# Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications

J. Cilleruelo and M. Z. Garaev

**Abstract**

In the present paper we obtain new upper bound estimates for the number of solutions of the congruence

$$x \equiv yr \pmod p; \quad x, y \in \mathbb{N}, \quad x, y \le H, \quad r \in \mathcal{U},$$

for certain ranges of $H$ and $|\mathcal{U}|$, where $\mathcal{U}$ is a subset of the field of residue classes modulo $p$ having small multiplicative doubling. We then use this estimate to show that the number of solutions of the congruence

$$x^n \equiv \lambda \pmod p; \quad x \in \mathbb{N}, \quad L < x < L + p/n,$$

is at most $p^{\frac{1}{3}-c}$ uniformly over positive integers $n, \lambda$ and $L$, for some absolute constant $c > 0$. This implies, in particular, that if $f(x) \in \mathbb{Z}[x]$ is a fixed polynomial without multiple roots in $\mathbb{C}$, then the congruence $x^{f(x)} \equiv 1 \pmod p$, $x \in \mathbb{N}$, $x \le p$, has at most $p^{\frac{1}{3}-c}$ solutions as $p \to \infty$, improving some recent results of Kurlberg, Luca and Shparlinski and of Balog, Broughan and Shparlinski. We use our results to show that almost all the residue classes modulo $p$ can be represented in the form $xg^y \pmod p$ with positive integers $x < p^{5/8+\varepsilon}$ and $y < p^{3/8}$. Here $g$ denotes a primitive root modulo $p$. We also prove that almost all the residue classes modulo $p$ can be represented in the form $xyzg^t \pmod p$ with positive integers $x, y, z, t < p^{1/4+\varepsilon}$.

## 1 Introduction

In what follows, $\varepsilon$ is a small fixed positive quantity, $\mathbb{F}_p$ is the field of residue classes modulo a prime number $p$, which we consider to be sufficiently large in terms of $\varepsilon$. The notation $A \lesssim B$ is used to denote that $|A| < |B|p^{o(1)}$, or equivalently, for any $\varepsilon > 0$ there is a constant $c = c(\varepsilon)$ such that $|A| < c|B|p^{\varepsilon}$. Given sets $\mathcal{A}$ and $\mathcal{B}$ their product-set $\mathcal{A} \cdot \mathcal{B}$ is defined by

$$\mathcal{A} \cdot \mathcal{B} = \{ab; \quad a \in \mathcal{A},\, b \in \mathcal{B}\}.$$

The distributional properties of powers of a primitive root modulo $p$ and subgroups of $\mathbb{F}_p^*$ has a long story, starting from the work of Vinogradov [22] in 1926. A substantial amount of information and results can be found in the book of Konyagin and Shparlinski [16]. In the present paper we continue the investigation on this topic. Our first result is closely related to the work of Bourgain, Konyagin and Shparlisnki [3] and to some results of Konyagin and Shparlinski from [16].

**Theorem 1.** *Let $H$ be a positive integer and let $\mathcal{U} \subset \mathbb{F}_p^*$ be such that*

$$|\mathcal{U} \cdot \mathcal{U}| < 10|\mathcal{U}|.$$

*Denote by $J$ the number of solutions of the congruence*

$$x \equiv yr \pmod p; \quad x, y \in \mathbb{N}, \quad x, y \le H, \quad r \in \mathcal{U}. \tag{1}$$

*Then the following two assertions hold:*

*(i). If for some positive integer constant $n$ we have*

$$|\mathcal{U}| < p^{n/(2n+1)}, \quad |\mathcal{U}|H^n < p,$$

*then $J \lesssim H$.*

*(ii). If $|\mathcal{U}| < p^{2/5}$, then*

$$J \lesssim H + \frac{|\mathcal{U}|H^2}{p} + \frac{|\mathcal{U}|^{3/4}H}{p^{1/4}}.$$

**Corollary 1.** *Let $H$ be a positive integer and let $\mathcal{U} \subset \mathbb{F}_p^*$ be such that*

$$|\mathcal{U} \cdot \mathcal{U}| < 10|\mathcal{U}|.$$

*Denote by $J$ the number of solutions of the congruence*

$$xr \equiv x_1 r_1 \pmod p; \quad x, x_1 \in \mathbb{N}, \quad x, x_1 \le H, \quad r, r_1 \in \mathcal{U}. \tag{2}$$

*Then the following two assertions hold:*

*(i). If for some positive integer constant $n$ we have*

$$|\mathcal{U}| < p^{n/(2n+1)}, \qquad |\mathcal{U}|H^n < p,$$

*then $J \lesssim H|\mathcal{U}|$.*

*(ii). If*

$$p^{1/3} < |\mathcal{U}| < p^{2/5}, \qquad |\mathcal{U}|H < p,$$

*then*

$$J \lesssim \frac{|\mathcal{U}|^{7/4}H}{p^{1/4}}.$$

We remark that in the case $\mathcal{U}$ is a subgroup and $n = 1$ the statement of the part $(i)$ of our Theorem 1 follows from Corollary 7.7 of the aforementioned book [16].

The proof of Theorem 1 is based on ideas and results of Bourgain, Konyagin and Shparlinski [3]. Nevertheless, in the indicated range of parameters, the upper bound estimate of our Theorem 1 improves one of the main results of [3].

We give several new applications of Theorem 1. Let $d \in \mathbb{N}$ and $\lambda$ be an integer coprime to $p$. For real numbers $L$ and $N \geq 1$, consider the problem of upper bound estimates for the number $T_p(d, \lambda, L, N)$ of solutions of the congruence

$$x^d \equiv \lambda \pmod p; \quad x \in \mathbb{N}, \quad L+1 \leq x \leq L+N. \tag{3}$$

Trivially, for $N < p$, we have the bound $T_p(d, \lambda, L, N) \leq \min\{d, N\}$. The problem of obtaining nontrivial upper bounds for $T(d, \lambda, L, N)$ is of a very high interest, with a variety of results in the literature, see, for example, the aforementioned work [3], and more recent work of Shkredov [20]. Several nontrivial results can also be derived using the arguments from [4]. For instance, it is possible to prove that if $N < p^{2/5}$, then one has the bound $T_p(d, \lambda, L, N) \lesssim d^{1/2}$. Using our Theorem 1 we shall obtain the following new result on $T_p(d, \lambda, L, N)$ for any range $d, N$ with $dN < p$.

**Theorem 2.** *There exists an absolute constant $c > 0$ such that*

$$T_p(d, \lambda, L, p/d) < p^{\frac{1}{3}-c}.$$

From Theorem 2 we can derive the following consequence.

**Corollary 2.** *Let $f(x) \in \mathbb{Z}[x]$ be a fixed non-constant polynomial without multiple roots in $\mathbb{C}$. Then the congruence*

$$x^{f(x)} \equiv 1 \pmod p; \quad x \in \mathbb{N}, \quad x \le p, \tag{4}$$

*has at most $p^{\frac{1}{3}-c}$ solutions as $p \to \infty$, for some absolute constant $c > 0$.*

Corollary 2 improves the upper bound of the size $p^{6/13+o(1)}$ obtained by Kurlberg, Luca and Shparlinski [17]. We remark that the upper bound of the size $p^{1/3+o(1)}$ was known in the particular case $f(x) = x$ from the work of Balog, Broughan and Shparlinski [1]. Our result improves this too.

The constant $c$ in Theorem 2 and Corollary 2 can easily be made explicit. In the special case $f(x) = x$, using a different approach, in Corollary 2 we can obtain the upper bound of the size $p^{27/82+o(1)}$. We hope to deal with these questions elsewhere.

