CONCENTRATION OF POINTS AND ISOMORPHISM CLASSES OF HYPERELLIPTIC CURVES OVER A FINITE FIELD IN SOME THIN FAMILIES

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

ABSTRACT. For a prime p and a polynomial $f \in \mathbb{F}_p[X]$, we obtain upper bounds on the number of solutions of the congruences

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

where (x, y) belongs to an arbitrary square with side length M. Further, we obtain non-trivial upper bounds for the number of hyperelliptic curves

$$Y^2 = X^{2g+1} + a_{2g-1}X^{2g-1} + \ldots + a_1X + a_0$$

over $\mathbb{F}_p$, with coefficients in a $2g$-dimensional cube

$$(a_0, \ldots, a_{2g-1}) \in [R_0 + 1, R_0 + M] \times \ldots \times [R_{2g-1} + 1, R_{2g-1} + M]$$

that are isomorphic to a given curve and give an almost sharp lower bound on the number of non-isomorphic hyperelliptic curves with coefficients in that cube.

1. INTRODUCTION

1.1. **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 $\{0, 1, \ldots, p-1\}$. 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 [22, 26]. 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 nontrivial estimate of $I_f(M; R, S)$ for $M < p^{1/4-\varepsilon}$ when $m = 3$, and for $M < p^{1/3-\varepsilon}$ when $m \ge 4$. In particular, in the case $m = 3$ our result improves on the range of M the bound obtained in [8]. We note that nontrivial bounds on the number of solutions (x, y) to the congruence

$$y \equiv f(x) \pmod p,$$

satisfying (2), have been obtained in [7] for any $M < p$. 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 [6]. 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 [27].

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

It follows from a more general result of Lockhart [18, 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 [16, 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

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

It is known (see [16, 20]) 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

$$\mathfrak{B} = [R_0 + 1, R_0 + M] \times \ldots \times [R_{2g-1} + 1, R_{2g-1} + M] \tag{5}$$

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.

We also give an upper bound for the number

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

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 [8] where this problem has been investigated for elliptic curves (that is, for $g = 1$).

First we observe that for large cubes one easily derive from the Weil bound (see [15, 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 [15, Theorem 21.4]).

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 (4).

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

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

For example, this follows from a bound of Heath-Brown [14, 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 $\mathcal{A}$ consist of all quadratic residues modulo p in $[1, M^{1/(2g+1)})$ and therefore $\#\mathcal{A} = 2\#\mathcal{Q} \sim M^{1/(2g+1)}$.

1.2. **Our results.** Throughout the paper, any implied constants in 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 $c > 0$.

We combine ideas from [6, 7, 8] 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 [8, Theorem 6] guarantees this bound only for $M \ll p^{1/9}$. 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 [8]. However, using a different approach we can obtain a nontrivial bound 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*

$$I_f(M; R, S) \le \max\{\left(M^{7/3}/p\right)^{1/81}, M^{-1/16}, (M^3/p)^{1/16}\} M^{1+o(1)}.$$

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*

$$I_f(M;R,S) < M^{1+o(1)} \begin{cases} M^{-2/3}, & \text{if } M < p^{1/8}, \\ (M^4/p)^{1/6}, & \text{if } p^{1/8} \le M < p^{15/62}, \\ (M^{7/3}/p)^{1/81}, & \text{if } p^{15/62} \le M < p^{195/617}, \\ (M^3/p)^{1/16}, & \text{if } p^{195/617} \le M < p^{1/3}, \end{cases}$$

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 $x_1, \dots, x_{2k}$:

$$\begin{gathered} x_1^m + \dots + x_k^m = x_{k+1}^m + \dots x_{2k}^m, \\ \dots \\ x_1 + \dots + x_k = x_{k+1} + \dots x_{2k}, \\ 1 \le x_1, \dots, x_{2k} \le H. \end{gathered} \tag{6}$$

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

$$J_{k,m}(H) \le C(k,d) H^{2k - m(m+1)/2 + o(1)}, \tag{7}$$

as $H \to \infty$. Note that by a recent result of Wooley [25, Theorem 1.1], that improves the previous estimate of [24], we have $\kappa(d) \le d^2 - 1$ for any $d \ge 3$.

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 $I_f(M;R,S) \ll M^{1-\delta}$.

Next, we turn to estimates on $N(H;\mathfrak{B})$. 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 [7] 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.

We prove the following result, which, besides of its application to bound the quantity $N(H; \mathfrak{B})$, is of independent interest.

