Bull. Aust. Math. Soc. **93** (2016), 364–371
doi:10.1017/S0004972715001240

SYSTEMS OF CONGRUENCES WITH PRODUCTS OF VARIABLES FROM SHORT INTERVALS

IGOR E. SHPARLINSKI

(Received 29 July 2015; accepted 6 August 2015; first published online 11 November 2015)

Abstract

We obtain an upper bound for the number of solutions to the system of m congruences of the type

$$\prod_{i=1}^{\nu}(x_i + s_i) \equiv \lambda_j \pmod p \quad j = 1, \ldots, m,$$

modulo a prime p, with variables $1 \le x_i \le h$, $i = 1, \ldots, \nu$ and arbitrary integers s_j, λ_j, $j = 1, \ldots, m$, for a parameter h significantly smaller than p. We also mention some applications of this bound.

2010 *Mathematics subject classification*: primary 11D79; secondary 11L40.

Keywords and phrases: multiplicative congruences, resultant, common roots.

1. Introduction

For a prime p, let $\mathbb{F}_p$ be the field of p elements and $\mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$. For positive integers h, m and ν and m-dimensional vectors

$$\mathbf{s} = (s_1, \ldots, s_m), \qquad \boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_m) \in \mathbb{F}_p^m,$$

we denote by $J_\nu(h, \mathbf{s}, \boldsymbol{\lambda})$ the number of solutions to the system of congruences

$$\begin{gathered}\prod_{i=1}^{\nu}(x_i + s_j) \equiv \lambda_j \pmod p \quad j = 1, \ldots, m, \\ 1 \le x_1, \ldots, x_\nu \le h.\end{gathered} \tag{1.1}$$

Similarly, we denote by $K_\nu(h, \mathbf{s})$ the number of solutions to the symmetric system of congruences

$$\begin{gathered}\prod_{i=1}^{\nu}(x_i + s_j) \equiv \prod_{i=1}^{\nu}(y_i + s_j) \not\equiv 0 \pmod p \quad j = 1, \ldots, m, \\ 1 \le x_1, y_1, \ldots, x_\nu, y_\nu \le h.\end{gathered} \tag{1.2}$$

Note that if zero values are allowed then we may have at least $h^{2\nu-2}$ solutions, while we are most interested in the cases with almost 'diagonal' behaviour.

For $m = 1$, this and several similar congruences have been studied in [4–6], where one can also find various applications of these bounds. For example, by [4, Lemma 33], if $\nu \geq 1$, $m = 1$, $\mathbf{s} = s \in \mathbb{F}_p$ and $\boldsymbol{\lambda} = \lambda \in \mathbb{F}_p^*$, then for

$$h \leq p^{1/(\nu^2-1)} \tag{1.3}$$

we have

$$J_\nu(h, s, \lambda) \leq \exp(c(\nu) \log h / \log\log h), \tag{1.4}$$

where $c(\nu)$ depends only on ν.

For the symmetric system (1.2) with $\nu \geq 3$, the bound

$$K_\nu(h, s) \leq h^\nu \exp(c(\nu) \log h / \log\log h), \tag{1.5}$$

is given in [5, Theorem 17] in a slightly wider range

$$h \leq p^{\gamma_\nu}, \tag{1.6}$$

where

$$\gamma_\nu = \min\left\{\frac{1}{\nu^2 - 2\nu - 2}, \frac{1}{\nu^2 - 3\nu + 4}\right\}.$$

Some generalisations to single multiplicative congruences with polynomials instead of linear functions have been considered in [8, 10, 15]. Note that the bounds (1.4) and (1.5) can be extended to arbitrary h by splitting the interval $[1, h]$ into several smaller intervals satisfying (1.3) and (1.6), respectively: see the formulation and proof of Theorem 2.1 below.

2. Main result

Most of the above results are based on careful estimates of the resultants of some auxiliary polynomials associated with solutions to the corresponding congruences. The goal of this paper is to show that the approach can be combined with a result of Gómez-Pérez *et al.* [7] and can lead to more relaxed restrictions on h in the case of systems of m congruences.

