POINTS ON CURVES IN SMALL BOXES AND APPLICATIONS

MEI-CHU CHANG, JAVIER CILLERUELO, MOUBARIZ Z. GARAEV, JOSÉ HERNÁNDEZ, IGOR E. SHPARLINSKI, AND ANA ZUMALACÁRREGUI

Abstract. We introduce several new methods to obtain upper bounds on the number of solutions of the congruences

$$f(x) \equiv y \pmod p \qquad \text{and} \qquad f(x) \equiv y^2 \pmod p,$$

with a prime p and a polynomial f, where (x, y) belongs to an arbitrary square with side length M. We give two applications of these results to counting hyperelliptic curves in isomorphism classes modulo p and to the diameter of partial trajectories of a polynomial dynamical system modulo p.

1. Introduction

1.1. **Motivation.** Studying the distribution of integer and rational points on curves, and more general on algebraic varieties that belong to a given box is a classical topic in analytic number theory. For the case of plane curves with integer coefficients, essentially the best possible results are due to Bombieri and Pila [6, 32, 33]. Furthermore, recently remarkable progress has been made in the case of hypersurfaces and varieties over the rationals, see the surveys [8, 21, 36] as well as the original works [27, 28, 34].

Significantly less is known about the distribution of points in boxes on curves and varieties in finite fields. For reasonably large boxes, bounds on exponential sums, that in turn are based on deep methods of algebraic geometry, lead to asymptotic formulas for the number of such points, see [17, 18, 26]. Certainly when the size of the box is decreasing then beyond a certain threshold no asymptotic formula is possible (in fact the expected number of points can be less than 1). In particular, for such a small box only one can expect to derive upper bounds on the number of points on curves that hit it. This question has recently been introduced in [13], where a series of general results has been obtained (we also mention the work [9, 12, 42], where this question has been studied for some very special curves).

1991 *Mathematics Subject Classification.* 11D79, 11G20.

In the present paper we introduce new ideas and make significant advances in this direction. We find connections between the problem of distribution of points in small boxes on modular curves with some delicate combinations of results from geometry of numbers, Diophantine approximation theory, the Vinogradov mean value theorem and the Weyl method.

Note that in the case of curves modulo p it is not quite clear what one can expect as an "optimal" result (in contrast to the case of estimating integer points in boxes on plane curves over $\mathbb{Q}$). Yet in some parameter ranges our results are the best possible and can be considered as modulo p analogue of the results of Bombieri and Pila [6, 32, 33].

Although our results are related to classical problems, here we also give two further applications:

First of all, we study the distribution of isomorphism classes of hyperelliptic curves of genus $g \ge 1$ in some families of curves associated with polynomials with coefficients in a small box. In the case of elliptic curves this question has been studied in [14]. Here we improve some of the results of [14] and also use new methods to study the case of $g \ge 2$. Surprisingly enough, in the case of the genus $g \ge 2$ we obtain estimates and use methods that do not apply to elliptic curves (that is, to $g = 1$).

Second, we consider polynomial dynamical systems and study for how long a particular trajectory of such a system can be "locked" in a given box. In particular, we extend and improve several results of [10, 11, 13, 19].

1.2. **Basic definitions and problem formulation.** For a prime p, let $\mathbb{F}_p$ denote the finite field of p elements, which we assume to be represented by the set $\{0, 1, \ldots, p-1\}$.

Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $m \ge 2$. Then for $1 \le M < p$ we define $J_f(M; R, S)$ as the number of solutions to the congruence

$$y \equiv f(x) \pmod p, \quad (x, y) \in [R+1, R+M] \times [S+1, S+M].$$

This quantity has been the primal object of study in [13]. Here we consider a substantially more complicated case.

Given a polynomial $f \in \mathbb{F}_p[X]$ of degree $m \ge 3$, and a positive integer $M < p$, we define by $I_f(M; R, S)$ the number of solutions to the congruence

$$y^2 \equiv f(x) \pmod p, \tag{1}$$

with

$$(x, y) \in [R+1, R+M] \times [S+1, S+M]. \tag{2}$$

If the polynomial $y^2 - f(x)$ is absolutely irreducible, it is known from the Weil bounds that

$$I_f(M;R,S) = \frac{M^2}{p} + O(p^{1/2}(\log p)^2), \tag{3}$$

where the implied constant depends only on m, see [37, 41]. It is clear that the main term is dominated by the error term for $M \le p^{3/4}\log p$, and for $M \le p^{1/2}(\log p)^2$ the result becomes weaker than the trivial upper bound $I_f(M;R,S) \le 2M$. Here we use a different approach and give a nontrivial estimate of $I_f(M;R,S)$ for $M < p^{1/3-\varepsilon}$ when $m \ge 3$. In particular, in the case $m = 3$ our result improves on the range of M the bound obtained in [14].

Furthermore, we also obtain a new bound on $J_f(M;R,S)$ which improves that of [13].

We also mention that nontrivial bounds on the number of solutions (x,y) to the congruences

$$xy \equiv a \pmod p,$$

and

$$y \equiv \vartheta^x \pmod p,$$

satisfying (2), have been given in [9] with further improvements in [12]. Similar results for the congruence

$$Q(x,y) \equiv 0 \pmod p,$$

where $Q(x,y)$ is an absolutely irreducible quadratic form with a nonzero discriminant, can be found in [42].

1.3. **General notation.** Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may occasionally depend, where obvious, on the degree of polynomial $f \in \mathbb{F}_p[X]$, on the genus g and the real positive parameters ε and δ, and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$.

The letters, h, m, n, r, s in both upper and lower case, always denote integer numbers.

2. Main Results

2.1. **Points on curves in small boxes.** We combine ideas from [12, 13, 14] with some new ideas and derive the following results.

Theorem 1. *Uniformly over all polynomials* $f \in \mathbb{F}_p[X]$ *of degree* $\deg f = 3$ *and* $1 \le M < p$*, we have*

$$I_f(M; R, S) < M^{1/3+o(1)} + \frac{M^{5/3+o(1)}}{p^{1/6}},$$

as $M \to \infty$.

One of the implications of Theorem 1 is that for elliptic curves, that is, when the polynomial f in (1) if cubic, the bound $I_f(M; R, S) < M^{1/3+o(1)}$ holds for $M \ll p^{1/8}$, while [14, Theorem 5.1] guarantees this bound only for $M \ll p^{1/9}$. The range in which we have $I_f(M; R, S) < M^{1/3+o(1)}$ is of interest as this bound is essentially the best possible. In fact it is easy to see that for any positive $M < p$ and, say $f(X) = X^m$, examining the points $(x, y) = (t^m, t^2)$, $1 \le t \le M^{1/m}$, we conclude that

$$I_f(M; 0, 0) \gg M^{1/m}.$$

We also note that when $\deg f = 3$, our upper bounds for $I_f(M; R, S)$ imply the same bounds for $N(H; \mathfrak{B})$ in the case of elliptic curves.

Further, when $M < p^{1/4-\varepsilon}$ for some $\varepsilon > 0$, Theorem 1 guarantees a nontrivial bound $I_f(M; R, S) \ll M^{1-\delta}$ with some $\delta > 0$ that depends only on ε, improving upon the range $M < p^{1/5-\varepsilon}$ obtained in [14]. However, using a new approach, we obtain the following bound which is nontrivial in the range $M < p^{1/3-\varepsilon}$.

Theorem 2. *Uniformly over all polynomials* $f \in \mathbb{F}_p[X]$ *of degree* $\deg f = 3$ *and* $M \ge 1$*, we have*

$$I_f(M; R, S) \le M^{1/3+o(1)} + \left(\frac{M^3}{p}\right)^{1/16} M^{1+o(1)}.$$

The proof of Theorem 2 is based on combinations of results from the geometry of numbers, the current state of art on Vinogradov's mean value theorem due to Wooley [39, 40] and the Diophantine approximation theory. Our use of the geometry of numbers is close to the ideas of the work Bourgain et. al. [7],

The combination of Theorems 1 and 2 gives the following estimate:

Corollary 3. *Uniformly over all polynomials* $f \in \mathbb{F}_p[X]$ *of degree* $\deg f = 3$ *and* $1 \le M < p$*, we have*

$$I_f(M; R, S) < M^{1+o(1)} \begin{cases} M^{-2/3}, & \text{if } M < p^{1/8}, \\ (M^4/p)^{1/6}, & \text{if } p^{1/8} \le M < p^{5/23}, \\ (M^3/p)^{1/16}, & \text{if } p^{5/23} \le M < p^{1/3}, \end{cases}$$

as $M \to \infty$.

Our next result shows that when $\deg f \ge 4$ we also have a nontrivial bound for $I_f(M; R, S)$ in the range $M < p^{1/3-\varepsilon}$.

To formulate our result, we define $J_{k,m}(H)$ as the number of solutions of the system of m diophantine equations in $2k$ integral variables $x_1, \ldots, x_{2k}$:

$$\begin{cases} x_1^m + \ldots + x_k^m = x_{k+1}^m + \ldots x_{2k}^m, \\ \qquad\qquad \ldots \\ x_1 + \ldots + x_k = x_{k+1} + \ldots x_{2k}, \end{cases} \tag{4}$$
$$1 \le x_1, \ldots, x_{2k} \le H.$$

We also define $\kappa(m)$ to be the smallest integer κ such that for any integer $k \ge \kappa$ there exists a constant $C(k,m)$ depending only on k and m and such that

$$J_{k,m}(H) \le C(k,m) H^{2k-m(m+1)/2+o(1)}, \tag{5}$$

as $H \to \infty$. Note that by a recent result of Wooley [40, Theorem 1.1], that improves the previous estimate of [39], we have $\kappa(m) \le m^2 - 1$ for any $m \ge 3$.

Theorem 4. *Uniformly over all polynomials $f \in \mathbb{F}_p[X]$ of degree $\deg f = m \ge 4$ and $1 \le M < p$, we have*

$$I_f(M; R, S) \le M(M^3/p)^{1/2\kappa(m)+o(1)} + M^{1-(m-3)/2\kappa(m)+o(1)},$$

as $M \to \infty$.

In particular, for any $\varepsilon > 0$, there exists $\delta > 0$ that depends only on ε and $\deg f$ such that if $M < p^{1/3-\varepsilon}$ and $\deg f \ge 4$, then $I_f(M; R, S) \ll M^{1-\delta}$.

2.2. **Polynomial values in small boxes.** We also prove a new estimate on $J_f(M; R, S)$.

Theorem 5. *Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree $m \ge 2$. Then for $1 \le M < p$ we have*

$$J_f(M; R, S) \ll \frac{M^2}{p} + M^{1-1/2^{m-1}} p^{o(1)}$$

as $p \to \infty$.

