Sparcity of the Intersection of Polynomial Images of an Interval *†

Mei-Chu Chang‡

Abstract

We show that the intersection of the images of two polynomial maps on a given interval is sparse. More precisely, we prove the following.

Let \( f(x), g(x) \in \mathbb{F}_p[x] \) be polynomials of degrees \( d \) and \( e \) with \( d \geq e \geq 2 \). Suppose \( M \in \mathbb{Z} \) satisfies

\[
p^{\frac{1}{p^2} (\frac{1}{d} - \frac{1}{e})} > M > p^\varepsilon,
\]

where \( E = \frac{e(e+1)}{2} \) and \( \kappa = \left( \frac{1}{d} - \frac{1}{e} \right) \frac{E-1}{E} + \varepsilon \). Assume \( f(x) - g(y) \) is absolutely irreducible. Then

\[
|f([0,M]) \cap g([0,M])| = M^{1-\varepsilon}.
\]

1 Introduction.

Our goal is to study the intersection of the images in \( \mathbb{F}_p \) of a given interval under two polynomial maps. What we prove is the following sparsity property.

Theorem. Let \( f(x), g(x) \in \mathbb{F}_p[x] \) be polynomials of degrees \( d \) and \( e \) with \( d \geq e \geq 2 \). Suppose \( M \in \mathbb{Z} \) satisfies

\[
p^{\frac{1}{p^2} (\frac{1}{d} - \frac{1}{e})} > M > p^\varepsilon,
\]

*2000 Mathematics Subject Classification. Primary 11P21, 11D79.
†Key words. counting solutions, congruence equations, lattice points, character sums.
‡Supported in part by NSF grant DMS 1301608
where $E = \frac{\varphi(e+1)}{2}$ and $\kappa = \left(\frac{1}{d} - \frac{1}{d^2}\right)^{-1} + \varepsilon$. Assume $f(x) - g(y)$ is absolutely irreducible. Then

$$|f([0, M]) \cap g([0, M])| = M^{1-\varepsilon}.$$

Let us stress that the above estimate is uniform in the sense that it does not depend on the choice of the polynomials $f$ and $g$.

Our approach consists in bounding the number of points on the curve $g(y) = f(x)$ over $\mathbb{F}_p$ inside the box $[0, M] \times [0, M]$. The problem of estimating the number of integral points in a box lying on a curve $C$ defined by an equation $F(x, y) = 0$ with $F(x, y) \in \mathbb{Z}[x, y]$ has been extensively studied by many authors ([1], [2], [9], [12], [13], [14], [15], [16], [17]), in particular in the celebrated paper of Bombieri and Pila [1]. The $\mod p$ analogue of this problem is much less understood. However, some natural motivations come from questions around the expansion properties of polynomial maps acting on $\mathbb{F}_p$, the study of orbits obtained by iteration of a given polynomial $\mod p$ and also certain issues in cryptography related to hyperelliptic curves. One could conjecture that if $M < p^{1-\varepsilon}$, then

$$\left|\{(x, y) \in [0, M]^2 : F(x, y) \equiv 0 \pmod p\}\right| < M^{1-\delta}$$

for $\delta = \delta(\varepsilon, d)$ and $F(x, y) \in \mathbb{Z}[x, y]$ of degree $d \geq 2$ and absolutely irreducible $\mod p$. Such results can be proven assuming $M$ is sufficiently small. Even in the special case $F(x, y) = g(y) - f(x)$ considered above, there is a size restriction on $M$ when $\deg f, \deg g > 1$. The method of attack consists indeed in removing the $\mod p$ property in order to be able to invoke results such as those in [1]. This lifting technique seems to require rather severe restrictions on $M$. In some sense, the challenge would be to deal with such questions directly $\mod p$, without the need to lift the problem to $\mathbb{Z}$.

Our result should be compared with earlier work in a similar spirit. (See [7], [8], [11] for large boxes, [6] for small boxes, and [3], [4], [19] for special curves.) In particular, the cases $g(y) = y$ and $g(y) = y^2$ are considered in [5]. Our focus here is only to relax as much as possible the size condition on $M$, required to obtain a non-trivial result, and not the quality of the estimate itself. In the case $g(y) = y^2$, [5] permits to treat only the range $M < p^{4-\varepsilon}$. The proposition below applied with $e = 2$ gives a less restrictive result.