We do this in the simplest cases of the system of congruences (1.1) and show that for $m \geq 2$ the restriction (1.3) on h can be relaxed.

As in [4, 5], we note that, for large values of h, one can use standard methods, based on bounds of exponential and multiplicative character sums to obtain various asymptotic formulas for $J_\nu(h, \mathbf{s}, \boldsymbol{\lambda})$. However, we are mostly interested in small values of h beyond the reach of these methods. On the other hand, for large values of ν there is a wide gap between the values of h, which are covered by these two approaches. Our result narrows this gap when m is large. For some values of m, the ranges of both approaches overlap and thus we have nontrivial results for all values of h.

https://doi.org/10.1017/S0004972715001240 Published online by Cambridge University Press

We define the following sets of vectors

$$\begin{aligned}\mathcal{S}_m &= \{\mathbf{s} = (s_1, \ldots, s_m) \in \mathbb{F}_p^m : s_j \neq s_k, 1 \le j < k \le m\},\\ \Lambda_m &= \{(\lambda_1, \ldots, \lambda_m) \in \mathbb{F}_p^m : \lambda_j \neq 0, 1 \le j \le m\}.\end{aligned}$$

For integers $\nu \ge 2$ and $m \ge 1$ we also define

$$\vartheta_{\nu,m} = \min\left\{\frac{\nu m}{\nu^2 - 1}, 1\right\}. \tag{2.1}$$

THEOREM 2.1. *Let $\nu \ge 2$ and $m \ge 1$ be fixed integers and let $\vartheta_{\nu,m}$ be given by (2.1). Then, uniformly over $\mathbf{s} \in \mathcal{S}_m$ and $\boldsymbol{\lambda} \in \Lambda_m$, we have the bound*

$$J_\nu(h, \mathbf{s}, \boldsymbol{\lambda}) \le (h^\nu p^{-\vartheta_{\nu,m}} + 1) \exp(c(\nu) \log h / \log\log h),$$

where $c(\nu)$ depends only on ν.

We now immediately derive the following corollary.

COROLLARY 2.2. *In the notation of Theorem 2.1, uniformly over $\mathbf{s} \in \mathcal{S}_m$,*

$$K_\nu(h, \mathbf{s}) \le (h^\nu p^{-\vartheta_{\nu,m}} + 1) h^\nu \exp(c(\nu) \log h / \log\log h).$$

3. Applications to character sums

Let $\mathcal{X}$ be the set of all $p - 1$ multiplicative characters of $\mathbb{F}_p^*$. We refer to [11, Ch. 3] for background on multiplicative characters. Given m-dimensional vectors

$$\mathbf{s} = (s_1, \ldots, s_m) \in \mathbb{F}_p^m \quad \text{and} \quad \boldsymbol{\chi} = (\chi_1, \ldots, \chi_m) \in \mathcal{X}^m,$$

we consider the character sums

$$T(h, \mathbf{s}, \boldsymbol{\chi}) = \sum_{x=1}^{h} \prod_{j=1}^{m} \chi_j(x + s_j).$$

One can easily show that if at least one of the characters $\chi_1, \ldots, \chi_m$ is nonprincipal then, for $\mathbf{s} \in \mathcal{S}_m$,

$$T(h, \mathbf{s}, \boldsymbol{\chi}) = O(p^{1/2} \log p), \tag{3.1}$$

where the implied constant depends only on m. Indeed, the bound (3.1) follows instantly from the Weil bound of hybrid sums of multiplicative and additive characters in its classical form given in [17, Example 12 of Appendix 5] and the standard reduction between bounds of complete and incomplete sums (see, for example, [11, Section 12.2]). Clearly, for (3.1) to be nontrivial, one needs $h \ge p^{1/2+\varepsilon}$ with some fixed $\varepsilon > 0$. For $m = 1$, the Burgess bound (see [11, Theorem 12.6]) gives a nontrivial result already for $h \ge p^{1/4+\varepsilon}$. For shorter sums, only bounds on average are known. Define

$$\mathfrak{T}_\nu(h, \mathbf{s}) = \frac{1}{(p-1)^m} \sum_{\boldsymbol{\chi} \in \mathcal{X}^m} |T(h, \mathbf{s}, \boldsymbol{\chi})|^{2\nu}.$$

https://doi.org/10.1017/S0004972715001240 Published online by Cambridge University Press