We remark that for large values of m some bounds of [13], obtained by a different method, are better than Theorem 5. However for small values of m (for example, for $m = 2, 3$) Theorem 5 gives stronger estimates.

3. Applications

3.1. **Isomorphism classes of hyperelliptic curves in thin families.** A special case of the equation (1) are hyperelliptic curves over $\mathbb{F}_p$. The problem of concentration of points on hyperelliptic curves and polynomial maps is connected with some problems on isomorphisms that preserve hyperelliptic curves. Let g be a fixed positive integer constant. We always assume that p is large enough so, in particular, we have $\gcd(p, 2(2g+1)) = 1$. Any hyperelliptic curve can be given by a non-singular *Weierstrass equation:*

$$H_{\mathbf{a}}: \quad Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1X + a_0,$$

where $\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathbb{F}_p^{2g}$ (we recall that the non-singularity condition is equivalent to non-vanishing of the discriminant of the polynomial $X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1X + a_0$). We refer to [1] for a background on hyperelliptic curves and their applications.

It follows from a more general result of Lockhart [25, Proposition 1.2] that isomorphisms that preserve hyperelliptic curves given by Weierstrass equations are all of the form $(x, y) \to (\alpha^2 x, \alpha^{2g+1} y)$ for some $\alpha \in \mathbb{F}_p^*$, see also [23, Section 3]. Thus $H_{\mathbf{a}}$ is isomorphic to $H_{\mathbf{b}}$, which we denote as $H_{\mathbf{a}} \sim H_{\mathbf{b}}$, if there exists $\alpha \in \mathbb{F}_p^*$ such that

$$a_i \equiv \alpha^{4g+2-2i} b_i \pmod p, \qquad i = 0, \ldots, 2g-1. \tag{6}$$

It is known (see [23, 30]) that the number of non isomorphic hyperelliptic curves of genus g over $\mathbb{F}_p$ is $2p^{2g-1} + O(gp^{2g-2})$. We address here the problem of estimating from below, the number of non-isomorphic hyperelliptic curves of genus g over $\mathbb{F}_p$, $H_{\mathbf{a}}$, when $\mathbf{a} = (a_0, \ldots, a_{2g-1})$ belongs to a small $2g$-dimensional cube

$$\mathfrak{B} = [R_0 + 1, R_0 + M] \times \ldots \times [R_{2g-1} + 1, R_{2g-1} + M] \tag{7}$$

with some integers R_j, M satisfying $0 \le R_j < R_j + M < p$, $j = 0, \ldots, 2g-1$.

In particular, we note that all components of a vector $\mathbf{a} \in \mathfrak{B}$ are non-zero modulo p. Our methods below work without this restriction as well, however they somewhat lose their efficiency.

We also give an upper bound for the number

$$N(H; \mathfrak{B}) = \#\{\mathbf{a} = (a_0, \ldots, a_{2g-1}) \in \mathfrak{B} : \ H_{\mathbf{a}} \sim H\} \tag{8}$$

of hyperelliptic curves $H_{\mathbf{a}}$ with $\mathbf{a} \in \mathfrak{B}$ that are isomorphic to a given curve H.

In particular, our estimates extend and improve some of the results of [14] where this problem has been investigated for elliptic curves (that is, for $g = 1$).

First we observe that for large cubes one easily derives from the Weil bound (see [22, Chapter 11]) an asymptotic formula

$$N(H;\mathfrak{B}) = \frac{M^{2g}}{p^{2g-1}} + O(p^{1/2}(\log p)^{2g})$$

(see also the proof of [22, Theorem 21.4]). So we have an asymptotic formula for $N(H;\mathfrak{B})$ as long as $M \ge p^{1-1/(4g)+\varepsilon}$ for any fixed $\varepsilon > 0$.

However, here we are mostly interested in small values of M.

We note that we always have the trivial upper bound

$$N(H;\mathfrak{B}) \le 2M.$$

To see this, let $H = H_{\mathbf{b}}$, $\mathbf{b} = (b_0, \ldots, b_{2g-1}) \in \mathbb{F}_p^{2g}$, be given by a Weierstrass equation. We observe that if $H_{\mathbf{a}} \sim H$ and $H = H_{\mathbf{b}}$, where $\mathbf{b} = (b_0, \ldots, b_{2g-1}) \in \mathbb{F}_p^{2g}$ then a_{2g-1} can take at most M values in $\mathbb{F}_p^*$, and each a_{2g-1} determines two possible values for α^2 in (6).

It is also useful to remark that one can not expect to get a general bound stronger than

$$N(H;\mathfrak{B}) = O(M^{1/(2g+1)}).$$

To see this we consider the set $\mathcal{Q}$ of quadratic residues modulo p in the interval $[1, M^{1/(2g+1)}]$. It is well-known that for almost all primes p (that is, for all except a set of relative density zero) we have

$$\#\mathcal{Q} \sim 0.5M^{1/(2g+1)}.$$

For example, this follows from a bound of Heath-Brown [20, Theorem 1] on average values of sums of real characters.

Consider now the set

$$\mathcal{A} = \{\alpha \in \mathbb{F}_p \ : \ \alpha^2 \in \mathcal{Q}\},$$

the curve $H : Y^2 = X^{2g+1} + X^{2g-1} + X^{2g-2} + \ldots + X + 1$ and the $2g$-dimensional cube $\mathfrak{B} = [1, M]^{2g}$. It is clear that $(\alpha^4, \alpha^6, \ldots, \alpha^{4g+2}) \in \mathfrak{B}$ for all $\alpha \in \mathcal{A}$. On the other hand $\#\mathcal{A} = 2\#\mathcal{Q} \sim M^{1/(2g+1)}$.

We now turn to estimates on $N(H;\mathfrak{B})$ given by (8). A simple observation shows that in the case of hyperelliptic curves with $g \ge 2$ the quantity $N(H;\mathfrak{B})$ is closely related to the problem of concentration of points of a quadratic polynomial map. Then one can apply the general result of [13] and get a nontrivial upper bound for $N(H;\mathfrak{B})$ for any range of M. However, here we use a different approach and we obtain a better bound.

Using (6), we derive from Theorem 5 and the bound of [13]

$$J_f(M;R,S) \ll M^{1/m+o(1)}$$

that holds for $M \le p^{2/(m^2+3)}$, the following consequence

Theorem 6. *For any hyperelliptic curve H of genus $g \ge 2$ over $\mathbb{F}_p$ and cube $\mathfrak{B}$ given by* (7) *with $1 \le M < p$, we have*

$$N(H; \mathfrak{B}) \ll \frac{M^2}{p} + M^{1/2+o(1)}.$$

Furthermore, as we have mentioned above, when $g = 1$ the problem of estimating $N(H; \mathfrak{B})$ is equivalent to estimating the concentration of points on certain curves of degree 3 (which are singular and thus are not elliptic curves) and Theorem 1 applies in this case. Using the idea of the proof of Theorem 1, we establish the following result which is valid for any hyperelliptic curve.

Theorem 7. *For any hyperelliptic curve H of genus $g \ge 1$ over $\mathbb{F}_p$, any cube $\mathfrak{B}$ given by* (7) *with $1 \le M < p$ and any odd integer $h \in [3, 2g+1]$, we have*

$$N(H; \mathfrak{B}) < \left(M^{1/h} + M \left(M^4/p\right)^{2/h(h+1)}\right) M^{o(1)},$$

as $M \to \infty$.

We observe that if $M < p^{1/(2g^2+2g+4)}$ then, taking $h = 2g + 1$ in Theorem 7, we obtain the estimate $N(H; \mathfrak{B}) \le M^{1/(2g+1)+o(1)}$ which, as we have seen, is sharp up to the $o(1)$ term.

Let $\mathcal{H}(\mathfrak{B})$ be a collection of representatives of all isomorphism classes of hyperelliptic curves $H_{\mathbf{a}}$, $\mathbf{a} \in \mathfrak{B}$, where $\mathfrak{B}$ is a $2g$-dimensional cube of side length M. In [14] the lower bound $\#\mathcal{H}(\mathfrak{B}) \gg \min\{p, M^{2+o(1)}\}$ has been obtained for elliptic curves (that is, for $g = 1$). We extend this result to $g \ge 2$. Certainly the upper bounds of our theorems lead to a lower bound on $\#\mathcal{H}(\mathfrak{B})$. However, using a different approach we obtain a near optimal bound for $\#\mathcal{H}(\mathfrak{B})$.

Theorem 8. *For $g \ge 1$ and any cube $\mathfrak{B}$ given by* (7) *with and $1 \le M < p$, we have*

$$\#\mathcal{H}(\mathfrak{B}) \gg \min\{p^{2g-1}, M^{2g+o(1)}\},$$

as $M \to \infty$. Furthermore, if $g \ge 2$ the $o(1)$ term can be removed when $M > p^{1/(2g)}$.

3.2. **Diameter of polynomial dynamical systems.** Results about concentration of points on curves are also closely related to the question about the diameter of partial trajectories of polynomial dynamical systems. Namely, given a polynomial $f \in \mathbb{F}_p[X]$ and an element $u_0 \in \mathbb{F}_p$, we consider the sequence of elements of $\mathbb{F}_p$ generated by iterations $u_n = f(u_{n-1})$, $n = 0, 1, \ldots$. Clearly the sequence u_n is eventually periodic. In particular, let T_{f,u_0} be the full trajectory length, that is, the smallest integer t such that $u_t = u_s$ for some $s < t$. The study of the diameter

$$D_{f,u_0}(N) = \max_{0\le k,m\le N-1} |u_k - u_m|$$

has been initiated in [19] and then continued in [10, 11, 13]. In particular, it follows from [19, Theorem 6] that for any fixed ε, for $T_{f,u_0} \ge N \ge p^{1/2+\varepsilon}$ we have the asymptotically best possible bound

$$D_{f,u_0}(N) = p^{1+o(1)}$$

as $p \to \infty$. For smaller values of N a series of lower bounds on $D_{f,u_0}(N)$ is given in [10, 11, 13].

One easily derives from Theorem 5 the following estimate, which improves several previous results to intermediate values of N (and is especially effective for small values of m).

Corollary 9. *For any polynomial $f \in \mathbb{F}_p[X]$ of degree $m \ge 2$ and positive integer $N \le T_{f,u_0}$, we have*

$$D_{f,u_0}(N) \gg \min\{N^{1/2}p^{1/2}, N^{1+1/(2^{m-1}-1)}p^{o(1)}\},$$

as $p \to \infty$.

On the other hand, we remark that our method and results do not affect the superpolynomial lower bounds of [10, 11] that hold for small values of N.

4. Preparations

4.1. **Uniform distribution and exponential sums.** The following result is well-known and can be found, for example, in [29, Chapter 1, Theorem 1] (which is a more precise form of the celebrated Erdős–Turán inequality).