Theorem 5. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $m \geq 2$ with the leading coefficient $a \not\equiv 0 \pmod p$. Then for $1 \leq M < p$ he number $J_f(M; R, S)$ of solutions to the congruence*

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

is bounded by

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

as $p \to \infty$.

We remark that in [7], the bound

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

has been given which is stronger than Theorem 5 for large values of m. Also in [7] for $M \leq p^{2/(m^2+3)}$, the bound

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

has been obtained. Thus from this result and from Theorem 5 we get the following consequence:

Corollary 6. *For any hyperelliptic curve H of genus $g \geq 2$ over $\mathbb{F}_p$ and a cube $\mathfrak{B}$ given by (5) with $1 \leq M < p$, we have*

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

We also notice that results about concentration of points on curves are 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 elements $u_0 \in \mathbb{F}_p$, 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

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

has been initiated in [13] and then continued in [7, 10]. In particular, it follows from [13, Theorem 6] that for any fixed ε, for $T_{f,u_0} \geq N \geq p^{1/2+\varepsilon}$ 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 [7, 10].

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

Corollary 7. *For any polynomial $f \in \mathbb{F}_p[X]$ of degree $m \geq 2$ with the leading coefficient $a \not\equiv 0 \pmod p$ and positive integer $N \leq T_{f,u_0}$, 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] that holds for small values of N.

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 8. *For any hyperelliptic curve H of genus $g \geq 1$ over $\mathbb{F}_p$, any cube $\mathfrak{B}$ given by (5) with $1 \leq M < p$ 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 8, we obtain the estimate $N(H; \mathfrak{B}) \leq M^{1/(2g+1)+o(1)}$ 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 [8] 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 $g \geq 2$. Certainly the upper bounds of our theorems lead to a lower bound on $\#\mathcal{H}(\mathfrak{B})$. However, here using a different approach we obtain a near optimal bound for $\#\mathcal{H}(\mathfrak{B})$.

Theorem 9. *For $g \geq 1$ and any cube $\mathfrak{B}$ given by (5) with and $1 \leq M < p$, we have*

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

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

2. Preparations

The following result is well-known and can be found, for example, in [19, Chapter 1, Theorem 1] (which 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 $K \geq 1$, 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 [15, 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 $m \geq 2$ with the leading coefficient $\vartheta \neq 0$. Then*

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

We also need the following estimate of Bombieri and Pila [5] on the number of integral points on polynomial curves.

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

The following result is used in the proofs of Theorems 1 and 8.

Lemma 13. *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*

$$f(x) \equiv g(y) \pmod{p}, \qquad 0 \leq x, y < p, \tag{8}$$

has at most mn solutions with

$$\det \begin{pmatrix} x^n & x^{n-1} & \dots & x & y \\ x_1^n & x_1^{n-1} & \dots & x_1 & y_1 \\ & & \dots & & \\ x_n^n & x_n^{n-1} & \dots & x_n & y_n \end{pmatrix} \equiv 0 \pmod p. \tag{9}$$

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 (9) is a unique modulo p linear combination of the previous columns. In particular, for every solution (x, y) to (8) and (9) 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 (8). We observe that now the right hand side of (8), that is $g(h(x))$, is a nontrivial polynomial of degree $m \deg h$. Thus, the congruence (8) is a nontrivial polynomial congruence of degree d with $n \le d \le mn$. Therefore it has at most mn solutions modulo p. □

We say that a set I is an interval in $\mathbb{F}_p$ of length $|I| = L$ if it consists of residues modulo p of L consecutive integers. We also use aI to denote the set obtained from I by element-wise multiplication by $a \in \mathbb{F}_p$ and $I_1 - I_2$ to denote for the difference set

$$I_1 - I_2 = \{t_1 - t_2 \ : \ t_1 \in I_1, \ t_2 \in I_2\}.$$

Lemma 14. *Let $\gamma \in (0, 1)$ and let I and J be two intervals in $\mathbb{F}_p$ such that*

$$2\gamma^{-1} < |I| \le |J| < \frac{\gamma p}{16}.$$

Assume that for some $a \in \mathbb{F}_p$ we have the bound

$$\#\left(aI \cap J\right) > \gamma |I|.$$

Then there exist integers t and u with

$$0 < t < \gamma^{-1}, \qquad |u| \le 4\gamma^{-2} \frac{|J|}{|I|},$$

such that

$$u \equiv at \pmod p.$$

Proof. From the pigeon-hole principle and the condition $\#(aI \cap J) > \gamma|I| \geq 2$ it follows that there exists $t \in I - I$ with $0 < t < \gamma^{-1}$ and $u \in J - J$ such that

