On the concentration of points of polynomial maps and applications

Javier Cilleruelo
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and
Departamento de Matemáticas
Universidad Autónoma de Madrid
28049, Madrid, España
franciscojavier.cilleruelo@uam.es

Moubariz Z. Garaev
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
garaev@matmor.unam.mx

Alina Ostafe
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
alina.ostafe@mq.edu.au

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

January 26, 2011

Abstract

For a polynomial $f \in \mathbb{F}_p[X]$, we obtain an upper bound on the number of points $(x, f(x))$ modulo a prime p which belong to an arbitrary square with the side length H. Our results is based on the Vinogradov mean value theorem. Using these estimates we obtain results on the expansion of orbits in dynamical systems generated by nonlinear polynomials and we obtain an asymptotic formula for the number of visible points on the curve $f(x) \equiv y \pmod p$, where $f \in \mathbb{F}_p[X]$ is a polynomial of degree $d \geq 2$. We also use some recent results and techniques from arithmetic combinatorics to study the values $(x, f(x))$ in more general sets.

Mathematical Subject Classification: 11B50, 37A45

Keywords: polynomial congruences, Vinogradov mean value theorem, additive combinatorics, orbits, visible points

1 Introduction

For a prime p, let $\mathbb{F}_p$ denote the finite field with p elements, which we always assume to be represented by the set $\{0, \ldots, p-1\}$.

Given a polynomial $f \in \mathbb{F}_p[X]$ of degree $d \geq 2$, a positive integer $H < p$ and integers K, L, we define by $N(H; K, L)$ the number of solutions to the congruence

$$f(x) \equiv y \pmod p \tag{1}$$

with

$$(x, y) \in [K+1, K+H] \times [L+1, L+H]. \tag{2}$$

Using a standard technique and the Weil bound on incomplete Kloosterman sums one can easily obtain the asymptotic formula

$$N(H; K, L) = \frac{H^2}{p} + O\left(p^{1/2}(\log p)^2\right). \tag{3}$$

where the implied constant depends only on d, see [7] for various generalisations of this estimate. It is clear that the main term is dominated by the error term for $H \leq p^{3/4} \log p$ and for $H \leq p^{1/2}(\log p)^2$ the result becomes weaker than the trivial upper bound $N(H;K,L) \le H$. Here we use a different approach and give a nontrivial estimate of $N(H;K,L)$ for any value of $H \le p$. We note that a nontrivial bound on the number of solutions (x,y) to congruences

$$xy \equiv a \pmod p \tag{4}$$

and

$$g^x \equiv y \pmod p, \tag{5}$$

satisfying (2) have been given in [4] and then has been improved in [5].

Here we use the approach of [5], combined with estimates on the *Vinogradov mean value* theorem (see [10, 11, 18] to estimate $N(H;K,L)$.

Further we consider some generalisations of the original problem. As usual, for two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$, we also employ the notation

$$\mathcal{A}+\mathcal{B} = \{a+b \ : \ a \in \mathcal{A}, b \in \mathcal{B}\}. \qquad \text{and} \qquad \mathcal{A}\cdot\mathcal{B} = \{ab \ : \ a \in \mathcal{A}, b \in \mathcal{B}\}.$$

We say that a set $\mathcal{I} \subseteq \mathbb{F}_p$ is an *almost interval* if

$$\#\left(\mathcal{I}+\mathcal{I}\right) = \left(\#\mathcal{I}\right)^{1+o(1)}.$$

Furthermore, for two almost intervals $\mathcal{I}$ and $\mathcal{J}$ we call the set $\mathcal{I} \times \mathcal{J}$ and almost box.

We consider the following two modifications of the congruence (1). For two almost intervals $\mathcal{I}$ and $\mathcal{J}$ we denote by $M(\mathcal{I},\mathcal{J})$ the number of solutions to

$$f(x) \equiv y \pmod p \tag{6}$$

in the almost box $\mathcal{I} \times \mathcal{J}$, that is, with $x \in \mathcal{I}$ and $y \in \mathcal{J}$.

We now obtain an upper bound on $M(\mathcal{I},\mathcal{J})$ using the approach of [4] combined with recent results from additive combinatorics due to Bukh and Tsimerman [3].

As usual, for a set $\mathcal{A} \subseteq \mathbb{F}_p$ and a rational function $F \in \mathbb{F}_p[X]$ we define the set

$$F(\mathcal{A}) = \{F(a) \ : \ a \in \mathcal{A}, \ a \text{ is not a pole of } F\}.$$

Also for two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$, we also employ the notation

$$\mathcal{A}+\mathcal{B} = \{a+b \ : \ a \in \mathcal{A}, b \in \mathcal{B}\} \qquad \text{and} \qquad \mathcal{A}\mathcal{B} = \{a+b \ : \ a \in \mathcal{A}, b \in \mathcal{B}\}.$$

In [4], a lower bound on $\max\{\#(\mathcal{A}+\mathcal{A}), \#(\mathcal{A}^{-1}+\mathcal{A}^{-1})\}$, due to Bourgain [2, Theorem 4.1], has been used. Here we apply a similar argument, but we use a bound of [3] on $\max\{\#(\mathcal{A}+\mathcal{A}), \#(f(\mathcal{A})+f(\mathcal{A})\}$ instead. This estimate is also complemented by an estimate obtained via the method of Garaev [6] that appears to be new and can be of independent interest.