Lemma 10. *Let $\gamma_1, \ldots, \gamma_M$ be a sequence of M points of the unit interval $[0,1]$. Then for any integer $K \ge 1$, and an interval $[\alpha,\beta] \subseteq [0,1]$, we have*

$$\#\{n = 1,\ldots,M \ : \gamma_n \in [\alpha,\beta]\} - M(\beta-\alpha) \ll \frac{M}{K} + \sum_{k=1}^{K}\left(\frac{1}{K} + \min\{\beta-\alpha, 1/k\}\right)\left|\sum_{n=1}^{M}\exp(2\pi i k\gamma_n)\right|.$$

To use Lemma 10 we also need an estimate on exponential sums with polynomials, which is essentially due to Weyl, see [22, Proposition 8.2].

Let $\|\xi\| = \min\{|\xi - k| \ : \ k \in \mathbb{Z}\}$ denote the distance between a real ξ and the closest integer.

Lemma 11. *Let $f(X) \in \mathbb{R}[X]$ be a polynomial of degree $m \ge 2$ with the leading coefficient $\vartheta \neq 0$. Then*

$$\left|\sum_{n=1}^{M} \exp(2\pi i f(n))\right|$$
$$\ll M^{1-m/2^{m-1}} \left(\sum_{-M<\ell_1,\ldots,\ell_{m-1}<M} \min\{M, \|\vartheta m! \ell_1 \ldots \ell_{m-1}\|^{-1}\} \right)^{2^{1-m}}.$$

4.2. **Integer points on curves and varieties.** We also need the following estimate of Bombieri and Pila [6] on the number of integral points on polynomial curves.

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

The following statement is a particular case of a more general result of Wooley [40, Theorem 1.1].

Lemma 13. *The number of solutions of the system of diophantine equations*

$$x_1^j + \ldots + x_8^j = x_9^j + \ldots + x_{16}^j, \quad j = 1, 2, 3$$

in integers x_i with $|x_i| \le M$, $i = 1, \ldots, 16$, is at most $M^{10+o(1)}$.

Proof. Writing $x_i = X_i - M - 1$ with a positive integer $X_i \le 2M + 1$, $i = 1, \ldots, 16$, after some trivial algebraic transformation we see that the number of solutions to the above equation is equal to $J_{8,3}(2M+1)$. Since by the result of Wooley [40, Theorem 1.1] we have $\kappa(3) \le 8$, the bound (5) applies with $H = 2M + 1$. □

We note that Lemma 13 can be formulated in a more general form with $\kappa(3)$ instead of 8 variables on each side, but this generalization (assuming possible improvements of the bound $\kappa(3) \le 8$) does not affect our main results.

4.3. **Congruences with many solutions.** The following result is used in the proofs of Theorems 1 and 7.

Lemma 14. *Let $f, g \in \mathbb{F}_p[X]$ be two polynomials of degrees n and m such that $m \nmid n$. Assume that the integers $x_1, \ldots, x_n$ are pairwise distinct modulo p and $y_1, \ldots, y_n$ are arbitrary integers. Then the congruence*

$$f(x) \equiv g(y) \pmod p, \qquad 0 \le x, y < p, \tag{9}$$

has at most mn solutions with

$$\det \begin{pmatrix} x^n & x^{n-1} & \dots & x & y \\ x_1^n & x_1^{n-1} & \dots & x_1 & y_1 \\ & & \dots & & \\ x_n^n & x_n^{n-1} & \dots & x_n & y_n \end{pmatrix} \equiv 0 \pmod p. \tag{10}$$

Proof. Since

$$\det \begin{pmatrix} x_1^n & x_1^{n-1} & \dots & x_1 \\ & & \dots & \\ x_n^n & x_n^{n-1} & \dots & x_n \end{pmatrix} = x_1 \dots x_n \prod_{1 \le i < j \le n} (x_i - x_j) \not\equiv 0 \pmod p,$$

we deduce that, for any x and y, the last column in (10) is a unique modulo p linear combination of the previous columns. In particular, for every solution (x, y) to (9) and (10) we have $y \equiv h(x) \pmod p$ for some nontrivial polynomial $h(X) \in \mathbb{F}_p[X]$ that does not depend on x and y.

Now we insert this into (9). We observe that now the right hand side of (9), that is $g(h(x))$, is a nontrivial polynomial of degree $m \deg h$. Thus, the congruence (9) is a nontrivial polynomial congruence of degree d with $n \le d \le mn$. Therefore, it has at most mn solutions modulo p. □

4.4. **Symmetric multiplicative congruences.** For given positive integers i, j, we define $T_{i,j}(R, S; M)$ as the number of solutions to the congruence

$$r^i v^j \equiv u^i s^j \pmod p$$

with $(r, s), (u, v) \in [R + 1, R + M] \times [S + 1, S + M]$.

It has been shown in [14, Theorem 4.1] that for a positive $M < p$ we have

$$T_{i,j}(R, S; M) = d \frac{M^4}{p-1} + O\left(M^2 p^{o(1)}\right) \tag{11}$$

as $M \to \infty$, where $d = \gcd(i, j, p - 1)$. We need a slight modification of that statement, where $p^{o(1)}$ is replaced by $M^{o(1)}$.

Lemma 15. *For any prime p and any integers M, R, S with*

$$R, S \ge 0, \ M \ge 1 \quad \text{and} \quad R + M, S + M < p$$

we have,

$$T_{i,j}(R, S; M) = d \frac{M^4}{p-1} + O\left(M^{2+o(1)}\right)$$

as $M \to \infty$, where $d = \gcd(i, j, p-1)$ and the implied constant depends only on i and j.

Proof. We note that for $M \ge p^{1/2}$ the result follows from (11). For $M < p^{1/2}$, the result is equivalent to the upper bound $T_{i,j}(R,S;M) \le M^{2+o(1)}$ since the implied constant is allowed to depend on d.

As in the proof of [14, Theorem 4.1], using the orthogonality of multiplicative characters, we write

$$\begin{aligned} T_{i,j}(R,S;M) &= \sum_{r,u=R+1}^{R+M} \sum_{s,v=S+1}^{R+M} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \chi\left((r/u)^i (v/s)^j\right) \\ &= \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \left| \sum_{r=R+1}^{R+M} \chi^i(r) \right|^2 \left| \sum_{s=S+1}^{S+M} \chi^j(s) \right|^2 . \end{aligned}$$

We estimate the contribution to the above sum from at most $i + j$ characters χ with $\chi^i = \chi_0$ or $\chi^j = \chi_0$, where χ_0 is the principal character, as $O(M^4/p) = O\left(M^{2+o(1)}\right)$.

The rest of the sum can also be estimated as $O\left(M^{2+o(1)}\right)$ by following exactly the same argument as in [14, Theorem 4.1] and using [14, Lemma 2.2]. □

4.5. **Background on geometry of numbers.** We recall that a lattice in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors. Let D be a symmetric convex body, that is, D is a compact convex subset of $\mathbb{R}^n$ with non-empty interior that is centrally symmetric with respect to 0. Then, for a lattice in $\Gamma \subseteq \mathbb{R}^n$ 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 number λ such that the set λD contains i linearly independent vectors of the lattice Γ. In particular $\lambda_1(D,\Gamma) \le \ldots \le \lambda_n(D,\Gamma)$. We recall the following result given in [3, Proposition 2.1] (see also [35, Exercise 3.5.6] for a simplified form that is still enough for our purposes).

Lemma 16. *We have,*

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

Using that

$$\frac{2i}{\lambda_i(D,\Gamma)} + 1 \le (2i+1) \max\left\{ \frac{1}{\lambda_i(D,\Gamma)}, 1 \right\}$$

and denoting, as usual, by $(2n+1)!!$ the product of all odd positive numbers up to $2n+1$, we derive:

Corollary 17. *We have,*

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

5. Proofs

5.1. **Proof of Theorem 1.** For the sake of brevity, in this section we denote $I = I_f(M;R,S)$. We can assume that I is large. We fix some integer L with

$$1 \le L \le 0.01I, \tag{12}$$

to be chosen later. By the pigeonhole principle, there exists Q such that the congruence

$$y^2 \equiv f(x) \pmod p, \qquad Q+1 \le x \le Q+M/L,\ S+1 \le y \le S+M,$$

has at least I/L solutions. We can split the interval $[Q+1, Q+M/L]$ into $k_0 = \lceil I/(30L)\rceil$ intervals of length not greater than $30M/I$. Since there are at most two solutions to the above congruence with the same value of x, and since we have at least $I/L > 20k_0$ solutions in total, from the pigeonhole principle it follows that there exists an interval of length $30M/I$ containing at least 10 pairwise distinct values of x. Let x_0 be the first of these values and let (x_0, y_0) be the corresponding solution. It is clear that I/L is bounded by the number of solutions of

$$(y_0+y)^2 \equiv f(x_0+x) \pmod p,$$
$$-M/L \le x \le M/L, \quad -M \le y \le M,$$

which is equivalent to

$$\begin{aligned} &y^2 \equiv c_3x^3 + c_2x^2 + c_1x + c_0y \pmod p,\\ &-M/L \le x \le M/L, \quad -M \le y \le M, \end{aligned} \tag{13}$$

with $(c_3, p) = 1$. Besides, there are at least 10 solutions (x, y) with x pairwise distinct and such that $0 \le x \le 30M/I$. From these 10 values we fix 3 solutions $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ and rewrite the congruence (13) in the matrix form

$$\begin{pmatrix} x^3 & x^2 & x & y \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod p. \tag{14}$$

By Lemma 14, we know that at most 6 pairs (x, y), with x pairwise distinct, satisfy both the congruence (14) and the congruence

$$\begin{vmatrix} x^3 & x^2 & x & y \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{vmatrix} \equiv 0 \pmod p.$$

Since there are at least 10 solutions to (14), for one of them, say (x_4, y_4), we have

$$\Delta = \begin{vmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{vmatrix} \not\equiv 0 \pmod p.$$

Note that $1 \le |\Delta| \ll (M/I)^6 M$. Now we solve the system of congruences

$$\begin{pmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_4^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod p \tag{15}$$

with respect to (c_3, c_2, c_1, c_0). We write Δ_j for the determinant of the matrix on the left hand side where we have substituted the column j by the vector $(y_4^2, y_3^2, y_2^2, y_1^2)$. With this notation we have that

$$c_j \equiv \Delta_{4-j}\Delta^* \pmod p, \quad j = 0, \ldots, 3,$$

where Δ^* is defined by $\Delta\Delta^* \equiv 1 \pmod p$, and the congruence (13) is equivalent to

$$\Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x + \Delta_4 y - \Delta y^2 \equiv 0 \pmod p.$$

