Polynomial Equations in Subgroups and Applications

Sergei V. Konyagin, Igor E. Shparlinski, and Ilya V. Vyugin

Dedicated to the Memory of Jean Bourgain

Abstract We obtain a new bound for the number of solutions to polynomial equations in cosets of multiplicative subgroups in finite fields, which generalizes previous results of P. Corvaja and U. Zannier (2013). We also obtain a conditional improvement of recent results of J. Bourgain, A. Gamburd, and P. Sarnak (2016) and S. V. Konyagin, S. V. Makarychev, I. E. Shparlinski, and I. V. Vyugin (2019) on the structure of solutions to the reduction of the Markoff equation $x^2 + y^2 + z^2 = 3xyz$ modulo a prime p.

2010 Mathematics Subject Classification 11D79, 11T06

S. V. Konyagin (✉)
Steklov Mathematical Institute, Moscow, Russia
e-mail: konyagin@mi-ras.ru

I. E. Shparlinski
Department of Pure Mathematics, University of New South Wales, Sydney, NSW, Australia
e-mail: igor.shparlinski@unsw.edu.au

I. V. Vyugin
Institute for Information Transmission Problems RAS, Moscow, Russia

HSE University, Moscow, Russia

Steklov Mathematical Institute, Moscow, Russia
e-mail: vyugin@gmail.com

A. Avila et al. (eds.), *Analysis at Large*, https://doi.org/10.1007/978-3-031-05331-3_12

1 Introduction

1.1 Background and Motivation

Bourgain, Gamburd, and Sarnak [2, 3] have recently initiated the study of reductions modulo p of the set $\mathcal{M}$ of *Markoff triples* $(x, y, z) \in \mathbb{N}^3$ which are positive integer solutions to the Diophantine equation

$$x^2 + y^2 + z^2 = 3xyz, \qquad (x, y, z) \in \mathbb{Z}^3. \tag{1}$$

Simple computation shows that the map

$$\mathcal{R}_1 : (x, y, z) \mapsto (3yz - x, y, z)$$

and similarly defined maps $\mathcal{R}_2$, $\mathcal{R}_3$ (which are all involutions) send one Markoff triple to another. Due to the symmetry of (1), the set $\mathcal{M}$ is also invariant under permutations. Let S_3 be the group of permutations of order 3. For $\sigma \in S_3$ we denote by Π_σ the mapping $\pi(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$. It is easy to check that the transformations $\mathcal{R}_i$, $i = 1, 2, 3$ and the mappings Π_σ generate a group of transformations acting on $\mathcal{M}$.

A celebrated result of Markoff [18, 19] asserts that all integer positive solutions to (1) can be generated from the solution (1, 1, 1) by using sequences of the above transformations.

This naturally leads to the notion of the *functional graph* on Markoff triples with the "root" (1, 1, 1) and edges $(x_1, y_1, z_1) \rightarrow (x_2, y_2, z_2)$, povided that $(x_2, y_2, z_2) = \mathcal{T}(x_1, y_1, z_1)$, where

$$\mathcal{T} \in \{\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3\} \cup \{\Pi_\sigma : \sigma \in S_3\}. \tag{2}$$

In this terminology, the result of Markoff [18, 19] asserts that this graph is *connected*.

Baragar [1, Section V.3] and, more recently, Bourgain, Gamburd, and Sarnak [2, 3] conjecture that this property is preserved modulo all sufficiently large primes p and the set of non-zero solutions $\mathcal{M}_p$ to (1) considered modulo p. In particular, this means that $\mathcal{M}_p$ can be obtained from the set of Markoff triples $\mathcal{M}$ reduced modulo p.

This conjecture, which we can also write as $\mathcal{M}_p = \mathcal{M} \pmod{p}$, means that the functional graph $\mathcal{X}_p$ associated with the transformation (2) remains connected.

Accordingly, if we define by $\mathcal{C}_p \subseteq \mathcal{M}_p$ the set of the triples in the largest connected component of the above graph $\mathcal{X}_p$, then we can state:

Conjecture 1.1 (Baragar [1]; Bourgain, Gamburd, and Sarnak [2, 3]) *For every prime p, we have $\mathcal{C}_p = \mathcal{M}_p$.*

Bourgain, Gamburd, and Sarnak [2, 3] have obtained several major results towards Conjecture 1.1; see also [4, 8, 9, 11]. For example, by [2, Theorem 1], we have

$$\#\left(\mathcal{M}_p \setminus \mathcal{C}_p\right) = p^{o(1)}, \qquad \text{as } p \to \infty, \tag{3}$$

and also by [2, Theorem 2], we know that Conjecture 1.1 holds for all but maybe at most $X^{o(1)}$ primes $p \le X$ as $X \to \infty$.

The bound (3) has been improved in [16, Theorem 1.2] as

$$\#\left(\mathcal{M}_p \setminus \mathcal{C}_p\right) \le \exp\left((\log p)^{2/3+o(1)}\right), \qquad \text{as } p \to \infty. \tag{4}$$

Furthermore, Bourgain, Gamburd, and Sarnak [2, 3] have also proved that the size of any connected component of the graphs $\mathcal{X}_p$ is at least

$$\#\mathcal{X}_p \ge c(\log p)^{1/3}, \tag{5}$$

for some absolute constant $c > 0$. In turn, the bound (5) has been improved in [16, Theorem 1.3] as

$$\#\mathcal{X}_p \ge c(\log p)^{7/9}. \tag{6}$$

The improvements in (4) and (6) are based on a bound of Corvaja and Zannier [7, Corollary 2], on the number of solutions to the equation

$$P(u, v) = 0, \quad (u, v) \in \mathcal{G}_1 \times \mathcal{G}_2,$$

where P is a bivariate absolutely irreducible polynomial over the finite field $\mathbb{F}_p$ of p elements and $\mathcal{G}_1, \mathcal{G}_2 \subseteq \overline{\mathbb{F}}_p$ are multiplicative groups in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$; see also [12, 14, 17, 20] for some related results.

Motivated by the above results and connections, here we

- Derive a new bound on the number of solutions in subgroups to a systems of several polynomials which covers under a unified setting the results of [7, 17, 20];
- Obtain an improvement of (4) under a very plausible conjecture on the number of solutions in subgroups of some particular equation over $\mathbb{F}_p^*$.

1.2 New Results

As before, for a prime p, we use $\overline{\mathbb{F}}_p$ to denote the algebraic closure of the finite field $\mathbb{F}_p$ of p elements.

We also say that a polynomial is irreducible if and only it is absolutely irreducible.