**Proposition.** Let $f(x) = \sum_{s=1}^d a_s x^s, g(x) = \sum_{s=0}^e b_s x^s \in \mathbb{F}_p[x]$ be polynomials over $\mathbb{F}_p$ with $d \geq e \geq 2$. Suppose $M \in \mathbb{Z}$ satisfies

$$p^{\frac{1}{d(1+\frac{e}{d})}} > M > p^e,$$  \hfill (1.1)


where \( E = \frac{e(e+1)}{2} \) and \( \kappa = (\frac{1}{d} - \frac{1}{e^2})^{E-1} + \varepsilon \). Assume \( f(x) - g(y) \) is absolutely irreducible. Then the congruence
\[
g(y) \equiv f(x) \pmod{p}, \quad 1 \leq x, y \leq M, \quad (1.2)
\]
has at most \( M^{1-\varepsilon} \) solutions.

In particular for \( e = 2, d = 3 \), the condition becomes \( M < p^{\frac{1}{4} + \frac{4}{23}} \).

For a more friendly version, we may use Fact 2 in §2 and restate the theorem as follows.

**Theorem’.** Let \( f(x), g(x) \in \mathbb{F}_p[x] \) be monic polynomials of degrees \( d \) and \( e \) with \( d \geq e \geq 2 \). Suppose \( M \in \mathbb{Z} \) satisfies
\[
p^{\frac{1}{E}(1 + \kappa - \lambda)} > M > p^\varepsilon,
\]
where \( E = \frac{e(e+1)}{2} \) and \( \kappa = (\frac{1}{d} - \frac{1}{e^2})^{E-1} + \varepsilon \). Assume \( \gcd(d, e) = 1 \). Then
\[
|f([0, M]) \cap g([0, M])| = M^{1-\varepsilon}.
\]

A similar version can be stated for the proposition.

**Notations and Conventions.**
1. \( e(\theta) = e^{2\pi i \theta} \), \( e_p(\theta) = e(\frac{\theta}{p}) \).
2. \( \|\alpha\| \) denotes the distance of \( \alpha \) to the nearest integer.
3. \( p \) = prime sufficiently large.
4. \( \varepsilon \) = various small constant.
5. \( I = \mathbb{Z} \cap I = \) an interval.
6. \( A \lesssim B \) means that \( |A| \leq cB \) for some constant \( c \).

2 Preliminary.

**Theorem BP.** ([1], Theorem 5) Let \( C \) be an absolute irreducible curve over \( \mathbb{R} \) of degree \( d \geq 2 \) and let \( M \geq \exp(d^6) \). Then the number of integral points on \( C \) and inside a square \([0, M] \times [0, M]\) does not exceed
\[
M^{1/d} \exp(12 \sqrt{d \log M \log \log M}).
\]
The following is Theorem 11.2 in [18] which is a slight refinement of Theorem 1.6 in [17]

**Theorem W.** Let $M$ be sufficiently large. Suppose

$$\left| \sum_{x=1}^{M} e\left( \sum_{j=1}^{d} a_j x^j \right) \right| > \frac{M}{B}.$$  

Then there exist integers $z, a'_1, \cdots, a'_d$ such that $1 \leq z \leq B^c$ and

$$za_j \equiv a'_j \quad \text{with} \quad |a'_j| \leq \frac{p}{M^j} B^c,$$

where

$$c = \begin{cases} 
  d + \varepsilon, & \text{if } d \geq 4, \\
  1 + \varepsilon, & \text{if } d = 2, 3.
\end{cases}$$

The following is elementary. (See (8.6) in [10].)

**Fact 1.** For $\alpha \not\in \mathbb{Z}$

$$\left| \sum_{x=1}^{M} e(\alpha x) \right| \leq \min \left( M, \frac{1}{2\|\alpha\|} \right).$$

**Fact 2.** Let $f(x), g(x) \in \mathbb{Z}[x]$ be monic polynomials with $\deg f = d$ and $\deg g = e$. Assume $\gcd(d, e) = 1$. Then the polynomial $f(x) - g(y) \in \mathbb{Z}[x, y]$ is absolutely irreducible.