In particular, since, as we have noticed, $c_3 \not\equiv 0 \pmod p$, we have that $\Delta_1 \not\equiv 0 \pmod p$. We can write this congruence as an equation over $\mathbb{Z}$:

$$\Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x + \Delta_4 y - \Delta y^2 = pz, \qquad (x, y, z) \in \mathbb{Z}^3. \tag{16}$$

We can easily check that

$$|\Delta_4| \ll (M/I)^6 M^2$$

and

$$|\Delta_j| \ll (M/I)^{2+j} M^3, \qquad j = 1, 2, 3.$$

Thus, collecting the above estimates and taking into account $L \ll I$, we derive

$$\begin{aligned}|z| &\ll \frac{1}{p}\left(|\Delta_1|(M/L)^3 + |\Delta_2|(M/L)^2 + |\Delta_3|(M/L) + |\Delta_4|M + |\Delta|M^2\right)\\ &\ll \frac{M^3}{p}\left(\frac{M^6}{I^3L^3} + \frac{M^6}{I^4L^2} + \frac{M^6}{I^5L} + \frac{M^6}{I^6}\right) \ll \frac{M^9}{pI^3L^3}.\end{aligned}$$

Since $\Delta_1 \neq 0$, $\Delta \neq 0$, for each z, the curve (16) is absolutely irreducible, and thus by Lemma 12 it contains at most $M^{1/3+o(1)}$ integer points (x, y) with $|x|, |y| \leq M$. Hence

$$\frac{I}{L} \leq M^{1/3+o(1)}\left(1 + \frac{M^9}{pI^3L^3}\right)$$

for any L satisfying (12). This implies, that

$$I \leq LM^{1/3+o(1)} + \frac{M^{7/3}}{p^{1/4}L^{1/2}}. \tag{17}$$

If $M < 10p^{1/8}$, then we take $L = 1$ and derive from (17) that

$$I \leq M^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}} \leq M^{1/3+o(1)}.$$

Let now $M > 10p^{1/8}$. We can assume that $I > M^{5/3}p^{-1/6}$, as otherwise there is nothing to prove. Then we take $L = \lfloor M^{4/3}p^{-1/6}\rfloor$ and note that the condition (12) is satisfied. Thus, we derive from (17) that

$$I \leq LM^{1/3+o(1)} + \frac{M^{7/3+o(1)}}{p^{1/4}L^{1/2}} \leq M^{5/3+o(1)}p^{-1/6}$$

and the result follows.

5.2. **Proof of Theorem 2.** Clearly we can assume that

$$M > p^{5/23} \tag{18}$$

as otherwise

$$(M^3/p)^{1/16}M \geq \frac{M^{5/3+o(1)}}{p^{1/6}}$$

and the result follows from Theorem 1. We can also assume that $M = o(p^{1/3})$.

We fix one solution (x_0, y_0) to the congruence (1) and by making the change of variables $(x, y) \mapsto (x - x_0, y - y_0)$, we see that it is enough to study a congruence of the form

$$y^2 - c_0y \equiv c_3x^3 + c_2x^2 + c_1x \pmod p, \quad |x|, |y| \leq M. \tag{19}$$

Let $\mathcal{W}$ be the set of pairs (x, y) that satisfy (19), and by $\mathcal{X}$ we denote the set of x for which $(x, y) \in \mathcal{W}$ for some y. Let

$$\rho = \frac{\#\mathcal{X}}{M}.$$

We now fix some $\varepsilon > 0$ and assume that

$$\rho \geq (M^3/p)^{1/16} M^{\varepsilon}. \tag{20}$$

We also assume that M is sufficiently large. In view of (18) and (20), we also have

$$\rho > M^{-1/10}. \tag{21}$$

For $\vartheta > 0$ we define the intervals

$$I_{\nu,\vartheta} = [-\vartheta M^{\nu}, \vartheta M^{\nu}], \qquad \nu = 1, 2, 3,$$

which we treat as intervals in $\mathbb{F}_p$, that is, sets of residues modulo p of several consecutive integers.

We now consider the set

$$\mathcal{S} \subseteq I_{1,8} \times I_{2,8} \times I_{3,8}$$

of all triples

$$\mathbf{s} \equiv (x_1 + \ldots + x_8,\, x_1^2 + \ldots + x_8^2,\, x_1^3 + \ldots + x_8^3) \pmod p, \tag{22}$$

where x_i, $i = 1, \ldots, 8$, independently run through the set $\mathcal{X}$. We observe that the system of congruences

$$x_1^j + \ldots + x_8^j \equiv x_9^j + \ldots + x_{16}^j \pmod p, \qquad j = 1, 2, 3, \tag{23}$$

has at most $M^{10+o(1)}$ solutions in integers x_i, y_i with $|x_i|, |y_i| \leq M$. Indeed, since $M = o(p^{1/3})$, the above congruence is converted to the system of diophantine equations

$$x_1^j + \ldots + x_8^j = x_9^j + \ldots + x_{16}^j, \quad j = 1, 2, 3,$$

which by Lemma 13 has at most $M^{10+o(1)}$ solutions in integers x_i with $|x_i| \leq M$, $i = 1, \ldots, 16$. Therefore, the congruence (23) has at most $M^{10+o(1)}$ solutions in $x_i \in \mathcal{X}$, $i = 1, \ldots, 16$, as well. Thus, collecting elements of the set $\mathcal{X}^8$ that correspond to the same vector $\mathbf{s}$ given by (22) and denoting the number of such representations by $N(\mathbf{s})$, by the Cauchy inequality, we obtain

$$(\#\mathcal{X})^8 = \sum_{\mathbf{s} \in \mathcal{S}} N(\mathbf{s}) \leq \left(\#\mathcal{S} \sum_{\mathbf{s} \in \mathcal{S}} N(\mathbf{s})^2 \right)^{1/2} \leq \left(\#\mathcal{S} M^{10+o(1)} \right)^{1/2}.$$

Thus

$$\#\mathcal{S} \geq \frac{(\#\mathcal{X})^{16}}{M^{10+o(1)}} = \rho^{16} M^{6+o(1)}.$$

Hence, there exist at least $\rho^{16}M^{6+o(1)}$ triples

$$(z_1, z_2, z_3) \in I_{1,8} \times I_{2,8} \times I_{3,8}$$

such that

$$c_3z_3 + c_2z_2 + c_1z_1 \equiv \widetilde{z}_2 - c_0\widetilde{z}_1 \pmod p$$

for some $\widetilde{z}_2 \in I_{2,8}$ and $\widetilde{z}_1 \in I_{1,8}$. In particular we have that the congruence

$$\begin{gathered} c_3z_3 + c_2z_2 + \widetilde{z}_2 + c_1z_1 + c_0\widetilde{z}_1 \equiv 0 \pmod p, \\ (z_1, \widetilde{z}_1, z_2, \widetilde{z}_2, z_3) \in I_{1,8} \times I_{1,8} \times I_{2,8} \times I_{2,8} \times I_{3,8}, \end{gathered}$$

has a set of solutions $\mathcal{S}$ with

$$\#\mathcal{S} \geq \rho^{16}M^{6+o(1)}. \tag{24}$$

The rest of the proof is based on the ideas from [7].

We define the lattice

$$\begin{aligned} \Gamma = \{(X_2, X_3, \widetilde{X}_2, X_1, \widetilde{X}_1) \in \mathbb{Z}^5 \ : \\ X_2 + c_3X_3 + c_2\widetilde{X}_2 + c_1X_1 + c_0\widetilde{X}_1 \equiv 0 \pmod p\} \end{aligned}$$

and the body

$$\begin{aligned} D = \{(x_2, x_3, \widetilde{x}_2, x_1, \widetilde{x}_1) \in \mathbb{R}^5 \ : \\ |x_1|, |\widetilde{x}_1| \leq 8M, \ |x_2|, |\widetilde{x}_2| \leq 8M^2, \ |x_3| \leq 8M^3\}. \end{aligned}$$

We see from (24) that

$$\#\,(D \cap \Gamma) \geq \rho^{16}M^{6+o(1)}.$$

Therefore, by Corollary 17, the successive minima $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1, \ldots, 5$, satisfy the inequality

$$\prod_{i=1}^{5} \min\{1, \lambda_i\} \ll \rho^{-16}M^{-6+o(1)}. \tag{25}$$

From the definition of λ_i it follows that there are five linearly independent vectors

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \widetilde{v}_{2,i}, v_{1,i}, \widetilde{v}_{1,i}) \in \lambda_i D \cap \Gamma, \quad i = 1, \ldots, 5. \tag{26}$$

Indeed, first we choose a nonzero vector $\mathbf{v}_1 \in \lambda_1 D \cap \Gamma$. Then assuming that for $1 \leq i \leq 5$ the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$ are chosen, we choose $\mathbf{v}_i$ as one of the vectors $\mathbf{v} \in \lambda_i D \cap \Gamma$ that are not in the linear space generated by $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}$.

We now note that

$$\lambda_3 < 1.$$

Indeed, otherwise from (25) we obtain

$$\min\{1, \lambda_1^2\} \leq \min\{1, \lambda_1\} \min\{1, \lambda_2\} \leq \rho^{-16}M^{-6+o(1)}.$$

Thus recalling (21) we see that

$$\lambda_1 \le \frac{1}{10M^2}.$$

Then the vector $\mathbf{v}_1$ must have $v_{2,1} = \widetilde{v}_{2,1} = v_{1,1} = \widetilde{v}_{1,1} = 0$. In turn this implies that $v_{3,1} \equiv 0 \pmod p$ and since we assumed that $M = o(p^{1/3})$, we obtain $v_{3,1} = 0$, which contradicts the condition that $\mathbf{v}_1$ is a nonzero vector.

We consider separately the following four cases.

Case 1: $\lambda_5 \le 1$. Then by (25), we have

$$\prod_{i=1}^{5} \lambda_i \le \rho^{-16} M^{-6+o(1)}.$$

We now consider the determinant Δ of the 5×5 matrix that is formed by the vectors (26). It follows that

$$\Delta \ll M^{2+3+2+1+1} \prod_{i=1}^{5} \lambda_i \le \rho^{-16} M^{3+o(1)},$$

which, by our assumption (20), implies that $|\Delta| < p$. On the other hand, since $\mathbf{v}_i \in \Gamma$, we have $\Delta \equiv 0 \pmod p$, thus $\Delta = 0$ provided that p is large enough, which contradicts the linear independence of the vectors in (26). Thus this case is impossible.