For a bivariate irreducible polynomial

$$P(X, Y) = \sum_{i+j \le d} a_{ij} X^i Y^j \in \overline{\mathbb{F}}_p[X, Y] \tag{7}$$

of total degree $\deg P \le d$, we define $P^\sharp(X, Y)$ as the homogeneous polynomial of degree $d^\sharp = \min\{i + j : a_{ij} \ne 0\}$ given by

$$P^\sharp(X, Y) = \sum_{i+j=d^\sharp} a_{ij} X^i Y^j. \tag{8}$$

We also consider the set of polynomials $\mathcal{P}$:

$$\mathcal{P} = \{P(\lambda X, \mu Y) \mid \lambda, \mu \in \overline{\mathbb{F}}_p^*\}.$$

Since $P(X, Y)$ is irreducible, it is not homogenous, and thus $P(X, Y) \ne P^\sharp(X, Y)$. Hence, we can define g as the greatest common divisor of the following set of differences:

$$g = \gcd\{i_1 + j_1 - i_2 - j_2 \ : \ a_{i_1,j_1} a_{i_2,j_2} \ne 0\}. \tag{9}$$

Given a multiplicative subgroup $\mathcal{G} \subseteq \overline{\mathbb{F}}_p$, we say that two polynomials $P, Q \in \overline{\mathbb{F}}_p[X, Y]$ are *$\mathcal{G}$-independent* if there is no $(u, v) \in \mathcal{G}^2$ and $\gamma \in \overline{\mathbb{F}}_p^*$ such that polynomials $P(X, Y)$ and $\gamma Q(uX, vY)$ coincide.

We now fix h polynomials

$$P_k(X, Y) = P(\lambda_k X, \mu_k Y) \in \mathcal{P}, \qquad k = 1, \dots, h, \tag{10}$$

which are $\mathcal{G}$-independent.

The following result generalizes a series of previous estimates of a similar type; see [7, 12, 14, 17, 20] and references therein.

Theorem 1.2 *Suppose that P is irreducible,*

$$\deg_X P = m \qquad \text{and} \qquad \deg_Y P = n$$

and also that $P^\sharp(X, Y)$ consists of at least two monomials. There exists a constant $c_0(m, n)$, depending only on m and n, such that for any multiplicative subgroup $\mathcal{G} \subseteq \overline{\mathbb{F}}_p$ of order $t = \#\mathcal{G}$ satisfying

$$\frac{1}{2} p^{3/4} h^{-1/4} \ge t \ge \max\{h^2, c_0(m, n)\},$$

and $\mathcal{G}$-independent polynomials (10) we have

$$\sum_{i=1}^{h} \# \left\{ (u, v) \in \mathcal{G}^2 \ : \ P_i(u, v) = 0 \right\} < 12mn(m+n)gh^{2/3}t^{2/3}.$$

Our next result is conditional on the following:

Conjecture 1.3 *There exist constants $\varepsilon_0 > 0$ and A such that for any prime p, any subgroup $\mathcal{G} \subseteq \overline{\mathbb{F}}_p$ with $\#\mathcal{G} \le p^{\varepsilon_0}$, and any elements $\alpha_{1,1}, \alpha_{1,2}, \alpha_{2,1}, \alpha_{2,2} \in \overline{\mathbb{F}}_p$ satisfying*

$$\alpha_{1,1} \neq 0, \quad \alpha_{1,2} \neq 0, \quad \alpha_{1,1}\alpha_{2,2} - \alpha_{1,2}\alpha_{2,1} \neq 0, \tag{11}$$

the equation

$$\frac{\alpha_{1,1}u - \alpha_{1,2}}{\alpha_{2,1}u - \alpha_{2,2}} = v \tag{12}$$

has at most A solutions in $u, v \in \mathcal{G}$.

Remark 1.4 It is likely that the constant A in Conjecture 1.3 cannot be taken less than 9, even for $\mathcal{G} \subseteq \mathbb{F}_p$ rather than for $\mathcal{G} \subseteq \overline{\mathbb{F}}_p$; see some heuristic arguments in Sect. 6. It is possible that this is optimal and Conjecture 1.3 holds with $A = 9$. Also we must have $\varepsilon_0 \le 1/2$; see Sect. 6.

Remark 1.5 It is easy to see that using the bound (4) instead of (3) in the argument of the proof of Theorem 1.6 immediately allows us to relax the condition of Conjecture 1.3 to counting solutions in subgroups $\mathcal{G} \subseteq \mathbb{F}_{p^2}$ of order $\#\mathcal{G} \le \exp\left((\log p)^{2/3+\varepsilon_0}\right)$. However, we believe Conjecture 1.3 holds as stated.

Theorem 1.6 *If Conjecture 1.3 holds for some ε_0 and A, then for sufficiently large p we have*

$$\#\left(\mathcal{M}_p \setminus \mathcal{C}_p\right) \le (\log p)^B,$$

where $B = 16 \log A + c$ for an absolute constant c.

Remark 1.7 Recently (after this work has been submitted) Chen [6] presented a striking result giving a full resolution of Conjecture 1.1 (for all sufficiently large p). However, we still believe that our present argument as well as the argument of [16] are of interest since they apply to more general equations than (1), for example, to equations of the form $x^2 + y^2 + z^2 = axyz + b$, which the method of [6] is limited to (1).

2 Solutions to Polynomial Equations in Subgroups of Finite Fields

2.1 Stepanov's Method

Consider a polynomial $\Phi \in \overline{\mathbb{F}}_p[X, Y, Z]$ such that

$$\deg_X \Phi < A, \quad \deg_Y \Phi < B, \quad \deg_Z \Phi < C,$$

that is,

$$\Phi(X, Y, Z) = \sum_{0\le a<A} \sum_{0\le b<B} \sum_{0\le c<C} \omega_{a,b,c} X^a Y^b Z^c.$$

We assume

$$A < t,$$

where $t = \#\mathcal{G}$ is the order of the subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$, and consider the polynomial

$$\Psi(X, Y) = Y^t \Phi(X/Y, X^t, Y^t).$$

Clearly,

$$\deg \Psi \le t + t(B-1) + t(C-1) = (B+C-1)t.$$

We now fix some $\mathcal{G}$-independent polynomials (10) and define the sets

$$\mathcal{F}_k = \left(\lambda_k^{-1}\mathcal{G} \times \mu_k^{-1}\mathcal{G}\right), \quad k = 1, \dots, h, \qquad \text{and} \qquad \mathcal{E} = \bigcup_{k=1}^{h} \mathcal{F}_k. \tag{13}$$

We also consider the locus of singularity

$$\mathcal{M}_{sing} = \Big\{(X, Y) \mid XY = P(X, Y) = 0 \text{ or } \\ \frac{\partial}{\partial Y} P(X, Y) = P(X, Y) = 0\Big\}.$$