We give two applications of our results.

First we consider orbits of the dynamical system generated by $f \in \mathbb{F}_p[X]$, that is, sequences

$$u_0 = u, \qquad u_n = f(u_{n-1}), \quad n = 1, 2, \ldots, \tag{7}$$

with some initial value $u \in \mathbb{F}_p$. Clearly, any such sequence becomes eventually periodic, so we denote by T_u the orbit length, that is, T_u be the smallest positive integer T with

$$\{u_n \ : \ n = 0, \ldots, T-1\} = \{u_n \ : \ n = 0, 1, \ldots\}.$$

Given an initial value $u \in \mathbb{F}_p$ we consider how far the sequence (7) propagates in N steps, that is, we study

$$L_u(N) = \max_{0 \le n \le N} |u_n - u|.$$

It has been shown in [8], that

$$L_u(N) = p^{1+o(1)} \tag{8}$$

provided that $N \ge p^{1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ (in fact a smilar statement is given for orbits of iterations of arbitrary rational functions). Here we obtain a lower bound for essentially arbitrary values of N and T_u. It is based on similar arguments as those used in [8] for orbits of iterations of linear rational functions.

Second, for a given polynomial $f \in \mathbb{F}_p[X]$ of degree $d \ge 2$, we also answer a question posed in [17] by giving a formula for the number of solutions to (1) in a given box $(x, y) \in [1, X] \times [1, Y]$ for real $1 \le X, Y \le p$, with the additional condition $\gcd(x, y) = 1$. Such points are called visible points as they are exactly those points of the lattice $\mathbb{Z}^2$ that are not obstructed by other integers points for an observer place at the origin $(0, 0)$. In particular, we denote

$$\mathcal{V}(X, Y) = \#\{(x, y) \in [1, X] \times [1, Y] \ : \ f(x) \equiv y \pmod p, \ \gcd(x, y) = 1\}.$$

In [17] an asymptotic formula for the number of solutions to the more general congruence $F(x, y) \equiv a \pmod p$ with an absolutely irreducible polynomial

$F \in \mathbb{F}_p[X, Y]$ is given, however only on average over $a \in \mathbb{F}_p$ (as well as some results on average over p). Obtaining, "individual" estimates, even in the case of $F(x, y) = f(x) - y$ has been posed in [17] as an open problem, which we are now able to address.

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \le cV$ holds with some constant $c > 0$. Throughout the paper, any implied constants in these symbols may occasionally depend, where obvious, on $d = \deg f$, but are absolute otherwise.

2 Main Results

2.1 Points on polynomial curves in small boxes

As usual for positive integers k, d and H we denote by $J_{k,d}(H)$ the number of solutions to the system of equations

$$x_1^\nu + \ldots + x_k^\nu = x_{k+1}^\nu + \ldots + x_{2k}^\nu, \quad \nu = 1, \ldots, d,$$

in positive integers $x_1, \ldots, x_{2k} \le H$.

We denote by $\kappa(d)$ the smallest integer κ such that for $k \ge \kappa$ there exists a constant $C(k, d)$ depending only on k and d and such that the bound

$$J_{k,d}(H) \le C(k, d) H^{2k - d(d+1)/2 + o(1)}$$

holds as $H \to \infty$.

The classical result of Hua [10, Theorem 15] on the Vinogradov mean value theorem implies that for $d \ge 11$

$$\kappa(d) \le \left\lfloor d^2(3 \log d + \log\log d + 4) \right\rfloor - 11,$$

see also [18, Theorem 7.4]. Furthermore, explicit numerical estimates on $\kappa(d)$ for $2 \le d \le 10$ can be found in [10, Chapter IV] By a very recent striking result of Wooley [19, Theorem 1.1] we have

$$\kappa(d) \le d(d + 1)$$

for any $d \ge 2$.

Theorem 1. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. Then for any positive integer $H < p$, uniformly over arbitrary integers K and L, we have*

$$N(H; K, L) \ll H(H/p)^{1/2\kappa(d)+o(1)} + H^{1-(d-1)/2\kappa(d)+o(1)}.$$

Proof. We can assume that, say, $H < p^{3/4}$ as otherwise the result follows from (3).

Making a change of variables, we can also assume that $K = L = 0$.

Let $\mathcal{X}$ be the set of x satisfying (1) and (2) (with $K = L = 0$). In particular, $N(H; 0, 0) = \#\mathcal{X}$. Then, for any integer $k \geq 1$ and any $x_1 \ldots, x_{2k} \in \mathcal{X}$, we have

$$f(x_1) + \ldots + f(x_k) - f(x_{k+1}) - \ldots - f(x_{2k}) \equiv z \pmod p \qquad (9)$$

for some $z \in [-kH, kH]$. In particular, there is $u \in [-kH, kH]$ such that

$$N(H; 0, 0)^{2k} \leq (2kH + 1)T_k(u; H), \qquad (10)$$

where $T_k(z; H)$ is the number of solutions to (9) in $1 \leq x_1 \ldots, x_{2k} \leq H$.