As an example, for $\nu = 2$ and $m = 1$, Ayyad *et al.* [2, Theorem 2] have shown that

$$\mathfrak{T}_2(h, s) = O(h^4/p + h^2(\log p)^2)$$

for arbitrary $h < p$. For $\nu \geq 3$ and $m = 1$ and using the orthogonality of multiplicative characters, as in the proof of Theorem 3.1 below, one can also reformulate (1.5) as the bound

$$y\,\mathfrak{T}_\nu(h, s) = h^\nu \exp(c(\nu) \log h/\log\log h),$$

provided that h satisfies (1.6). We obtain the following improved bound for arbitrary $m \geq 1$ and $\nu \geq 2$.

Theorem 3.1. *Let $\nu \geq 2$ and $m \geq 1$ be fixed integers and let $\vartheta_{\nu,m}$ be given by (2.1). Then, uniformly over $\mathbf{s} \in \mathcal{S}_m$, we have the bound*

$$\mathfrak{T}_\nu(h, \mathbf{s}) \leq (h^\nu p^{-\vartheta_{\nu,m}} + 1)h^\nu \exp(c(\nu) \log h/\log\log h).$$

In particular, for $h \leq p^{\vartheta_{\nu,m}/\nu+o(1)}$ the bounds of Theorem 2.1, Corollary 2.2 and Theorem 3.1 become, respectively,

$$J_\nu(h, \mathbf{s}, \boldsymbol{\lambda}) \leq h^{o(1)}, \quad K_\nu(h, \mathbf{s}) \leq h^{\nu+o(1)} \quad \text{and} \quad \mathfrak{T}_\nu(h, \mathbf{s}) \leq h^{\nu+o(1)}.$$

4. Preparations

We need the following bound of the resultant Res(P, Q) with restricted coefficients, which is given by [4, Corollary 32].

Lemma 4.1. *Let $H \geq 1$ and let $2 \leq k, \ell \leq \nu$ be fixed integers. Let $P(Z)$ and $Q(Z)$ be polynomials*

$$P_1(Z) = \sum_{i=0}^{k-1} a_i Z^i \quad \textit{and} \quad P_2(Z) = \sum_{i=0}^{\ell-1} b_i Z^i$$

such that

$$a_{k-1}, b_{\ell-1} \neq 0 \quad \textit{and} \quad |a_i|, |b_i| < H^{\nu-i} \quad i = 0, \ldots, \nu-1.$$

Then

$$|\mathrm{Res}(P_1, P_2)| \leq C(\nu) H^{\nu^2-1},$$

where $C(\nu)$ depends only on ν.

Our second result is a generalisation of the well know fact that if two univariate polynomials $f(X), g(X) \in \mathbb{Z}[X]$ have a common zero modulo p then their resultant Res(f, g) is divisible by p. We need the following extension of this property, due to Gómez-Pérez *et al.* [7], to polynomials with several common roots modulo a prime p. We use $\overline{\mathbb{F}}_p$ to denote the algebraic closure of $\mathbb{F}_p$.

