Product of subsets of small intervals and points on exponential curves modulo a prime

C. A. Díaz, M. Z. Garaev and J. Hernández

Abstract

Let p be a large prime number, $h > 0$ and s be integers, and $\mathcal{X} \subseteq [1, h] \cap \mathbb{Z}$. Following the work of Bourgain, Garaev, Konyagin and Shparlinski (2013), we obtain nontrivial upper bounds for the number of solutions to the congruence

$$\prod_{i=1}^{4}(x_i + s) \equiv \prod_{j=1}^{4}(y_j + s) \not\equiv 0 \pmod p, \quad x_i, y_j \in \mathcal{X}.$$

We apply these bounds to obtain new results on the number of integer points on exponential curves modulo a prime.

2010 Mathematics Subject Classification: 11B50, 11D79, 11P21

Keywords: multiplicative congruences, exponential congruences, small intervals

1 Introduction

Let p be a large prime number, h be a positive integer and g be an integer of multiplicative order $T > h$. Let also s and a be integers with $\gcd(a, p) = 1$. Denote by $J_{a,g}(s; h)$ the number of solutions to the congruence

$$x \equiv ag^y \pmod p, \quad s + 1 \le x, y \le s + h.$$

From the theory of exponential and character sum estimates it is known that if $h < p^{3/4}$, then

$$J_{a,g}(s; h) \ll p^{1/2},$$

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

see, for example, Montgomery [9] or Garaev [7]. However, in the range $h < p^{1/2}$ this estimate becomes worse than the trivial bound $J_{a,g}(s;h) \le h$. The problem of obtaining nontrivial bounds to $J_{a,g}(s;h)$ for all ranges of h was initiated in the work of Chan and Shparlinski [4], with subsequent refinements in [6] and [2, 3]. More precisely, for a positive integer n and an integer $\lambda \not\equiv 0 \pmod p$ denote by $I_n(s,h,\lambda)$ the number of solutions to the congruence

$$(x_1+s)\cdots(x_n+s) \equiv \lambda \pmod p, \quad 1 \le x_1,\dots,x_n \le h.$$

It was shown by Cilleruelo and Garaev [6] (for the case $n \in \{2,3\}$), and by Bourgain, Garaev, Konyagin and Shparlinski [2] (for any n), that if $h < p^{1/(n^2-1)}$ then $I_n(s,h,\lambda) \le h^{o(1)}$. This, in particular, easily implies that if $h < p^{1/(n^2-1)}$, then we have the bound

$$J_{a,g}(s;h) \le h^{1/n+o(1)}.$$

Further improvement on the range for h was obtained by Bourgain et. al. [3] for $n \in \{2,3\}$. More precisely, let $\mathcal{X}$ be an arbitrary subset of integers of the interval $[1,h]$ with $|\mathcal{X}| = \#\mathcal{X}$ elements. Denote by $L_n(p,\mathcal{X};s)$ the number of solutions to the congruence

$$\prod_{i=1}^{n}(x_i+s) \equiv \prod_{j=1}^{n}(y_j+s) \not\equiv 0 \pmod p, \quad x_i, y_j \in \mathcal{X}. \tag{1}$$

Bourgain et. al. [3] proved that if $h^3/|\mathcal{X}| < p$, then $L_2(p,\mathcal{X};s) \le |\mathcal{X}|^2 h^{o(1)}$. They also proved that if $h^8/|\mathcal{X}|^4 < p$, then $L_3(p,\mathcal{X};s) \le |\mathcal{X}|^3 h^{o(1)}$. As a consequence of these estimates, they showed

$$J_{a,g}(s;h) \le \begin{cases} h^{1/2+o(1)} & if \quad h < p^{2/5}; \\ h^{1/3+o(1)} & if \quad h < p^{3/20}. \end{cases}$$

One can believe that if $h < p^{1/2}$ then $J_{a,g}(s;h) \le h^{o(1)}$. At the present time this seems to be a hopeless task to prove. A much weaker, but still a challenging task would be to establish the existence of an absolute positive constant $c < 2$ such that if $n \ge 2$ is a fixed integer and $h < p^{1/n^c}$, then $J_{a,g}(s;h) \le h^{1/n+o(1)}$.