Writing

$$\lambda_i = x_1^j + \ldots + x_k^j - x_{k+1}^j - \ldots - x_{2k}^j, \qquad j = 1, \ldots, d, \qquad (11)$$

we see that $\lambda_j \in [-kH^j, kH^j]$.

For each of $O(H^{d(d-1)/2})$ choices of

$$(\lambda_1, \ldots, \lambda_{d-1}) \in [-kH, kH] \times \ldots [-kH^{d-1}, kH^{d-1}],$$

we see that for any solution to (9) we have

$$\lambda_d \equiv \lambda \pmod p$$

for some λ depending only on z and $\lambda_1, \ldots, \lambda_{d-1}$. Therefore λ_d can take $O(H^d/p + 1)$ possible values. We now see that for some integers $\mu_1, \ldots, \mu_d$

$$T_k(u; H) = (H^d/p + 1)H^{d(d-1)/2} J_{k,d}(\mu_1, \ldots, \mu_d; H), \qquad (12)$$

where $J_{k,d}(\lambda_1, \ldots, \lambda_d; H)$ is the number of solution to the system of equations (11) in variables $1 \leq x_1 \ldots, x_{2k} \leq H$. We denote

$$\mathbf{e}(z) = \exp(2\pi i z).$$

Since for any integer w,

$$\int_0^1 \mathbf{e}(\alpha w) d\alpha = \begin{cases} 1, & \text{if } w = 0, \\ 0, & \text{if } w \neq 0, \end{cases}$$

we have the following integral representation of $J_{k,d}(\lambda_1, \ldots, \lambda_d; H)$:

$$\begin{aligned} & J_{k,d}(\lambda_1, \ldots, \lambda_d; H) \\ & \quad = \sum_{x_1 \ldots, x_{2k}=1}^{H} \int_0^1 \ldots \int_0^1 \prod_{j=1}^{d} \mathbf{e}\left(\alpha_j \left(\sum_{\nu=1}^{2k} (-1)^\nu x_\nu^j - \lambda_j\right)\right) d\alpha_1 \ldots d\alpha_d \\ & \quad = \int_0^1 \ldots \int_0^1 \left| \sum_{x=1}^{H} \mathbf{e}\left(\sum_{j=1}^{d} \alpha_j x^j\right) \right|^{2k} \mathbf{e}\left(-\sum_{j=1}^{d} \alpha_j \lambda_j\right) d\alpha_1 \ldots d\alpha_d. \end{aligned}$$

Therefore,

$$J_{k,d}(\lambda_1, \ldots, \lambda_d; H) \leq J_{k,d}(0, \ldots, 0; H) = J_{k,d}(H).$$

Thus, recalling (10) and (12), we derive

$$N(H; 0, 0)^{2k} \ll (H^d/p + 1) H^{d(d-1)/2+1} J_{k,d}(H).$$

We now take $k = \kappa(d)$ which leads us to the estimate

$$N(H; 0, 0)^{2k} \ll (H^d/p + 1) H^{2k-d+1+o(1)} = H^{2k+1+o(1)}/p + H^{2k-d+1+o(1)}$$

and concludes the proof. □

For the number of points in very small boxes we can get a better bound by using the following estimate of Bombieri and Pila [1] on the number of integral points on polynomial curves.

Lemma 2. *Let $\mathcal{C}$ be an absolutely irreducible curve of degree $d \geq 2$ and $H \geq \exp(d^6)$. Then the number of integral points on $\mathcal{C}$ and inside of a square $[0, H] \times [0, H]$ does not exceed $H^{1/d} \exp(12\sqrt{d \log H \log\log H})$.*

We use Lemma 2 to prove an almost sharp estimate for $N(H; K, L)$ when $H \ll p^{2/(d^2+3)}$.

Theorem 3. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. Then for any positive integer $H \leq p^{2/(d^2+3)}$, uniformly over arbitrary integers K and L, we have*

$$N(H; K, L) \ll H^{1/d+o(1)}.$$

Proof. Again we can assume that $K = L = 0$. For a given integer $v \not\equiv 0 \pmod p$, by v^* denote its multiplicative inverse (the least positive integer such that $vv^* \equiv 1 \pmod p$).

Let $f(X) = a_0 + a_1X + \ldots + a_dX^d$ and suppose that there are N solutions of the congruence $f(x) \equiv y \pmod p$, $\quad 1 \le x, y \le H$. We may assume that $N \ge 2(d+1)$. Then, there exist $d+1$ solutions $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ such that $x_1, \ldots, x_{d+1}$ lie in an interval of length $2(d+1)H/N$.