$$at \equiv u \pmod{p}. \tag{10}$$

It remains to show that in fact

$$|u| \leq 4\gamma^{-2}\frac{|J|}{|I|}. \tag{11}$$

Clearly $a \not\equiv 0 \pmod{p}$. Hence $u \neq 0$. Denote

$$L = \left\lfloor \frac{|I|}{t} \right\rfloor$$

and consider the arithmetic progression

$$P = t\{1, \dots, L\} \subseteq [1, |I|].$$

We see from (10) that

$$aP \equiv u\{1, \dots, L\} \pmod{p}.$$

We can obviously assume that the interval I starts from zero. We can cover the interval I with $2t$ shifts of P

$$I = \{0, \dots, |I| - 1\} \subseteq \sum_{r=-t}^{t-1}(P + r).$$

Hence, we get

$$\begin{aligned} \gamma|I| < \#(aI \cap J) &\leq \sum_{r=-t}^{t-1} \#((ar + aP) \cap J) \\ &= \sum_{r=-t}^{t-1} \#(\{1, \dots, L\}u \cap (J - ar)). \end{aligned} \tag{12}$$

If $|u|L \leq p$, using that $|u| \leq |J|$ we see that for every $r = -t, \dots, t-1$,

$$\#(\{1, \dots, L\}u \cap (J - ar)) \leq 1 + \frac{|J|}{|u|} \leq \frac{2|J|}{|u|}.$$

Thus, by (12)

$$\gamma|I| \leq (2t)\frac{2|J|}{|u|} \leq 4\gamma^{-1}\frac{|J|}{|u|}$$

which gives the desired estimate on $|u|$.

If $|u|L > p$ we cover $\{1, \dots, L\}$ by intervals of length $\lfloor p/|u| \rfloor$ and we obtain

$$\begin{aligned}\#\left(\{1,\dots,L\}u \cap (J - ar)\right) &\le \frac{2|J|}{|u|}\left(1 + \frac{L}{\lfloor p/|u| \rfloor}\right)\\ &\le \frac{4|J|L}{|u|\,\lfloor p/|u| \rfloor} \le \frac{4|J|L}{p - |u|} \le \frac{4|J|L}{p - |J|} \le \frac{8|J||I|}{pt},\end{aligned}$$

since $|J| < p/2$ and $L \le |I|/t$. Therefore, by (12), we have

$$\gamma|I| < 2t\left(\frac{8|J||I|}{pt}\right)$$

and then $|J| > \gamma p/16$, which contradicts our assumption. □

Corollary 15. *Let $J_0, \dots, J_k$ be intervals in $\mathbb{F}_p$. Let $\mathcal{S}$ be a subset of the set of the solutions $(x_0, x_1, \dots, x_k) \in J_0 \times \dots \times J_k$ to the congruence*

$$a_0x_0 + \dots + a_kx_k \equiv 0 \pmod p,$$

where $a_i \in \mathbb{F}_p$ and $a_0 \ne 0$. Define

$$\gamma = \frac{\#\mathcal{S}}{|J_1| \dots |J_k|}$$

and assume that

$$2\gamma^{-1} < |J_k| \le \dots \le |J_1| \le |J_0| < \frac{\gamma p}{16}.$$

Then, for any $i = 1, \dots, k$ there exist elements t_i, u_i with

$$0 < t_i < \gamma^{-1}, \quad |u_i| \le 4\gamma^{-2}\frac{|J_0|}{|J_i|}$$

such that

$$a_i \equiv a_0\frac{u_i}{t_i} \pmod p.$$

Proof. By the pigeonhole principle it is clear that for any $i = 1, \dots, k$ there exists μ such the equation $a_0x_0 + a_ix_i \equiv \mu \pmod p$ has at least

$$\frac{\#\mathcal{S}|J_i|}{|J_1| \dots |J_k|} = \gamma|J_i|$$

distinct solutions $(x_0, x_i) \in J_0 \times J_i$. If $a_i \ne 0$ we apply Lemma 14 with $I = J_i$, $J = -J_0 + \mu/a_0$, $a = a_i/a_0$. If $a_i = 0$, the result holds with $u_i = 0$ and $t_i = 1$. □

The following statement is a particular case of a more general result of Wooley [25, Theorem 1.1].

Lemma 16. *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 solution is equal to $J_{8,3}(2M + 1)$. Since by the result of Wooley [25, Theorem 1.1] we have $\kappa(3) \le 8$, the bound (7) applies with $H = 2M + 1$. □

We note that Lemma 16 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 out main results.