We shall give two more applications of Theorem 1. Let

$$\mathcal{I} = \{1, 2, 3, \dots, H\} \pmod p$$

be an interval of $\mathbb{F}_p$ with $|\mathcal{I}| = H$ elements. Denote by $\mathcal{G}$ either a subgroup of $\mathbb{F}_p^*$ or the set

$$\{1, g, g^2, \dots, g^{N-1}\} \pmod p$$

with $|\mathcal{G}| = N$ elements, formed with powers of a primitive root $g$ modulo $p$.

**Theorem 3.** *For any fixed $\varepsilon > 0$, if $|\mathcal{I}| > p^{5/8+\varepsilon}$, $|\mathcal{G}| > p^{3/8}$, then*

$$|\mathcal{I} \cdot \mathcal{G}| = p + O(p^{1-\delta})$$

*for some $\delta = \delta(\varepsilon) > 0$.*

**Theorem 4.** *For any fixed $\varepsilon > 0$, if $|\mathcal{I}| > p^{1/4+\varepsilon}$, $|\mathcal{G}| > p^{1/4}$, then*

$$|\mathcal{I} \cdot \mathcal{I} \cdot \mathcal{I} \cdot \mathcal{G}| = p + O(p^{1-\delta})$$

*for some $\delta = \delta(\varepsilon) > 0$.*

Let us mention several results relevant to Theorems 3, 4. In [11] it was shown that if $|\mathcal{I}| > p^{\frac{2}{3}-\frac{1}{192}+\varepsilon}$ and $\mathcal{A}$ is an arbitrary subset of $\mathbb{F}_p$ with $|\mathcal{A}| > p^{\frac{2}{3}-\frac{1}{192}+\varepsilon}$ then

$$|\mathcal{I} \cdot \mathcal{A}| = p + O(p^{1-\delta}); \quad \delta = \delta(\varepsilon) > 0.$$

Later, the exponent $\frac{2}{3} - \frac{1}{192}$ was improved by Bourgain to $\frac{5}{8}$ (unpublished). We also mention that if $|\mathcal{I}| > p^{1/2+\varepsilon}$, then one has

$$|\mathcal{I} \cdot \mathcal{I}| = p + O(p^{1-\delta}); \quad \delta = \delta(\varepsilon) > 0,$$

see, for example, [12].

Theorem 3 and its proof imply that if $|\mathcal{I}| > p^{5/8+\varepsilon}$, $|\mathcal{G}| > p^{3/8}$, then

$$\mathbb{F}_p^* \subset \mathcal{I} \cdot \mathcal{I} \cdot \mathcal{G}.$$

We remark that from the arguments of Heath-Brown [13] it follows that if $|\mathcal{I}| > p^{5/8+\varepsilon}$, then one has

$$\mathbb{F}_p^* \subset \mathcal{I} \cdot \mathcal{I} \cdot \mathcal{I}.$$

Theorem 4 can be compared with the result from [10], where it was shown that under the same condition $|\mathcal{I}| > p^{1/4+\varepsilon}$ one has

$$|\mathcal{I} \cdot \mathcal{I} \cdot \mathcal{I} \cdot \mathcal{I}| = p + O(p^{1-\delta}); \quad \delta = \delta(\varepsilon) > 0.$$

However, the presence of $\mathcal{G}$ in our theorems is an additional obstacle which we are able to overcome using Theorem 1.

Theorem 4 implies, in particular, that any $\lambda \not\equiv 0 \pmod p$ can be represented in the form

$$\lambda \equiv xyzuvwg^t \pmod p$$

for some positive integers $x, y, z, t, u, v, w < p^{1/4+\varepsilon}$.

In passing, we remark that in Theorem 1 the condition $|\mathcal{U} \cdot \mathcal{U}| < 10|\mathcal{U}|$ can be relaxed up to $|\mathcal{U} \cdot \mathcal{U}| < |\mathcal{U}|p^{o(1)}$. However, the formulation in the form $|\mathcal{U} \cdot \mathcal{U}| < 10|\mathcal{U}|$ already applies for the set $\mathcal{G}$ and is sufficient to prove Theorems 2, 3, 4.

In what follows $\chi$ denotes a character modulo the prime number $p$ and $\chi_0$ denotes the principal character.

# 2 Auxiliary Lemmas

We start with the following lemma of Bourgain, Konyagin and Shparlinski [3], see also [7] for a different proof with refined constants.

**Lemma 1.** *Let $\mathcal{A}$ be a non-empty subset of $\mathcal{F}_Q$, where*

$$\mathcal{F}_Q = \left\{\frac{r}{s};\, r, s \in \mathbb{N},\, \gcd(r,s) = 1,\, r, s \leq Q\right\}$$

*is the set of Farey fractions of order $Q$. Then for a given positive integer $m$, the $m$-fold product set $\mathcal{A}^{(m)}$ of $\mathcal{A}$ satisfies*

$$|\mathcal{A}^{(m)}| > \exp\Big(-C(m)\frac{\log Q}{\sqrt{\log\log Q}}\Big)|\mathcal{A}|^m,$$

*where $C(m) > 0$ depends only on $m$, provided that $Q$ is large enough.*

We recall that the $m$-fold product set $\mathcal{A}^{(m)}$ of $\mathcal{A}$ is defined as

$$\mathcal{A}^{(m)} = \{a_1 \cdots a_m; \quad a_1, \ldots, a_m \in \mathcal{A}\}.$$

Our next lemma stems from the work of Bourgain et. al. [4]. Recall that a lattice in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by $n$ linearly independent vectors. Take an arbitrary convex compact and symmetric with respect to 0 body $D \subset \mathbb{R}^n$. Recall that, for a lattice $\Gamma \subset \mathbb{R}^n$ and $i = 1, \ldots, n$, the $i$-th successive minimum $\lambda_i(D, \Gamma)$ of the set $D$ with respect to the lattice $\Gamma$ is defined as the minimal number $\lambda$ such that the set $\lambda D$ contains $i$ linearly independent vectors of the lattice $\Gamma$. Obviously, $\lambda_1(D, \Gamma) \le \ldots \le \lambda_n(D, \Gamma)$. From [2, Proposition 2.1] it is known that

$$\prod_{i=1}^{n} \min\{\lambda_i(D, \Gamma), 1\} \le \frac{(2n+1)!!}{|D \cap \Gamma|}. \tag{5}$$

**Lemma 2.** *For any $s_0 \in \mathbb{F}_p$, the number of solutions of the congruence*

$$x \equiv s_0 y \pmod p; \quad x, y \in \mathbb{N}, \quad x \le X, \quad y \le Y, \quad \gcd(x, y) = 1, \tag{6}$$

*is bounded by $O(1 + XYp^{-1})$.*

*Proof.* Consider the lattice

$$\Gamma = \{(u, v) \in \mathbb{Z}^2; \quad u \equiv s_0 v \pmod p\}$$

and the body

$$D = \{(u, v) \in \mathbb{R}^2; \quad |u| \le X, \ |v| \le Y\}.$$

Let $\lambda_1, \lambda_2$ be the consecutive minimas of the body $D$ with respect to the lattice $\Gamma$. If $\lambda_2 > 1$ then there is at most one independent vector in $\Gamma \cap D$, implying that $J \le 1$, where $J$ is the number of solutions of (6).