Now, we consider the system

$$\begin{cases} a_0 + a_1x_1 + \ldots + a_dx_1^d & \equiv & y_1 \pmod p; \\ & \ldots & \\ a_0 + a_1x_{d+1} + \ldots + a_dx_{d+1}^d & \equiv & y_{d+1} \pmod p. \end{cases}$$

The determinant of this system is the determinant of Vandermonde,

$$v = \begin{vmatrix} 1 & x_1 & \ldots & x_1^d \\ \ldots & \ldots & \ldots & \ldots \\ 1 & x_{d+1} & \ldots & x_{d+1}^d \end{vmatrix} = \prod_{1 \le i < j \le d+1} (x_j - x_i). \tag{13}$$

Note that $v \not\equiv 0 \pmod p$. Thus, we have that $a_i \equiv u_iv^* \pmod p$, where

$$u_i = \begin{vmatrix} 1 & \ldots & x_1^{i-1} & y_1 & x_1^{i+1} & \ldots & x_1^d \\ \ldots & \ldots & \ldots & \ldots & & & \\ 1 & \ldots & x_{d+1}^{i-1} & y_{d+1} & x_{d+1}^{i+1} & \ldots & x_{d+1}^d \end{vmatrix} = \sum_{j=1}^{d+1} (-1)^{i+j} y_j V_{ij} \tag{14}$$

and V_{ij} is the determinant of the matrix obtained from the Vandermonde matrix after removing the j-th row and the i-th column.

We note that V_{ij} is a polynomial in d variables $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{d+1}$ of degree $d(d+1)/2 - i$ which vanishes when $x_r = x_l$ for distinct r and l. Thus

$$V_{ij} = \prod_{\substack{1 \le r < s \le d+1 \\ r,s \ne j}} (x_s - x_r) W(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{d+1}), \tag{15}$$

where W is a polynomial (that does not depend on f or p) of degree $d - i$. Therefore, we have $|V_{ij}| \ll (H/N)^{d(d-1)/2} H^{d-i}$. This estimate and (14) together imply the bound

$$|u_i| \ll (H/N)^{d(d-1)/2} H^{d+1-i}. \tag{16}$$

On the other hand, it is clear that

$$|v| \ll (H/N)^{d(d+1)/2}. \tag{17}$$

Then, the congruence $f(x) \equiv y \pmod p$, $1 \le x, y \le H$ is equivalent to the congruence

$$u_0 + u_1 x + \ldots + u_d x^d \equiv vy \pmod p, \quad 1 \le x, y \le H$$

where $u_i = va_i$, $i = 0, \ldots, d$.

We can write this congruence as the diophantine equation

$$u_0 + u_1 x + \ldots + u_d x^d - vy = pt, \qquad 1 \le x, y \le H, \ t \in \mathbb{Z}. \tag{18}$$

We have

$$\begin{aligned} |t| &\le \frac{|u_0| + \ldots + |u_d| H^d + |v| H}{p} \ll \frac{(H/N)^{d(d-1)/2} H^{d+1}}{p} \\ &\ll \frac{(H/N)^{d(d-1)/2} H^{d+1}}{H^{(d^2+3)/2}} \ll (H^{1/d}/N)^{d(d-1)/2}. \end{aligned}$$

For each value of t, we see from Lemma 2 that the number of integer solutions $1 \le x, y \le H$ to the equation (18) in Lemma 2 is bounded by $H^{1/d+o(1)}$. Thus

$$N \ll \left((H^{1/d}/N)^{d(d-1)/2} + 1\right) H^{1/d+o(1)},$$

which implies $N \ll H^{1/d+o(1)}$. □

2.2 Sum-product estimates

Some of our results are based on estimating the size of the sets $\mathcal{A} + \mathcal{A}$ and $f(\mathcal{A}) + f(\mathcal{A})$. For small sets $\mathcal{A} \subseteq \mathbb{F}_p$ of size at most $\sqrt{p}$, a sum-product estimate with polynomials $f \in \mathbb{F}_p[X]$ is given by [3, Theorem 1].

Lemma 4. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \ge 2$. Then for every set $\mathcal{A} \subseteq \mathbb{F}_p$ of size $\#\mathcal{A} \le \sqrt{p}$ we have*

$$\max\{\#(\mathcal{A} + \mathcal{A}), \#(f(\mathcal{A}) + f(\mathcal{A})\} \gg (\#\mathcal{A})^{1+1/16\cdot 6^d}.$$

For large sets $\mathcal{A} \subseteq \mathbb{F}_p$ of size $\#\mathcal{A} > \sqrt{p}$, we use the method of Garaev [6]. We first estimate exponential sums with two arbitrary sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$

$$S_\lambda(\mathcal{U}, \mathcal{V}) = \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \mathbf{e}_p(\lambda f(u - v)),$$

where $\mathbf{e}_p(z) = \exp(2\pi i z/p)$ and using exactly the same technique as in [4] we have the following result.

Lemma 5. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \ge 2$. Then for any two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$, we have the following estimate*

$$\max_{\lambda \in \mathbb{F}_p^*} |S_\lambda(\mathcal{U}, \mathcal{V})| \le \sqrt{p\#\mathcal{U}\#\mathcal{V}}.$$

Proof. Using the orthogonality of additive characters, we write

$$\begin{aligned} |S_\lambda(\mathcal{U},\mathcal{V})| &= \left| \sum_{t=0}^{p-1} \mathbf{e}_p\left(\lambda f(t)\right) \frac{1}{p} \sum_{b=0}^{p-1} \sum_{u\in\mathcal{U}} \sum_{v\in\mathcal{V}} \mathbf{e}_p\left(b(t-u+v)\right) \right| \\ &= \left| \frac{1}{p} \sum_{b=0}^{p-1} \sum_{t=0}^{p-1} \sum_{u\in\mathcal{U}} \sum_{v\in\mathcal{V}} \mathbf{e}_p(b(t-u+v)+\lambda f(t)) \right| \\ &\le \frac{1}{p} \sum_{b=0}^{p-1} \left| \sum_{u\in\mathcal{U}} \mathbf{e}_p(bu) \right| \left| \sum_{v\in\mathcal{V}} \mathbf{e}_p(bv) \right| \left| \sum_{t=0}^{p-1} \mathbf{e}_p(bt+\lambda f(t)) \right|. \end{aligned}$$