3. Proof of Theorem 1

For the brevity, in this section we denote $I = I_f(M; R, S)$. We can assume that I is large. We fix some L with

$$1 \le L \le \frac{I}{20}, \tag{13}$$

to be chosen later. By the pigeon-hole 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. Since there are at most two solutions to the above congruence with the same value of x, by the pigeon-hole principle, there exists an interval of length $20M/I$ containing at least 10 solutions (x, y) with pairwise distinct values 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

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

which is equivalent to

$$\begin{gathered}y^2 \equiv c_3x^3 + c_2x^2 + c_1x + c_0y \pmod p,\\ -M/L \le x \le M/L, \quad -M \le y \le M,\end{gathered} \tag{14}$$

with $(c_3, p) = 1$. Besides, there are at least 10 solutions (x, y) with x pairwise distinct and such that $0 \le x \le 20M/I$. From these 10

values we fix 3 solutions $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ and rewrite the congruence (14) in the matrix form

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

By Lemma 13, we know that at most 6 pairs (x, y), with x pairwise distinct, satisfy both the congruence (15) 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 10 solutions to (15), 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

$$\begin{pmatrix} x_4^3 & x_4^2 & x_4 & y_4 \\ x_3^3 & x_3^2 & x_3 & y_3 \\ x_2^3 & x_2^2 & x_2 & y_2 \\ x_1^3 & x_1^2 & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_4^2 \\ y_3^2 \\ y_2^2 \\ y_1^2 \end{pmatrix} \pmod p \tag{16}$$

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

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

where Δ^* is defined by $\Delta\Delta^* \equiv 1 \pmod p$, and the congruence (14) 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 $\mathbb{Z}$:

$$\Delta_1 x^3 + \Delta_2 x^2 + \Delta_3 x + \Delta_4 y - \Delta y^2 = pz, \qquad (x, y, z) \in \mathbb{Z}^3. \tag{17}$$

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

$$\begin{aligned} |z| &\ll \frac{1}{p}\left(|\Delta_1|(M/L)^3 + |\Delta_2|(M/L)^2 + |\Delta_3|(M/L) + |\Delta_4|M + |\Delta|M^2\right) \\ &\ll \frac{M^3}{p}\left(\frac{M^6}{I^3L^3} + \frac{M^7}{I^4L^2} + \frac{M^6}{I^5L} + \frac{M^6}{I^6}\right) \ll \frac{M^9}{pI^3L^3}. \end{aligned}$$

Since $\Delta_1 \neq 0$, $\Delta \neq 0$, for each z, the curve (17) 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 (13). This implies, that

$$I \leq LM^{1/3+o(1)} + \frac{M^{7/3}}{p^{1/4}L^{1/2}}. \tag{18}$$

If $M < 10p^{1/8}$, then we take $L = 1$ and derive from (18) 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 $L = \left\lfloor M^{4/3}p^{-1/6} \right\rfloor$ and note that the condition (13) is satisfied. Thus, we derive from (18) 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.

4. Proof of Theorem 2

Clearly we can assume that $M = o(p^{1/3})$ as otherwise the result is trivial.

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

$$y^2 - c_0 y \equiv c_3x^3 + c_2x^2 + c_1x \pmod{p}, \quad |x|, |y| \leq M. \tag{19}$$

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

$$\rho \ge \max\{M^{-(1-\varepsilon)/16}, (M^{3-\varepsilon}/p)^{1/16}\}. \tag{20}$$

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 $\mathbb{F}_p$ (as in Lemma 14).

We now consider the set

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

of all triples

$$\mathbf{s} \equiv (x_1 + \ldots + x_8,\, x_1^2 + \ldots + x_8^2,\, x_1^3 + \ldots + x_8^3) \pmod p, \tag{21}$$

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

$$x_1^j + \ldots + x_8^j \equiv x_9^j + \ldots + x_{16}^j \pmod p, \qquad j = 1, 2, 3, \tag{22}$$

has at most $M^{10+o(1)}$ solutions in integers x_i, y_i with $|x_i|, |y_i| \le M$. Indeed, since $M < p^{1/3-\varepsilon}$, 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 16 has at most $M^{10+o(1)}$ solutions in integers x_i with $|x_i| \le M$, $i = 1, \ldots, 16$. Therefore, the congruence (22) 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 the same vector $\mathbf{s}$ given by (21) and denoting the number of such representations by $N(\mathbf{s})$, by the Cauchy inequality, we obtain