Let now $\lambda_2 \le 1$. Then, by (5), we get

$$\lambda_1\lambda_2 \le \frac{15}{|\Gamma \cap D|} \le \frac{15}{J}.$$

Let $(u_i, v_i) \in \lambda_i D \cap \Gamma$, $i = 1, 2$, be linearly independent. Then

$$0 \ne \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \equiv 0 \pmod p.$$

Therefore,

$$p \le \left|\det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}\right| = |u_1v_2 - u_2v_1| \le 2\lambda_1\lambda_2 XY \le \frac{30XY}{J}$$

and the result follows.

□

We also need the following simple lemma.

**Lemma 3.** *Let $X, Y$ be positive numbers with $XY < p$. Then for any $\lambda$ there is at most one solution to the congruence*

$$\frac{x}{y} \equiv \lambda \pmod p; \quad x, y \in \mathbb{N}, \quad x \le X,\ y \le Y, \quad \gcd(x, y) = 1.$$

*Proof.* Assuming that there is at least one solution $(x_0, y_0)$, we get that

$$xy_0 \equiv x_0 y \pmod p,$$

and since the both hand sides are not greater than $XY < p$, the congruence is converted to an equality, which together with $\gcd(x, y) = \gcd(x_0, y_0) = 1$ implies that $x = x_0$, $y = y_0$. □

To prove our Theorem 2, we shall need the following lemma, which can be found in [18, Chapter 1, Theorem 1].

**Lemma 4.** *Let $\gamma_1, \ldots, \gamma_d$ be a sequence of $d$ points of the unit interval $[0, 1]$. Then for any integer $K \ge 1$, and an interval $[\alpha, \beta] \subseteq [0, 1]$, we have*

$$\begin{aligned} &\#\{n = 1, \ldots, d \ : \gamma_n \in [\alpha, \beta]\} - d(\beta - \alpha) \\ &\qquad \ll \frac{d}{K} + \sum_{k=1}^{K} \left(\frac{1}{K} + \min\{\beta - \alpha, 1/k\}\right) \left|\sum_{n=1}^{d} \exp(2\pi i k \gamma_n)\right|. \end{aligned}$$

We shall also need the well-known character sum bounds of Burgess [5, 6].

**Lemma 5.** *For any fixed positive integer constant $r$ the following bound holds:*

$$\max_{\chi\neq\chi_0}\Big|\sum_{n=L+1}^{L+N}\chi(n)\Big| < N^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}+o(1)}.$$

We also recall the following bound of exponential sum estimates over subgroups due to Konyagin [15].

**Lemma 6.** *If $\mathcal{G}$ is a subgroup of $\mathbb{F}_p^*$ with $|\mathcal{G}| < p^{1/2}$ then*

$$\max_{a\not\equiv 0(\bmod p)}\Big|\sum_{x\in G}e_p(ax)| \ll |G|^{29/36}p^{1/18}.$$

Here and below we use the abbreviation $e_p(z) = e^{2\pi iz/p}$. Lemma 6 will be used in the proof of Theorem 2. We recall that a better bound follows from the work of Shteinikov [21], but since in Theorem 2 we do not specify the constant $c$, for our current purposes Lemma 6 suffices.

# 3 Proof of Theorem 1

Given a positive integer $d$ we let $J_d(H,\mathcal{U})$ be the number of solutions of (1) with the additional condition $\gcd(x,y) = d$. Then we have

$$J = \sum_{d\leq H}J_d(H,\mathcal{U}) = \sum_{d\leq H}J_1(H/d,\mathcal{U}). \tag{7}$$

Since each pair of relatively prime positive integers $(x,y)$ can be defined by the rational number $x/y$, it follows that $J_1(H/d,\mathcal{U})$ is equal to the cardinality of the set

$$\mathcal{J}_d = \Big\{\frac{x}{y};\quad x,y\in\mathbb{N},\, x,y\leq\frac{H}{d},\, \gcd(x,y)=1,\, \frac{x}{y}\pmod p\in\mathcal{U}\Big\}.$$

We observe that the $m$-fold product set $\mathcal{J}_d^{(m)}$ satisfies

$$\mathcal{J}_d^{(m)} \subset \Big\{\frac{u}{v};\quad u,v\in\mathbb{N},\, u,v\leq(H/d)^m,\, \gcd(u,v)=1,\, \frac{u}{v}\pmod p\in\mathcal{U}^{(m)}\Big\}.$$

The Plünecke inequality (see, [19, Theorem 7.7]) together with the condition $|\mathcal{U}\cdot\mathcal{U}| < 10|\mathcal{U}|$ implies that $|\mathcal{U}^{(m)}| < 10^m|\mathcal{U}|$. Thus, using Lemma 2, we derive that

$$|\mathcal{J}_d^{(m)}| \ll \sum_{r\in\mathcal{U}^{(m)}} \left(1+\frac{(H/d)^{2m}}{p}\right) \ll |\mathcal{U}|\left(1+\frac{(H/d)^{2m}}{p}\right),$$

the implied constant may depend on $m$. On the other hand Lemma 1 implies that $|\mathcal{J}_d^{(m)}| \gtrsim |\mathcal{J}_d|^m$. Thus,

$$J_1(H/d,\mathcal{U}) = |\mathcal{J}_d| \lesssim |\mathcal{U}|^{1/m} + \frac{|\mathcal{U}|^{1/m}H^2}{p^{1/m}d^2}. \tag{8}$$

We first prove the part $(i)$ of our theorem. It suffices to prove that for any $\delta>0$ there exists $c=c(\delta)>0$ such that $J_1(H/d,\mathcal{U}) < (H/d)p^{\delta}$. In particular, since $J_1(H/d,\mathcal{U}) \le (H/d)^2$, we can assume that $H/d > p^{\delta}$. Let $m$ be the smallest positive integer such that $|\mathcal{U}| < (H/d)^m$. Clearly, $m < 1+1/\delta$. It is easy to see that $(H/d)^m < p/|\mathcal{U}|$. Indeed, if $(H/d)^m \ge p/|\mathcal{U}|$, then from the condition of the theorem it follows that $m \ge n+1$. On the other hand, by the definition of $m$ we have $(H/d)^{m-1} \le |\mathcal{U}|$. Hence, the lower and the upper bounds for $H/d$ give

$$|\mathcal{U}| \ge p^{(m-1)/(2m-1)} \ge p^{n/(2n+1)},$$

which contradicts the condition of the theorem.

Thus, we have

$$|\mathcal{U}| < (H/d)^m < p/|\mathcal{U}|.$$

Combining this with (8), we get that

$$J_1(H/d,\mathcal{U}) \lesssim \frac{H}{d},$$

which, in view of the remark above, finishes the proof of the part $(i)$ of the theorem.

Now we prove the part $(ii)$ of the theorem. In the inequality (7) we split the summation over $d<H$ into at most $H^{o(1)}$ dyadic intervals of the form $[H/2^j, H/2^{j-1}]$. It then follows from (7) that for some $1\le L\le H$ one has

$$J \lesssim \sum_{H/(2L)\le d\le H/L} J_1(H/d,\mathcal{U}).$$

Using (8) we get that for any fixed positive integer constant $m$ we have the bound

$$J \lesssim H\Big(\frac{|\mathcal{U}|^{1/m}}{L} + \frac{|\mathcal{U}|^{1/m}L}{p^{1/m}}\Big). \qquad (9)$$

We can assume that $L > p^{\delta}$ for some small positive constant $\delta > 0$, as otherwise, the result follows from (9) for a sufficiently large constant $m$.

If $L \ge |\mathcal{U}|$, then applying (9) with $m = 1$ and using $L \le H$ we obtain that

$$J \lesssim H + \frac{|\mathcal{U}|H^2}{p}.$$

Thus in this case we get the desired estimate. So, in what follows, we assume that $L \le |\mathcal{U}|$. Consider two cases.