On the other hand, here we state the following conjecture which we believe to be somehow accessible to prove.

Conjecture 1. *Let $n \geq 2$ be a fixed integer constant and*

$$h < p^{\frac{n}{(n-1)(n^2+1)}}.$$

Then

$$J_{a,g}(s;h) \leq h^{1/n+o(1)}.$$

From this perspective, the aforementioned work [3] establishes the validity of Conjecture 1 for $n = 2$ and $n = 3$. In the present paper, based on the arguments of [3], we obtain the following estimate for $L_4(p, \mathcal{X}; s)$, which leads to the proof of Conjecture 1 for $n = 4$.

Theorem 1. *Let $\mathcal{X} \subseteq [1, h]$ be a set of integers with*

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} < p.$$

Then,

$$L_4(p, \mathcal{X}; s) \leq |\mathcal{X}|^4 e^{C\frac{\log h}{\log\log h}}$$

for some absolute positive constant C.

Corollary 1. *For $h < p^{4/51}$ we have the bound $J_{a,g}(s;h) \leq h^{1/4+o(1)}$.*

The paper is organized as follows. In section 2 we state the auxiliary Lemmas which are used in section 3 to prove Theorem 1. In section 4 from Theorem 1 we derive our Corollary 1.

In what follows, we use the notation $A \ll B$ to mean that $|A| = O(B)$, that is, $|A| \leq cB$ for some constant c.

2 Lemmas

The following lemma is a particular case of a more general result from [3].

Lemma 1. *Let $h \geq 1$ and $\sigma, \vartheta \in \mathbb{R}$ be such that $\vartheta \geq 0$ and let $m \geq 1$ be a fixed integer. Let $P_1(Z)$ and $P_2(Z)$ be nonconstant polynomials with integer coefficients,*

$$P_1(Z) = \sum_{i=0}^{m} a_i Z^{m-i} \quad \textit{and} \quad P_2(Z) = \sum_{i=0}^{m} b_i Z^{m-i}$$

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

such that

$$|a_i| < Ah^{i+\sigma}, \quad |b_i| < Ah^{i+\vartheta}, \quad i = 0, 1, \ldots, m,$$

for some A. Then

$$\mathrm{Res}(P_1, P_2) \ll h^{m^2+m(\sigma+\vartheta)},$$

where the implicit constant in $\ll$ depends only on A and m.

We recall that the logarithmic height of an algebraic number α is defined as the logarithmic height $H(P)$ of its minimal polynomial P, that is, the maximum logarithm of the largest (by absolute value) coefficient of P.

We need the bound of Chang [5, Proposition 2.5] for the divisor function in number fields.

Lemma 2. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}$ of degree $d = [\mathbb{K} : \mathbb{Q}]$ and let $\mathbb{Z}_K$ be the ring of integers in $\mathbb{K}$. Let also $\gamma \in \mathbb{Z}_K$ be an algebraic integer of logarithmic height at most $H \geq 2$. Then the number of pairs (γ_1, γ_2) of algebraic integers $\gamma_1, \gamma_2 \in \mathbb{Z}_K$ of logarithmic height at most H with $\gamma = \gamma_1\gamma_2$ is at most $e^{O(H/\log H)}$, where the implied constant depends on d.*

We recall the following consequence of [8, Theorem 4.4] (see also [3]).

Lemma 3. *Let $P, Q \in \mathbb{Z}[Z]$ be two univariate nonzero polynomials with $Q \mid P$. If P is of logarithmic height at most $H \geq 1$ then Q is of logarithmic height at most $H + O(1)$, where the implied constant depends only on* $\deg P$.