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

Thus

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

Hence, there exists 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

$$c_3 z_3 + c_2 z_2 + c_1 z_1 = z_4 - c_0 z_0$$

for some $z_4 \in I_{2,8}$ and $z_0 \in I_{1,8}$. In particular we have that, the congruence

$$c_3z_3 + c_2z_2 - z_4 + c_1z_1 + c_0z_0 \equiv 0 \pmod{p},$$
$$(z_3, z_2, z_1, z_0, z_4) \in I_{3,8} \times I_{2,8} \times I_{2,8} \times I_{1,8} \times I_{1,8}$$

has a set of solutions $\mathcal{S}$ with $\#\mathcal{S} \geq \rho^{16}M^{6+o(1)}$. Next, we apply Corollary 15 with the coefficients $(a_0, a_1, a_2, a_3, a_4) = (c_3, c_2, -1, c_1, c_0)$ and the intervals

$$(J_0, J_1, J_2, J_3, J_4) = (I_{3,8}, I_{2,8}, I_{2,8}, I_{1,8}, I_{1,8}).$$

We observe that $\gamma = \rho^{16}M^{o(1)}$ and that the inequalities $\rho \geq M^{-(1-\varepsilon)/16}$ and $\rho \geq (M^{3-\epsilon}/p)^{1/16}$ in (20) imply that the conditions $2\gamma^{-1} < |J_4|$ and $|J_0| < \gamma p/16$ in Corollary 15 are satisfied.

Corollary 15 implies that there exist u_i, t_i such that

$$c_2 \equiv c_3\frac{u_1}{t_1} \pmod{p}, \quad 0 < t_1 < \gamma^{-1},\ |u_1| \leq 4\gamma^{-2}M$$
$$-1 \equiv c_3\frac{u_2}{t_2} \pmod{p}, \quad 0 < t_2 < \gamma^{-1},\ |u_2| \leq 4\gamma^{-2}M$$
$$c_1 \equiv c_3\frac{u_3}{t_3} \pmod{p}, \quad 0 < t_3 < \gamma^{-1},\ |u_3| \leq 4\gamma^{-2}M^2$$
$$c_0 \equiv c_3\frac{u_4}{t_4} \pmod{p}, \quad 0 < t_4 < \gamma^{-1},\ |u_4| \leq 4\gamma^{-2}M^2$$

Thus, the original elliptic equation is equivalent to the equation

$$t_1t_2t_3t_4x^3 + u_1t_2t_3t_4x^2 + t_1u_2t_3t_4y^2 + t_1t_2u_3t_4x + t_1t_2t_3u_4y \equiv 0 \pmod{p}$$

where $|x|, |y| \leq M$. We observe that the left side is bounded by $21\gamma^{-5}M^3 = \rho^{-80}M^{3+o(1)}$, provided that p is large enough. Thus, the above congruence becomes one of the equations

$$t_1t_2t_3t_4x^3 + u_1t_2t_3t_4x^2 + t_1u_2t_3t_4y^2 + t_1t_2u_3t_4x + t_1t_2t_3u_4y - \lambda p = 0,$$

for some integer λ with $|\lambda| \leq \rho^{-80}M^{3+o(1)}p^{-1}$ and by Lemma 12 we conclude that the above congruence has $O\left(M^{1/3}\left(\rho^{-80}M^{o(1)}p^{-1} + 1\right)\right)$ solutions. Thus we have

$$M\rho \ll M^{1/3}\left(\rho^{-80}M^{3+o(1)}p^{-1} + 1\right),$$

which implies

$$\ll \rho \leq \max\left\{\left(\frac{M^{7/3+o(1)}}{p}\right)^{1/81}, M^{-2/3}\right\}.$$

So we have the desired result, provided that (20) holds.

If the condition (20) fails, then since $\varepsilon > 0$ is arbitrary, the result follows as well.

5. Proof of Theorem 4

Let $\mathcal{I}$ be the set of solutions (x, y) of (1). When two solutions with the same value of x appear in $\mathcal{I}$ we remove one of them. Let $\mathcal{I}_0$ be the set of solutions after the removing process and write $I_0 = \#\mathcal{I}_0$ so

$$I_f(M; R, S) = \#\mathcal{I} \le 2I_0. \tag{23}$$

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

$$\mathcal{Y}_k = \{y_1^2 + \ldots + y_k^2 \ : \ (x_i, y_i) \in \mathcal{I}_0\}.$$

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

$$\mathcal{Y}_k = \{z_1^2 + \ldots + z_k^2 + 2S(z_1 + \ldots + z_k) + kS^2 \ : \\ (x_i, S + z_i) \in \mathcal{I}, \ i = 1, \ldots, k\}.$$