Lemma 2.1 *Let $P(X, Y)$ be an irreducible polynomial of bi-degree*

$$\left(\deg_X P, \deg_Y P\right) = (m, n)$$

and let $n \ge 1$. Then, for the cardinality of the set $\mathcal{M}_{sing}$, the following holds:

$$\#\mathcal{M}_{sing} \le (m+n)^2.$$

Proof If the polynomial $P(X, Y)$ is irreducible, then the polynomials $P(X, Y)$ and $\frac{\partial P}{\partial Y}(X, Y)$ are relatively prime. Thus, the Bézout theorem yields the bound $L \le (m+n)(m+n-1)$, where L is the number of roots of the system

$$\frac{\partial}{\partial Y} P(X, Y) = P(X, Y) = 0.$$

Clearly, the number of X with $P(X, 0) = 0$ is less than or equal to $\deg_X P(X, Y) = m$, the number of pairs $(0, Y)$ on the curve

$$P(X, Y) = 0, \tag{14}$$

where P is given by (7), is less than or equal to $\deg_Y P(X, Y) = n$. The total numbers of such pairs is at most $L + m + n \le (m+n)^2$. □

Assume that the polynomial Ψ and the $\mathcal{G}$-independent polynomials (10) satisfy the following conditions:

- All pairs in the set

  $$\left\{(X, Y) \in \mathcal{E} \setminus \mathcal{M}_{sing} \mid P(X, Y) = 0\right\}$$

  are zeros of orders at least D of the function $\Psi(X, Y)$ on the curve (14);
- The polynomials $\Psi(X, Y)$ and $P(X, Y)$ are relatively prime.

If these conditions are satisfied, then the *Bézout theorem* gives us the upper bound $D^{-1} \deg \Psi \deg P + \#\mathcal{M}_{sing}$ for the number of roots (x, y) of the system

$$\Psi(X, Y) = P(X, Y) = 0, \qquad (X, Y) \in \mathcal{G}.$$

Since the polynomials P_k are $\mathcal{G}$-independent, the sets $\mathcal{F}_k$ given by (13) are disjoint, and also there is a one-to-one correspondence between the zeros:

$$\begin{aligned} &P_k(X, Y) = 0,\ (X, Y) \in \mathcal{G}^2, \\ &\qquad\qquad \Longleftrightarrow P(u, v) = 0,\ (u, v) = (\lambda_k^{-1} X, \mu_k^{-1} Y) \in \mathcal{F}_k. \end{aligned}$$

Therefore, we obtain the bound

$$\begin{aligned} N_h &\le \frac{\deg \Psi \cdot \deg P}{D} + \#\mathcal{M}_{sing} \\ &\le \frac{(m+n)(B+C-1)t}{D} + \#\mathcal{M}_{sing} \end{aligned} \tag{15}$$

on the total number of zeros of P_k in $\mathcal{G}^2$, $k = 1, \dots, h$:

$$N_h = \sum_{k=1}^{h} \#\{(u, v) \in \mathcal{G}^2 \;:\; P_k(u, v) = 0\}.$$

For completeness, we present proofs of several results from [17] which we use here as well.

2.2 Some Divisibilities and Non-divisibilities

We begin with some simple preparatory results on the divisibility of polynomials.

Lemma 2.2 *Suppose that $Q(X, Y) \in \mathbb{F}_p[X, Y]$ is an irreducible $\mathcal{G}$-independent polynomial such that*

$$Q(X, Y) \mid \Psi(X, Y)$$

and $Q^\sharp(X, Y)$ consists of at least two monomials. Then,

$$Q^\sharp(X, Y)^{\lfloor t/e \rfloor} \mid \Psi^\sharp(X, Y),$$

where $Q^\sharp(X, Y)$ and $\Psi^\sharp(X, Y)$ are defined as in (8) and e is defined as g in (9) with respect to $Q(X, Y)$ instead of $P(x, y)$.

Proof Consider $\rho \in \mathcal{G}$ and substitute $X = \rho\widetilde{X}$ and $Y = \rho\widetilde{Y}$ in the polynomials $Q(X, Y)$ and $\Psi(X, Y)$. Then,

$$Q(X, Y) \longmapsto Q_\rho(\widetilde{X}, \widetilde{Y}) = Q(\rho\widetilde{X}, \rho\widetilde{Y}),$$

and

$$\begin{aligned}\Psi(X, Y) &= \Psi(\rho\widetilde{X}, \rho\widetilde{Y}) \\ &= (\rho\widetilde{Y})^t \Phi((\rho\widetilde{X})/(\rho\widetilde{Y}), (\rho\widetilde{X})^t, (\rho\widetilde{Y})^t) = \Psi(\widetilde{X}, \widetilde{Y}),\end{aligned}$$

because $\rho^t = 1$. Hence, for any $\rho \in \mathcal{G}$, we have

$$Q_\rho(X, Y) \mid \Psi(X, Y),$$

and we also note that $Q_\rho(X, Y)$ is irreducible.

Since $Q(X, Y)$ is irreducible, $e \geqslant 1$ is correctly defined, and there exist at least $s = \lfloor t/e \rfloor$ elements $\rho_1, \ldots, \rho_s \in \mathcal{G}$ such that all nontrivial ratios $Q_{\rho_i}(X, Y)/Q_{\rho_j}(X, Y)$ are not constants, that is,

$$Q_{\rho_i}(X, Y)/Q_{\rho_j}(X, Y) \notin \overline{\mathbb{F}}_p, \qquad 1 \le i < j \le s. \tag{16}$$

Obviously, the polynomials $Q_{\rho_1}(X, Y), \ldots, Q_{\rho_s}(X, Y)$ are pairwise relatively prime, because they are irreducible and satisfy (16). Furthermore, the polynomials $Q^{\sharp}_{\rho_i}(X, Y)$ are homogeneous of degree $d^{\sharp}$, and the following holds

$$Q^{\sharp}(X, Y) = \rho_1^{-d^{\sharp}} Q^{\sharp}_{\rho_1}(X, Y) = \ldots = \rho_s^{-d^{\sharp}} Q^{\sharp}_{\rho_s}(X, Y).$$

So, we have

$$Q_{\rho_1}(X, Y) \cdot \ldots \cdot Q_{\rho_s}(X, Y) \mid \Psi(X, Y);$$

consequently,

$$Q^{\sharp}_{\rho_1}(X, Y) \cdot \ldots \cdot Q^{\sharp}_{\rho_s}(X, Y) \mid \Psi^{\sharp}(X, Y).$$