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 $D \subseteq \mathbb{R}^n$. Recall that, for a lattice $\Gamma \subseteq \mathbb{R}^n$ and $i = 1, \ldots, n$, the *i-th successive minimum $\lambda_i(D, \Gamma)$ of the set D with respect to the lattice* Γ is defined as the minimal positive number λ such that the set λD contains i linearly independent vectors of the lattice Γ. Obviously, $\lambda_1(D, \Gamma) \leq \ldots \leq \lambda_n(D, \Gamma)$. We need the following result proven in [1, Proposition 2.1].

Lemma 4. *For any lattice Γ in $\mathbb{R}^n$ and any centrally symmetric convex body $D \subseteq \mathbb{R}^n$, we have*

$$|D \cap \Gamma)| \leq \prod_{i=1}^{n} \left(\frac{2i}{\lambda_i(D, \Gamma)} + 1 \right)$$

Corollary 2. *For any lattice Γ in $\mathbb{R}^n$ and any centrally symmetric convex body $D \subseteq \mathbb{R}^n$, we have*

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

where $(2n+1)!!$ stands for the product of all the odd natural numbers less than or equal to $2n+1$.

3 Proof of Theorem 1

Denote $X = |\mathcal{X}|$. Let ε be a small positive constant. We observe that it suffices to prove the theorem under the condition

$$\frac{h^{14}}{X^6} + \frac{h^{15}}{X^9} < \varepsilon p. \tag{2}$$

Indeed, if $X > \varepsilon h$, then the result follows from [3, Theorem 17]. Thus, we can assume that $X < \varepsilon h$. But then we can find $\mathcal{X}'$ such that $\mathcal{X} \subset \mathcal{X}' \subset [1,h] \cap \mathbb{Z}$ and $|\mathcal{X}'| = \lfloor X/\varepsilon \rfloor$. Hence, for $\mathcal{X}'$ we have that

$$\frac{h^{14}}{|\mathcal{X}'|^6} + \frac{h^{15}}{|\mathcal{X}'|^9} < \varepsilon p$$

and then we proceed with $\mathcal{X}'$ instead of $\mathcal{X}$. Thus, we can assume that (2) holds.

We can also assume that $L_4(p,\mathcal{X};s) > X^4 e^{C\frac{\log h}{\log\log h}}$, for a large constant $C > 0$ (as otherwise there is nothing to prove).

From (2) it follows that $h^6 < h^8 < \varepsilon p$. In particular, if $s \equiv 0 \pmod{p}$, then the congruence is converted to an equality with $s = 0$ and the contradiction follows from the bound for the divisor function. Thus, $s \not\equiv 0 \pmod{p}$.

From [3, Theorem 22], we see that the contribution to $L_4(p,\mathcal{X};s)$ from the set of solutions with $x_i = y_j$ for some $1 \le i,j \le 4$ is at most $X^4 e^{O(\log h/\log\log h)}$. Hence, since C is large, we can assume that the number J of solutions of the congruence

$$\prod_{i=1}^{4}(x_i + s) \equiv \prod_{j=1}^{4}(y_j + s) \not\equiv 0 \pmod{p}, \quad x_i, y_j \in \mathcal{X}. \tag{3}$$

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

subject to the condition

$$\{x_1, x_2, x_3, x_4\} \cap \{y_1, y_2, y_3, y_4\} = \emptyset \tag{4}$$

satisfies

$$J > X^4 e^{0.6C \frac{\log h}{\log\log h}}. \tag{5}$$

We follow the idea of the proof of [3, Theorem 22]. With any solution $\mathbf{x} = (x_1, x_2, x_3, x_4)$ and $\mathbf{y} = (y_1, y_2, y_3, y_4)$ of (3) subject to (4), we associate the polynomials

$$P_{\mathbf{x}}(Z) = \prod_{i=1}^{4}(Z + x_i) \quad \text{and} \quad P_{\mathbf{y}}(Z) = \prod_{i=1}^{4}(Z + x_i).$$