Case 2: $\lambda_4 \le 1$, $\lambda_5 > 1$. Let

$$V = \begin{pmatrix} v_{3,1} & \widetilde{v}_{2,1} & v_{1,1} & \widetilde{v}_{1,1} \\ v_{3,2} & \widetilde{v}_{2,2} & v_{1,2} & \widetilde{v}_{1,2} \\ v_{3,3} & \widetilde{v}_{2,3} & v_{1,3} & \widetilde{v}_{1,3} \\ v_{3,4} & \widetilde{v}_{2,4} & v_{1,4} & \widetilde{v}_{1,4} \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} -v_{2,1} \\ -v_{2,2} \\ -v_{2,3} \\ -v_{2,4} \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix}.$$

We have

$$V\mathbf{c} \equiv \mathbf{w} \pmod p.$$

Let

$$\Delta = \det V$$

and let Δ_j be the determinant of the matrix obtained by replacing the j-th column of V by $\mathbf{w}$, $j = 1, \ldots, 4$.

Recalling (25), we have

$$|\Delta| \ll \lambda_1\lambda_2\lambda_3\lambda_4 M^{3+2+1+1} \le \rho^{-16} M^{1+o(1)} \tag{27}$$

and similarly

$$\begin{aligned} &|\Delta_1| \le \rho^{-16} M^{o(1)}, \qquad |\Delta_2| \le \rho^{-16} M^{1+o(1)}, \\ &|\Delta_3| \le \rho^{-16} M^{2+o(1)}, \qquad |\Delta_4| \le \rho^{-16} M^{2+o(1)}. \end{aligned} \tag{28}$$

Note that, in view of (20), in particular we have

$$|\Delta|, |\Delta_j| < p, \quad j = 1, \ldots, 4.$$

If $\Delta \equiv 0 \pmod p$ then since $\mathbf{c}$ is nonzero modulo p we also have $\Delta_j \equiv 0 \pmod p$, $j = 1, \ldots, 4$, implying that $\Delta = 0$, $\Delta_j = 0$. Then the matrix formed by $\mathbf{v}_1, \ldots, \mathbf{v_4}$ is of rank at most 3, which contradicts their linear independence. Therefore $\Delta \not\equiv 0 \pmod p$ and thus we have

$$c_i \equiv \frac{\Delta_{4-i}}{\Delta} \pmod p, \qquad i = 0, 1, 2, 3.$$

Since $c_3 \not\equiv 0 \pmod p$, we have $\Delta_1 \neq 0$. We now substitute this in (19) and get that

$$\Delta y^2 - \Delta_4 y \equiv \Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x \pmod p, \quad |x|, |y| \le M.$$

We see from (20), (27) and (28) that for sufficiently large M the absolute values of the expressions on both sides are less than $p/2$, implying the equality

$$\Delta y^2 - \Delta_4 y = \Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x, \qquad |x|, |y| \le M.$$

Now we use Lemma 12 and conclude that the number of solutions is at most $M^{1/3+o(1)}$.

Case 3: $\lambda_3 \le (10M)^{-1}$, $\lambda_4 > 1$. By (25), we have

$$\prod_{i=1}^{3} \lambda_i \le \rho^{-16} M^{-6+o(1)}.$$

Since $\lambda_3 \le (10M)^{-1}$, we also have

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \widetilde{v}_{2,i}, 0, 0), \quad i = 1, 2, 3. \tag{29}$$

In particular,

$$\begin{pmatrix} v_{2,1} & v_{3,1} & \widetilde{v}_{2,1} \\ v_{2,2} & v_{3,2} & \widetilde{v}_{2,2} \\ v_{2,3} & v_{3,3} & \widetilde{v}_{2,3} \end{pmatrix} \begin{pmatrix} 1 \\ c_3 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \pmod p.$$

Thus, for the determinant

$$\Delta = \det \begin{pmatrix} v_{2,1} & v_{3,1} & \widetilde{v}_{2,1} \\ v_{2,2} & v_{3,2} & \widetilde{v}_{2,2} \\ v_{2,3} & v_{3,3} & \widetilde{v}_{2,3} \end{pmatrix}$$

we have

$$\Delta \equiv 0 \pmod p.$$

On the other hand, from (21) we derive that

$$|\Delta| \ll \lambda_1 \lambda_2 \lambda_3 M^7 < \frac{M^{1+o(1)}}{\rho^{16}} < M^{2.6+o(1)}.$$

Hence, $\Delta = 0$, which together with (29) implies that the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly dependent, which is impossible.

Case 4: $(10M)^{-1} < \lambda_3 \le 1$, $\lambda_4 > 1$. By (25), we have

$$\prod_{i=1}^{3} \lambda_i \le \rho^{-16} M^{-6+o(1)}$$

and since $\lambda_3 > (10M)^{-1}$, we obtain

$$\lambda_1\lambda_2 < \rho^{-16} M^{-5+o(1)}.$$

We again note that $\lambda_1 > (10M^2)^{-1}$, as otherwise $\mathbf{v}_1$ must have $v_{2,1} = \widetilde{v}_{2,1} = v_{1,1} = \widetilde{v}_{1,1} = 0$. In turn this implies that $v_{3,1} \equiv 0 \pmod p$ and since we assumed that $M = o(p^{1/3})$, we obtain $v_{3,1} = 0$, which contradicts the condition that $\mathbf{v}_1$ is a nonzero vector.

Since $\lambda_1 > (10M^2)^{-1}$ and $\rho > M^{-1/10}$, we get that $\lambda_2 < (10M)^{-1}$. Thus, we have

$$\mathbf{v}_i = (v_{2,i}, v_{3,i}, \widetilde{v}_{2,i}, 0, 0), \qquad i = 1, 2.$$

Next,

$$\begin{pmatrix} v_{3,1} & \widetilde{v}_{2,1} \\ v_{3,2} & \widetilde{v}_{2,2} \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} -v_{2,1} \\ -v_{2,2} \end{pmatrix} \pmod p.$$

Now we observe that

$$\Delta = \det \begin{pmatrix} v_{3,1} & \widetilde{v}_{2,1} \\ v_{3,2} & \widetilde{v}_{2,2} \end{pmatrix} \ll \lambda_1\lambda_2 M^5 < \frac{M^{o(1)}}{\rho^{16}}. \tag{30}$$

Furthermore,

$$\Delta_1 = \det \begin{pmatrix} -v_{2,1} & \widetilde{v}_{2,1} \\ -v_{2,2} & \widetilde{v}_{2,2} \end{pmatrix} \ll \lambda_1\lambda_2 M^4 < \frac{M^{-1+o(1)}}{\rho^{16}}, \tag{31}$$

and

$$\Delta_2 = \det \begin{pmatrix} v_{3,1} & -v_{2,1} \\ v_{3,2} & -v_{2,2} \end{pmatrix} \ll \lambda_1\lambda_2 M^5 < \frac{M^{o(1)}}{\rho^{16}}. \tag{32}$$

In particular, $|\Delta|, |\Delta_1|, |\Delta_2| < p$. Therefore, if $\Delta \equiv 0 \pmod p$, then $\Delta_1 \equiv \Delta_2 \equiv 0 \pmod p$ and we see that $\Delta = \Delta_1 = \Delta_2 = 0$. Thus, in this case the rank of the matrix formed with vectors $\mathbf{v}_1, \mathbf{v}_2$ is at most 1, which contradicts the linear independence of the vectors $\mathbf{v}_1, \mathbf{v}_2$.

Hence, $\Delta \not\equiv 0 \pmod p$ and we get that

$$c_3 \equiv \frac{\Delta_1}{\Delta} \pmod p, \qquad c_2 \equiv \frac{\Delta_2}{\Delta} \pmod p.$$

We now substitute this in (19) and get that

$$\Delta y^2 - a_0 y \equiv \Delta_1 x^3 + \Delta_2 x^2 + b_0 x \pmod p, \qquad |x|, |y| \le M,$$

for some integers a_0, b_0. We observe that the condition $c_3 \not\equiv 0 \pmod p$ implies that $\Delta_1 \neq 0$.

Let now

$$T = \left\lfloor \left(\frac{p}{M}\right)^{1/3} \rho^{16/3} \right\rfloor.$$

Note that $M^{2/3} < T < T^2 < p/2$. By the pigeonhole principle, there exists a positive integer $1 \le t_0 \le T^2 + 1$ such that

$$|(t_0 a_0)_p| \le \frac{p}{T}, \qquad |(t_0 b_0)_p| \le \frac{p}{T},$$

where $(x)_p$ is the element of the residue class $x \pmod p$ with the least absolute value, see also [14, Lemma 3.2]. Hence

$$t_0\Delta y^2 - (t_0a_0)_p y \equiv t_0\Delta_1 x^3 + t_0\Delta_2 x^2 + (t_0 b_0)_p x \pmod p, \quad |x|, |y| \le M.$$

By (30), (31), (32), the absolute values of the expressions on both sides are bounded by $pM^{1+o(1)}T^{-1}$. Thus, we get

$$t_0\Delta y^2 - (t_0a_0)_p y = t_0\Delta_1 x^3 + t_0\Delta_2 x^2 + (t_0 b_0)_p x + pz,$$

where

$$|x|, |y| \le M, \quad |z| < M^{1+o(1)}T^{-1}.$$

Now we use Lemma 12 and conclude that the number of solutions is at most

$$\begin{aligned}\left(\frac{M}{T} + 1\right) M^{1/3+o(1)} &< \left(\frac{M^{4/3}}{p^{1/3}}\rho^{-16/3} + 1\right) M^{1/3+o(1)} \\ &< M^{2/3+o(1)} < \left(\frac{M^3}{p}\right)^{1/16} M.\end{aligned}$$

Since $\varepsilon > 0$ is arbitrary, the result now follows.