It is elementary to verify Fact 2. Assume $f(x) - g(y) = \Phi(x, y)\Psi(x, y)$. We let $x = t^e$ and $y = t^d$. Then the highest term of $t$ in $f(x) - g(y)$ is at most $t^{de-1}$. On the other hand, the assumption $\gcd(d, e) = 1$ implies that $md + ne \neq m'd + n'e$ for $(m, n) \neq (m', n')$ and $m, m' < e$. Hence there is no cancelation among the terms in $\Phi(x, y)$ (respectively, $\Psi(x, y)$). Therefore the highest term in $\Phi(x, y)\Psi(x, y)$ is $t^{de}$. This is a contradiction.

### 3 The Proof.

We assume (1.2) has $\sim M$ solutions. We choose
\[ \delta \sim \min \left\{ \left( \frac{p^\frac{1}{p}}{M} \right)^{\frac{p}{p-1}}, 1 \right\}. \quad (3.1) \]

Then there exists \( J = [u, u + \delta M] \) such that
\[ |\{(x, y) \in [0, M] \times J : (x, y) \text{satisfies (1.2)}\}| \gtrsim \delta M. \quad (3.2) \]

For \( y \in J \), writing \( y = u + y_1 \) with \( y_1 \in [0, \delta M] \), we have
\[ g(y) = \sum_{s=0}^{e} b_s(u + y_1)^s := \sum_{s=0}^{e} \bar{b}_s y_1^s \in Q, \quad (3.3) \]

where
\[ Q = \sum_{s=0}^{e} \bar{b}_s [0, \delta^s M^s] \quad (3.4) \]

with
\[ |Q| \sim \delta^E M^E. \quad (3.5) \]

Let \( I_Q \) be the indicator function of \( Q \) and let \( \tilde{I}_Q(\xi) = \sum_x I_Q(x) e_p(\xi x) \) be its Fourier transform.

Claim. There exists \( \xi \neq 0 \) such that
\[ \left| \sum_{x=1}^{M} e_p(-\xi f(x)) \right| \gtrsim \frac{\delta M}{p^\varepsilon} \quad (3.6) \]

and
\[ |\tilde{I}_Q(\xi)| \gtrsim \frac{|Q|}{p^\varepsilon}. \quad (3.7) \]

Proof of Claim.

Let
\[ \Lambda = \left\{ \xi \neq 0 : |\tilde{I}_Q(\xi)| > \frac{|Q|}{p^\varepsilon} \right\}. \]

It is easy to see, by Plancherel theorem, that
\[ |\Lambda| < \frac{p^{1+2\varepsilon}}{|Q|}. \quad (3.8) \]
Denote by \( \mu \) the normalized \( r \)-th convolution of \( I_Q \),

\[
\mu = \frac{I_Q * (I_Q * I_{-Q}) * \cdots * (I_Q * I_{-Q})}{|Q|^{r-1}}.
\]

It is straightforward to show that

\[
\mu \geq \frac{I_Q}{2^r} \quad \text{and} \quad |\hat{\mu}| = \frac{|\hat{I}_Q|^r}{|Q|^{r-1}}. \tag{3.9}
\]

From (3.2) and (3.9),

\[
\delta M \lesssim \sum_{x=1}^M I_Q(f(x)) \leq 2^r \sum_{x=1}^M \mu(f(x)) = \frac{2^r}{p} \sum_{\xi} \hat{\mu}(\xi) \sum_{x=1}^M e_p(-\xi f(x))
\lesssim \frac{|Q|}{p} M + \frac{1}{p} \sum_{\xi \in \Lambda \setminus 0} \hat{\mu}(\xi) \sum_{x=1}^M e_p(-\xi f(x)) + \frac{1}{p} \sum_{\xi \in \Lambda} \hat{\mu}(\xi) \sum_{x=1}^M e_p(-\xi f(x)). \tag{A}
\]

\[
\leq \frac{1}{p} |Q| \frac{|Q|}{p^r} M \sim \frac{|Q|}{p} M. \tag{3.10}
\]