**Case 1.** $|\mathcal{U}|^{1/2} \le L \le |\mathcal{U}|$. Since we also have $L \le H$, taking $m = 1$ we get

$$J \lesssim \frac{H|\mathcal{U}|}{L} + \frac{|\mathcal{U}|H^2}{p}.$$

Now take $m = 2$ in (9) and get

$$J \lesssim H + \frac{|\mathcal{U}|^{1/2}HL}{p^{1/2}}.$$

Putting the last two inequalities together, we obtain that

$$J \lesssim H + \frac{|\mathcal{U}|H^2}{p} + \min\Big\{\frac{H|\mathcal{U}|}{L}, \frac{|\mathcal{U}|^{1/2}HL}{p^{1/2}}\Big\}.$$

Since

$$\min\Big\{\frac{H|\mathcal{U}|}{L}, \frac{|\mathcal{U}|^{1/2}HL}{p^{1/2}}\Big\} \le \frac{H|\mathcal{U}|^{3/4}}{p^{1/4}},$$

the result follows in this case.

**Case 2.** $|\mathcal{U}|^{1/(n+1)} \le L \le |\mathcal{U}|^{1/n}$ for some integer $n \ge 2$. Since $L > p^{\delta}$ for some positive constant $\delta$, we get that $n \le n_0$ for some integer constant $n_0$. We apply the bound (9) with $m = n+1$ and obtain

$$J \lesssim H + \frac{H|\mathcal{U}|^{(2n+1)/n(n+1)}}{p^{1/(n+1)}}.$$

Since $n \ge 2$ and $|\mathcal{U}| < p^{2/5}$ we get

$$|\mathcal{U}|^{(2n+1)/n} \le p.$$

Therefore, we obtain $J \lesssim H$ and finish the proof of our theorem.

To derive Corollary 1, we fix $r = r_0 \in \mathcal{U}$ such that

$$J \le |\mathcal{U}| J',$$

where $J'$ is the number of solutions of the congruence

$$x \equiv x_1 r_0^{-1} r_1 \pmod p; \quad 1 \le x, x_1 \le H, \quad r_1 \in \mathcal{U}.$$

Now we simply denote

$$\mathcal{U}' = \{r_0^{-1} r_1; \quad r_1 \in \mathcal{U}\}$$

and apply Theorem 1 with $\mathcal{U}$ substituted by $\mathcal{U}'$.

# 4 Proof of Theorem 2 and Corollary 2

We can assume that $\lambda \not\equiv 0 \pmod p$. Denote $N = \lfloor p/d \rfloor$. If $d_1 = (d, p-1)$, then the congruence (3) becomes equivalent to a congruence of the form

$$x^{d_1} \equiv \lambda_1 \pmod p; \quad x \in \mathbb{N}, \quad L+1 \le x \le L+N,$$

for some $\lambda_1 \not\equiv 0 (\mathrm{mod} p)$, and we have $d_1 | p-1$ and $N_1 = \lfloor p/d_1 \rfloor \ge N$. Thus, without loss of generality we can assume that $d | p-1$. We can also assume that

$$p^{\frac{1}{3}-0.001} < d < p^{\frac{2}{3}+0.001}, \tag{10}$$

as otherwise the claim would follow from the trivial bound $T_p(d, \lambda, L, N) \le \min\{d, N\}$.

Let $\mathcal{G}_d$ be the subgroup of $\mathbb{F}_p^*$ of order $d$. We fix one solution $x = x_0$ to (3). Clearly, $T_p(d, \lambda, L, N)$ is equal to the number of solutions of the congruence

$$x (\mathrm{mod} p) \in x_0 \mathcal{G}_d, \quad x \in \mathbb{N}, \quad L+1 \le x \le L+N.$$

In view of (10), we have

$$d \in [p^{\frac{1}{3}-0.001}, p^{\frac{1}{3}+0.001}] \cup [p^{\frac{2}{3}-0.001}, p^{\frac{2}{3}+0.001}] \cup [p^{\frac{1}{3}+0.001}, p^{\frac{2}{3}-0.001}].$$

Accordingly, we consider three cases.

**Case 1.** $p^{\frac{1}{3}-0.001} < d < p^{\frac{1}{3}+0.001}$. In this case we express $T_p(d, \lambda, L, N)$ in terms of exponential sums and obtain

$$T_p(d, \lambda, L, N) = \frac{1}{p} \sum_{a=0}^{p} \sum_{u \in x_0 \mathcal{G}_d} \sum_{L+1 \le x \le L+N} e_p(a(u - x)).$$

We separate the term corresponding to $a = 0$ and using the standard arguments and Lemma 6, we obtain

$$T_p(d, \lambda, L, N) \ll \frac{dN}{p} + d^{29/36} p^{1/18} \Big( \frac{1}{p} \sum_{a=1}^{p-1} \Big| \sum_{L+1 \le x \le L+N} e_p(ax) \Big| \Big). \qquad (11)$$

We recall the well-known elementary bound

$$\frac{1}{p} \sum_{a=1}^{p-1} \Big| \sum_{L+1 \le x \le L+N} e_p(ax) \Big| \ll \log p,$$

see, for example, the solution to the exercise 11 of Chapter 3 in the book of Vinogradov [23]. Substituting this in (11), we obtain that

$$T_p(d, \lambda, L, N) \lesssim d^{29/36} p^{1/18}.$$

Since $d < p^{\frac{1}{3}+0.001}$, we get $d^{29/36} p^{1/18} < p^{\frac{1}{3}-0.001}$ and the result follows in this case.

**Case 2.** $p^{\frac{2}{3}-0.001} < d < p^{\frac{2}{3}+0.001}$. In this case we denote by $\mathcal{T}$ the set of integers $x \in [L+1, L+N]$ for which $x (\mathrm{mod} p) \in x_0 \mathcal{G}_d$. Then

$$T_p(d, \lambda, L, N) = |\mathcal{T}|. \qquad (12)$$

Clearly, if $x_1, \ldots, x_m \in \mathcal{T}$, we get that $x_1 \cdots x_m (\mathrm{mod} p) \in x_0^m \mathcal{G}_d$. Thus, $|\mathcal{T}|^m$ is not greater, than the number of solutions of the congruence

$$x_1 \cdots x_m (\mathrm{mod} p) \in x_0^m \mathcal{G}_d, \quad L+1 \le x_i \le L+N.$$

Therefore, for some fixed $\lambda_0 \in x_0^m \mathcal{G}_d$ we have

$$|\mathcal{T}|^m < dR, \qquad (13)$$

where $R$ is the number of solutions of the congruence

$$x_1 \cdots x_m \equiv \lambda_0 (\mathrm{mod} p), \quad L+1 \le x_i \le L+N.$$

We express $R$ in terms of character sums and obtain that

$$R = \frac{1}{p-1}\sum_{\chi}\Big(\sum_{L+1\le x\le L+N}\chi(x)\Big)^m \chi(\lambda_0^{-1}),$$

where $\chi$ runs through the set of characters modulo $p$. Separating the term that corresponds to the principal character $\chi_0$, we get that

$$R \le \frac{N^m}{p-1} + \max_{\chi\ne\chi_o}\Big|\sum_{L+1\le x\le L+N}\chi(x)\Big|^m.$$

We apply Lemma 5 with $r = 5$. Since $N > 0.5p^{\frac{1}{3}-0.001}$, it follows that

$$\max_{\chi\ne\chi_o}\Big|\sum_{L+1\le x\le L+N}\chi(x)\Big| \ll N^{59/60}.$$

Hence, taking $m = 200$, we get

$$R \ll \frac{N^{200}}{p} + \frac{N^{200}}{N^{10/3}} \ll \frac{N^{200}}{p}.$$

Therefore, from (13) we obtain that

$$|\mathcal{T}| \ll (dR)^{1/200} \le N\Big(\frac{d}{p}\Big)^{1/200} \le \Big(\frac{p}{d}\Big)^{199/200} < p^{\frac{1}{3}-0.0001}.$$

Hence, substituting this in (12), we get the desired estimate.