Since

$$Q^{\sharp}_{\rho_1}(X, Y) \cdot \ldots \cdot Q^{\sharp}_{\rho_s}(X, Y) = (\rho_1 \cdot \ldots \cdot \rho_s)^{d^{\sharp}} Q^{\sharp}(X, Y)^s,$$

we obtain the desired result. □

Lemma 2.3 *Let $G(X, Y), H(X, Y) \in \mathbb{F}_p[X, Y]$ be two homogeneous polynomials. Also suppose that $G(X, Y)$ consists of at least two nonzero monomials,* $\deg H < p$, *and the number of monomials of the polynomial $H(X, Y)$ does not exceed s for some positive integer $s < p$. Then,*

$$G(X, Y)^s \nmid H(X, Y).$$

Proof Clearly, if $G(X, Y)^s \mid H(X, Y)$, then $G(X, 1)^s \mid H(X, 1)$. The polynomial $G(X, 1)$ has at least one nonzero root. It has been proved in [14, Lemma 6] that such a polynomial $H(X, 1)$ cannot have a nonzero root of order s and the result follows. □

Lemma 2.4 *If $AB < t/g$ and* $\deg \Psi < p$, *then for the polynomial $P(X, Y)$ given by (7) we have*

$$P(X, Y) \nmid \Psi(X, Y).$$

2.3 Derivatives on Some Curves

There we study derivatives on an algebraic curve and define some special differential operators. Throughout this section, we use

$$\frac{\partial}{\partial X}, \quad \frac{\partial}{\partial Y} \qquad \text{and} \qquad \frac{d}{dX}$$

for standard partial derivatives with respect to X and Y and for the derivative with respect to X along the curve (14), respectively. In particular,

$$\frac{d}{dX} = \frac{\partial}{\partial X} + \frac{dY}{dX}\frac{\partial}{\partial Y}, \tag{17}$$

where by the implicit function theorem from the Eq. (14), we have

$$\frac{dY}{dX} = -\frac{\frac{\partial P}{\partial X}(X, Y)}{\frac{\partial P}{\partial Y}(X, Y)}.$$

We also define inductively

$$\frac{d^k}{dX^k} = \frac{d}{dX}\frac{d^{k-1}}{dX^{k-1}}$$

the k-th derivative on the curve (14).

Consider the polynomials $q_k(X, Y)$ and $r_k(X, Y)$, $k \in \mathbb{N}$, which are defined inductively as

$$q_1(X, Y) = -\frac{\partial}{\partial X}P(X, Y), \qquad r_1(X, Y) = \frac{\partial}{\partial Y}P(X, Y),$$

and

$$\begin{aligned} q_{k+1}(X, Y) = {} & \frac{\partial q_k}{\partial X}\left(\frac{\partial P}{\partial Y}\right)^2 \\ & - \frac{\partial q_k}{\partial Y}\frac{\partial P}{\partial X}\frac{\partial P}{\partial Y} - (2k-1)q_k(X, Y)\frac{\partial^2 P}{\partial X \partial Y}\frac{\partial P}{\partial Y} \\ & + (2k-1)q_k(X, Y)\frac{\partial^2 P}{\partial Y^2}\frac{\partial P}{\partial X}, \\ r_{k+1}(X, Y) = {} & r_k(X, Y)\left(\frac{\partial P}{\partial Y}\right)^2 = \left(\frac{\partial P}{\partial Y}\right)^{2k+1}. \end{aligned} \tag{18}$$

We now show by induction that

$$\frac{d^k}{dX^k}Y = \frac{q_k(X, Y)}{r_k(X, Y)}, \qquad k \in \mathbb{N}. \tag{19}$$

The base of induction is

$$\frac{d}{dX}Y = -\frac{\frac{\partial}{\partial X}P(X,Y)}{\frac{\partial}{\partial Y}P(X,Y)} = \frac{q_1(X,Y)}{r_1(X,Y)}.$$

One can now easily verify that assuming (19) and (17) we have

$$\frac{d^{k+1}}{dX^{k+1}}Y = \frac{d}{dX}\frac{d^k}{dX^k}Y = \frac{d}{dX}\frac{q_k(X,Y)}{r_k(X,Y)} = \frac{q_{k+1}(X,Y)}{r_{k+1}(X,Y)},$$

where q_{k+1} and r_{k+1} are given by (18), which concludes the induction and proves the formula (19).

The implicit function theorem gives us the derivatives $\frac{d^{k+1}}{dX^{k+1}}Y$ at a point (X, Y) on the algebraic curve (14), if the denominator $r_k(X, Y)$ is not equal to zero. Otherwise, $r_k(X, Y) = 0$ if and only if the following system holds:

$$\frac{\partial}{\partial Y}P(X,Y) = P(X,Y) = 0.$$

Let us give the following estimates:

Lemma 2.5 *For all integers $k \geq 1$, the degrees of the polynomials $q_k(X, Y)$ and $r_k(X, Y)$ satisfy the bounds*

$$\deg_X q_k \leq (2k-1)m - k, \qquad \deg_Y q_k \leq (2k-1)n - 2k + 2,$$
$$\deg_X r_k \leq (2k-1)m, \qquad \deg_Y r_k \leq (2k-1)(n-1).$$

Proof Direct calculations show that

$$\deg_X q_1 \leq m - 1 \qquad \text{and} \qquad \deg_Y q_1 \leq n,$$

and using (18) (with $k - 1$ instead of k) and examining the degree of each term, we obtain the inequalities

$$\deg_X q_k \leq \deg_X q_{k-1} + 2m - 1 \leq (2k-1)m - k,$$
$$\deg_Y q_k \leq \deg_y q_{k-1} + 2n - 2 \leq (2k-1)n - 2k + 2.$$

We now obtain the desire bounds on $\deg_X q_k$ and $\deg_Y q_k$ by induction.

For the polynomials r_k, the statement is obvious. □

Lemma 2.6 *Let $Q(X, Y) \in \mathbb{F}_p[X, Y]$ be a polynomial such that*

$$\deg_X Q(X,Y) \leq \mu, \quad \deg_Y Q(X,Y) \leq \nu \tag{20}$$

and $P(X, Y) \in \mathbb{F}_p[X, Y]$ be a polynomial such that

$$\deg_X P(X,Y) \le m, \quad \deg_Y P(X,Y) \le n.$$

Then, the divisibility condition

$$P(X,Y) \mid Q(X,Y) \tag{21}$$

on the coefficients of the polynomial $Q(X,Y)$ is equivalent to a certain system of not more than $(\mu+\nu+1)mn$ homogeneous linear algebraic equations in coefficients of $Q(X,Y)$ as variables.