Denote

$$R_{\mathbf{x},\mathbf{y}}(Z) = P_{\mathbf{y}}(Z) - P_{\mathbf{x}}(Z).$$

Since $R_{\mathbf{x},\mathbf{y}}(s) \equiv 0 \pmod p$ and $h < p^{\frac{1}{8}}$, it follows that $R_{\mathbf{x},\mathbf{y}}(Z)$ is not a constant polynomial (as otherwise it is identically zero, which contradicts (4)). By the Dirichlet pigeonhole principle there exist x_1^* such that we have at least J/X solutions of (3) subject to (4) with the same $x_1 = x_1^*$. We claim that any polynomial R induced by these solutions occurs at most $e^{O(\log h/\log\log h)}$ times. Indeed, fix R and assume that $R = R_{\mathbf{x},\mathbf{y}}$. We have

$$R(-x_1^*) = R_{\mathbf{x},\mathbf{y}}(-x_1^*) = -(y_1 - x_1^*)(y_2 - x_1^*)(y_3 - x_1^*)(y_4 - x_1^*).$$

Since R is fixed, from the bound for the divisor function it follows that there are at most $e^{O(\log h/\log\log h)}$ possibilities for y_1, y_2, y_3, y_4. Once y_i are fixed, we have at most $e^{O(\log h/\log\log h)}$ possibilities for x_i and the claim follows.

It then follows that there are at least $X^3 e^{0.5C \frac{\log h}{\log\log h}}$ different polynomials $R_{\mathbf{x},\mathbf{y}}(Z)$. In other words, the congruence

$$us^3 + vs^2 + ws + t \equiv 0 \pmod p,$$

has at least $X^3 e^{0.5C \frac{\log h}{\log\log h}} > X^3 \log h$ solutions in integers u, v, w, t subject to

$$|u| \le 4h, \quad |v| \le 6h^2, \quad |w| \le 4h^3, \quad |t| \le h^4.$$

We define the lattice

$$\Gamma = \{(u, v, w, t) \in \mathbb{Z}^4 \colon us^3 + vs^2 + ws + t \equiv 0 \pmod p\}$$

and the convex body

$$D = \{(u,v,w,t) \in \mathbb{R}^4 \colon |u| \le 4h, \quad |v| \le 6h^2, \quad |w| \le 4h^3, \quad |t| \le h^4\}.$$

For the previously seen, we have that $|D \cap \Gamma| \ge X^3 \log h$. Therefore, by the Corollary 2, the successive minima $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1,2,3,4$, satisfy the inequality

$$\prod_{i=1}^{4} \min\{1, \lambda_i\} \ll (X^3 \log h)^{-1}. \tag{6}$$

Since h is sufficiently large, we have $\lambda_1 \le 1$. By the definition of λ_i, there are linearly independent vectors $(u_i, v_i, w_i, t_i) \in \lambda_i D \cap \Gamma$, $i = 1,2,3,4$. We have the following four cases.

Case 1: $\lambda_4 \le 1$. By the inequality (6), we have $\lambda_1\lambda_2\lambda_3\lambda_4 \ll (X^3 \log h)^{-1}$. We consider the determinant

$$\Delta = \det \begin{pmatrix} u_1 & v_1 & w_1 & t_1 \\ u_2 & v_2 & w_2 & t_2 \\ u_3 & v_3 & w_3 & t_3 \\ u_4 & v_4 & w_4 & t_4 \end{pmatrix}.$$

Since $(u_i, v_i, w_i, t_i) \in \lambda_i D \cap \Gamma$, we have that

$$|u_i| \le 4h\lambda_i, \quad |v_i| \le 6h^2\lambda_i, \quad |w_i| \le 4h^3\lambda_i, \quad |t_i| \le h^4\lambda_i.$$

Hence,

$$\Delta \ll \lambda_1\lambda_2\lambda_3\lambda_4 h^{10} \ll \frac{h^{10}}{X^3 \log h} = o(p)$$

as $p \to \infty$. We also have that

$$u_i s^3 + v_i s^2 + w_i s + t_i \equiv 0 \pmod p, \quad i = 1,2,3,4,$$

implying that $\Delta \equiv 0 \pmod p$. Thus, $\Delta = 0$, which contradicts the fact that (u_i, v_i, w_i, t_i), $i = 1,2,3,4$, are linearly independent vectors. Therefore, this case is impossible.