**Case 3.** $p^{\frac{1}{3}+0.001} < d < p^{\frac{2}{3}-0.001}$. In particular, we get

$$N = \lfloor p/d\rfloor \gg p^{\frac{1}{3}+0.001}.$$

We apply Lemma 4 with

$$\{\gamma_n\}_n = \Big\{\frac{x_0h}{p};\, h\in\mathcal{G}_d\Big\},\quad \alpha = \frac{L+1}{p},\quad \beta = \frac{L+N}{p},\quad K = d.$$

It follows that

$$T_p(d,\lambda,L,N) \ll 1 + \frac{1}{d}\sum_{k=1}^{d}\Big|\sum_{h\in\mathcal{G}_d} e_p(kx_0h)\Big|. \tag{14}$$

Since $\mathcal{G}_d$ is cyclic (and therefore consists of all powers of some element) and $d > p^{\frac{1}{3}+0.001}$, there exists a subset $\mathcal{U} \subset \mathcal{G}_d$ such that

$$0.1p^{\frac{1}{3}+0.001} < |\mathcal{U}| < 0.2p^{\frac{1}{3}+0.001}, \quad |\mathcal{U}\cdot\mathcal{U}| \le 2|\mathcal{U}|.$$

Clearly, $r\mathcal{G}_d = \mathcal{G}_d$ for any $r \in \mathcal{U}$. It then follows that

$$\frac{1}{d}\sum_{k=1}^{d}\Big|\sum_{h\in\mathcal{G}_d} e_p(kx_0h)\Big| = \frac{1}{d|\mathcal{U}|}\sum_{k=1}^{d}\sum_{r\in\mathcal{U}}\Big|\sum_{h\in\mathcal{G}_d} e_p(krx_0h)\Big|. \qquad (15)$$

Let $I(\mu)$ be the number of solutions of the congruence

$$kr \equiv \mu \pmod p, \quad k \in \mathbb{N}, \quad k \le d, \quad r \in \mathcal{U}.$$

Note that, by Corollary 1, we have

$$\sum_{\mu=0}^{p-1} I(\mu)^2 \lesssim \frac{|\mathcal{U}|^{7/4}d}{p^{1/4}}. \qquad (16)$$

Indeed, the left hand side is equal to the number of solutions of the congruence

$$kr \equiv k_1r_1 \pmod p, \quad k, k_1 \in \mathbb{N}; \quad k, k_1 \le d; \quad r, r_1 \in \mathcal{U}.$$

Moreover,

$$p^{1/3} < |\mathcal{U}| < p^{2/5}, \quad |\mathcal{U}\cdot\mathcal{U}| < 10|\mathcal{U}|, \quad |\mathcal{U}|d < p^{\frac{2}{3}-0.001}p^{\frac{1}{3}+0.001} = p.$$

Thus, we are at the condition of $(ii)$ of Corollary 1. Therefore, the estimate (16) holds.

Now, we use the Cauchy-Schwarz inequality and obtain

$$\begin{aligned}\sum_{k=1}^{d}\sum_{r\in\mathcal{U}}\Big|\sum_{h\in\mathcal{G}_d} e_p(krx_0h)\Big| &= \sum_{\mu=0}^{p-1} I(\mu)\Big|\sum_{h\in\mathcal{G}_d} e_p(\mu x_0h)\Big| \\ &\le \Big(\sum_{\mu=0}^{p-1} I(\mu)^2\Big)^{1/2}\Big(\sum_{\mu=0}^{p-1}\Big|\sum_{h\in\mathcal{G}_d} e_p(\mu x_0h)\Big|^2\Big)^{1/2} \\ &\lesssim \frac{|\mathcal{U}|^{7/8}d^{1/2}}{p^{1/8}}(pd)^{1/2} = |\mathcal{U}|^{7/8}dp^{3/8}.\end{aligned}$$

Substituting this in (15), we obtain

$$\frac{1}{d}\sum_{k=1}^{d}\left|\sum_{h\in\mathcal{G}_d} e_p(kx_0h)\right| \lesssim \frac{p^{3/8}}{|\mathcal{U}|^{1/8}} \lesssim p^{\frac{1}{3}-0.0001}.$$

This together with (14) proves Theorem 2.

We shall now derive Corollary 2. Let $J$ be the number of solutions of (4). Clearly, if $\gcd(f(x),p-1)=d$, then (4) implies that $x^d\equiv 1 \pmod p$. Hence,

$$J=\sum_{d|p-1} J_d, \tag{17}$$

where $J_d$ is the number of solutions of the congruence

$$x^d\equiv 1 \pmod p;\quad x\in\mathbb{N},\quad x<p,\quad \gcd(f(x),p-1)=d.$$

Since $f(x)$ does not have multiple roots, by the Nagell-Ore theorem (see [14], even for a stronger form) the set of $x$ with $f(x)\equiv 0 \pmod d$ consists on the union of arithmetic progressions of the form $x\equiv k \pmod d$ for at most $d^{o(1)}$ different values of $k$. Thus, for each $d|p-1$ there exists a non-negative integer $k_0<d$ such that

$$J_d\lesssim J_d', \tag{18}$$

where $J_d'$ is the number of solutions of the congruence

$$x^d\equiv 1 \pmod p;\quad x\in\mathbb{N},\quad x<p,\quad x\equiv k_0 \pmod d.$$

Representing $x=k_0+dy$, we get the congruence

$$(k_0+dy)^d\equiv 1 \pmod p;\quad y\in\mathbb{N}\cup\{0\},\quad y<p/d.$$

Hence, if we denote by $d_1$ the multiplicative inverse of $d \pmod p$, we get that $J_d'$ is not greater than the number of solutions of the congruence

$$(y+k_0d_1)^d\equiv d_1^d \pmod p;\quad y\in\mathbb{N}\cup\{0\},\quad y<p/d.$$

According to Theorem 2, we have $J_d'\lesssim p^{\frac{1}{3}-c}$ for some absolute constant $c>0$. Combining this bound with (18) and (17), we conclude the proof.

# 5 Proof of Theorem 3

We first establish the following statement, based on Corollary 1.