Thus

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

It is clear that

$$\begin{aligned} I_0^k &\le \#\{((x_1, y_1), \ldots, (x_k, y_k)) \in \mathcal{I}_0^k \ : \\ &\qquad f(x_1) + \ldots + f(x_k) \equiv y_1^2 + \ldots + y_k^2 \pmod p\} \\ &\le \sum_{\lambda \in \mathcal{Y}_k} r(\lambda), \end{aligned}$$

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

$$I_0^{2k} \le \#\mathcal{Y}_k \sum_{\lambda \in \mathcal{Y}_k} r^2(\lambda) \le k^2M^3T_k(R, M),$$

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 [7] for $R = 0$ but making a change of variables, it is clear that the same bound holds for any R (see also the argument in the proof of Lemma 16). In particular, it is proved in [7] 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 (6) with $H = M$.

Taking $k = \kappa(m)$ so that the bound (7) holds, we derive

$$\begin{aligned} I_0^{2k} &\le M^3 \left(M^m/p + 1\right) M^{m(m-1)/2} M^{2k-m(m+1)/2+o(1)} \\ &\le \left(M^m/p + 1\right) M^{2k+3-m+o(1)} \end{aligned}$$

and obtain

$$I_0 \le M(M^3/p)^{1/2\kappa+o(1)} + M^{1-(m-3)/2\kappa+o(1)},$$

which together with (23) concludes the proof.

6. 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

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

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

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

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

$$J \ll \frac{M^2}{p} + M^{1-1/2^{m-1}} + \frac{M^{2-m/2^{m-1}}}{p} W. \tag{24}$$

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

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

which after the substitution in (24) concludes the proof.

7. Proof of Corollary 6

Let $H = H_{\mathbf{b}}$ for some $\mathbf{b} = (b_0, \ldots, b_{2g-1}) \in \mathbb{F}_p^{2g}$. We recall that all components of any vector $\mathbf{a} \in \mathfrak{B}$ are non-zeros modulo p. Hence,

$b_0 \in \mathbb{F}_p^*$ and we see from (4) (combinig the equations with $i = 2g+1-h$ and $i = 2g-1$) that

$$\begin{aligned} a_{2g-1}^h \equiv & \lambda a_{g+1-h}^2 \pmod p, \\ R_{g+1-h} + 1 \le & a_{g+1-h} \le R_{g+1-h} + M, \\ R_{2g-1} + 1 \le & a_{2g-1} \le R_{2g-1} + M, \end{aligned} \tag{25}$$

where

$$\lambda = b_{2g-1}^h / b_{g+1-h}^2. \tag{26}$$

We also observe that

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

Thus, each solution (a_{g+1-h}, a_{2g-1}) of (25) determines the value of α^2 and therefore, all other values of $a_0, a_1, \ldots, a_{2g-1}$.

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

$$x^h \equiv \lambda y^2 \pmod p, \quad R+1 \le x \le R+M,\ S+1 \le y \le S+M, \tag{27}$$

where $R = R_{g+1-h}$, $S = R_{2g-1}$ and λ is given by (26).

We now observe that the congruence (27) taken with $h = 4$, which is admissible for $g \ge 2$, implies

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

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

8. Proof of Theorem 8

As in the proof of of Corollary 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 is weaker than the trivial upper bound $N(H; \mathfrak{B}) \ll M$.

Also we can assume that $T > M^{1/h}$, where, as before, T is the number of solutions (x, y) to the congruence (27) as otherwise there is nothing to prove.

We follow the proof of Theorem 1. We fix some L with

$$1 \le L \le \frac{T}{8(h+1)}, \tag{28}$$

to be chosen later. Note that if $T < 16g+16$ there is nothing to prove. Thus, there exists Q such that the congruence

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

has at least T/L solutions. Since there are at most two solutions to the above congruence with the same value of x, by the pigeon-hole principle, there exists an interval of length $4(h+1)M/T$ containing at least $2(h+1)$ solutions (x,y) with pairwise distinct values 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

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

which is equivalent to

$$\begin{gathered}c_h x^h + \ldots + c_1 x + c_0 y \equiv y^2 \pmod p,\\ -M/L \le x \le M/L, \quad -M \le y \le M,\end{gathered} \tag{29}$$