Now, for $\lambda \in \mathbb{F}_p^*$, applying the Weil bound (see [14, Theorem 5.38]) to the sum over t, and applying the Cauchy-Schwarz inequality to the sum over u and v, we obtain

$$\begin{aligned} |S_\lambda(\mathcal{U},\mathcal{V})| \le \frac{d}{p^{1/2}} &\left(\sum_{b=0}^{p-1} \left| \sum_{u\in\mathcal{U}} \mathbf{e}_p(bu) \right|^2 \right)^{1/2} \left(\sum_{b=0}^{p-1} \left| \sum_{v\in\mathcal{V}} \mathbf{e}_p(bv) \right|^2 \right)^{1/2} \\ &= \frac{d}{p^{1/2}} (p\#\mathcal{U})^{1/2} (p\#\mathcal{V})^{1/2} = d\sqrt{p\#\mathcal{U}\#\mathcal{V}} \end{aligned} \tag{19}$$

provided that $\gcd(\lambda, p) = 1$. □

Following exactly the argument of Garaev [6] and using the estimate of Lemma 5, we obtain the following result for large sets $\mathcal{A} \subseteq \mathbb{F}_p$.

Lemma 6. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \ge 2$. Then for every set $\mathcal{A} \subseteq \mathbb{F}_p$ of size $\#\mathcal{A} \ge \sqrt{p}$ we have*

$$\#(\mathcal{A}+\mathcal{A}) \cdot \#(f(\mathcal{A}) + f(\mathcal{A})) \gg \min\left\{ p\#\mathcal{A}, \frac{(\#\mathcal{A})^4}{p} \right\}.$$

Proof. We consider the equation

$$f(a_1) + f(b-a_2) = c, \qquad (a_1, a_2, b, c) \in \mathcal{A} \times \mathcal{A} \times \mathcal{B} \times \mathcal{C}, \tag{20}$$

where

$$\mathcal{B} = \mathcal{A} + \mathcal{A} \qquad \text{and} \qquad \mathcal{C} = f(\mathcal{A}) + f(\mathcal{A}).$$

Let J be the number of solutions to (20).

For any triple $(a_1, a_2, a_3) \in \mathcal{A} \times \mathcal{A} \times \mathcal{A}$, we see that the vector

$$(a_1, a_2, b, c) = (a_1, a_2, a_2 + a_3, f(a_1) + f(a_3))$$

is a solution to (20) and different triples (a_1, a_2, a_3) give different solutions. Therefore

$$J \geq (\#\mathcal{A})^3. \tag{21}$$

We can also express J via exponential sums

$$J = \sum_{a_1 \in \mathcal{A}} \sum_{a_2 \in \mathcal{A}} \sum_{b \in \mathcal{B}} \sum_{c \in \mathcal{C}} \frac{1}{p} \sum_{\lambda=0}^{p-1} \mathbf{e}_p \left(\lambda \left(f(a_1) + f(b - a_2) - c \right) \right).$$

Changing the order of summation, separating the term $(\#\mathcal{A})^2 \#\mathcal{B} \#\mathcal{C}/p$ corresponding to $\lambda = 0$ and recalling (21), we obtain

$$(\#\mathcal{A})^3 \leq \frac{(\#\mathcal{A})^2 \#\mathcal{B} \#\mathcal{C}}{p} + \frac{1}{p} \sum_{\lambda=1}^{p-1} |S_\lambda(\mathcal{B}, \mathcal{A})| \left| \sum_{a \in \mathcal{A}} \sum_{c \in \mathcal{C}} \mathbf{e}_p \left(\lambda \left(f(a) - c \right) \right) \right|.$$

By (19) we obtain

$$\begin{aligned} (\#\mathcal{A})^3 \ll & \frac{(\#\mathcal{A})^2 \#\mathcal{B} \#\mathcal{C}}{p} \\ & + \sqrt{p^{-1} \#\mathcal{A} \#\mathcal{B}} \sum_{\lambda=1}^{p-1} \left| \sum_{a \in \mathcal{A}} \mathbf{e}_p \left(\lambda f(a) \right) \right| \left| \sum_{c \in \mathcal{C}} \mathbf{e}_p \left(\lambda c \right) \right|. \end{aligned} \tag{22}$$

Adding to the sum over λ the term corresponding to $\lambda = 0$ and then applying the Cauchy-Schwarz inequality, as in (19), we obtain

$$\begin{aligned} \sum_{\lambda=1}^{p-1} & \left| \sum_{a \in \mathcal{A}} \mathbf{e}_p \left(\lambda f(a) \right) \right| \left| \sum_{c \in \mathcal{C}} \mathbf{e}_p \left(\lambda c \right) \right| \\ & \leq \left(\sum_{\lambda=0}^{p-1} \sum_{a_1, a_2 \in \mathcal{A}} \mathbf{e}_p \left(\lambda (f(a_1) - f(a_2)) \right) \right)^{1/2} \\ & \qquad \cdot \left(\sum_{\lambda=0}^{p-1} \sum_{c_1, c_2 \in \mathcal{C}} \mathbf{e}_p \left(\lambda (c_1 - c_2) \right) \right)^{1/2}. \end{aligned}$$