**Lemma 7.** *Let* $0 < \varepsilon < 0.01$ *be fixed,* $\mathcal{U} \subset \mathbb{F}_p^*$ *be such that* $|\mathcal{U} \cdot \mathcal{U}| \le 10|\mathcal{U}|$ *and*

$$H = \lfloor p^{1/4+\varepsilon} \rfloor, \quad 2H < |\mathcal{U}| \le p^{3/8-0.5\varepsilon}.$$

*Then the number* $T$ *of solutions of the congruence*

$$qxr \equiv q_1 x_1 r_1 \pmod p \tag{19}$$

*in positive integers* $x, x_1$*, prime numbers* $q, q_1$ *and elements* $r, r_1 \in \mathcal{U}$ *with*

$$x, x_1 \le H, \quad 0.5|\mathcal{U}| < q, q_1 \le |\mathcal{U}| \tag{20}$$

*satisfies*

$$T \lesssim |\mathcal{U}|^2 H.$$

*Proof.* We have

$$T = T_1 + T_2,$$

where $T_1$ is the number of solutions of (19) satisfying (20) with the additional condition $q = q_1$, and $T_2$ is the number of solutions with $q \ne q_1$. We observe that $|\mathcal{U}| < p^{3/8} < p^{2/5}$ and

$$|\mathcal{U}|H^2 < p^{3/8-0.5\epsilon} p^{1/2+2\epsilon} < p^{7/8+3\epsilon/2} < p.$$

Thus, we can apply Corollary 1 with $n = 2$ and get

$$T_1 \lesssim |\mathcal{U}|^2 H.$$

In order to estimate $T_2$, we fix $x_1, r, r_1$ such that

$$T_2 \le |\mathcal{U}|^2 H T_2',$$

where $T_2'$ is the number of solutions of the congruence

$$\frac{qx}{q_1} \equiv \frac{x_1 r_1}{r} \pmod p$$

in positive integers $x \le H$ and prime numbers $q, q_1$ with

$$q \ne q_1, \quad 0.5|\mathcal{U}| < q, q_1 \le |\mathcal{U}|.$$

From $x \le H < q_1$, it follows that $\gcd(qx, q_1) = 1$. Since $H|\mathcal{U}|^2 < p$, from Lemma 3 we get that $xq$ and $q_1$ are uniquely determined. Since $x < q$, the value $xq$ uniquely determines $x$ and $q$. Hence, $T_2' \le 1$, whence $T_2 \le |\mathcal{U}|^2 H$ concluding the proof of our lemma.

□

We now proceed to prove Theorem 3. Assuming $\varepsilon < 0.01$, we define

$$m_0 = \left\lceil \frac{1}{\varepsilon} \right\rceil, \quad L = \lfloor p^{1/m_0} \rfloor, \quad H = \lfloor p^{1/4+\varepsilon} \rfloor, \quad N = \lfloor p^{3/8-0.5\varepsilon} \rfloor.$$

From Lemma 5 it follows that there exists $\delta = \delta(\varepsilon) > 0$ such that for any non-principal character $\chi$ modulo $p$ the following bound holds:

$$\left| \sum_{x \le H} \chi(x) \right| \le H^{1-\delta}. \tag{21}$$

Let $\mathcal{G}'$ be a subset of $\mathcal{G}$ such that $|\mathcal{G}'| = N$ and $|\mathcal{G}'\mathcal{G}'| \le 2|\mathcal{G}'|$. The existence of such a subset is obvious, since either $\mathcal{G}$ consists on consecutive powers of a primitive root or it is a subgroup of $\mathbb{F}_p^*$, which is cyclic.

It suffices to prove that for some $\delta_0 = \delta_0(\varepsilon) > 0$ there are $p + O(p^{1-\delta_0})$ residue classes modulo $p$ of the form $zxqr \pmod p$, with positive integers $x, z$, prime numbers $q$ and elements $r$ satisfying

$$z \le L, \quad x \le H, \quad \frac{N}{2} < q \le N, \quad r \in \mathcal{G}'.$$

Let $\Lambda \subset \mathbb{F}_p^*$ be the exceptional set, that is, assume that the congruence

$$zxqr \equiv \lambda \pmod p$$

has no solutions in $\lambda \in \Lambda$ and $z, x, q, r$ as above. We write this condition in the form of character sums

$$\frac{1}{p-1} \sum_{\chi} \sum_{z \le L} \sum_{x \le H} \sum_{\substack{0.5N < q < N \\ q \text{ is prime}}} \sum_{r \in \mathcal{G}'} \sum_{\lambda \in \Lambda} \chi(zxqr\lambda^{-1}) = 0,$$

where $\chi$ runs through the set of characters modulo $p$. Separating the term corresponding to the principal character $\chi = \chi_0$, we get

$$LHN^2|\Lambda| \lesssim \sum_{\chi \ne \chi_0} \left| \sum_{z \le L} \chi(z) \right| \left| \sum_{x \le H} \sum_{\substack{0.5N < q < N \\ q \text{ is prime}}} \sum_{r \in \mathcal{G}'} \chi(xqr) \right| \left| \sum_{\lambda \in \Lambda} \chi(\lambda) \right|.$$

Following [8, 9], we split the set of nonprincipal characters $\chi$ into two subsets $\mathcal{X}_1$ and $\mathcal{X}_2$ as follows. To the set $\mathcal{X}_1$ we allot those characters $\chi$, for which

$$\Big|\sum_{z\le L}\chi(z)\Big| \ge L^{1-0.1\delta},$$

where $\delta$ is defined from (21). The remaining characters we include to the set $\mathcal{X}_2$, these are the characters that satisfy

$$\Big|\sum_{z\le L}\chi(z)\Big| < L^{1-0.1\delta}.$$

Thus, we have

$$LHN^2|\Lambda| \lesssim W_1 + W_2, \tag{22}$$

where

$$W_i = \sum_{\chi\in\mathcal{X}_i}\Big|\sum_{z\le L}\chi(z)\Big|\Big|\sum_{x\le H}\sum_{\substack{0.5N<q<N\\ q \text{ is prime}}}\sum_{r\in\mathcal{G}'}\chi(xqr)\Big|\Big|\sum_{\lambda\in\Lambda}\chi(\lambda)\Big|.$$

To deal with $W_1$, we show that the cardinality of $\mathcal{X}_1$ is small. We have

$$|\mathcal{X}_1|L^{2m_0(1-0.1\delta)} \le \sum_{\chi\in\mathcal{X}_1}\Big|\sum_{z\le L}\chi(z)\Big|^{2m_0} \le \sum_{\chi}\Big|\sum_{z\le L}\chi(z)\Big|^{2m_0} = (p-1)T,$$

where $T$ is the number of solutions of the congruence

$$x_1\cdots x_{m_0} \equiv y_1\cdots y_{m_0} \pmod p; \quad x_i, y_j \in \mathbb{N}; \quad x_i, y_j \le L.$$

Since $L^{m_0} < p$, the congruence is converted to an equality and we have, by the estimate for the divisor function, at most $L^{m_0+o(1)}$ solutions. Thus,

$$|\mathcal{X}_1|L^{2m_0(1-0.1\delta)} \lesssim pL^{m_0+o(1)},$$

whence, in view of $L^{m_0} = p^{1+o(1)}$, we get

$$|\mathcal{X}_1| \lesssim p^{0.2\delta}.$$

Thus, estimating in $W_1$ the sums over $z, q, r, \lambda$ trivially and applying (21) to the sum over $x$, we get

$$\begin{aligned} W_1 &= \sum_{\chi\in\mathcal{X}_1}\Big|\sum_{z\le L}\chi(z)\Big|\Big|\sum_{x\le H}\chi(x)\Big|\Big|\sum_{\substack{0.5N<q<N\\ q \text{ is prime}}}\sum_{r\in\mathcal{G}'}\chi(qr)\Big|\Big|\sum_{\lambda\in\Lambda}\chi(\lambda)\Big| \\ &\lesssim |\mathcal{X}_1|\cdot L\cdot N^2\cdot|\Lambda|\max_{\chi\ne\chi_0}\Big|\sum_{x\le H}\chi(x)\Big| \lesssim p^{0.2\delta}LN^2|\Lambda|H^{1-\delta}. \end{aligned}$$