Lemma 4.2. *Let p be a prime and let $f, g \in \mathbb{Z}[X]$ be two polynomials whose reductions modulo p have N common roots in $\overline{\mathbb{F}}_p$ counted with multiplicities. Then $p^N \mid$ Res(f, g).*

We remark that, for our applications, the result of [12, Lemma 5.3] (which counts only simple roots) is sufficient.

https://doi.org/10.1017/S0004972715001240 Published online by Cambridge University Press

5. Proof of Theorem 2.1

We define $\alpha_{1,m} = 1$ and also, for $\nu \geq 2$,

$$\alpha_{\nu,m} = \vartheta_{\nu,m}/\nu = \min\left\{\frac{m}{\nu^2-1}, \frac{1}{\nu}\right\}.$$

We follow quite closely the proof of [4, Lemma 33]. Let $\varepsilon < 1$ be a sufficiently small positive number, to be chosen later. Cover the interval $[1, h]$ by at most $\varepsilon^{-1}hp^{-\alpha_{\nu,m}} + 1$ intervals of length at most $H = \varepsilon p^{\alpha_{\nu,m}}$. Then for some collection $\mathcal{I}_1, \ldots, \mathcal{I}_\nu$ of these intervals, we have the bound

$$J_\nu(h, \mathbf{s}, \lambda) \leq (\varepsilon^{-1}hp^{-\alpha_{\nu,m}} + 1)^\nu J^*, \tag{5.1}$$

where J^* is the number of solutions to the system of congruences

$$\begin{gathered}\prod_{i=1}^{\nu}(x_i + s_i) \equiv \lambda_j \pmod p \quad j = 1, \ldots, m,\\ x_1 \in \mathcal{I}_1, \ldots, x_\nu \in \mathcal{I}_\nu.\end{gathered} \tag{5.2}$$

Hence, we see from (5.1) that it suffices to prove the bound

$$J^* \leq \exp(c^*(\nu)\log h/\log\log h), \tag{5.3}$$

where $c^*(\nu)$ depends only on ν.

The claim is trivial for $\nu = 1$ and we prove it for $\nu \geq 2$ by induction on ν.

We can assume that $J^* > \nu!$ as otherwise there is nothing to prove. In particular, we can fix two solutions $(x_1, \ldots, x_\nu) = (a_1, \ldots, a_\nu)$ and $(x_1, \ldots, x_\nu) = (b_1, \ldots, b_\nu)$ to (5.2) such that

$$P_0(Z) = (a_1 + Z)\ldots(a_\nu + Z) - (b_1 + Z)\ldots(b_\nu + Z)$$

is a nonzero polynomial.

By the induction hypothesis, the set $(x_1, \ldots, x_\nu)$ of solutions to the system of congruences (5.2) for which $x_i \in \{b_1, \ldots, b_\nu\}$ for some i, contributes to J^* at most

$$\nu^2 \exp\left(c(\nu-1)\frac{\log h}{\log\log h}\right) \leq \exp\left(\frac{c(\nu)}{2}\,\frac{\log h}{\log\log h}\right),$$

provided that h is large enough (and $c(\nu) > 2c(\nu-1)$).

Consider now the set $\mathcal{P}$ of polynomials of the form

$$P(Z) = (x_1 + Z)\ldots(x_\nu + Z) - (b_1 + Z)\ldots(b_\nu + Z),$$

where $(x_1, \ldots, x_\nu)$ runs through the set of all solutions to the congruence (5.2) such that

$$\{x_1, \ldots, x_\nu\} \cap \{b_1, \ldots, b_\nu\} = \emptyset. \tag{5.4}$$

We note that each such polynomial $P(Z)$ is nonzero and has the form

$$P(Z) = A_1 Z^{\nu-1} + \cdots + A_{\nu-1}Z + A_\nu,$$

https://doi.org/10.1017/S0004972715001240 Published online by Cambridge University Press

with

$$|A_i| \le c_0(\nu) H^i \quad i = 1, \dots, \nu,$$

where $c_0(\nu)$ depends only on ν. In particular, since $P(s_1) \equiv 0 \pmod p$, it follows that $P(Z)$ is not a constant polynomial. Indeed, if $P(Z) = c \in \mathbb{Z}$, then $A_\nu = P(0) = c \equiv P(s_1) \equiv 0 \pmod p$. Now, since

$$|A_\nu| \le c_0(\nu) H^\nu < p$$

for a sufficiently small $\varepsilon > 0$, we conclude that $c = A_\nu = 0$. However, (5.4) implies that P is a nonzero polynomial.