Case 2: $\lambda_3 \le 1$, $\lambda_4 > 1$. The argument we use in this case is based on the proof of [3, Lemma 15]. We have that $\lambda_1\lambda_2\lambda_3 \ll (X^3 \log h)^{-1}$. Since $(u_i, v_i, w_i, t_i) \in \Gamma$ for $i = 1,2,3$, it follows that

$$\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix} \begin{pmatrix} s^3 \\ s^2 \\ s \end{pmatrix} \equiv \begin{pmatrix} -t_1 \\ -t_2 \\ -t_3 \end{pmatrix} \pmod p. \tag{7}$$

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

Let

$$\Delta = \det\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}, \quad \Delta_1 = \det\begin{pmatrix} -t_1 & v_1 & w_1 \\ -t_2 & v_2 & w_2 \\ -t_3 & v_3 & w_3 \end{pmatrix}$$

$$\Delta_2 = \det\begin{pmatrix} u_1 & -t_1 & w_1 \\ u_2 & -t_2 & w_2 \\ u_3 & -t_3 & w_3 \end{pmatrix}, \quad \Delta_3 = \det\begin{pmatrix} u_1 & v_1 & -t_1 \\ u_2 & v_2 & -t_2 \\ u_3 & v_3 & -t_3 \end{pmatrix}.$$

Then

$$\Delta \ll \frac{h^6}{X^3 \log h}, \quad \Delta_i \ll \frac{h^{10-i}}{X^3 \log h}, \quad i = 1, 2, 3. \tag{8}$$

We note that

$$\Delta \not\equiv 0 \pmod p. \tag{9}$$

Otherwise, from the congruence (7) we get

$$\Delta \equiv \Delta_1 \equiv \Delta_2 \equiv \Delta_3 \equiv 0 \pmod p.$$

Then, by the estimates (8) it follows that

$$\Delta = \Delta_1 = \Delta_2 = \Delta_3 = 0.$$

This implies that the rank of the matrix

$$\begin{pmatrix} u_1 & v_1 & w_1 & t_1 \\ u_2 & v_2 & w_2 & t_2 \\ u_3 & v_3 & w_3 & t_3 \end{pmatrix}$$

is strictly less than 3, which is impossible since the vectors (u_i, v_i, w_i, t_i), $i = 1, 2, 3$, are linearly independent.

Thus, we have (9). Then, solving the system (7) we get

$$s^3 \equiv \frac{\Delta_1}{\Delta} \pmod p, \quad s^2 \equiv \frac{\Delta_2}{\Delta} \pmod p, \quad s \equiv \frac{\Delta_3}{\Delta} \pmod p. \tag{10}$$

From these we obtain that

$$\Delta_3^2 \equiv \Delta_2 \Delta \pmod p.$$

From (8) it follows that the absolute value of both sides of this congruence is less than $p/2$. Thus, this congruence is, in fact, an equality. Then

$$\Delta_3^2 = \Delta_2 \Delta.$$

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

Therefore, letting $d = \pm\gcd(\Delta_2, \Delta)$ for a suitable choice of the sign $\pm$, it follows that

$$\Delta_2 = da^2, \Delta = db^2, \Delta_3 = dab$$

for some relatively prime integers a and b. Substituting this in (10), we get

$$da^3 \equiv \Delta_1 b \pmod{p}.$$

Now, from (8) we see that

$$|da^3| = O\Big(\frac{h^{12}}{X^{4.5}}\Big) < \frac{p}{2} \quad \text{and} \quad |\Delta_1 b| = O\Big(\frac{h^{12}}{X^{4.5}}\Big) < \frac{p}{2}.$$