Therefore, since $H > p^{1/4}$ we have, for sufficiently large $p$, the estimate

$$W_1 < LHN^2|\Lambda|p^{-0.01\delta}.$$

Inserting this bound into (22), we get

$$LHN^2|\Lambda| \lesssim W_2. \tag{23}$$

We next estimate $W_2$. By the definition of $\mathcal{X}_2$, we have

$$W_2 \le L^{1-0.1\delta} \sum_{\chi} \Big| \sum_{x \le H} \sum_{\substack{0.5N<q<N \\ q \text{ is prime}}} \sum_{r \in \mathcal{G}'} \chi(xqr) \Big| \Big| \sum_{\lambda \in \Lambda} \chi(\lambda) \Big|. \tag{24}$$

Next, we have

$$\sum_{\chi} \Big| \sum_{\lambda \in \Lambda} \chi(\lambda) \Big|^2 = (p-1)|\Lambda|$$

and

$$\sum_{\chi} \Big| \sum_{x \le H} \sum_{\substack{0.5N<q<N \\ q \text{ is prime}}} \sum_{r \in \mathcal{G}'} \chi(xqr) \Big|^2 = (p-1)T,$$

where $T$ is the number of solutions of the congruence

$$xqr \equiv x_1 q_1 r_1 \pmod{p},$$

in positive integers $x, x_1$ prime numbers $q, q_1$ and elements $r, r_1 \in \mathcal{G}'$ satisfying

$$x_1, x_2 \le H, \quad 0.5N < q, q_1 < N, \quad r, r_1 \in \mathcal{G}'.$$

From Lemma 7 with $\mathcal{U} = \mathcal{G}'$ it follows that

$$T \lesssim N^2 H.$$

Therefore, applying the Cauchy-Schwarz inequality in (24), and using (23), we obtain that

$$L^2H^2N^4|\Lambda|^2 \lesssim W_2^2 \lesssim L^{2-0.02\delta}(p-1)^2|\Lambda|T \lesssim L^{2-0.02\delta}p^2|\Lambda|N^2H.$$

Thus,

$$|\Lambda| \lesssim \frac{p^2L^{-0.02\delta}}{HN^2} \lesssim pL^{-0.02\delta}.$$

Therefore,

$$|\Lambda| < p^{1-\delta_0}$$

for some $\delta_0 = \delta_0(\epsilon)$, which concludes the proof.

# 6 Proof of Theorem 4

The proof follows the same line as the proof of Theorem 3, however, instead of Lemma 7 we shall use Lemma 8 .

**Lemma 8.** *Let* $0 < \varepsilon < 0.01$ *be fixed,* $\mathcal{U} \subset \mathbb{F}_p^*$ *be such that* $|\mathcal{U} \cdot \mathcal{U}| \le 10|\mathcal{U}|$ *and*

$$H = \lfloor p^{1/4+\varepsilon} \rfloor, \quad Q = \lfloor p^{1/4} \rfloor, \quad |\mathcal{U}| \le p^{1/4-\varepsilon}.$$

*Then the number* $T$ *of solutions of the congruence*

$$q_1 q_2 x r \equiv q_1' q_2' x' r' \pmod p \tag{25}$$

*in positive integers* $x, x'$, *prime numbers* $q_1, q_2, q_1', q_2'$ *and elements* $r, r' \in \mathcal{U}$ *with*

$$x, x' \le H, \quad \frac{Q}{4} < q_1, q_1' < \frac{Q}{2}, \quad \frac{Q}{2} < q_2, q_2' < Q, \tag{26}$$

*satisfies*

$$T \lesssim Q^2 H |\mathcal{U}|.$$

Let us prove the lemma. We have

$$T = T_1 + T_2 + T_3 + T_4, \tag{27}$$

where $T_1$ is the number of solutions of (25) satisfying (26) and with the additional condition $q_1 = q_2$, $q_1' = q_2'$, $T_2$ is the number of solutions with $q_1 \ne q_1'$, $q_2 \ne q_2'$, $T_3$ is the number of solutions with $q_1 = q_1'$, $q_2 \ne q_2'$ and $T_4$ is the number of solutions with $q_1 \ne q_1'$, $q_2 = q_2'$.

We have $T_1 \le Q^2 T_1'$, where $T_1'$ is the number of solutions of the congruence

$$xr \equiv x'r' \pmod p; \quad x, x' \le H, \quad r, r' \in \mathcal{U}.$$

Applying Corollary 1 with $n = 1$ or $n = 2$, we get that $T_1' \lesssim |\mathcal{U}| H$. Therefore,

$$T_1 \lesssim Q^2 H |\mathcal{U}|. \tag{28}$$

To estimate $T_2$, we fix $x, r, x', r'$ and see that

$$T_2 \lesssim |\mathcal{U}|^2 |H|^2 T_2',$$

where $T_2'$ is the number of solutions of the congruence

$$\frac{q_1 q_2}{q_1' q_2'} \equiv \frac{x' r'}{x r} \pmod p$$

in prime numbers $q_1, q_1', q_2, q_2'$ with

$$\frac{Q}{4} < q_1, q_1' < \frac{Q}{2}, \quad \frac{Q}{2} < q_2, q_2' < Q, \quad q_1 \neq q_1', \quad q_2 \neq q_2'.$$

Since $\gcd(q_1 q_2, q_1' q_2') = 1$ and $Q^4 < p$, it follows from Lemma 3 that the numbers $q_1 q_2$ and $q_1' q_2'$ are uniquely determined. Since $q_1 < q_2$ and $q_1' < q_2'$, this implies that in fact all the prime numbers $q_1, q_2, q_1', q_2'$ are uniquely determined. Therefore, $T_2' \leq 1$ and we get

$$T_2 \lesssim |\mathcal{U}|^2 |H|^2 \lesssim Q^2 H |\mathcal{U}|. \tag{29}$$

In order to estimate $T_3$ and $T_4$, we note that

$$T_3 + T_4 \leq Q T_5,$$

where $T_5$ is the number of solutions of the congruence

$$qxr \equiv q'x'r' \pmod{p},$$

in positive integers $x, x'$, prime numbers $q, q'$ and elements $r, r' \in \mathcal{U}$ with

$$x, x' \leq H, \quad \frac{Q}{4} < q, q' < Q, \quad q \neq q'.$$

We introduce variables $x_1, x_2$ with

$$x_1 = qx, \quad x_2 = q'x'$$

and note that

$$x_1 r \equiv x_2 r' \pmod{p}; \quad x_1, x_2 \leq QH, \quad r, r' \in \mathcal{U}.$$

We can apply Corollary 1 with $n = 1$ and $H$ substituted by $QH$ (clearly, the conditions of Corollary 1 are satisfied). It then follows that there are at most $QH|\mathcal{U}|p^{o(1)}$ possibilities for the quadruple $(x_1, x_2, r, r')$. Each such quadruple determines $q, x, q', x'$ with at most $p^{o(1)}$ possibilities, because $q, x, q', x'$ are divisors of $x_1 x_2 < p$. Therefore, we get that

$$T_5 \lesssim QH|\mathcal{U}|,$$

implying that

$$T_3 + T_4 \lesssim Q^2 H |\mathcal{U}|.$$

Inserting this estimate together with (28) and (29) into (27), we conclude the proof of our lemma.

Now we proceed to prove Theorem 4. Assuming $\varepsilon < 0.01$, we define

$$m_0 = \left\lceil \frac{1}{\varepsilon} \right\rceil, \quad L = \lfloor p^{1/m_0} \rfloor, \quad H = \lfloor p^{1/4+\varepsilon} \rfloor, \quad Q = \lfloor p^{1/4} \rfloor, \quad N = \lfloor p^{1/4-\varepsilon} \rfloor.$$

Following the proof of Theorem 3, we denote by $\delta = \delta(\varepsilon) > 0$ a positive constant such that for any non-principal character $\chi$ modulo $p$ the following bound holds:

$$\left| \sum_{x \le H} \chi(x) \right| \le H^{1-\delta}. \tag{30}$$

We again let $\mathcal{G}'$ be a subset of $\mathcal{G}$ such that $|\mathcal{G}'| = N$ and $|\mathcal{G}'\mathcal{G}'| \le 2|\mathcal{G}'|$.