Since we have $P(s_j) \equiv 0 \pmod p$, $j = 1, \dots, m$, for every $P \in \mathcal{P}$ (in particular, for $P = P_0$), we see from Lemma 4.2, and the pairwise distinctness of $s_1, \dots, s_m$, that the resultant $\mathrm{Res}(P, P_0)$ satisfies

$$p^m \mid \mathrm{Res}(P, P_0). \tag{5.5}$$

On the other hand, from Lemma 4.1,

$$|\mathrm{Res}(P, P_0)| \le C_0(\nu) H^{\nu^2 - 1},$$

with come constant $C_0(\nu)$ that depends only on ν. Therefore, taking $\varepsilon < C_0(\nu)^{-1/(\nu^2-1)}$ we have $|\mathrm{Res}(P, P_0)| < p$, which in view of (5.5) implies that $\mathrm{Res}(P, P_0) = 0$.

The rest of the proof follows that of [4, Lemma 33] without any changes and implies (5.3) and thus the desired result.

6. Proof of Theorem 3.1

Using the orthogonality of multiplicative characters

$$\sum_{\chi \in \mathcal{X}} \chi(u) = \begin{cases} 0 & \text{if } u \ne 1, \\ 1 & \text{if } u = 1, \end{cases} \qquad u \in \mathbb{F}_p^*,$$

we write $K_\nu(h, \mathbf{s})$ as the following character sum

$$K_\nu(h, \mathbf{s}) = \frac{1}{(p-1)^m} \sum_{x_1, y_1, \dots, x_\nu, y_\nu = 1}^{h} \prod_{j=1}^{m} \sum_{\chi_j \in \mathcal{X}} \chi_j\Big(\prod_{i=1}^{\nu} (x_i + s_j)\Big) \overline{\chi}_j\Big(\prod_{i=1}^{\nu} (y_i + s_j)\Big),$$

where $\overline{\chi}$ denotes the complex conjugate character of χ (thus $\chi(u^{-1}) = \overline{\chi}(u)$ for $u \in \mathbb{F}_p^*$). Changing the order of summations, we obtain

$$\begin{aligned} K_\nu(h, \mathbf{s}) &= \frac{1}{(p-1)^m} \sum_{x_1, y_1, \dots, x_\nu, y_\nu = 1}^{h} \sum_{\chi_1, \dots, \chi_m \in \mathcal{X}} \prod_{j=1}^{m} \prod_{i=1}^{\nu} (\chi_j(x_i + s_j) \overline{\chi}_j(y_i + s_j)) \\ &= \frac{1}{(p-1)^m} \sum_{\chi_1, \dots, \chi_m \in \mathcal{X}} \sum_{x_1, y_1, \dots, x_\nu, y_\nu = 1}^{h} \prod_{i=1}^{\nu} \prod_{j=1}^{m} (\chi_j(x_i + s_j) \overline{\chi}_j(y_i + s_j)) \\ &= \frac{1}{(p-1)^m} \sum_{\chi_1, \dots, \chi_m \in \mathcal{X}} |T(h, \mathbf{s}, \chi)|^{2\nu} = \mathfrak{T}_\nu(h, \mathbf{s}). \end{aligned}$$

Applying Corollary 2.2, we conclude the proof.

https://doi.org/10.1017/S0004972715001240 Published online by Cambridge University Press

7. Comments

We note that one of the natural interpretations of Theorem 3.1 is as a bound on average on multidimensional correlations of vectors

$$(\chi(s+1),\dots,\chi(s+h)) \in \mathbb{C}^h, \tag{7.1}$$

formed by m distinct pairs $(\chi, s) = (\chi_j, s_j)$, $j = 1,\dots,m$, taken over $(\chi_1,\dots,\chi_m) \in \mathcal{X}^m$. Similar correlations of (7.1) for a fixed χ but on average over $(s_1,\dots,s_m) \in \mathcal{S}_m$ have also been studied by Lamzouri [13]. We also remark that the vectors (7.1) have frequently been recommended as sources of pseudorandom numbers (see [1, 9, 14, 16] and references therein), where some of the measures of pseudorandomness are very similar to the sums $T(h, \mathbf{s}, \chi)$.

