda \in \Lambda} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \sum_{x \le h} \sum_{z \le \ell} \sum_{\chi \in \mathcal{X}_p} \chi(qvxz\lambda^{-1}) = 0.$$

We now clear the denominator, change the order of summations, and separate the term corresponding to the principal character $\chi = \chi_0$. This leads us to the equation

$$h\ell LM\#\mathcal{Q} + \sum_{\chi \in \mathcal{X}_p^*} \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(qvx) \sum_{z \le \ell} \chi(z) \sum_{\lambda \in \Lambda} \chi(\lambda) = 0.$$

Therefore,

$$h\ell LM\#\mathcal{Q} \le W, \tag{19}$$

where

$$W = \sum_{\chi \in \mathcal{X}_p^*} \left| \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(xqv) \right| \left| \sum_{z \le \ell} \chi(z) \right| \left| \sum_{\lambda \in \Lambda} \chi(\lambda) \right|.$$

Because $\varepsilon < 1 - 2\alpha$, if Q is sufficiently large, condition (17) is satisfied for our choice of h. Therefore, the bound (16) holds, and we write

$$\left| \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(xqv) \right| \le (h^{1-\delta} M\#\mathcal{Q})^{1/m} \left| \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(xqv) \right|^{(m-1)/m}.$$

Using the fact that

$$\frac{m-1}{2m} + \frac{1}{2m} + \frac{1}{2} = 1,$$

and extending the summation over all $\chi \in \mathcal{X}_p$, we obtain

$$W \le (h^{1-\delta} M \# \mathcal{Q})^{1/m} \Bigg(\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(xqv) \Bigg|^2 \Bigg)^{(m-1)/2m} \times \Bigg(\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{z \le \ell} \chi(z) \Bigg|^{2m} \Bigg)^{1/2m} \Bigg(\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{\lambda \in \Lambda} \chi(\lambda) \Bigg|^2 \Bigg)^{1/2}. \tag{20}$$

First, using the orthogonality of characters, we obtain

$$\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{\lambda \in \Lambda} \chi(\lambda) \Bigg|^2 = (p-1)L \tag{21}$$

and

$$\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{z \le \ell} \chi(z) \Bigg|^{2m} = (p-1)S,$$

where S is the number of solutions of the following equation over $\mathbb{F}_p$:

$$z_1 \cdots z_m = z_{m+1} \cdots z_{2m}, \quad 1 \le z_j \le \ell, i = 1, \ldots, 2m.$$

Since $L^m < p$, this is in fact an equation over $\mathbb{Z}$, and from the well-known bounds of the divisor function we obtain $S \le \ell^{m+o(1)}$ solutions. Hence, we have

$$\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{z \le \ell} \chi(z) \Bigg|^{2m} \le p \ell^{m+o(1)}. \tag{22}$$

Furthermore, the same orthogonality property implies that

$$\sum_{\chi \in \mathcal{X}_p} \Bigg| \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(qvx) \Bigg|^2 = (p-1)T, \tag{23}$$

where T is the number of solutions of the following equation over $\mathbb{F}_p$:

$$q_1 v_1 x_1 = q_2 v_2 x_2, \quad q_i \in Q, v_i \in \mathcal{V}, 1 \le x_i \le h, i = 1, 2. \tag{24}$$

Using $\alpha \ge 1/3$, we verify that for any $k \ge 2$ and a sufficiently large Q, we have

$$h \le M/2.$$

Furthermore, if we define an integer $k \ge 1$ by the inequalities

$$\frac{k-1}{2k-1} < \alpha < \frac{k}{2k+1},$$

then we have

$$M \le p^{\alpha} \le p^{k/(2k+1)}$$

and

$$h^k M < p^{k(1-2\alpha)+\alpha} = p^{k-(2k-1)\alpha} < p.$$

Hence, due to the choice of $\mathcal{V}$, we see that Lemma 14 applies to equation (24) and implies $T \le hM^{2+o(1)}$, which, together with (23), yields

$$\sum_{\chi \in \mathcal{X}_p} \left| \sum_{x \le h} \sum_{q \in \mathcal{Q}} \sum_{v \in \mathcal{V}} \chi(qvx) \right|^2 \le phM^{2+o(1)}. \tag{25}$$

Substituting (21), (22), and (25) into (20) and recalling (19), we obtain

$$h\ell LM\#\mathcal{Q} \le (h^{1-\delta} M\#\mathcal{Q})^{1/m} (p\ell^m)^{1/2m} (pL)^{1/2} (phM^{2+o(1)})^{(m-1)/2m}.$$

Since $\#\mathcal{Q} = M^{1+o(1)}$, we obtain

$$h\ell LM^2 \le h^{(m+1)/2m-\delta/m} \ell^{1/2} pL^{1/2} M^{(m+1)/m+o(1)}$$

or

$$L \le h^{-2\delta/m} \ell^{-1} p^2 (hM^2)^{-1+1/m}.$$

Finally, since

$$hM^2 = p^{1+o(1)},$$

we derive

$$L \le h^{-2\delta/m} \ell^{-1} p^{1+1/m+o(1)} = h^{-2\delta/m} p^{1+o(1)}.$$

Recalling the choice of m and δ, we conclude the proof. □

In the case where $\mathcal{U}$ is a subgroup of $\mathbb{F}_p^*$, we prove a more general and stronger result under the GRH, which is nontrivial for any H and N as long as $HN > p^{1+\kappa}$ for some fixed $\kappa > 0$.