Proof The dimension of the vector space $\mathcal{L}$ of polynomials $Q(X,Y)$ that satisfy (20) is equal to $(\mu+1)(\nu+1)$. Let us call the vector subspace of polynomials $Q(X,Y)$ that satisfy (20) and (21) by $\widetilde{\mathcal{L}}$. Because $Q(X,Y) = P(X,Y)R(X,Y)$ where the polynomial $R(X,Y)$ is such that

$$\deg_X R(X,Y) \le \mu - m \qquad \text{and} \qquad \deg_Y R(X,Y) \le \nu - n, \tag{22}$$

then the vector space $\widetilde{\mathcal{L}}$ is isomorphic to the vector space of the coefficients of the polynomials $R(x,y)$ satisfying (22). The dimension of the vector space $\widetilde{\mathcal{L}}$ is equal to

$$\dim \widetilde{\mathcal{L}} = (\mu - m + 1)(\nu - n + 1).$$

It means that the subspace $\widetilde{\mathcal{L}}$ of the space $\mathcal{L}$ is given by a system of

$$(\mu+1)(\nu+1) - (\mu-m+1)(\nu-n+1)$$
$$= \mu n + \nu m - mn + m + n + 1 \le (\mu+\nu+1)mn$$

homogeneous linear algebraic equations. □

As in [17], we now consider the differential operators:

$$D_k = \left(\frac{\partial P}{\partial Y}\right)^{2k-1} X^k Y^k \frac{d^k}{dX^k}, \qquad k \in \mathbb{N}, \tag{23}$$

where, as before, $\frac{d^k}{dX^k}$ denotes the k-th derivative on the algebraic curve (14) with the local parameter X. We note now that the derivative of a polynomial in two variables along a curve is a rational function. As one can see from the inductive formula for $\frac{d^k}{dX^k}$, the result of applying any operator D_k to a polynomial in two variables is again a polynomial in two variables.

Consider non-negative integers a, b, c such that $a < A$, $b < B$, $c < C$. From the formulas (19) for derivatives on the algebraic curve (14), we obtain by induction the following relations:

$$\begin{aligned} D_k \left(\frac{X}{Y}\right)^a X^{bt} Y^{(c+1)t} &= R_{k,a,b,c}(X,Y) \left(\frac{X}{Y}\right)^a X^{bt} Y^{(c+1)t}, \\ D_k \Psi(X,Y)|_{X,Y\in\mathcal{F}_i} &= R_{k,i}(X,Y)|_{X,Y\in\mathcal{F}_i}, \end{aligned} \tag{24}$$

where $\mathcal{F}_i$ are from formula (13),

$$\begin{aligned} &R_{k,i}(X,Y) \\ &= \sum_{0\le a<A} \sum_{0\le b<B} \sum_{0\le c<C} \omega_{a,b,c} R_{k,a,b,c}(X,Y) \left(\frac{X}{Y}\right)^a \lambda_i^{-bt} \mu_i^{-(c+1)t} \end{aligned} \tag{25}$$

for some coefficients $\omega_{a,b,c} \in \mathbb{F}_p$, $a < A$, $b < B$, $c < C$, and λ_i, μ_i from (13).

We now define

$$\widetilde{R}_{k,i}(X,Y) = Y^{A-1} R_{k,i}(X,Y). \tag{26}$$

Lemma 2.7 *The rational functions $R_{k,a,b,c}(X,Y)$ and $\widetilde{R}_{k,i}(X,Y)$, given by (24) and (26), are polynomials of degrees*

$$\deg_X R_{k,a,b,c} \le 4km, \qquad \deg_Y R_{k,a,b,c} \le 4kn,$$

and

$$\deg_X \widetilde{R}_{k,i} \le A + 4km, \qquad \deg_Y \widetilde{R}_{k,i} \le A + 4kn.$$

Proof We have

$$\begin{aligned} \frac{d^k}{dX^k} X^{a+bt} Y^{(c+1)t-a} = \sum_{(\ell_1,\ldots,\ell_s)} & C_{\ell_1,\ldots,\ell_s} X^{a+bt-k+\sum_{i=1}^s \ell_i} \\ & Y^{(c+1)t-a-s} \left(\frac{d^{\ell_1} Y}{dX^{\ell_1}}\right) \ldots \left(\frac{d^{\ell_s} Y}{dX^{\ell_s}}\right), \end{aligned} \tag{27}$$

where $(\ell_1,\ldots,\ell_s)$ runs through all s-tuples of positive integers with $\ell_1 + \ldots + \ell_s \le k$, $s = 0,\ldots,k$, and $C_{\ell_1,\ldots,\ell_s}$ are some constants.

By the formula (27) and the form of the operator (23), we obtain that $R_{k,a,b,c}(x,y)$ are polynomials and $R_{k,i}(x,y)$ are rational functions. Actually, from the formulas (27) and (19), we easily obtain that the denominator of

$$\frac{d^k}{dX^k} \left(\frac{X}{Y}\right)^a X^{bt} Y^{(c+1)t}$$

divides $\left(\frac{\partial P}{\partial Y}(X, Y)\right)^{2k-1}$. Hence, we obtain that $R_{k,a,b.c}(X, Y)$ are polynomials. From the formula (25), we obtain that $R_{k,i}$ is a rational function with denominator divided by Y^{A-1}. Consequently, $\widetilde{R}_{k,i}$ are polynomials.

The result now follows from Lemma 2.5 and the formulas (23) and (24). □

2.4 Multiplicity Points on Some Curves

We recall that D_k, $k = 1, 2, \ldots$ are the differential operators defined by (23).

Lemma 2.8 *If $P(X, Y) \mid \Psi(X, Y)$ and $P(X, Y) \mid D_j\Psi(X, Y)$, $j = 1, \ldots, k-1$, then at least one of the following alternatives holds:*

- *either (x, y) is a root of order at least k of $\Psi(X, Y)$ on the algebraic curve (14).*
- *or $(x, y) \in \mathcal{M}_{sing}$.*

Proof If $D_j\Psi(X, Y)$ vanishes on the curve $P(X, Y) = 0$, then either

$$\frac{d^j}{dX^j}\Psi(x, y) = 0, \tag{28}$$

where, as before, $\frac{d^j}{dX^j}$ is j-th derivative on the algebraic curve (14) with the local parameter X, or

$$xy = 0, \tag{29}$$

or

$$\frac{\partial P}{\partial Y}(x, y) = 0, \tag{30}$$

on the curve (14).

If we have (28) for $j = 1, \ldots, k-1$ and also $\Psi(x, y) = 0$, then the pair (x, y) satisfies the first case of conditions of Lemma 2.8.

If we have (29) or (30) on the curve (14), then the pair (x, y) satisfies the second case of conditions of Lemma 2.8. □

3 Small Divisors of Integers

3.1 Smooth Numbers

As usual, we say that a positive integer is y-smooth if it is composed of prime numbers up to y. Then, we denote by $\psi(x, y)$ the number of y-smooth positive integers $n \le x$. Among a large variety of bounds and asymptotic formulas for $\psi(x, y)$ (see [13, 15, 22]), the most convenient bound for our applications is given by [22, Theorem 5.1].