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 $1 \le \lambda^* < p$. In particular, $c_h \not\equiv 0 \pmod p$. Besides, there are at least $2h+1$ solutions (x,y) of (29) with x pairwise distinct and such that $1 \le x \le 4(h+1)M/T$. From these $2h+1$ values we fix h: $(x_1,y_1),\ldots,(x_h,y_h)$ and rewrite (29) in the form

$$\begin{pmatrix} x^h & \ldots & x & y \\ x_h^h & \ldots & x_h & y_h \\ & \ldots & & \\ x_1^h & \ldots & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_h \\ \ldots \\ c_1 \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y^2 \\ y_h^2 \\ \ldots \\ y_1^2 \end{pmatrix} \pmod p. \tag{30}$$

Since h is odd, by Lemma 13, we know that at most $2h$ pairs (x,y), with x pairwise distinct, satisfy both the congruence (30) and the congruence

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

Since there are at least $2h+1$ solutions of (30), for one of them, say (x_{h+1},y_{h+1}), we have

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

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

$$\begin{pmatrix} x_{h+1}^h & \dots & x_{h+1} & y_{h+1} \\ x_h^h & \dots & x_h & y_h \\ & \dots & & \\ x_1^h & \dots & x_1 & y_1 \end{pmatrix} \begin{pmatrix} c_h \\ c_{h-1} \\ \dots \\ c_0 \end{pmatrix} \equiv \begin{pmatrix} y_{h+1}^2 \\ y_h^2 \\ \dots \\ y_1^2 \end{pmatrix} \pmod p \tag{31}$$

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 (29) 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 $\mathbb{Z}$:

$$\Delta_1 x^h + \Delta_2 x^{h-1} + \dots + \Delta_h x + \Delta_{h+1} y - \Delta y^2 = pz, \qquad z \in \mathbb{Z}. \tag{32}$$

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 (32) is absolutely irreducible. Thus by a result of Bombieri and Pila [5] it contains at most $M^{1/h+o(1)}$ integer points (x, y) with $|x|, |y| \le M$. Hence

$$T \le LM^{1/h+o(1)}\left(1 + \frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h}\right) \tag{33}$$

for any L satisfying (28).

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

$$T > M^{1/h} \qquad \text{and} \qquad T > 16(h+1)\left(M(M^4/p)^{2/h(h+1)} + 1\right) \tag{34}$$

since otherwise there is nothing to prove.

Take $L = \left\lfloor 1 + (M^{h(h+1)/2+3}/p)^{2/h(h+1)} \right\rfloor$. We note that (28) holds as otherwise $L \geq 2$ and we have

$$\begin{aligned}\left(\frac{M^{h(h+1)/2+3}}{p}\right)^{2/h(h+1)} &\geq L - 1 \geq \frac{L}{2} > \frac{T}{16(h+1)} \\ &> M\left(\frac{M^4}{p}\right)^{2/h(h+1)} = \left(\frac{M^{h(h+1)/2+4}}{p}\right)^{2/h(h+1)},\end{aligned}$$

which is impossible.

If $M < p^{1/(h(h+1)/2+3)}$ we have $L = 1$ and also

$$\frac{M^{h(h+1)/2+3}}{pT^{h(h-1)/2}L^h} \leq \frac{M^{h(h+1)/2+3}}{p} < 1.$$

In this case, the bound (33) yields

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

If $M \geq p^{1/(h(h+1)/2+3)}$, we have

$$(M^{h(h+1)/2+3}/p)^{2/h(h+1)} \ll L \ll (M^{h(h+1)/2+3}/p)^{2/h(h+1)}$$

and, recalling our assumption (34) and the choice of L, we obtain

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

Hence, in this case we derive from (33) that

$$\begin{aligned}T &\leq (M^{h(h+1)/2+3}/p)^{2/h(h+1)} M^{1/h+o(1)} \\ &\leq M\left(M^4/p\right)^{2/h(h+1)+o(1)},\end{aligned}$$

which concludes the proof.

9. Proof of Theorem 9

Clearly

$$\sum_{H \in \mathcal{H}(\mathfrak{B})} N(H;\mathfrak{B}) = M^{2g} \qquad \text{and} \qquad \sum_{H \in \mathcal{H}(\mathfrak{B})} N(H;\mathfrak{B})^2 = T(\mathfrak{B}). \tag{35}$$

As in [8], using (35) and the Cauchy inequality we derive

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

From (4) 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

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

In particular,

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

Thus, by [8, Theorem 7] 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 (4) can take at most 4 values, and thus for every choice of $(a_0, \dots, a_{2g-3})$ there are only 4 choices for $(b_0, \dots, b_{2g-3})$. Therefore,

$$T(\mathfrak{B}) \leq M^{2g-2}\left(M^4/p + M^{2+o(1)}\right). \tag{36}$$

When $M < p^{1/(2g)}$ we obtain $T(\mathfrak{B}) \leq M^{2g+o(1)}$ and $\#\mathcal{H}(\mathfrak{B}) \geq M^{2g+o(1)}$, which proves Theorem 9 in this range.