THEOREM 16. *Fix $\kappa > 0$. Assuming the GRH, for any prime p, any initial interval $\mathcal{I} \subseteq \mathbb{F}_p$ of length H, and any subgroup $\mathcal{U} \subseteq \mathbb{F}_p^*$ of size N such that $HN > p^{1+\kappa}$, we have*

$$\#(\mathcal{I} \cdot \mathcal{U}) = p + O(p^{1-\kappa+o(1)}).$$

Proof. It suffices to prove that for some $\rho > 0$ depending only on ε, there are at most $O(p^{1-\rho})$ values of $\lambda \in \mathbb{F}_p^*$ for which the equation over the field $\mathbb{F}_p$

$$ux = \lambda \tag{26}$$

has no solution in $u \in \mathcal{U}$ and positive integers $x \le H$.

Let $\Lambda \subset \mathbb{F}_p^*$ be the set of this elements λ, and let $L = \#\Lambda$.

We use the orthogonality of characters $\chi \in \mathcal{X}_p$ to express the number of solutions to (26) for $\lambda \in \Lambda$ via the following character sums:

$$\frac{1}{p-1} \sum_{\lambda \in \Lambda} \sum_{u \in \mathcal{U}} \sum_{x \le H} \sum_{\chi \in \mathcal{X}_p} \chi(ux\lambda^{-1}) = 0.$$

As in the proof of Theorem 15, this leads us to the equation

$$HLN + \sum_{\chi \in \mathcal{X}_p^*} \sum_{x \le H} \sum_{u \in \mathcal{U}} \chi(ux) \sum_{\lambda \in \Lambda} \chi(\lambda) = 0.$$

Therefore,

$$HLN \le W, \tag{27}$$

where

$$W = \sum_{\chi \in \mathcal{X}_p^*} \left| \sum_{x \le h} \sum_{u \in \mathcal{U}} \chi(xu) \right| \left| \sum_{\lambda \in \Lambda} \chi(\lambda) \right|.$$

Using the Cauchy inequality and extending the summation over all $\chi \in \mathcal{X}_p$, we obtain

$$W \le \left(\sum_{\chi \in \mathcal{X}_p^*} \left| \sum_{x \le H} \sum_{u \in \mathcal{U}} \chi(xu) \right|^2 \right)^{1/2} \left(\sum_{\chi \in \mathcal{X}_p} \left| \sum_{\lambda \in \Lambda} \chi(\lambda) \right|^2 \right)^{1/2}. \tag{28}$$

Now we use the fact that

$$\sum_{u \in \mathcal{U}} \chi(u) = 0$$

if χ is nontrivial over the subgroup $\mathcal{U}$. Hence, there are at most $(p-1)/N$ characters such that the last sum does not vanish, in which case it is equal to N.

Therefore, proceeding as in the proof of Theorem 15 and using the bound (4), we obtain

$$W \le \left(\frac{p}{N} (NH^{1/2} p^{o(1)})^2 \right)^{1/2} (pL)^{1/2}.$$

Substituting this inequality into (27) yields

$$HLN \le (pN)^{1/2} H^{1/2} (pL)^{1/2} p^{o(1)},$$

giving the bound

$$L \le \frac{p^{2+o(1)}}{NH},$$

which concludes the proof. □

7. Comments

Our proof of Corollary 6 uses (3) (with $\nu = 1$) and thus does not extend to more general weighted sums $S_q(\chi; h; \mathcal{A})$. However, for some interesting sequences $\mathcal{A}$ that admit a version of (3), we can obtain such a result. For example, combining our argument with a bound of Karacuba [16], we can derive a version of Corollary 6 for the sequence of shifted primes, that is, for the sequence $a_n = 1$ if $n = \ell + a$ for a prime ℓ and $a_n = 0$ otherwise (where $a \ne 0$ is a fixed integer).

We note that we have slightly modified the scheme of the proof of [8, Thm. 3], which has allowed us to extract the optimal saving η from the preliminary bounds used in the proof of Theorem 15. In particular, instead of separating the sum W into contribution from "good" and "bad" characters and balancing them, we have used a more direct approach via the Hölder inequality, which makes the optimal use of bounds on the moments of the character sums involved (including the "∞-moment", that is, the bound on the maximum value of some of these sums).

It is easy to see that if for some p instead of (4), we have a weaker bound

$$\max_{\chi \in \mathcal{X}_p \setminus \{\chi_0\}} |S_p(\chi; h)| \le h^{1-\delta} p^{o(1)}$$

with some fixed $\delta \le 1/2$, the method of proof of Theorem 16 still applies and in the case where $\mathcal{U}$ is a subgroup of $\mathbb{F}_p^*$, leads to a nontrivial bound under the condition $H^{2\delta}N > p^{1+\kappa}$. For example, this observation can be combined with Corollary 6 to a nontrivial bound under the condition $H^{3/7}N > p^{1+\kappa}$ for almost all p. On the other hand, using the conditional under the GRH bound (4) in the proof of Theorem 15, we can get the same result for all primes and also with a larger $\eta = \kappa/(1+\kappa)$.