Lemma 3.1 *There is an absolute constant c_0 such that for any fixed real-positive $x \ge y \ge 2$, we have*

$$\psi(x, y) \le c_0 e^{-u/2} x,$$

where

$$u = \frac{\log x}{\log y}.$$

3.2 Number of Small Divisors of Integers

For a real z and an integer n, we use $\tau_z(n)$ to denote the number of positive integer divisors $d \mid n$ with $d \le z$. We present a bound on $\tau_z(n)$ for small values of z (which we put in a slightly more general form than we need for our applications).

Lemma 3.2 *There is an absolute constant C_0 such that for any fixed real-positive $\varepsilon < 1$, there is $n(\varepsilon)$ such that if $n \ge n(\varepsilon)$ and $z \ge (\log n)^{2\log(1/\varepsilon)}$, then*

$$\tau_z(n) \le C_0 \varepsilon z.$$

Proof Let s be the number of all distinct prime divisors of n, and let $p_1, \dots, p_s$ be the first s primes. We note that

$$\tau_z(n) \le \psi(z, p_s). \tag{31}$$

By the prime number theorem, we have $n \ge p_1 \dots p_s = \exp(p_s + o(p_s))$, and thus

$$p_s \ll \log n \le z^{1/b}, \tag{32}$$

where $b = 2\log(1/\varepsilon)$. Combining Lemma 3.1 with (31) and (32), we see that

$$\tau_z(n) \le \psi(z, z^{1/b+o(1)}) \le c_0 e^{-b/2+o(1)} z = (c_0 + o(1)) e^{-b/2} z \le C_0 \varepsilon z$$

for any $C_0 > c_0$ (where c_0 is as in Lemma 3.1), provided that n and thus z are large enough. □

4 Proof of Theorem 1.2

4.1 Preliminary Estimates

We define the following parameters:

$$A = \left\lfloor \frac{t^{2/3}}{gh^{1/3}} \right\rfloor, \quad B = C = \left\lfloor h^{1/3} t^{1/3} \right\rfloor, \qquad D = \left\lfloor \frac{t^{2/3}}{4gh^{1/3}mn} \right\rfloor.$$

The exact values of A, B, C, and D play no role until the optimization step at the very end of the proof. However, it is important to note that their choice ensures (36) and (37).

If $P_i(x, y) = 0$ for at least one $i = 1, \ldots, h$, then

$$D_k \Psi(x, y) = 0, \qquad (x, y) \in \bigcup_{i=1}^{h} \mathcal{F}_i, \tag{33}$$

with the operators (23), where the sets $\mathcal{F}_i$ are as in (13). The condition (33) is given by a system of linear homogeneous algebraic equations in the variables $\omega_{a,b,c}$. The number of equations can be calculated by means of Lemmas 2.6 and 2.7. To satisfy the condition (33) for some k, we have to make sure that the polynomials $\widetilde{R}_{k,i}(X, Y)$, $i = 1, \ldots, h$, given by (26), vanish identically on the curve (14). The bi-degree of $\widetilde{R}_{k,i}(X, Y)$ is given by Lemma 2.7:

$$\deg_X \widetilde{R}_{k,i} \le A + 4km, \qquad \deg_Y \widetilde{R}_{k,i} \le A + 4kn.$$

The number of equations on the coefficients that guarantee the vanishing of the polynomial $\widetilde{R}_{k,i}(X, Y)$ on the curve (14) is given by Lemma 2.6 and is equal to $(\mu + \nu + 1)mn$, where μ, ν are as in Lemma 2.6 and

$$\mu \le A + 4km, \quad \nu \le A + 4kn.$$

Finally, the condition (33) for some k is given by $h(\mu + \nu + 1)mn \le mnh(2A + 4k(m + n))$ linear algebraic homogeneous equations. Consequently, the condition (33) for all $k = 0, \ldots, D - 1$ is given by the system of

$$L = hmn \sum_{k=0}^{D-1} (4k(m + n) + 2A + 1)$$

linear algebraic homogeneous equations in variables $\omega_{a,b,c}$. Now it is easy to see that

$$L = h\left((2A + 1)Dmn + 2nm(m + n)D(D - 1)\right)$$

$$\leq 2hADmn + 2hmn(m+n)D^2 = 2hmn(AD + (m+n)D^2).$$

4.2 Optimization of Parameters

The system has a nonzero solution if the number of equations is less than to the number of variables, in particular, if

$$2hmn(AD + (m+n)D^2) < ABC, \tag{34}$$

as we have ABC variables. It is easy to get an upper bound for the left-hand side of (34). For sufficiently large $t > c_0(m,n)$, where $c_0(m,n)$ is some constant depending only on m and n, we have

$$\begin{aligned} &2hmn(AD + (m+n)D^2) \\ &\quad < 2hmn\left(\frac{h^{-1/3}t^{2/3}}{g}\frac{h^{-1/3}t^{2/3}}{4mng} + (m+n)\frac{h^{-2/3}t^{4/3}}{16m^2n^2g^2}\right) \\ &\quad < \frac{3}{4}\frac{h^{1/3}t^{4/3}}{g^2}. \end{aligned} \tag{35}$$

Assuming that $c_0(m,n)$ is large enough, we obtain

$$ABC = \left\lfloor \frac{h^{-1/3}t^{2/3}}{g} \right\rfloor \lfloor h^{1/3}t^{1/3} \rfloor^2 > \frac{3}{4}\frac{h^{1/3}t^{4/3}}{g^2},$$

which together with (35) implies (34).

It is clear that

$$gAB \leq t. \tag{36}$$

We also require that the degree of the polynomial $\Psi(x,y)$ should be less than p,

$$\deg \Psi(x,y) \leq (B-1)t + Ct < p. \tag{37}$$

Actually, the inequality $(B-1)t + Ct < 2h^{1/3}t^{4/3} < p$ is satisfied because $t < \frac{1}{2}p^{3/4}h^{-1/4}$.

Finally, recalling Lemmas 2.2, 2.3 and 2.4, and also the irreducibility of the polynomial $P(x,y)$, we see that $P_k(X,Y)$ and $\Psi(X,Y)$ are co-prime. Hence, by Lemmas 2.1 and 2.8 and the inequality (15), we obtain that N_h satisfies the inequality

$$\begin{aligned} N_h &\le \#\mathcal{M}_{sing} + (m+n)\frac{(B+C-1)t}{D} \\ &< (m+n)^2 + (m+n)\frac{2h^{1/3}t^{4/3}}{\lfloor h^{-1/3}t^{2/3}/(4mng)\rfloor} \\ &< 12mn(m+n)gh^{2/3}t^{2/3} \end{aligned}$$

for sufficiently large $t > c_0(m,n)$, which concludes the proof.

