ACTA ARITHMETICA
165.3 (2014)

Sparsity of the intersection of polynomial images of an interval

by

MEI-CHU CHANG (Riverside, CA)

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*

$$p^{\frac{1}{E}(1+\frac{\kappa}{1-\kappa})} > M > p^{\varepsilon},$$

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

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

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]–[17]), in particular in the celebrated paper of Bombieri and Pila [1]. The modulo 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 modulo p and also certain issues in cryptography related to hyperelliptic curves. One could conjecture that if $M < p^{1-\varepsilon}$, then

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

2010 *Mathematics Subject Classification*: Primary 11P21, 11D79.
Key words and phrases: counting solutions, congruence equations, lattice points, character sums.

DOI: 10.4064/aa165-3-3

for $\delta = \delta(\varepsilon, d)$ and $F(x, y) \in \mathbb{Z}[x, y]$ of degree $d \geq 2$ and absolutely irreducible modulo 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 modulo 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 modulo 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], [18] 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 one to treat only the range $M < p^{1/3-\varepsilon}$. 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*

$$p^{\frac{1}{E}(1+\frac{\kappa}{1-\kappa})} > M > p^{\varepsilon}, \tag{1.1}$$

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

$$g(y) \equiv f(x) \pmod{p}, \qquad 1 \leq x, y \leq M, \tag{1.2}$$

has at most $M^{1-\varepsilon}$ *solutions.*

In particular for $e = 2, d = 3$, the condition becomes $M < p^{1/3+4/69}$.

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*

$$p^{\frac{1}{E}(1+\frac{\kappa}{1-\kappa})} > M > p^{\varepsilon},$$

where $E = e(e+1)/2$ *and* $\kappa = (\frac{1}{d} - \frac{1}{d^2})\frac{E-1}{E} + \varepsilon$. *Assume* $\gcd(d, e) = 1$. *Then*

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

A similar version can be stated for the Proposition.

Notations and conventions

1. $e(\theta) = e^{2\pi i\theta}$, $e_p(\theta) = e(\theta/p)$.
2. $\|\alpha\|$ denotes the distance of α to the nearest integer.
3. $p =$ prime sufficiently large.
4. $\epsilon =$ various small constant.

5. $I = \mathbb{Z} \cap I =$ an interval.
6. $A \ll B$ means that $|A| \le cB$ for some constant c. Similarly, $A \sim B$ means A is equal to B asymptotically.

2. Preliminaries

Theorem BP ([1, Theorem 5]). *Let C be an absolute irreducible curve over $\mathbb{R}$ of degree $d \ge 2$ and let $M \ge \exp(d^6)$. 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 1.6 in [17].

Theorem W. *Let $d \ge 2$ be an integer and let $M \in \mathbb{Z}$ be sufficiently large. Suppose*

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

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

$$|za_j - a'_j| \le \frac{p}{M^j} B^c, \quad \textit{where} \quad c = d + \varepsilon.$$

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

Fact 1. *For $\alpha \notin \mathbb{Z}$,*

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

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 $md + ne \ne m'd + n'e$ for $(m, n) \ne (m', n')$ 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

$$\delta = \min\big\{(p^{1/E}/M)^{E/(E-1)}, 1\big\}. \tag{3.1}$$

Then there exists $J = [u, u + \delta M]$ such that

$$|\{(x, y) \in [0, M] \times J : (x, y) \text{ satisfies } (1.2)\}| \gtrsim \delta M. \tag{3.2}$$

For $y \in J$, writing $y = u + y_1$ with $y_1 \in [0, \delta M]$, we have

$$g(y) = \sum_{s=0}^{e} b_s (u + y_1)^s := \sum_{s=0}^{e} \widetilde{b}_s y_1^s \in Q, \tag{3.3}$$

where

$$Q = \sum_{s=0}^{e} \widetilde{b}_s [0, \delta^s M^s] \tag{3.4}$$

with

$$|Q| \sim \delta^E M^E. \tag{3.5}$$

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

Claim. *There exists* $\xi \neq 0$ *such that*

$$\Big| \sum_{x=1}^{M} e_p(-\xi f(x)) \Big| \gtrsim \frac{\delta M}{p^{\varepsilon}} \tag{3.6}$$

and

$$|\widehat{I}_Q(\xi)| > \frac{|Q|}{p^{\varepsilon}}. \tag{3.7}$$

Proof of Claim. Let

$$\Lambda = \{\xi \neq 0 : |\widehat{I}_Q(\xi)| > |Q|/p^{\varepsilon}\}.$$

It is easy to see, by Plancherel's theorem, that

$$|\Lambda| < p^{1+2\varepsilon}/|Q|. \tag{3.8}$$

Denote by μ the normalized rth convolution of I_Q,

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

It is straightforward to show that

$$\mu \geq I_Q/2^r \quad \text{and} \quad |\widehat{\mu}| = |\widehat{I}_Q|^r/|Q|^{r-1}. \tag{3.9}$$

From (3.2) and (3.9),

$$\begin{aligned} \delta M &\ll \sum_{x=1}^{M} I_Q(f(x)) \leq 2^r \sum_{x=1}^{M} \mu(f(x)) = \frac{2^r}{p} \sum_{\xi} \widehat{\mu}(\xi) \sum_{x=1}^{M} e_p(-\xi f(x)) \\ &\sim \frac{|Q|M}{p} + \underbrace{\frac{1}{p} \sum_{\xi \in \Lambda \setminus 0} \widehat{\mu}(\xi) \sum_{x=1}^{M} e_p(-\xi f(x))}_{(A)} + \underbrace{\frac{1}{p} \sum_{\xi \notin \Lambda} \widehat{\mu}(\xi) \sum_{x=1}^{M} e_p(-\xi f(x))}_{(B)}. \end{aligned} \tag{3.10}$$