Take \( r \sim 1/\varepsilon \). Then

\[
(B) \leq \frac{1}{p} \frac{|Q|}{p^r} \sim \frac{|Q|}{p} M. \tag{3.11}
\]

By (3.8),

\[
(A) \leq \frac{1}{p} \frac{p^{1+2\varepsilon}}{|Q|} \max_{\xi \in \Lambda \setminus 0} \left| \sum_{x=1}^M e_p(-\xi f(x)) \right| \tag{3.12}
\]

Putting together (3.10)-(3.12) and using (3.5) and (3.1), we obtain

\[
\delta M \lesssim p^{2\varepsilon} \max_{\xi \in \Lambda \setminus 0} \left| \sum_{x=1}^M e_p(-\xi f(x)) \right| \tag{3.13}
\]

and prove the claim.

It follows from (3.7) and (3.4) that

\[
\frac{|Q|}{p^r} < |\hat{I}_Q(\xi)| = \left| \sum_x I_Q(x)e_p(\xi x) \right| = \left| \sum_x e_p(\xi x) \right| = \prod_{j=1}^e \left| \sum_{t_j=0}^{(\delta M)^j} e_p(\tilde{b}_j t_j \xi) \right|. \tag{3.14}
\]
Therefore, by (3.5),
\[
\left| \sum_{t_j=0}^{(\delta M)^j} e_p(\tilde{b}_j t_j \xi) \right| > \frac{(\delta M)^j}{p^\varepsilon}, \quad \text{for } j = 1, \ldots, e. \tag{3.15}
\]
Applying Fact 1, we have
\[
\left\| \frac{\tilde{b}_j \xi}{p} \right\| \lesssim \frac{p^{1+\varepsilon}}{(\delta M)^j}
\]
i.e.
\[
\text{dist}(\tilde{b}_j \xi, p\mathbb{Z}) \lesssim \frac{p^{1+\varepsilon}}{(\delta M)^j}.
\]
Hence,
\[
\tilde{b}_j \xi \equiv b'_j \pmod{p} \quad \text{with} \quad |b'_j| \lesssim \frac{p^{1+\varepsilon}}{(\delta M)^j}, \tag{3.16}
\]
On the other hand, applying Theorem W to (3.6), we obtain $z, a'_1, \ldots, a'_d$ such that
\[
1 \leq z \leq \left( \frac{p^{\varepsilon}}{\delta} \right)^c, \quad z(-a_j \xi) \equiv a'_j \pmod{p}, \quad \text{and} \quad |a'_j| \leq \frac{p}{M^j} \left( \frac{p^{\varepsilon}}{\delta} \right)^c, \tag{3.17}
\]
where
\[
c = \begin{cases} 
d + \varepsilon, & \text{if } d \geq 4, \\
1 + \varepsilon, & \text{if } d = 2, 3.
\end{cases}
\]
Multiplying (1.2) by $z \xi$ and using (3.16) and (3.17), we have
\[
\sum_{j=0}^{e} z b'_j y_1^j = \sum_{j=1}^d a'_j x^j + wp \tag{3.18}
\]
for some $w \in \mathbb{Z}$.
Since $x \in [0, M], y_1 \in [0, \delta M]$, combining (3.16)-(3.18) gives
\[
w \lesssim \left( \frac{p^{\varepsilon}}{\delta} \right)^c. \tag{3.19}
\]
Fix $w$ in (3.18), Theorem BP implies that the number of solutions $(x, y_1) \in [0, M] \times [0, M]$ is bounded by $M^{1/d+\varepsilon}$. Hence, by our assumption on the number of solutions of (1.2),
\[
M \lesssim \left( \frac{p^{\varepsilon}}{\delta} \right)^c M^{1/d+\varepsilon}. \tag{3.20}
\]
Together with (3.1), this gives
\[ p^{1/E - \varepsilon} < M^{1-(1-\frac{1}{3}) \frac{E-1}{3E}} \leq M^{1-\kappa}, \]
(3.21)
which contradicts to (1.1).

Acknowledgement. The author is grateful to Trevor Wooley for discussions and useful references to Theorem W. The author would also like to thank the mathematics department of University of California at Berkeley for its hospitality.

References


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, RIVERSIDE, CA 92521, USA

*Email address: mcc@math.ucr.edu*