5 Proof of Theorem 1.6

5.1 Outline of the Proof

Before giving technical details, we first outline the sequence of the following steps:

- We consider the set $\mathcal{R} = \mathcal{M}_p \setminus \mathcal{C}_p$ and show that if it is large then by Lemma 3.2 there is a large set $\mathcal{L} \subseteq \mathcal{R}$ elements of large orders.
- Each element $x \in \mathcal{L}$ has an orbit of size at least $t(x)/2$, which is also in $\mathcal{R}$.
- Using Conjecture 1.3, we estimate the size of intersections of these orbits for distinct elements $x_1, x_2 \in \mathcal{L}$.
- We conclude that all intersections together are small, and so to fit all orbits in $\mathcal{R}$, the size of $\mathcal{R}$ must be even larger than we have initially assumed.

5.2 Formal Argument

We always assume that p is large enough. Define the mapping

$$\mathcal{T}_0\,(x,y,z) \mapsto (x,z,3xz-y)\,,$$

where $\mathcal{T}_0 = \Pi_{1,3,2} \circ \mathcal{R}_2$ is the composition of the permutations

$$\Pi_{1,3,2} = (x,y,z) \mapsto (x,z,y)$$

and the involution

$$\mathcal{R}_2 : (x,y,z) \mapsto (x,3xz-y,z)$$

as in the above.

Therefore, the orbit $\Gamma(x,y,z)$ of (x,y,z) under the above group of transformations Γ contains, in particular, the triples (x,u_n,u_{n+1}), $n = 1,2,\ldots$, where the sequence u_n satisfies a binary linear recurrence relation

$$u_{n+2} = 3xu_{n+1} - u_n, \qquad n = 1, 2, \dots, \tag{38}$$

with the initial values, $u_1 = y$, $u_2 = z$. This also means that $\Gamma(x, y, z)$ contains all triples obtained by the permutations of the elements in (x, u_n, u_{n+1}).

Let $\xi, \xi^{-1} \in \mathbb{F}_{p^2}^*$ be the roots of the characteristic polynomial $Z^2 - 3xZ + 1$ of the recurrence relation (38). In particular, $3x = \xi + \xi^{-1}$. Then, it is easy to see that unless $(x, y, z) = (0, 0, 0)$, which we eliminate from the consideration, the sequence u_n is periodic with period $t(x)$ which is the order of ξ in $\mathbb{F}_{p^2}^*$.

Let B be a fixed positive number to be chosen later. We denote

$$M_0 = (\log p)^B \qquad \text{and} \qquad M_1 = M_0^{1/4}/3 = (\log p)^{B/4}/3.$$

Assume that the remaining set of nodes $\mathcal{R} = \mathcal{M}_p \setminus \mathcal{C}_p$ is of size $\#\mathcal{R} > M_0$. Note that if $(x, y, z) \in \mathcal{R}$, then also $(y, x, z) \in \mathcal{R}$, and for any x, y, there are at most two values of z such that $(x, y, z) \in \mathcal{R}$. Therefore, there are more than $(M_0/2)^{1/2}$ elements $x \in \mathbb{F}_p^*$ with $(x, y, z) \in \mathcal{R}$ for some $y, z \in \mathbb{F}_p$.

Since there are obviously at most $T(T+1)/2$ elements $\xi \in \mathbb{F}_{p^2}^*$ of order at most T, we conclude that there is a triple $(x^*, y^*, z^*) \in \mathcal{R}$ with

$$t(x^*) > \sqrt{(M_0/2)^{1/2}} > 2M_1, \tag{39}$$

where $t(x^*)$ is the period of the sequence u_n which is defined as in (38) with respect to (x^*, y^*, z^*).

Then, the orbit $\Gamma(x^*, y^*, z^*)$ of this triple has at least $2M_1$ elements. Let M be the cardinality of the set $\mathcal{X}$ of projections along the first components of all triples $(x, y, z) \in \Gamma(x^*, y^*, z^*)$. Since the orbits are closed under the permutation of coordinates and permutations of the triples

$$(x^*, u_n, u_{n+1}), \qquad n = 1, \dots, t(x^*),$$

where as above the sequence u_n is defined as in (38) with respect to (x^*, y^*, z^*) and $t(x^*)$ is its period, produce the same projection no more than twice, we obtain

$$M \geq \frac{1}{2} t(x^*). \tag{40}$$

Recalling (39), we obtain

$$M > M_1 = (\log p)^{B/4}/3. \tag{41}$$

Using that $(x, y, z) \notin \mathcal{M}_p$, we notice that by the bound (3),

$$M = p^{o(1)}. \tag{42}$$

For $t \mid p^2 - 1$, we denote $g(t)$ the number of $x \in \mathcal{X}$ for which the period of the sequence u_n defined as in (38) satisfies $t(x) = t$. Observe that

$$\sum_{t \mid p^2-1} g(t) = M.$$

The same argument as used in the bound (40) implies that

$$g(t) = 0 \quad \text{for} \quad t > 2M. \tag{43}$$

We apply Lemma 3.2 with

$$\varepsilon = \frac{1}{40AC_0}, \tag{44}$$

where A is a bound from Conjecture 1.3 and C_0 is as in Lemma 3.1. Take

$$B = 16 \log(1/\varepsilon) + 1. \tag{45}$$

Since $g(t) < t$ for any t and also since due to (41) we have

$$4\sqrt{AM} > (\log p)^{B/8} \ge (\log(p^2-1))^{2\log(1/\varepsilon)},$$

by Lemma 3.2,

$$\begin{aligned} \sum_{\substack{t \le 4\sqrt{AM} \\ t \mid p^2-1}} g(t) < \sum_{\substack{t \le 4\sqrt{AM} \\ t \mid p^2-1}} t &\le 4\sqrt{AM}\tau_{4\sqrt{AM}}(p^2-1) \\ &\le C_0\varepsilon(4\sqrt{AM})^2 = 0.4M. \end{aligned}$$