Therefore

$$\sum_{\lambda=1}^{p-1} \left| \sum_{a_1 \in \mathcal{A}} \mathbf{e}_p\left(\lambda f(a_1)\right) \right| \left| \sum_{c \in \mathcal{C}} \mathbf{e}_p\left(\lambda c\right) \right| \ll p\sqrt{\#\mathcal{A}\#\mathcal{C}},$$

which after inserting into (22) implies the desired result. □

In particular, using Lemma 4 directly if $\#\mathcal{A} < p^{1/2}$, applying it to any subset $\mathcal{A}_0 \subseteq \mathcal{A}$ with $\#\mathcal{A}_0 = \lfloor p^{1/2} \rfloor$ for $p^{1/2} \le \#\mathcal{A} \le p^{1/2+1/64\cdot 6^d}$ and using Lemma 6, otherwise, we see that, for every set $\mathcal{A} \subseteq \mathbb{F}_p$

$$\max\{\#(\mathcal{A}+\mathcal{A}), \#(f(\mathcal{A})+f(\mathcal{A}))\} \gg \begin{cases} (\#\mathcal{A})^{1+1/16\cdot 6^d}, & \text{if } \#\mathcal{A} \le p^{1/2}, \\ p^{1/2+1/32\cdot 6^d}, & \text{if } p^{1/2} < \#\mathcal{A} \le p^{1/2+1/64\cdot 6^d}, \\ p^{-1/2}(\#\mathcal{A})^2, & \text{if } p^{1/2+1/64\cdot 6^d} < \#\mathcal{A} \le p^{2/3}, \\ p^{1/2}(\#\mathcal{A})^{1/2}, & \text{if } p^{2/3} < \#\mathcal{A} \le p. \end{cases}$$

In particular, for $\#\mathcal{A} \le p^{2/3}$ we have

$$\max\{\#(\mathcal{A}+\mathcal{A}), \#(f(\mathcal{A})+f(\mathcal{A}))\} \gg (\#\mathcal{A})^{1+\eta(d)}, \tag{23}$$

where

$$\eta(d) = \frac{1}{32 \cdot 6^d + 1}.$$

We also note that in the range $\#\mathcal{A} > p^{2/3}$ the above result implies the optimal bound

$$\max\{\#(\mathcal{A}+\mathcal{A}), \#(f(\mathcal{A})+f(\mathcal{A}))\} \gg p^{1/2}(\#\mathcal{A})^{1/2} \tag{24}$$

in the general setting (the optimality can be shown via the same pigeon-hole principles as in [6]).

2.3 Points on polynomial curves in almost boxes

Following the same ideas as in [4, Theorem 3], putting together Lemmas 4 and 6, we have the following result.

Theorem 7. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. Then for any almost intervals $\mathcal{I}, \mathcal{J} \subseteq \mathbb{F}_p$ with $\#\mathcal{I}, \#\mathcal{J} \leq H$, we have*

$$M(\mathcal{I}, \mathcal{J}) \ll \frac{H^{2+o(1)}}{p} + H^{1-\vartheta(d)+o(1)},$$

where

$$\vartheta(d) = \frac{1}{32 \cdot 6^d + 2}.$$

Proof. We consider the set $\mathcal{A}$ of smallest nonnegative residues modulo p of $x \in \mathcal{I}$ such that $f(x)$ is congruent modulo p to some integer $y \in \mathcal{J}$. Thus $M(\mathcal{I}, \mathcal{J}) = \#\mathcal{A}$

Clearly

$$\#(\mathcal{A} + \mathcal{A}) \leq \#(\mathcal{I} + \mathcal{I}) \leq (\#\mathcal{I})^{1+o(1)}$$

and

$$\#(f(\mathcal{A}) + f(\mathcal{A})) \leq \#(\mathcal{J} + \mathcal{J}) \leq (\#\mathcal{I})^{1+o(1)}.$$

Using (23) and (24), we conclude the proof. □

3 Applications

3.1 Expansion of polynomial iterations

Applying now Theorem 1 we have the following estimate for the expansion of orbits in polynomial dynamical systems.

Theorem 8. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$ and let $\{u_n\}$ be the sequence generated by* (7) *on the initial value $u \in \mathbb{F}_p$. Then for $T_u \geq N \geq 1$ we have*

$$L_u(N) \gg \min\{N^{2\kappa(d)/(1+2\kappa(d))+o(1)} p^{1/(1+2\kappa(d))}, N^{1+(d-1)/(2\kappa(d)-d+1)+o(1)}\}.$$

Proof. We can assume that $N \leq p^{2/3}$ since otherwise the bound (8) holds. Clearly the pairs $(u_n, u_{n+1}) = (u_n, f(u_n))$, $n = 0, 1, ..., N-1$, are all distinct (since $N \leq T_u$) and all belong to the square $[u - L_u(N), u + L_u(N)] \times [u - L_u(N), u + L_u(N)]$. Therefore

$$N \leq N\left(2L_u(N); u - L_u(N), u - L_u(N)\right).$$

Using now Theorem 1, we derive

$$N \ll L_u(N)(L_u(N)/p)^{1/(2\kappa(d)+o(1)} + L_u(N)^{1-(d-1)/(2\kappa(d)+o(1)},$$

which concludes the proof. □

Certainly for large values of N one can improve Theorem 8 by using (3) instead of Theorem 1.