Therefore, we get the equality

$$da^3 = \Delta_1 b.$$

Since $\gcd(a, b) = 1$, it follows that $\Delta_1 = a^3 t$ and $d = bt$. Then we also have $\Delta = b^3 t$. Hence, from (8) we have

$$a \ll \frac{h^3}{X} \quad \text{and} \quad b \ll \frac{h^2}{X}. \tag{11}$$

Then, from $s \equiv \frac{\Delta_3}{\Delta} \equiv \frac{a}{b} \pmod{p}$, and from (11) we derive that

$$s \equiv \frac{a}{b} \pmod{p}.$$

Substituting this in (3)), we get that

$$(bx_1 + a) \cdots (bx_4 + a) - (by_1 + a) \cdots (by_4 + a) \equiv 0 \pmod{p}.$$

From (8) and the condition of the theorem it follows that the absolute value of the left-hand side is less than p. Therefore, we get the equality

$$(bx_1 + a) \cdots (bx_4 + a) = (by_1 + a) \cdots (by_4 + a).$$

We observe that $bx_i + a \neq 0$ (as otherwise, $x_i + a/b \equiv 0 \pmod{p}$ which contradicts (3)). Now, there are X^4 ways to fix (y_1, y_2, y_3, y_4), and for each of them the left-hand side can have at most $e^{O(\log h/\log\log h)}$ solutions in x_1, x_2, x_3, x_4. We obtain a contradiction for sufficiently large C.

Case 3: $\lambda_2 \le 1$, $\lambda_3 > 1$. In this case we have that $\lambda_1\lambda_2 \ll (X^3 \log h)^{-1}$. And we have two linearly independent vectors

$$\begin{gathered}(u_i, v_i, w_i, t_i) \in \lambda_i D \cap \Gamma \\ |u_i| \le 4\lambda_i h, \quad |v_i| \le 6\lambda_i h^2, \quad |w_i| \le 4\lambda_i h^3, \quad |t_i| \le \lambda_i h^4,\end{gathered}$$

for $i = 1, 2$. Consider the polynomials

$$R_i(Z) = u_i Z^3 + v_i Z^2 + w_i Z + t_i, \quad i = 1, 2.$$

Clearly, these are not constant polynomials, as otherwise $u_i = v_i = w_i = 0$, and then $t_i \equiv 0 \pmod p$ implying that $t_i = 0$ (recall that $|t_i| \le \lambda_i h^4 < p$).

Next, from $R_1(s) \equiv R_2(s) \equiv 0 \pmod p$ we also have that $\mathrm{Res}(R_1, R_2) \equiv 0 \pmod p$. We claim that, in fact, $\mathrm{Res}(R_1, R_2) = 0$. Indeed, if $\lambda_1 \le \lambda_2 < 1/(4h)$, then $u_1 = u_2 = 0$. Applying Lemma 1 with $m = 2$ and $\sigma = \vartheta = 1$, we get $\mathrm{Res}(R_1, R_2) \ll h^8$. Since $h^8 < \varepsilon p$ for a small positive constant ε, it follows that $|\mathrm{Res}(R_1, R_2)| < p$. This, together with $\mathrm{Res}(R_1, R_2) \equiv 0 \pmod p$, implies the claim.

If $\lambda_2 \ge 1/(4h)$, then we apply Lemma 1 with $m = 3$ and

$$\sigma = 1 + \tfrac{\log(6\lambda_1)}{\log h}, \quad \vartheta = 1 + \tfrac{\log(6\lambda_2)}{\log h} > 0.$$

Recalling that $\lambda_1\lambda_2 \ll X^{-3}$ we get

$$\mathrm{Res}(R_1, R_2) \ll \frac{h^{15}}{X^9}.$$

Since $h^{15}/X^9 < \varepsilon p$, we get that $|\mathrm{Res}(R_1, R_2)| < p$ and again the claim follows.

Thus, we have that $\mathrm{Res}(R_1, R_2) = 0$. In other words, the polynomials $R_1(Z)$ and $R_2(Z)$ have a common root, say β_0. Since $R_1(\beta_0) = 0$, it follows from Lemma 3 that at least one of the numbers $u_1\beta_0, v_1\beta_0, w_1\beta_0$ is a nonzero algebraic integer of logarithmic height $O(\log h)$. It then follows that $\beta_0 = \alpha_0/q$, where q is a positive integer, $q < h^3$, and α_0 is an algebraic integer of logarithmic height $O(\log h)$.