It is also natural to attempt to improve the bound of Corollary 2.2 by estimating $K_\nu(h, \mathbf{s})$ directly via an extension of the arguments from [5] (rather than via the reduction to bounds on $J_\nu(h, \mathbf{s}, \boldsymbol{\lambda})$). However, this may require nontrivial technical effort and possibly new ideas.

Finally, we recall that Bourgain and Garaev [3] have recently obtained a series of results for congruences with inverses from short intervals. The approach of [3] can also be combined with our argument and so one can obtain new bounds on the number of solutions to the following system of congruences with reciprocals

$$\sum_{i=1}^{\nu} \frac{1}{x_i + s_i} \equiv \lambda_j \pmod p \qquad j = 1,\dots,m,$$
$$1 \le x_1,\dots,x_\nu, \le h,$$

and similar symmetric congruences.

References

[1] R. Ahlswede, C. Mauduit and A. Sárközy, 'Large families of pseudorandom sequences of k symbols and their complexity I', in: *General Theory of Information Transfer and Combinatorics*, Lecture Notes in Computer Science, 4123 (Springer, Berlin, 2006), 293–307.

[2] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean values of character sums', *J. Number Theory* **59** (1996), 398–413.

[3] J. Bourgain and M. Z. Garaev, 'Sumsets of reciprocals in prime fields and multilinear Kloosterman sums', *Izv. Math.* **78** (2014), 656–707.

[4] 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.

[5] J. Bourgain, M. Z. Garaev, S. V. Konyagin and and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Inst. Math.* **280** (2013), 67–96.

[6] J. Bourgain, M. Z. Garaev, S. V. Konyagin and and I. E. Shparlinski, 'Multiplicative congruences with variables from short intervals', *J. d'Anal. Math.* **124** (2014), 117–147.

[7] D. Gómez-Pérez, J. Gutierrez, A. Ibeas and D. Sevilla, 'Common factors of resultants modulo p', *Bull. Aust. Math. Soc.* **79** (2009), 299–302.

[8] D. Gómez-Pérez and I. E. Shparlinski, 'Subgroups generated by rational functions in finite fields', *Monatsh. Math.* **176** (2015), 241–253.

[9] P. Hubert, C. Mauduit and A. Sárközy, ‘On pseudorandom binary lattices’, *Acta Arith.* **125** (2006), 51–62.

[10] G. Ivanyos, M. Karpinski, M. Santha, N. Saxena and and I. E. Shparlinski, ‘Polynomial interpolation and identity testing from high powers over finite fields’, Preprint, 2015, arXiv:1502.06631.

[11] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).

[12] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications* (Cambridge University Press, Cambridge, 1999).

[13] Y. Lamzouri, ‘The distribution of short character sums’, *Math. Proc. Cambridge Philos. Soc.* **155** (2013), 207–218.

[14] L. Mérai, ‘Construction of pseudorandom binary lattices based on multiplicative characters’, *Period. Math. Hungar.* **59** (2009), 43–51.

[15] I. E. Shparlinski, ‘Polynomial values in small subgroups of finite fields’, *Rev. Mat. Iberoam.*, to appear.

[16] V. Tóth, ‘Extension of the notion of collision and avalanche effect to sequences of k symbols’, *Period. Math. Hungar.* **65** (2012), 229–238.

[17] A. Weil, *Basic Number Theory* (Springer, New York, 1974).

IGOR E. SHPARLINSKI, Department of Pure Mathematics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

https://doi.org/10.1017/S0004972715001240 Published online by Cambridge University Press