3.2 Visible points on polynomial curves

Following exactly the proof of [17, Theorem 2] and the estimate given by Theorem 1 we obtain an asymptotic formula for the number of visible points $\#\mathcal{V}(X,Y)$.

Theorem 9. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geq 2$. For any positive $\varepsilon > 0$ there exists some positive $\eta > 0$, such that for real positive $X, Y \leq p$ with*

$$\min\{X,Y\} > p^{1-1/(4\kappa(d)+2)+\varepsilon}$$

we have

$$\#\mathcal{V}(X,Y) = \left(\frac{6}{\pi^2} + O(p^{-\eta})\right)\frac{XY}{p}.$$

Proof. For an integer n, we define

$$M(n;X,Y) = \#\{(s,t) \in [1,X/n] \times [1,Y/n] \ : \ f(ns) \equiv nt \pmod p\}.$$

Using [17, Bound (5)], we see that for any $D \geq 1$ we have

$$\left|\#\mathcal{V}(X,Y) - \frac{6}{\pi^2}\cdot\frac{XY}{p}\right| \ll \frac{XY}{Dp} + Dp^{1/2}(\log p)^2 + \sum_{n>D} M(n;X,Y). \qquad (25)$$

We further split the last sum into two parts:

$$\sum_{n>D} M(n;X,Y) = \Sigma_1 + \Sigma_2 \qquad (26)$$

where

$$\Sigma_1 = \sum_{D<n<E} M(n;X,Y) \qquad \text{and} \qquad \Sigma_2 = \sum_{n\geq E} M(n;X,Y)$$

with a suitable number $E \geq D$ to be chosen later.

We observe that Σ_2 is bounded by the number of solutions of the congruence

$$f(zx) \equiv zy \pmod p, \quad 1 \leq x \leq X/E, \quad 1 \leq y \leq Y/E, \quad z \geq 1.$$

For each given x, y we have a polynomial congruence in variable z of degree d which has, at most d solutions. Hence,

$$\Sigma_2 \ll XY/E^2 \ll Z^2/E^2, \tag{27}$$

where $Z = \max\{X, Y\}$.

Now, by Theorem 1 we have

$$M(n; X, Y) \ll \frac{Z}{n}\left(\frac{Z}{np}\right)^{1/2\kappa(d)+o(1)} + \left(\frac{Z}{n}\right)^{1-(d-1)/2\kappa(d)+o(1)}.$$

Therefore,

$$\Sigma_1 \ll Z^{1+1/2\kappa(d)+o(1)} D^{-1/2\kappa(d)} p^{-1/2\kappa(d)} + Z^{1-(d-1)/2\kappa(d)+o(1)} E^{(d-1)/2\kappa(d)}. \tag{28}$$

Putting together (25), (26), (27) and (28) we have

$$\begin{aligned} \left|\#\mathcal{V}(X,Y) - \frac{6}{\pi^2}\cdot\frac{XY}{p}\right| \ll\ & \frac{Z^2}{Dp} + Dp^{1/2}(\log p)^2 + Z^{1+o(1)}(Z/pD)^{1/2\kappa(d)} \\ & + Z^{1-(d-1)/2\kappa(d)+o(1)} E^{(d-1)/\kappa(d)} + Z^2/E^2. \end{aligned}$$

Choosing D to satisfy

$$Dp^{1/2} = Z^{1+1/2\kappa(d)} D^{-1/2\kappa(d)} p^{-1/2\kappa(d)}$$

and E to satisfy

$$Z^{1-(d-1)/2\kappa(d)} E^{(d-1)/2\kappa(d)} = Z^2/E^2,$$

that is,

$$D = Zp^{-(\kappa(d)+1)/(2\kappa(d)+1)} \qquad \text{and} \qquad E = Z^{1/2+(d-1)/(8\kappa(d)+2d-2)}$$

and replacing powers of $\log p$ with $p^{o(1)}$, we derive

$$\begin{aligned} & \left|\#\mathcal{V}(X,Y) - \frac{6}{\pi^2}\cdot\frac{XY}{p}\right| \\ & \qquad \ll Zp^{-\kappa(d)/(4\kappa(d)+2)} + Zp^{-1/(4\kappa(d)+2)+o(1)} + Z^{1-(d-1)/(4\kappa(d)+d-1)+o(1)} \\ & \qquad \ll \frac{XY}{p}\left(\frac{p^{1-1/(4\kappa(d)+2)+o(1)}}{\min\{X,Y\}} + \frac{p}{\min\{X,Y\}^{1+(d-1)/(4\kappa(d)+d-1)+o(1)}}\right). \end{aligned}$$

In view of the condition $\min\{X, Y\} > p^{1-1/(4\kappa(d)+2)+\epsilon}$, the result now follows.