5.3. **Proof of Theorem 4.** Let $\mathcal{X}$ be the set of integers $x \in [R+1, R+M]$ such that the congruence (1) is satisfied for some integer $y \in [S+1, S+M]$. In particular, letting $X = \#\mathcal{X}$ we have

$$I_f(M; R, S) \le 2X. \tag{33}$$

Fix some integer $k \ge 1$ and consider the set

$$\mathcal{Y}_k = \{y_1^2 + \ldots + y_k^2 \pmod p \ : \ S+1 \le y_i \le S+M,\ i = 1, \ldots, k\}.$$

By making the change of variables $y_i = S + z_i$, $i = 1, \ldots, k$, we observe that

$$\begin{aligned}\mathcal{Y}_k = \{z_1^2 + \ldots + z_k^2 + 2S(z_1 + \ldots + z_k) + kS^2 \pmod p \ :& \\ 1 \le z_i \le M,\ i = 1, \ldots, k\}.&\end{aligned}$$

In particular,

$$\#\mathcal{Y}_k \le \# \left\{ r + 2Ss + kS^2 \ : \ 1 \le r \le kM^2, \ 1 \le s \le kM \right\} \le k^2 M^3.$$

For any $(x_1, \ldots, x_k) \in \mathcal{X}^k$ there exists $\lambda \in \mathcal{Y}_k$ such that

$$f(x_1) + \ldots + f(x_k) \equiv \lambda \pmod p.$$

Thus,

$$X^k \le \sum_{\lambda \in \mathcal{Y}_k} r(\lambda)$$

where

$$r(\lambda) = \#\{(x_1, \ldots, x_k) \in [R+1, R+M]^k \ : \\ f(x_1) + \ldots + f(x_k) \equiv \lambda \pmod p\}.$$

Using the Cauchy inequality, we derive

$$X^{2k} \le \#\mathcal{Y}_k \sum_{\lambda \in \mathcal{Y}_k} r^2(\lambda) \le k^2 M^3 T_k(R, M),$$

where $T_k(R; M)$ is the number of solutions of

$$\begin{aligned} f(x_1) + \ldots + f(x_k) &\equiv f(x_{k+1}) + \ldots + f(x_{2k}) \pmod p, \\ (x_1, \ldots, x_{2k}) &\in [R+1, R+M]^{2k}. \end{aligned}$$

The quantity $T_k(R; M)$ has been defined and estimated in [13] for $R = 0$ but making a change of variables, it is clear that the same bound holds for any R. In particular, it is proved in [13] that

$$T_k(R; M) \ll (M^m/p + 1)\, M^{m(m-1)/2} J_{k,m}(M),$$

where, as before, $J_{k,m}(M)$ is the number of solutions of the system of equations (4) with $H = M$.

Taking $k = \kappa(m)$ so that the bound (5) holds, we derive

$$\begin{aligned} X^{2k} &\le M^3\, (M^m/p + 1)\, M^{m(m-1)/2} M^{2k - m(m+1)/2 + o(1)} \\ &\le (M^m/p + 1)\, M^{2k+3-m+o(1)} \end{aligned}$$

and obtain

$$X \le M(M^3/p)^{1/2\kappa + o(1)} + M^{1-(m-3)/2\kappa + o(1)},$$

which together with (33) concludes the proof.

5.4. **Proof of Theorem 5.** Let $J = J_f(M; R, S)$.

Without loss of generality we can assume that

$$0 \le M + 1 < M + S < p.$$

Applying Lemma 10 to the sequence of fractional parts $\gamma_n = \{f(n)/p\}$, $n = 1, \ldots, M$, with

$$\alpha = (S+1)/p, \qquad \beta = (S+M+1)/p, \qquad K = \lfloor p/M \rfloor,$$

so that we have

$$\frac{1}{K} + \min\{\beta - \alpha, 1/k\} \ll \frac{M}{p}$$

for $k = 1, \ldots, K$, we derive

$$J \ll \frac{M^2}{p} + \frac{M}{p} \sum_{k=1}^{K} \left| \sum_{n=1}^{M} \exp(2\pi i k f(n)/p) \right|.$$

Therefore, by Lemma 11, we have

$$J \ll \frac{M^2}{p} + \frac{M^{2-m/2^{m-1}}}{p}$$
$$\times \sum_{k=1}^{K} \left(\sum_{-M<\ell_1,\ldots,\ell_{m-1}<M} \min\left\{ M, \left\| \frac{a}{p} m! k \ell_1 \ldots \ell_{m-1} \right\|^{-1} \right\} \right)^{2^{1-m}}.$$

Now, separating the contribution from the terms with $\ell_1 \ldots \ell_{m-1} = 0$ we obtain

$$J \ll \frac{M^2}{p} + \frac{M^{2-m/2^{m-1}}}{p} K (M^{m-1})^{2^{1-m}} + \frac{M^{2-m/2^{m-1}}}{p} W,$$

where

$$W = \sum_{k=1}^{K} \left(\sum_{0<|\ell_1|,\ldots,|\ell_{m-1}|<M} \min\left\{ M, \left\| \frac{a}{p} m! k \ell_1 \ldots \ell_{m-1} \right\|^{-1} \right\} \right)^{2^{1-m}}.$$

Hence, recalling the choice of K, we derive

$$J \ll \frac{M^2}{p} + M^{1-1/2^{m-1}} + \frac{M^{2-m/2^{m-1}}}{p} W. \tag{34}$$

The Hölder inequality implies the bound

$$W^{2^{m-1}} \ll K^{2^{m-1}-1} \sum_{k=1}^{K}$$
$$\sum_{0<|\ell_1|,\ldots,|\ell_{m-1}|<M} \min\left\{ M, \left\| \frac{a}{p} m! k \ell_1 \ldots \ell_{m-1} \right\|^{-1} \right\}.$$

Collecting together the terms with the same value of $z = m!k\ell_1 \ldots \ell_{m-1}$ and recalling the well-known bound on the divisor function, we conclude that

$$W^{2^{m-1}} \ll K^{2^{m-1}-1} p^{o(1)} \sum_{|z|<m!KM^{m-1}} \min\left\{M, \left\|\frac{a}{p}z\right\|^{-1}\right\}.$$

Since the sequence $\|am/p\|$ is periodic with period p, we see that

$$\begin{aligned} W^{2^{m-1}} &\ll K^{2^{m-1}-1} p^{o(1)} \frac{KM^{m-1}}{p} \sum_{z=1}^{p} \min\left\{M, \left\|\frac{a}{p}z\right\|^{-1}\right\} \\ &\ll K^{2^{m-1}-1} p^{o(1)} \frac{KM^{m-1}}{p} \left(M + \sum_{z=1}^{p} \left\|\frac{z}{p}\right\|^{-1}\right) \\ &\ll K^{2^{m-1}} M^{m-1} p^{o(1)}. \end{aligned}$$

Thus, recalling the choice of K, we derive

$$W \leq KM^{(m-1)/2^{m-1}} p^{o(1)} \leq M^{(m-1)/2^{m-1}-1} p^{1+o(1)},$$

which after the substitution in (34) concludes the proof.

5.5. **Proof of Theorem 6.** Assume that $H = H_{\mathbf{b}}$ for some vector $\mathbf{b} = (b_0, \ldots, b_{2g-1}) \in \mathbb{F}_p^{2g}$. We recall that all components of any vector $\mathbf{a} \in \mathfrak{B}$ are non-zero modulo p. Hence, $b_0 \in \mathbb{F}_p^*$ and we see from (6) (combining the equations with $i = 2g+1-h$ and $i = 2g-1$) that

$$\begin{aligned} a_{2g-1}^h &\equiv \lambda a_{2g+1-h}^2 \pmod p, \\ R_{2g+1-h} + 1 &\leq a_{2g+1-h} \leq R_{2g+1-h} + M, \\ R_{2g-1} + 1 &\leq a_{2g-1} \leq R_{2g-1} + M, \end{aligned} \tag{35}$$

where

$$\lambda = b_{2g-1}^h / b_{2g+1-h}^2. \tag{36}$$

We also observe that

$$\alpha^4 = b_{2g-1}/a_{2g-1}.$$

Thus, each solution (a_{g+1-h}, a_{2g-1}) of (35) determines at most two values of α^2, each of which in turn determines all other values of $a_0, a_1, \ldots, a_{2g-1}$.

Thus we have seen that $N(H; \mathfrak{B}) \leq 2T$, where T is the number of solutions (x, y) of the congruence

$$x^h \equiv \lambda y^2 \pmod p, \quad R+1 \leq x \leq R+M, \ S+1 \leq y \leq S+M, \tag{37}$$

where $R = R_{g+1-h}$, $S = R_{2g-1}$ and λ is given by (36).

We now observe that the congruence (37) taken with $h = 4$, which is admissible for $g \geq 2$, implies

$$x^2 \equiv \mu y \pmod p, \quad R+1 \leq x \leq R+M, \ S+1 \leq y \leq S+M,$$

where μ is one of the two square roots of λ (we recall that $g \geq 2$). Applying Theorem 5 with a quadratic polynomial f, we immediately obtain the desired result.

5.6. **Proof of Theorem 7.** As in the proof of Theorem 6 we let $H = H_{\mathbf{b}}$ for some $\mathbf{b} = (b_0, \ldots, b_{2g-1}) \in \mathbb{F}_p^{2g}$.

We can assume that $M < p^{1/4}$ as otherwise the results are weaker than the trivial upper bound $N(H; \mathfrak{B}) \ll M$.

Let T be the number of solutions (x, y) to the congruence (37).

We follow the proof of Theorem 1. We can assume that T is sufficiently large (recall that g is fixed integer constant). We fix some integer L with

$$1 \leq L \leq \frac{T}{12(h+1)}, \tag{38}$$

to be chosen later. Thus, there exists Q such that the congruence

$$x^h \equiv \lambda y^2 \pmod p, \qquad Q+1 \leq x \leq Q+M/L, \ S+1 \leq y \leq S+M,$$

has at least T/L solutions. We can split the interval $[Q+1, Q+M/L]$ into $k_0 = \lceil T/(6(h+1)L) \rceil$ intervals of length at most $6(h+1)M/T$. Since there are at most two solutions to the above congruence with the same value of x, and since we have at least $T/L > 4(h+1)k_0$ solutions in total, from the pigeonhole principle it follows that there exists an interval of length $6(h+1)M/T$ containing at least $2(h+1)$ pairwise distinct values of x. Let x_0 be the first of these values and (x_0, y_0) the solution. It is clear that T/L is bounded by the number of solutions of

$$\begin{gathered} (x_0 + x)^h \equiv \lambda (y_0 + y)^2 \pmod p, \\ -M/L \leq x \leq M/L, \quad -M \leq y \leq M, \end{gathered}$$

which is equivalent to

$$\begin{gathered} c_h x^h + \ldots + c_1 x + c_0 y \equiv y^2 \pmod p, \\ -M/L \leq x \leq M/L, \quad -M \leq y \leq M, \end{gathered} \tag{39}$$

where

$$c_0 = -2y_0 \qquad \text{and} \qquad c_j = \lambda^* \binom{h}{j} x_0^{h-j}, \ j = 1, \ldots, h,$$

where λ^* is defined by $\lambda^* \lambda \equiv 1 \pmod p$ and $1 \leq \lambda^* < p$. In particular, $c_h \not\equiv 0 \pmod p$. Besides, there are at least $2h+1$ solutions (x, y)

of (39) with x pairwise distinct and such that $1 \le x \le 6(h+1)M/T$. From these $2h+1$ values we fix h: $(x_1, y_1), \dots, (x_h, y_h)$ and rewrite (39) in the form

$$\begin{pmatrix} x^h & \dots & x & y \\ x_h^h & \dots & x_h & y_h \\ & \dots & & \\ x_1^h & \dots & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_h \\ \dots \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y^2 \\ y_h^2 \\ \dots \\ y_1^2 \end{pmatrix} \pmod p. \tag{40}$$