It suffices to prove that for some $\delta_0 = \delta_0(\varepsilon) > 0$ there are $p + O(p^{1-\delta_0})$ residue classes modulo $p$ of the form $zxq_1q_2r \pmod p$, with positive integers $z, x$, prime numbers $q_1, q_2$ and elements $r$ satisfying

$$z \le L, \quad x \le H, \quad \frac{Q}{4} < q_1 \le \frac{Q}{2}, \quad \frac{Q}{2} < q_2 \le Q, \quad r \in \mathcal{G}'.$$

Let $\Lambda \subset \mathbb{F}_p^*$ be the exceptional set, that is, assume that the congruence

$$zxq_1q_2r \equiv \lambda \pmod p$$

has no solutions in $\lambda \in \Lambda$ and $z, x, q_1, q_2, r$ as above. Following the proof of Theorem 3, we derive that

$$LHQ^2N|\Lambda| \lesssim \sum_{\chi \ne \chi_0} \left| \sum_{z \le L} \chi(z) \right| \left| \sum_{x \le H} \sum_{\substack{Q/4<q_1<Q/2 \\ Q/2<q_2<Q \\ q_1,q_2 \text{ are primes}}} \sum_{r \in \mathcal{G}'} \chi(xq_1q_2r) \right| \left| \sum_{\lambda \in \Lambda} \chi(\lambda) \right|.$$

We define the set of characters $\mathcal{X}_1$ and $\mathcal{X}_2$ exactly the same way as in the proof of Theorem 4 and write

$$LHQ^2N|\Lambda| \lesssim W_1 + W_2, \tag{31}$$

where

$$W_i = \sum_{\chi \in \mathcal{X}_i} \left| \sum_{z \le L} \chi(z) \right| \left| \sum_{x \le H} \sum_{\substack{Q/4<q_1<Q/2 \\ Q/2<q_2<Q \\ q_1,q_2 \text{ are primes}}} \sum_{r \in \mathcal{G}'} \chi(xq_1q_2r) \right| \left| \sum_{\lambda \in \Lambda} \chi(\lambda) \right|.$$

From the proof of Theorem 3 it follows that

$$|\mathcal{X}_1| \lesssim p^{0.2\delta}.$$

Thus, estimating in $W_1$ the sums over $z, q_1, q_2, r, \lambda$ trivially and applying (30) to the sum over $x$, we get

$$W_1 < LHQ^2N|\Lambda|p^{-0.01\delta}.$$

Inserting this bound into (31), we get

$$LHQ^2N|\Lambda| \lesssim W_2.$$

Following the argument of the proof of Theorem 3 we have

$$L^2H^2Q^4N^2|\Lambda|^2 \lesssim W_2^2 \lesssim L^{2-0.02\delta}(p-1)^2|\Lambda|T,$$

where $T$ is the number of solutions of the congruence

$$xq_1q_2r \equiv x'q_1'q_2'r' \pmod p,$$

in positive integers $x, x'$ prime numbers $q_1, q_2, q_1', q_2'$ and elements $r, r_1 \in \mathcal{G}'$ satisfying

$$x_1, x_2 \le H, \quad \frac{Q}{4} < q_1, q_1' < \frac{Q}{2}, \quad \frac{Q}{2} < q_1, q_1' < Q, \quad r, r_1 \in \mathcal{G}'.$$

From Lemma 8 with $\mathcal{U} = \mathcal{G}'$ it follows that

$$T \lesssim HQ^2N.$$

Therefore,

$$L^2H^2Q^4N^2|\Lambda|^2 \lesssim L^{2-0.02\delta}p^2HQ^2|\Lambda|.$$

Thus,

$$|\Lambda| \lesssim \frac{p^2}{HQ^2N}L^{-0.02\delta},$$

whence

$$|\Lambda| < p^{1-\delta_0}$$

for some $\delta_0 = \delta_0(\epsilon)$. This finishes the proof of Theorem 4.

# References


[1] A. Balog, K. A. Broughan and I. E. Shparlinski, 'On the number of solutions of exponential congruences', *Acta Arith.*, **148** (2011), 93–103.

[2] U. Betke, M. Henk and J. M. Wills, 'Successive-minima-type inequalities', *Discr. Comput. Geom.*, **9** (1993), 165–175.

[3] 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.* (2008), Art. ID rnn 090, 29 pp.

[4] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Inst. Math.* **280** (2013), 61–90.

[5] D. A. Burgess, 'On character sums and $L$-series', *Proc. London Math. Soc.*, **12** (1962), 193-206.

[6] D. A. Burgess, 'On character sums and $L$-series. II.', *Proc. London Math. Soc.*, **13** (1963), 524-536.

[7] J. Cilleruelo, 'A note on product sets of fractions', Preprint.

[8] J. Cilleruelo and M. Z. Garaev, 'Least totients in arithmetic progressions', *Proc. Amer. Math. Soc.*, **137** (2009), 2913–2919.

[9] M. Z. Garaev, 'A note on the least totient of a residue class', *Quart. J. Math.*, **60** (2009), 53–56.

[10] M. Z. Garaev, 'On multiplicative congruences', *Math. Zeitschrift.*, **272** (2012), 473–482.

[11] M. Z. Garaev and A. A. Karatsuba, 'On character sums and the exceptional set of a congruence problema ', *J. Number Theory*, **114** (2005), 182–192.

[12] M. Z. Garaev and A. A. Karatsuba, 'The representation of residue classes by products of small integers', *Proc. Edinburgh Math. Soc.*, **50** (2007), 363–375.

[13] D. R. Heath-Brown, ‘The divisor function $d_3(n)$ in an arithmetic progressions’, *Acta Arith.*, **47** (1986), 29–56.

[14] M. N. Huxley, ‘A note on polynomial congruences’, *Recent progress in analytic number theory*, Vol. 1 (Durham, 1979), Academic Press, London-New York, 1981, 193-196.

[15] S. V. Konyagin, ‘Estimates for trigonometric sums over subgroups and for Gauss sums’, (Russian) IV International Conference ‘Modern Problems of Number Theory and its Applications’: Part III (2002), 86-114.

[16] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[17] P. Kurlberg, F. Luca and I. E. Shparlinski, ‘On the fixed points of the map $x \to x^x$ modulo a prime’, *Math. Res. Letters*, (to appear).

[18] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Amer. Math. Soc., Providence, RI, 1994.

[19] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets,* Grad. Texts in Math., Vol 165, Springer-Verlag, New York 1996, 293 pp.

[20] I. Shkredov, ‘Some new inequalities in additive combinatorics’, Mosc. J. Comb. Number Theory, **3** (2011), 237–288.

[21] Yu. N. Shteinokov,‘Estimates of trigonometric sums modulo a prime’, *Preprint*, 2014.

[22] I. M. Vinogradov, On the distribution of indices, *Doklady Akad. Nauk SSSR*, **20** (1926), 73-76 (in Russian).

[23] I. M. Vinogradov, “An introduction to the theory of numbers”, Pergamon Press, London & New York, 1955.

Address of the authors:

J. Cilleruelo, Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, Madrid-28049, Spain.
Email:`francisco javier.cilleruelo@uam.es`.

M. Z. Garaev, Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México,
Email:`garaev@matmor.unam.mx`