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

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

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,

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

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 $1 \leq |r|, s \leq p^{1/2}$, $(r, s) = 1$ and such that $\alpha \equiv r/s \pmod{p}$. Thus

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

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

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

Therefore

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

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

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

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

Thus we have

$$T(\mathfrak{B}) \ll \begin{cases} M^2 \log M + M^4/p, & \text{if } g = 1, \\ M^{2g} + M^{4g}/p^{2g-1}, & \text{if } g \geq 2, \end{cases} \tag{37}$$

which gives

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

and proves Theorem 9 in the range $M \geq p^{1/2g}$.

10. Comments

The problem of obtaining a nontrivial upper bound for $I_f(M; R, S)$ in the range $p^{1/4} < M < p^{1/2}$ for cubic polynomials and in the range $p^{1/3} < M < p^{1/2}$ for polynomials of higher degree is still open.

On the other hand, we note that using bounds of exponential sums obtained within the method of Vinogradov instead of Lemma 11, see [4, 12, 21, 23] and references therein, also leads to some nontrivial on $J_f(M; R, S)$ but these results seem to be weaker that a combination of Theorem 5 with the bounds from [7].

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 [11], each admissible value of t, that is, with $|t| \leq 2p^{1/2}$, is taken and hence there are about $4p^{1/2}$ isogeny classes. Furthermore, Birch [3] 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 [17] 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 given by (35)

Thus, using (35) and (37), 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 is given by

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

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

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

Acknowledgement

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 2008-03880 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 DP1092835 and by NRF Grant CRP2-2007-03, Singapore.

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 $x_1 x_2 \equiv x_3 x_4 \pmod p$, the equation $x_1 x_2 = x_3 x_4$ and the mean value of character sums', *J. Number Theory*, **59** (1996), 398–413.

[3] 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.
[4] K. D. Boklan, and T. D. Wooley, 'On Weyl sums for smaller exponents', *Funct. et Approx. Commen. Math.*, (to appear).
[5] E. Bombieri and J. Pila, 'The number of integral points on arcs and ovals', *Duke Math. J.*, **59** (1989), 337–357.
[6] 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.
[7] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Math. Zeitschrift*, (to appear).
[8] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, 'Isomorphism classes of elliptic curves over a finite field in some thin families', *Preprint*, 2011, 1–18.
[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, 'Expansions of quadratic maps in prime fields', *Preprint*, 2011, 1–11.
[11] M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.*, **14** (1941), 197–272.
[12] 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.
[13] J. Gutierrez and I. E. Shparlinski, 'Expansion of orbits of some dynamical systems over finite fields', *Bul. Aust. Math. Soc.*, **82** (2010), 232–239.
[14] D. R. Heath-Brown, 'A mean value estimate for real character sums', *Acta Arith.*, **72** (1995), 235–275.
[15] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
[16] K. Karabina and B. Ustaoglu, 'Invalid-curve attacks on hyperelliptic curve cryptosystems', *Adv. Math. of Comm.*, **4** (2010), 307–321.
[17] H. W. Lenstra, 'Factoring integers with elliptic curves', *Annals Math.*, **126** (1987), 649–673.
[18] P. Lockhart, 'On the discriminant of a hyperelliptic curve', *Trans. Amer. Math. Soc.*, **342** (1994), 729–752.
[19] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Amer. Math. Soc., Providence, RI, 1994.
[20] E. Nart, 'Counting hyperelliptic curves', *Adv. Math.*, **221** (2009), 774–787.
[21] S. T. Parsell, 'On the Bombieri-Korobov estimate for Weyl sums', *Acta Arith.*, **138** (2009), 363–372.
[22] 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.
[23] R. C. Vaughan, *The Hardy–Littlewood method*, Cambridge Univ. Press, Cambridge, 1981.
[24] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing', *Ann. Math.*, (to appear).
[25] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing, II', *Preprint* 2011, (available from `http://arxiv.org/abs/1112.0358`).

[26] Z. Zheng, 'The distribution of zeros of an irreducible curve over a finite field', *J. Number Theory* **59** (1996), 106–118.
[27] A. Zumalacárregui, 'Concentration of points on modular quadratic forms', *Intern. J. Number Theory*, (to appear).

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