Now, given a solution $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) \in \mathcal{X}^8$ counted in J, we form the polynomial

$$R(Z) = \prod_{i=1}^{4}(Z + x_i) - \prod_{j=1}^{4}(Z + y_j).$$

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

Since $R(s) \equiv 0 \pmod p$, $R(Z)$ can not be a constant polynomial, as otherwise $R(Z)$ would be identically zero, which contradicts (4). We have that

$$R(Z) = UZ^3 + VZ^2 + WZ + T,$$
$$|U| \le 4h, \quad |V| \le 6h^2, \quad |W| \le 4h^3, \quad |T| \le h^4.$$

Hence, from $R(s) \equiv 0 \pmod p$ it follows that $(U, V, W, T) \in D \cap \Gamma$. Since $\lambda_3 > 1$, we get that (U, V, W, T) is a linear combination of (u_1, v_1, w_1, t_1) and (u_2, v_2, w_2, t_2). This implies that

$$R(Z) = r_1 R_1(Z) + r_2 R_2(Z), \tag{12}$$

for some $r_1, r_2 \in \mathbb{R}$.

It then follows that $R(\alpha_0/q) = R(\beta_0) = 0$, that is,

$$\prod_{i=1}^{4} (qx_i + \alpha_0) = \prod_{j=1}^{4} (qy_j + \alpha_0). \tag{13}$$

In particular, this equation has at least J solutions with $x_i, y_j \in \mathcal{X}$ and $x_i \ne y_j$. Hence, recalling (5), we see that there is a fixed tuple $(y_1, y_2, y_3, y_4) = (b_1, b_2, b_3, b_4) \in \mathcal{X}^4$ such that the equation

$$\prod_{i=1}^{4} (qx_i + \alpha_0) = \prod_{j=1}^{4} (qb_j + \alpha_0),$$

has at least

$$\frac{J}{X^4} \ge e^{0.5C \log h / \log\log h} \tag{14}$$

solutions in $(x_1, x_2, x_3, x_4) \in \mathcal{X}^4$ with $\{x_1, x_2, x_3, x_4\} \cap \{b_1, b_2, b_3, b_4\} = \emptyset$. In particular,

$$(b_1 + \beta_0)(b_2 + \beta_0)(b_3 + \beta_0)(b_4 + \beta_0) \ne 0.$$

We recall that $1 \le x_i \le h$, $1 \le q < h^3$, and α_0 is an algebraic integer of logarithmic height at most $O(\log h)$. From the simple properties of algebraic integers it follows that the numbers $qx_i + \alpha_0$ and $qb_j + \alpha_0$, as well as the numbers

$$\prod_{i=1}^{4} (qx_i + \alpha_0) \quad \text{and} \quad \prod_{j=1}^{4} (qb_j + \alpha_0),$$

are also algebraic integers; moreover they are the roots of polynomials from $\mathbb{Z}[X]$ whose coefficients are bounded (by absolute value) by $h^{O(1)}$. Hence, by Lemma 3, these numbers are of logarithmic height at most $O(\log h)$.

Therefore, by Lemma 2 we conclude that for a sufficiently large h the equation (13) has at most $e^{C_1 \log h/\log\log h}$ solutions with $x_i \in \mathcal{X}$, $i = 1, 2, 3, 4$. This contradicts (14) for C large enough.