□

We note that the result of Theorem 9 seems to be new and nontrivial even for $X = Y = p$. In this case the argument of the proof of Theorem 9 gives a more explicit estimate

$$\#\mathcal{V}(p,p) = \frac{6}{\pi^2}p + O\left(p^{1-1/(4\kappa(d)+2)+o(1)}\right).$$

4 Comments

We remark that the method of proof of Theorem 3 resembles that of [15]. On the other hand, the result of [15] has been improved by Konyagin and Steger [13]. So it is natural to try to use the method of [13] (and thus consider higher dimensional determinants with the entries of the form $x_h^i y_h^j$). We leave the exploring this direction as an open problem.

We say that a set $\mathcal{G} \subseteq \mathbb{F}_p$ is an *almost group* if

$$\#\left(\mathcal{G}\cdot\mathcal{G}\right) = \left(\#\mathcal{G}\right)^{1+o(1)}.$$

Now, for an almost interval $\mathcal{I}$ and an almost group $\mathcal{G}$ we denote by $T(\mathcal{G},\mathcal{I})$ the number of solutions to

$$f(z) \equiv y \pmod p$$

where $y \in \mathcal{I}$, $z \in \mathcal{G}$, which is a generalisation of the congruence (5). Using [3, Theorem 2] instead of [3, Theorem 1], as well as analogues of other results of Section 2.2, and repeating the argument of the proof of Theorem 7, one can obtain a nontrivial upper bound on $T(\mathcal{G},\mathcal{I})$. Furthermore, using the argument of [4], one can also estimate the number of solutions to (4) in almost boxes. In fact, using [9, 12] one can obtain and explicit form of the estimate of Bourgain [2, Theorem 4.1] on $\max\{\#(\mathcal{A}+\mathcal{A}), \#(\mathcal{A}^{-1}+\mathcal{A}^{-1})\}$, and thus obtain a explicit estimate on the number of solutions to (4) in almost boxes.

This method however does not seem to apply to the congruence

$$f(x) \equiv z \pmod p$$

where $x \in \mathcal{I}$, $z \in \mathcal{G}$ for an almost interval $\mathcal{I}$ and an almost group $\mathcal{G}$, which is certainly an interesting object of study.

Acknowledgements

The authors are very grateful to Robert Vaughan and Trevor Wooley for information about the progress on the Vinogrdadov mean value theorem.

During the preparation of this paper, J. C. was supported in part by the Spanish Grant of MICINN MTM 2008-03880, A. O. was supported in part by the Swiss National Science Foundation Grant 133399. I. S. was supported in part by the Australian Research Council Grant DP1092835.

References

[1] E. Bombieri and J. Pila, 'The number of integral points on arcs and ovals', *Duke Math. J.*, **59** (1989), 337–357.

[2] J. Bourgain, 'More on the sum-product phenomenon in prime fields and its applications', *Int. J. Number Theory*, **1** (2005), 1–32.

[3] B. Bukh and J. Tsimerman, 'Sum-product estimates for rational functions', *Preprint*, 2010 (available from http://arxiv.org/abs/1002.2554).

[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] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Preprint*, 2010 (available from http://arxiv.org/abs/1007.1526).

[6] M. Z. Garaev, 'The sum-product estimate for large subsets of prime fields', *Proc. Amer. Math. Soc.*, **136** (2008), 2735–2739.

[7] A. Granville, I. E. Shparlinski and A. Zaharescu, 'On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races', *J. Number Theory*, **112** (2005), 216–237.

[8] J. Gutierrez and I. E. Shparlinski, 'Expansion of orbits of some dynamical systems over finite fields', *Bul. Aust. Math. Soc.*, **82** (2010), 232–239.

[9] H. A. Helfgott and M. Rudnev, 'An explicit incidence theorem in $\mathbb{F}_p$', *Mathematika*, (to appear).

[10] L. K. Hua, *Additive theory of prime numbers*, Amer. Math. Soc., Providence, RI, 1965.

[11] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[12] T. G. F. Jones, 'Explicit incidence bounds over general finite fields', *Preprint*, 2010 (available from `http://arxiv.org/abs/1009.3899`).

[13] S. V. Konyagin and T. Steger, 'On the number of solutions of polynomial congruences', *Matem. Zametki*, **55** (1994), no. 1, 73–79 (in Russian).

[14] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge Univ. Press, Cambridge, 1997.

[15] I. E. Shparlinski, 'On polynomial congruences', *Acta Arith*, **58** (1991), 153–156.

[16] I. E. Shparlinski, 'Distribution of points on modular hyperbolas. *Sailing on the Sea of Number Theory: Proc. 4th China-Japan Seminar on Number Theory*, Weihai, 2006, World Scientific, 2007, 155–189.

[17] I. E. Shparlinski and J. F. Voloch, 'Visible points on curves over finite fields', *Bull. Polish Acad. Sci. Math.*, **55** (2007), 193–199.

[18] R. C. Vaughan, *The Hardy-littlewood method*, Cambridge Univ. Press, Cambridge, 1981.

[19] T. D. Wooley, 'VinogradovÕs mean value theorem via efficient congruencing', *Preprint*, 2010 (available from `http://arxiv.org/abs/1101.0574`).