Since h is odd, by Lemma 14, we know that at most $2h$ pairs (x, y), with x pairwise distinct, satisfy both the congruence (40) and the congruence

$$\begin{vmatrix} x^h & \dots & x & y \\ x_h^h & \dots & x_h & y_h \\ & \dots & & \\ x_1^h & \dots & x_1 & y_1 \end{vmatrix} \equiv 0 \pmod p.$$

Since there are at least $2h+1$ solutions of (40), for one of them, say (x_{h+1}, y_{h+1}), we have

$$\Delta = \begin{vmatrix} x_{h+1}^h & \dots & x_{h+1} & y_{h+1} \\ x_h^h & \dots & x_h & y_h \\ & \dots & & \\ x_1^h & \dots & x_1 & y_1 \end{vmatrix} \not\equiv 0 \pmod p.$$

Note that $1 \le |\Delta| \ll (M/T)^{h(h+1)/2} M$. Now we solve the system

$$\begin{pmatrix} x_{h+1}^h & \dots & x_{h+1} & y_{h+1} \\ x_h^h & \dots & x_h & y_h \\ & \dots & & \\ x_1^h & \dots & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_h \\ c_{h-1} \\ \dots \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_{h+1}^2 \\ y_h^2 \\ \dots \\ y_1^2 \end{pmatrix} \pmod p \tag{41}$$

with respect to $(c_h, \dots, c_1, c_0)$. We write Δ_j for the determinant of the matrix on the left hand side where we have substituted the column j by the vector $(y_{h+1}^2, \dots, y_1^2)$. With this notation we have that

$$c_j = \frac{\Delta_{h+1-j}}{\Delta}, \quad j = 0, \dots h,$$

and the congruence (39) is equivalent to

$$\Delta_1 x^h + \Delta_2 x^{h-1} + \dots + \Delta_h x + \Delta_{h+1} y - \Delta y^2 \equiv 0 \pmod p.$$

In particular, $\Delta_1 \not\equiv 0 \pmod p$. We can write this congruence as an equation over $\mathbb{Z}$:

$$\Delta_1 x^h + \Delta_2 x^{h-1} + \dots + \Delta_h x + \Delta_{h+1} y - \Delta y^2 = pz, \qquad z \in \mathbb{Z}. \tag{42}$$

We can easily check that

$$|\Delta_{h+1}| \ll (M/T)^{h(h+1)/2} M^2$$

and

$$|\Delta_j| \ll (M/T)^{h(h-1)/2+j-1}M^3, \qquad j = 1, \dots, h.$$

Thus, collecting the above estimates, we derive

$$\begin{aligned} |z| &\ll \frac{1}{p}\left(\sum_{j=1}^{h}|\Delta_j|(M/L)^{h-j+1} + |\Delta_{h+1}|M + |\Delta|M^2\right) \\ &\ll \frac{M^3}{p}\left(\sum_{j=1}^{h}(M/T)^{h(h-1)/2+j-1}(M/L)^{h-j+1} + (M/T)^{h(h+1)/2}\right) \\ &\ll \frac{M^3}{p}\left(M^{h(h+1)/2}T^{-h(h-1)/2}L^{-h}\sum_{j=1}^{h}(TL)^{-j+1} + (M/T)^{h(h+1)/2}\right) \\ &\ll \frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h}. \end{aligned}$$

Since h is odd, and $\Delta \neq 0$, $\Delta_1 \neq 0$, we have that, for each z, the curve (42) is absolutely irreducible. Thus by Lemma 12 it contains at most $M^{1/h+o(1)}$ integer points (x, y) with $|x|, |y| \le M$. Hence

$$T \le LM^{1/h+o(1)}\left(1 + \frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h}\right) \tag{43}$$

for any L satisfying (38).

We can assume that the following lower bounds hold for T:

$$T > M^{1/h} \qquad \text{and} \qquad T > 24(h+1)\left(M(M^4/p)^{2/h(h+1)} + 1\right) \tag{44}$$

since otherwise there is nothing to prove.

Take $L = \left\lfloor 1 + (M^{(h^2+7)/2}/p)^{2/h(h+1)}\right\rfloor$. We note that (38) holds as otherwise $L \ge 2$ and we have

$$\begin{aligned} \left(\frac{M^{(h^2+7)/2}}{p}\right)^{2/h(h+1)} &\ge L - 1 \ge \frac{L}{2} > \frac{T}{24(h+1)} \\ &> M\left(\frac{M^4}{p}\right)^{2/h(h+1)} = \left(\frac{M^{h(h+1)/2+4}}{p}\right)^{2/h(h+1)}, \end{aligned}$$

which is impossible.

If $M < p^{2/(h^2+7)}$ we have $L = 1$ and in view of (44), also

$$\frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h} \le \frac{M^{h(h+1)/2+3}}{pM^{(h-1)/2}} = \frac{M^{(h^2+7)/2}}{p} < 1$$

In this case, the bound (43) yields

$$T \ll M^{1/h+o(1)}.$$

If $M \ge p^{2/(h^2+7)}$, we have

$$(M^{(h^2+7)/2}/p)^{2/h(h+1)} \ll L \ll (M^{(h^2+7)/2}/p)^{2/h(h+1)}$$

and, recalling our assumption (44) we obtain

$$\frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h} \ll \frac{M^{h(h+1)/2+3}}{pM^{h(h-1)/2}(M^4/p)^{(h-1)/(h+1)}(M^{(h^2+7)/2}/p)^{2/(h+1)}} = 1.$$

Hence, in this case we derive from (43) that

$$T \le (M^{(h^2+7)/2}/p)^{2/h(h+1)} M^{1/h+o(1)} = M\left(M^4/p\right)^{2/h(h+1)+o(1)},$$

which concludes the proof.

5.7. **Proof of Theorem 8.** Clearly

$$\sum_{H \in \mathcal{H}(\mathfrak{B})} N(H;\mathfrak{B}) = M^{2g} \qquad \text{and} \qquad \sum_{H \in \mathcal{H}(\mathfrak{B})} N(H;\mathfrak{B})^2 = T(\mathfrak{B}). \tag{45}$$

As in [14], using (45) and the Cauchy inequality we derive

$$\#\mathcal{H}(\mathfrak{B}) \ge M^{4g}T(\mathfrak{B})^{-1}.$$

From (6) we observe that $T(\mathfrak{B})$ is the numbers of pairs of vectors $(\mathbf{a},\mathbf{b})$, $\mathbf{a},\mathbf{b} \in \mathfrak{B}$, such that there exists α such that

$$a_i \equiv \alpha^{4g+2-2i} b_i \pmod p, \qquad i = 0,\ldots,2g-1.$$

In particular,

$$a_{2g-1}^3 b_{2g-2}^2 \equiv a_{2g-2}^2 b_{2g-1}^3 \pmod p.$$

Now by Lemma 15, we see that there are only $O\left(M^4/p + M^{2+o(1)}\right)$ possibilities for the quadruple $(a_{2g-1}, a_{2g-2}, b_{2g-1}, b_{2g-2})$. When it is fixed, the parameter α in (6) can take at most 4 values, and thus for every choice of $(a_0,\ldots,a_{2g-3})$ there are only 4 choices for $(b_0,\ldots,b_{2g-3})$. Therefore,

$$T(\mathfrak{B}) \le M^{2g-2}\left(M^4/p + M^{2+o(1)}\right). \tag{46}$$

When $M < p^{1/(2g)}$ we obtain $T(\mathfrak{B}) \le M^{2g+o(1)}$ and $\#\mathcal{H}(\mathfrak{B}) \ge M^{2g+o(1)}$, which proves Theorem 8 in this range.

When $M \ge p^{1/(2g)}$ we use a different approach. Using the notation

$$N_i(\lambda) = \#\{(a_i,b_i) \ : \ a_i/b_i \equiv \lambda \pmod p, \ R_i+1 \le a_i, b_i \le R_i + M\},$$

we can write

$$T(\mathfrak{B}) = \sum_{\alpha=1}^{p-1} N_0(\alpha^{4g+2})N_1(\alpha^{4g})\dots N_{2g-1}(\alpha^4).$$

Thus,

$$\begin{aligned} T^{2g}(\mathfrak{B}) &\le \left(\sum_{\alpha=1}^{p-1} N_0^{2g}(\alpha^{4g+2})\right)\dots\left(\sum_{\alpha\neq 0} N_{2g-1}^{2g}(\alpha^4)\right) \\ &\le \left((4g+2)\sum_{\alpha=1}^{p-1} N_0^{2g}(\alpha)\right)\dots\left(4\sum_{\alpha=1}^{p-1} N_{2g-1}^{2g}(\alpha)\right) \end{aligned}$$

and then we have

$$T(\mathfrak{B}) \ll \max_i \sum_{\alpha=1}^{p-1} N_i^{2g}(\alpha).$$

We observe that for any $\alpha \not\equiv 0 \pmod p$ there exist integers r, s with $1 \le |r|, s \le p^{1/2}$, $(r,s) = 1$ and such that $\alpha \equiv r/s \pmod p$. Thus

$$\sum_{\alpha=1}^{p-1} N_i^{2g}(\alpha) \le \sum_{\substack{1\le r,s<p^{1/2} \\ \gcd(r,s)=1}} N_i^{2g}(r/s) + \sum_{\substack{1\le r,s<p^{1/2} \\ \gcd(r,s)=1}} N_i^{2g}(-r/s).$$

Our estimate of $N_i(r/s)$ is based on an argument that is very close to that used in the proof of [2, Lemma 1]. Namely, we observe that $N_i(r/s)$ is the number of solutions (x, y) to the congruence

$$x/y \equiv r/s \pmod p, \qquad R_i + 1 \le x, y \le R_i + M,$$

which is equivalent to the congruence

$$sx - ry \equiv c \pmod p, \quad 1 \le x, y \le M,$$

for a suitable c. We can write the congruence as an equation in integers

$$sx - ry = c + zp, \quad 1 \le x, y \le M, \quad z \in \mathbb{Z}.$$

We observe that

$$|z| \le \frac{|s|M + |r|M + |c|}{p} \le \frac{(|s| + |r|)M}{p} + 1.$$

For each z we consider, in case it has, a solution (x_z, y_z), $1 \le x_z, y_z \le M$. The solutions of the diophantine equation above is given by $(x, y) = (x_z + rt, y_z + st)$, $t \in \mathbb{Z}$. The restriction $1 \le x, y \le M$ implies that $|t| \le M/\max\{r, s\}$.