Case 4: $\lambda_1 \le 1$, $\lambda_2 > 1$. Let $(u_1, v_1, w_1, t_1) \in \mathbb{Z}^4$ be the nonzero vector corresponding to λ_1. We know that

$$u_1 s^3 + v_1 s^2 + ws + t \equiv 0 \pmod p.$$

We consider the polynomial

$$R_1(Z) = u_1 Z^3 + v_1 Z^2 + w_1 Z + t_1.$$

As in the Case 3, we have that $R_1(Z)$ is a nonconstant polynomial. Given a solution $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4) \in \mathcal{X}^8$ counted in J, we consider the polynomial

$$R(Z) = \prod_{i=1}^{4}(Z + x_i) - \prod_{j=1}^{4}(Z + y_j).$$

Since $R(s) \equiv 0 \pmod p$, we see that $R(Z)$ is also a nonconstant polynomial (as otherwise it would be identically zero, contradicting (4)). As in the previous case, we write $R(Z)$ as

$$R(Z) = UZ^3 + VZ^2 + WZ + T,$$
$$|U| \le 4h, \quad |V| \le 6h^2, \quad |W| \le 4h^3, \quad |T| \le h^4.$$

From $R(s) \equiv 0 \pmod p$ it follows that $(U, V, W, T) \in D \cap \Gamma$. Since $\lambda_2 > 1$, the vectors (U, V, W, T) and (u_1, v_1, w_1, t_1) are linearly dependent. Thus, $R_1(Z)|R(Z)$ in $\mathbb{Q}[Z]$.

Since $R_1(Z)$ is nonconstant, it has a root β_0. Then β_0 is also a root of $R(Z)$. From this moment on, the proof proceeds as in the Case 3.

□

4 Proof of Corollary 1

Let $\mathcal{X}$ be the set of those $x \in \{s + 1, \dots, s + h\}$ for which $x \equiv ag^y \pmod{p)}$ for some $y \in \{s + 1, \dots, s + h\}$. We observe that $|\mathcal{X}| = J_{a,g}(s; h)$.

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

For each $(x_1, \ldots, x_4, y_1, \ldots, y_4) \in \mathcal{X}^8$ we have that

$$\frac{x_1x_2x_3x_4}{y_1y_2y_3y_4} \in \{g^t \pmod p \colon t \in [-4h+4, 4h-4]\}.$$

Hence, there exists $t = t_0 \in [-4h+4, 4h-4]$ such that the congruence

$$x_1x_2x_3x_4 \equiv g^{t_0}y_1y_2y_3y_4 \pmod p, \quad x_i, y_i \in \mathcal{X}$$

has at least $|\mathcal{X}|^8/(8h)$ solutions. From the well-known application of the Cauchy-Schwarz inequality, it follows that the congruence

$$x_1x_2x_3x_4 \equiv y_1y_2y_3y_4 \pmod p, \quad x_i, y_i \in \mathcal{X}$$

has at least $|\mathcal{X}|^8/(8h)$ solutions.

If

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} \geq p,$$

then the condition $h < p^{4/51}$ implies that $|\mathcal{X}| < h^{\frac{1}{4}}$ and the claim follows

Let

$$\frac{h^{14}}{|\mathcal{X}|^6} + \frac{h^{15}}{|\mathcal{X}|^9} < p.$$

Then by Theorem 1 we get that

$$\frac{|\mathcal{X}|^8}{8h} \leq |\mathcal{X}|^{4+o(1)}.$$

Hence $|\mathcal{X}| \leq h^{\frac{1}{4}+o(1)}$ and the result follows. □

References

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

[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] 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.

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.

[4] T. H. Chan and I. E. Shparlinski, 'On the concentration of points on modular hyperbolas and exponential curves', *Acta Arith.*, **142** (2010), 59–66.

[5] M.-C. Chang, 'Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems', *Geom. and Funct. Anal.*, **13** (2003), 720–736.

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

[7] M. Z. Garaev, 'On the logarithmic factor in error term estimates in certain additive congruence problems', *Acta Arith.* **124** (2006), 27–39.

[8] M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, Berlin, 1992.

[9] H. L. Montgomery, 'Distribution of small powers of a primitive root', *Advances in Number Theory* (Kingston, ON, 1991), Oxford Sci. Publ., Oxford University Press, New York, 1993, pp. 137–149.

2 May 2019 15:42:17 PDT
Version 2 - Submitted to Acta Arith.