Take $r \sim 1/\varepsilon$. Then

$$(B) \le \frac{1}{p} p \frac{|Q|}{p^{r\varepsilon}} M \sim \frac{|Q|M}{p}. \tag{3.11}$$

By (3.8),

$$(A) \le \frac{1}{p} \frac{p^{1+2\varepsilon}}{|Q|} |Q| \max_{\xi \in \Lambda \setminus 0} \Big| \sum_{x=1}^{M} e_p(-\xi f(x)) \Big| \tag{3.12}$$

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

$$\delta M \ll p^{2\varepsilon} \max_{\xi \in \Lambda \setminus 0} \Big| \sum_{x=1}^{M} e_p(-\xi f(x)) \Big|, \tag{3.13}$$

which proves the claim.

It follows from (3.7) and (3.4) that

$$\frac{|Q|}{p^{\varepsilon}} < |\widehat{I}_Q(\xi)| = \Big| \sum_{x} I_Q(x) e_p(\xi x) \Big| = \Big| \sum_{x \in Q} e_p(\xi x) \Big| = \prod_{j=1}^{e} \Big| \sum_{t_j=0}^{(\delta M)^j} e_p(\widetilde{b}_j t_j \xi) \Big|. \tag{3.14}$$

Therefore, by (3.5),

$$\Big| \sum_{t_j=0}^{(\delta M)^j} e_p(\widetilde{b}_j t_j \xi) \Big| > \frac{(\delta M)^j}{p^{\varepsilon}} \quad \text{for } j = 1, \dots, e. \tag{3.15}$$

Applying Fact 1, we have

$$\|\widetilde{b}_j \xi / p\| \ll p^{\varepsilon}/(\delta M)^j,$$

i.e.

$$\operatorname{dist}(\widetilde{b}_j \xi, p\mathbb{Z}) \ll p^{1+\varepsilon}/(\delta M)^j.$$

Hence,

$$\widetilde{b}_j \xi \equiv b'_j \pmod{p} \quad \text{with } |b'_j| \ll p^{1+\varepsilon}/(\delta M)^j. \tag{3.16}$$

On the other hand, applying Theorem W to (3.6), we obtain $z, a'_1, \dots, a'_d$ such that

$$1 \le z \le (p^{\varepsilon}/\delta)^c, \quad z(-a_j \xi) \equiv a'_j \pmod{p}, \quad |a'_j| \le \frac{p}{M^j} (p^{\varepsilon}/\delta)^c, \tag{3.17}$$

where $c = d + \varepsilon$.

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

$$w \ll (p^{\varepsilon}/\delta)^c. \tag{3.19}$$

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),

$$M \ll (\,p^{\varepsilon}/\delta)^c M^{1/d+\varepsilon}. \tag{3.20}$$

Together with (3.1), this gives

$$p^{1/E\,-\varepsilon} < M^{1-(1-1/d)\frac{E-1}{cE}} \le M^{1-\kappa}, \tag{3.21}$$

which contradicts (1.1).

Acknowledgments. 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.

This research was supported in part by NSF grant DMS 1301608.

References

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

[2] T. D. Browning, *Quantitative Arithmetic of Projective Varieties*, Progr. Math. 277, Birkhäuser, Basel, (2009).

[3] T. H. Chan and I. E. Shparlinski, *On the concentration of points on modular hyperbolas and exponential curves*, Acta Arith. 142 (2010), 59–66.

[4] M.-C. Chang, *Expansions of quadratic maps in prime fields*, Proc. Amer. Math. Soc. 142 (2014), 85–92.

[5] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, *Points on curves in small boxes and applications*, Michigan Math. J. 63 (2014), 503–534.

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

[7] K. Ford, *Recent progress on the estimation of Weyl sums*, in: Proc. IV Intern. Conf. "Modern Problems of Number Theory and its Applications": Current Problems, Part II (Tula, 2001), Moscow State Univ., Moscow, 2002, 48–66.

[8] É. Fouvry, *Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums*, Israel J. Math. 120 (2000), 81–96.

[9] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. 72 (1995), 235–275.

[10] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[11] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. 342 (1994), 729–752.

[12] W. Luo, *Rational points on complete intersections over* $\mathbb{F}_p$, Int. Math. Res. Notices 1999, 901–907.

[13] O. Marmon, *The density of integral points on hypersurfaces of degree at least four*, Acta Arith. 141 (2010), 211–240.

[14] S. T. Parsell, *On the Bombieri–Korobov estimate for Weyl sums*, Acta Arith. 138 (2009), 363–372.

[15] J. Pila, *Density of integral and rational points on varieties*, in: Columbia University Number Theory Seminar (New York, 1992), Astérisque 228 (1995), 183–187.

[16] J. Pila, *Density of integer points on plane algebraic curves*, Int. Math. Res. Notices 1996, 903–912.

[17] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Ann. of Math. 175 (2012), 1575–1627.

[18] Z. Zheng, *The distribution of zeros of an irreducible curve over a finite field*, J. Number Theory 59 (1996), 106–118.

Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521, U.S.A.
E-mail: mcc@math.ucr.edu

Received on 26.8.2013
and in revised form on 7.8.2014 (7567)