Thus we have

$$N_i(r/s) \le \left(1 + \frac{2M}{\max\{r,s\}}\right)\left(1 + \frac{2M(s+r)}{p}\right)$$
$$\le 1 + \frac{4M\max\{r,s\}}{p} + \frac{2M}{\max\{r,s\}} + \frac{4M^2}{p}.$$

Therefore

$$\sum_{\substack{1\le r,s<p^{1/2}\\ \gcd(r,s)=1}} N_i^{2g}(r/s)$$
$$\ll \sum_{1\le r,s<p^{1/2}} \left(1 + \frac{M^{2g}\left(\max\{r,s\}\right)^{2g}}{p^{2g}} + \frac{M^{2g}}{\left(\max\{r,s\}\right)^{2g}} + \frac{M^{4g}}{p^{2g}}\right)$$
$$\ll \sum_{1\le r<s<p^{1/2}} \left(1 + \frac{M^{2g}s^{2g}}{p^{2g}} + \frac{M^{2g}}{s^{2g}} + \frac{M^{4g}}{p^{2g}}\right)$$
$$\ll \sum_{1\le s<p^{1/2}} \left(s + \frac{M^{2g}s^{2g+1}}{p^{2g}} + \frac{M^{2g}}{s^{2g-1}} + \frac{M^{4g}s}{p^{2g}}\right)$$
$$\ll p + \frac{M^{2g}}{p^{g-1}} + M^{2g}\sum_{1\le s<p^{1/2}} \frac{1}{s^{2g-1}} + \frac{M^{4g}}{p^{2g-1}}.$$

The estimate of the sum with $N_i^{2g}(-r/s)$ is fully analogous.

Assume that $M \ge p^{1/(2g)}$ and observe that

$$\sum_{1\le s<p^{1/2}} \frac{1}{s^{2g-1}} \ll \begin{cases} \log M, & \text{if } g = 1,\\ 1, & \text{if } g \ge 2.\end{cases}$$

Thus we have

$$T(\mathfrak{B}) \ll \begin{cases} M^2\log M + M^4/p, & \text{if } g = 1,\\ M^{2g} + M^{4g}/p^{2g-1}, & \text{if } g \ge 2,\end{cases} \tag{47}$$

which gives

$$\#\mathcal{H}(\mathfrak{B}) \ge M^{4g}T(\mathfrak{B})^{-1} \gg \begin{cases} \min\{p, M^{2+o(1)}\}, & \text{if } g = 1,\\ \min\{p^{2g-1}, M^{2g}\}, & \text{if } g \ge 2,\end{cases}$$

and proves Theorem 8 in the range $M \ge p^{1/2g}$.

6. Comments

The problem of obtaining a nontrivial upper bound for $I_f(M;R,S)$ in the range $p^{1/3} < M < p^{1/2}$ is still open.

On the other hand, we note that using bounds of exponential sums obtained with the method of Vinogradov instead of Lemma 11, see [5, 16, 31, 38] and references therein, also leads to some nontrivial bounds on $J_f(M; R, S)$ but these results seem to be weaker than a combination of Theorem 5 with the bounds from [13].

Similar ideas can be exploited to obtain lower bounds for the cardinality of the set $\mathcal{I}(\mathcal{B})$ of non-isomorphic isogenous elliptic curves $H_{\mathbf{a}}$ with coefficients in a cube $\mathcal{B}$.

Indeed, let us denote by $\mathcal{I}_t$ the isogeny class consisting of elliptic curves over $\mathbb{F}_p$ with the same number $p+1-t$ of $\mathbb{F}_p$-rational points. By a result of Deuring [15], each admissible value of t, that is, with $|t| \le 2p^{1/2}$, is taken and hence there are about $4p^{1/2}$ isogeny classes. Furthermore, Birch [4] has actually given a formula via the Kronecker class number for the number of isomorphism classes of elliptic curves over a finite field $\mathbb{F}_q$ lying in $\mathcal{I}_t$. Finally, Lenstra [24] has obtained upper and lower bounds for this number and, in particular, shown that the number of isomorphism classes of elliptic curves of a given order is $O\left(p^{1/2}\log p\,(\log\log p)^2\right)$.

Observe that once again bounds for $N(H; \mathfrak{B})$ can be translated into bounds for the number of isogenous non-isomorphic curves with coefficients in $\mathfrak{B}$, via multiplication by $p^{1/2+o(1)}$. However, as we have done before, one can obtain better bounds in terms of $T(\mathfrak{B})$ which is given by (45).

Thus, using (45) and (47), with $g = 1$, we see that for the set $\mathcal{H}(t, \mathfrak{B})$ of elliptic curves $H_{\mathbf{a}} \in \mathcal{I}_t$ with $\mathbf{a} \in \mathfrak{B}$, we have

$$\begin{aligned}
\#\mathcal{H}(t, \mathfrak{B}) &= \sum_{H \in \mathcal{H}(\mathfrak{B}) \cap \mathcal{I}_t} N(H, \mathfrak{B}) \\
&\le (\#\mathcal{I}_t)^{1/2} \left(\sum_{H \in \mathcal{H}(\mathfrak{B})} N(H, \mathfrak{B})^2 \right)^{1/2} = (\#\mathcal{I}_t)^{1/2} T(\mathfrak{B})^{1/2} \\
&\ll \left(M^2 p^{-1/4} + p^{1/4} M \log^{1/2} M \right) (\log p)^{1/2} \log\log p.
\end{aligned}$$

This improves the trivial bound

$$\mathcal{H}(N, \mathfrak{B}) \ll \min\{M^2, p^{3/2} (\log p)^{1/2} \log\log p\}$$

for $p^{1/4+\varepsilon} \le M \le p^{7/8-\varepsilon}$ (with any fixed $\varepsilon > 0$). Furthermore, it also implies the lower bound

$$\begin{aligned} \#\mathcal{I}(\mathcal{B}) &\gg \frac{M^2}{\max_{|t|\in 2p^{1/2}} \mathcal{H}(t,\mathfrak{B})} \\ &\gg \min\{p^{1/4}, Mp^{-1/4}\log^{-1/2} M\}(\log p)^{-1/2}(\log\log p)^{-1}. \end{aligned}$$

Acknowledgements

The authors are grateful to Alfred Menezes for discussions and useful references on isomorphism classes of hyperelliptic curves.

M.-C. Chang is very grateful to the Department of Mathematics of the University of California at Berkeley for its hospitality.

During the preparation of this paper, M.-C. Chang was supported in part by NSF, J. Cilleruelo was supported by Grant MTM 2011-22851 of MICINN (Spain), M. Z. Garaev was supported in part by the Red Iberoamericana de Teoría de Números, I. E. Shparlinski was supported in part by ARC grant DP130100237 and by NRF Grant CRP2-2007-03, Singapore, A. Zumalacárregui was supported by a FPU grant from Ministerio de Educación, Ciencia y Deporte, Spain.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and hyperelliptic curve cryptography: Theory and practice*, CRC Press, 2005.

[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 value of character sums', *J. Number Theory*, **59** (1996), 398–413.

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

[4] B. J. Birch, 'How the number of points of an elliptic curve over a fixed prime field varies', *J. London Math. Soc.*,**43** (1968), 57–60.

[5] K. D. Boklan, and T. D. Wooley, 'On Weyl sums for smaller exponents', *Funct. et Approx. Commen. Math.*, **46** (2012), 91–107.

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

[7] 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 Math. Inst.*, (to appear).

[8] T. D. Browning, *Quantitative arithmetic of projective varieties*, Progr. in Math., vol. 277. Birkhäuser Verlag, Basel, 2009.

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

[10] M.-C. Chang, 'Polynomial iteration in characteristic p', *J. Functional Analysis*, **263** (2012), 3412–3421.

[11] M.-C. Chang, 'Expansions of quadratic maps in prime fields', *Proc. Amer. Math. Soc.*, (to appear).

[12] 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.

[13] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Math. Zeit.*, **272** (2012), 825–837.

[14] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, 'Isomorphism classes of elliptic curves over a finite field in some thin families', *Math. Res. Letters*, **19** (2012), 335–343.

[15] M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.*, **14** (1941), 197–272.

[16] K. Ford, 'Recent progress on the estimation of Weyl sums', *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.

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

[18] É. Fouvry and N. Katz, 'A general stratification theorem for exponential sums, and applications', *J. Reine Angew. Math.*, **540** (2001), 115–166.

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

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

[21] D. R. Heath-Brown, 'Analytic methods for the distribution of rational points on algebraic varieties', *Equidistribution in number theory, An introduction*, Springer, Dordrecht, 2007, 139–168.

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

[23] K. Karabina and B. Ustaoglu, 'Invalid-curve attacks on hyperelliptic curve cryptosystems', *Adv. Math. of Comm.*, **4** (2010), 307–321.

[24] H. W. Lenstra, 'Factoring integers with elliptic curves', *Annals Math.*, **126** (1987), 649–673.

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

[26] W. Luo, 'Rational points on complete intersections over $\mathbb{F}_p$', *Inter. Math. Res. Notices*, **1999** (1999), 901–907.

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

[28] O. Marmon, 'A generalization of the Bombieri-Pila determinant method', *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, **377** (2010), 63–77, 242 (Trans. in *J. Math. Sci.*, **171** (2010), 736–744.

[29] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Amer. Math. Soc., Providence, RI, 1994.

[30] E. Nart, 'Counting hyperelliptic curves', *Adv. Math.*, **221** (2009), 774–787.

[31] S. T. Parsell, 'On the Bombieri-Korobov estimate for Weyl sums', *Acta Arith.*, **138** (2009), 363–372.

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

[33] J. Pila, 'Density of integer points on plane algebraic curves', *Inter. Math. Res. Notices*, **1996** (1996), 903–912.

[34] P. Salberger and T. D. Wooley, 'Rational points on complete intersections of higher degree, and mean values of Weyl sums', *J. Lond. Math. Soc.*, **82** (2010), 317–342.

[35] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge University Press, Cambridge, 2006.

[36] Y. Tschinkel, 'Algebraic varieties with many rational points', *Arithmetic geometry*, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009. 243–334.

[37] M. Vâjâitu and A. Zaharescu, 'Distribution of values of rational maps on the $\mathbb{F}_p$-points on an affine curve', *Monatsh. Math.*, **136** (2002), 81–86.

[38] R. C. Vaughan, *The Hardy–Littlewood method*, Cambridge Univ. Press, Cambridge, 1981.

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

[40] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing, II', *Duke Math. J.*, **162** (2013), 673–730.

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

[42] A. Zumalacárregui, 'Concentration of points on modular quadratic forms', *Intern. J. Number Theory*, **7** (2011), 1835–1839.

Department of Mathematics, University of California, Riverside, CA 92521, USA
E-mail address: mcc@math.ucr.edu

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

Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: garaev@matmor.unam.mx

Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: stgo@matmor.unam.mx

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor.shparlinski@mq.edu.au

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049, Madrid, España
E-mail address: ana.zumalacarregui@uam.es