The question about the set of elements missing from the set product $\mathcal{I} \cdot \mathcal{U}$, which is considered in Theorems 15 and 16, is a multiplicative version of the question of [22] about the set of elements missing from the set difference $\mathcal{I} - \mathcal{U}$ (only in the case where $\mathcal{U}$ is a subgroup of $\mathbb{F}_p^*$). The argument of [22] also works for the set sum $\mathcal{I} + \mathcal{U}$ without any changes. However, in [22] mostly the case of large subgroups of size $\#\mathcal{U} > p^{1/2}$ is of interest, and so the technique used is different.

Finally, clearly slightly changing the values of η, we can also include the value $\alpha = 1/2$ in the range of Theorem 15 (for example, we can apply it with $\alpha = 1/2 - \kappa/2$ instead of $1/2$ and $\kappa/2$ instead of $\kappa/2$).

ACKNOWLEDGMENTS. The authors are very grateful to Ben Green for sketching them a proof of Lemma 10.

The authors also would like to thank CIRM (Luminy) for its support and hospitality during the Research in Pairs program in May 2014, where the idea of this work was formed.

References

[1] J. Bourgain, K. Ford, S. V. Konyagin, and I. E. Shparlinski, *On the divisibility of Fermat quotients,* Michigan Math. J. 59 (2010), 313–328.

[2] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, *On the hidden shifted power problem,* SIAM J. Comput. 41 (2012), 1524–1557.

[3] ———, *On congruences with products of variables from short intervals and applications,* Proc. Steklov Inst. Math. 280 (2013), 67–96.

[4] J. Bourgain, S. Konyagin, C. Pomerance, and I. E. Shparlinski, *On the smallest pseudopower,* Acta Arith. 140 (2009), 43–55.

[5] J. Bourgain, S. V. Konyagin, and I. E. Shparlinski, *Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm,* Int. Math. Res. Not. IMRN 2008 (2008), 1–29 (Corrigenda: Int. Math. Res. Not. IMRN, 2009 (2009), 3146–3147).

[6] ———, *Distribution of elements of cosets of small subgroups and applications,* Int. Math. Res. Not. IMRN 2012 (2012), Article rnn097, 1968–2009.

[7] J. Cilleruelo and M. Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications,* Geom. Funct. Anal. 21 (2011), 892–904.

[8] ———, *Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications,* preprint, 2014, arXiv:1404.5070.

[9] M. Z. Garaev, *Character sums in short intervals and the multiplication table modulo a large prime,* Monatsh. Math. 148 (2006), 127–138.

[10] ———, *On multiplicative congruences,* Math. Z. 272 (2012), 473–482.

[11] M. Z. Garaev and A. A. Karatsuba, *On character sums and the exceptional set of a congruence problem,* J. Number Theory 114 (2005), 182–192.
[12] ———, *The representation of residue classes by products of small integers,* Proc. Edinb. Math. Soc. (2) 50 (2007), 363–375.
[13] A. Granville and K. Soundararajan, *Large character sums,* J. Amer. Math. Soc. 14 (2001), 365–397.
[14] G. Harman and I. E. Shparlinski, *Products of small integers in residue classes and additive properties of Fermat quotients,* Int. Math. Res. Not. IMRN, to appear.
[15] H. Iwaniec and E. Kowalski, *Analytic number theory,* Amer. Math. Soc., Providence, RI, 2004.
[16] A. A. Karacuba, *Sums of characters over prime numbers,* Izv. Akad. Nauk SSSR Ser. Mat. 34 (1970), 299–321.
[17] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications,* Cambridge Univ. Press, Cambridge, 1999.
[18] ———, *On the consecutive powers of a primitive root: gaps and exponential sums,* Mathematika 58 (2012), 11–20.
[19] H. L. Montgomery, *Topics in multiplicative number theory,* Lecture Notes in Math., 227, Springer-Verlag, Berlin, 1971.
[20] I. Z. Ruzsa, *Arithmetical progressions and the number of sums,* Period. Math. Hungar. 25 (1992), 105–111.
[21] ———, *Sumsets and structure,* Combinatorial number theory and additive group theory, Adv. Courses Math. CRM Barcelona, pp. 87–210, Birkhäuser Verlag, Basel, 2009.
[22] I. E. Shparlinski and W. Steiner, *On digit patterns in expansions of rational numbers with prime denominator,* Q. J. Math. 64 (2013), 1231–1238.
[23] T. Tao and V. Vu, *Additive combinatorics,* Cambridge Stud. Adv. Math., 105, Cambridge University Press, Cambridge, 2006.

M. Munsch
CRM
Université de Montréal
5357 Montréal
Québec
Canada

munsch@dms.umontreal.ca

I. E. Shparlinski
Department of Pure Mathematics
University of New South Wales
Sydney, NSW 2052
Australia

igor.shparlinski@unsw.edu.au