Hence, we conclude that

$$\sum_{\substack{t > 4\sqrt{AM} \\ t \mid p^2-1}} g(t) \ge 0.6M.$$

Let $\mathcal{L}$ be the set of $x \in \mathcal{X}$ with $t(x) > 4\sqrt{AM}$. We have shown that

$$\#\mathcal{L} \ge 0.6M. \tag{46}$$

For each $x \in \mathcal{L}$, we fix some $y, z \in \mathbb{F}_p$ such $(x, y, z) \in \Gamma(x^*, y^*, z^*)$ and again consider the sequence u_n, $n = 1, 2, \ldots$, given by (38) having the period $t(x) = t_0$, so we consider the set

$$\mathcal{Z}(x) = \{u_n \ : \ n = 1, \dots, t_0\}.$$

Let $\mathcal{H}_x$ be the subgroup of $\mathbb{F}_{p^2}^*$ of order $t(x)$ and $\xi(x)$ satisfy the equation $3x = \xi(x) + \xi(x)^{-1}$. One can easily check, using an explicit expression for binary recurrence sequences via the roots of the characteristic polynomial, that

$$\mathcal{Z}(x) = \left\{\alpha(x)u + \frac{r(x)}{\alpha(x)u} \ : \ u \in \mathcal{H}_x\right\},$$

where

$$r(x) = \frac{(\xi(x)^2 + 1)^2}{9(\xi(x)^2 - 1)^2},$$

and $\alpha(x) \in \mathbb{F}_{p^2}^*$. If for some r an element $\xi = \xi_0$ satisfies the equation

$$r = \frac{(\xi^2 + 1)^2}{9(\xi^2 - 1)^2},$$

then other solutions are $-\xi_0$, $1/\xi_0$, $-1/\xi_0$. Moreover, $3x = \xi + \xi^{-1}$ can take, for a fixed r, at most two values whose sum is 0. Since every value is taken at most twice among the elements of the sequence u_n, $n = 1, \dots, t(x)$, we have

$$\#\mathcal{Z}(x) \geq \frac{1}{2}t(x) > 2\sqrt{AM}. \tag{47}$$

Now we construct a set $\mathcal{L}^* \subseteq \mathcal{L}$. If $x, x^* \in \mathcal{L}$ and $x + x^* = 0$, then we put one of the elements x, x^* in $\mathcal{L}^*$. If $x \in \mathcal{L}$ and $-x \notin \mathcal{L}$, then we set $x \in \mathcal{L}^*$. Due to (46), we get

$$\#\mathcal{L}^* \geq 0.3M. \tag{48}$$

Moreover, for any distinct $x, x^* \in \mathcal{L}^*$, we have $x+x^* \neq 0$ and, hence, $r(x) \neq r(x^*)$.

We claim that under Conjecture 1.3 for any distinct $x, x^* \in \mathcal{L}^*$, the inequality

$$\#\left(\mathcal{Z}(x) \bigcap \mathcal{Z}(x^*)\right) \leq 2A \tag{49}$$

holds.

Indeed, take distinct elements $x, x^* \in \mathcal{L}^*$. By $\mathcal{G}$, we denote the subgroup of $\mathbb{F}_{p^2}^*$ generated by $\mathcal{H}_x$ and $\mathcal{H}_{x^*}$. Notice that due to (42) and (43), we have

$$\#\mathcal{G} = p^{o(1)}. \tag{50}$$

Next, $\#(Z(x) \cap Z(x^*)$ is the number of solutions to the equation

$$\alpha(x)u + \frac{r(x)}{\alpha(x)u} = \alpha(x^*)v + \frac{r(x^*)}{\alpha(x^*)v}, \qquad (u, v) \in \mathcal{H}_x \times \mathcal{H}_{x^*},$$

as in the above or, equivalently,

$$P_{x,x^*}(u, v) = 0, \qquad (u, v) \in \mathcal{H}_x \times \mathcal{H}_{x^*},$$

where

$$P_{x,x^*}(X, Y) = \alpha(x)^2\alpha(x^*)X^2Y - \alpha(x)\alpha(x^*)^2XY^2 - \alpha(x)r(x^*)X + \alpha(x^*)r(x)Y.$$

The number of solutions to the last equation in $(u, v) \in \mathcal{H}_x \times \mathcal{H}_{x^*}$ does not exceed the number of solutions in $(u, v) \in \mathcal{G}^2$. Let $Z = X/Y$. Then, the equation is reduced to

$$\frac{\alpha(x)^2\alpha(x^*)Z - \alpha(x)\alpha(x^*)^2}{\alpha(x)r(x^*)Z - \alpha(x^*)r(x)} = U, \tag{51}$$

where $U = Y^{-2}Z^{-1}$.

Now we are in position to use Conjecture 1.3. The conditions (11) on the coefficients of linear functions in the numerator and in the denominator of the fraction in (51) are satisfied since $\alpha(x) \neq 0$, $\alpha(x^*) \neq 0$, and $r(x) \neq r(x^*)$.

Also, for large p we have $\#\mathcal{G} \leq p^{\varepsilon_0}$ due to (50). By Conjecture 1.3, Eq. (51) has at most A solutions in Z, Y. For each solution, there are at most two possible values of Y. Fixing Y, we determine X. So, the inequality (49) holds.

Denote

$$h = [\sqrt{M/A}] + 1.$$

Due to (41) and (48), we have $\#\mathcal{L}^* \geq h$ provided that p is large enough. We choose h elements $x_1, \dots, x_h$ from $\mathcal{L}^*$. It follows from (49) that for $j = 1, \dots, h$ we have

$$\sum_{i=1}^{j-1} \# \left(\mathcal{Z}\left(x_j\right) \bigcap \mathcal{Z}\left(x_i\right) \right) \leq 2(j-1)A,$$

which implies by (47)

$$\# \left(\mathcal{Z}\left(x_j\right) \setminus \bigcup_{i=1}^{j-1} \mathcal{Z}\left(x_i\right) \right) \geq 2\sqrt{AM} - 2(j-1)A.$$

Observe that

$$\#\left(\bigcup_{j=1}^{h} \mathcal{Z}\left(x_j\right)\right) = \sum_{j=1}^{h} \#\left(\mathcal{Z}\left(x_j\right) \setminus \bigcup_{i=1}^{j-1} \mathcal{Z}\left(x_i\right)\right).$$

Hence,

$$\begin{aligned}\#\left(\bigcup_{j=1}^{h} \mathcal{Z}\left(x_j\right)\right) &> 2\sqrt{AM}h - (h-1)hA \\ &= (2\sqrt{AM} - (h-1)A)h \\ &> (2\sqrt{AM} - \sqrt{AM})\sqrt{M/A} > M,\end{aligned}$$

but this inequality contradicts the definition of M. Together with the choice of B given by (44) and (45), this concludes the proof.

6 Comments

Let $P(n)$ be the largest primitive prime divisor of $2^n - 1$, that is, the largest prime which divides $2^n - 1$, but does not divide any of the numbers $2^d - 1$ for $1 \le d < n$. Note that $P(n) \equiv 1 \pmod{n}$. By a striking result of Stewart [21, Theorem 1.1], we have

$$P(n) \ge n \exp\left(\frac{\log n}{104 \log\log n}\right),$$

provided that n is large enough. It is also natural to assume that $\log P(n)/\log n \to \infty$ for $n \to \infty$. However, for us a weaker assumption is sufficient. Namely, assume that

$$\limsup \frac{\log P(24m)}{\log m} = \infty.$$

We then take $n = 24m$, $m \in \mathbb{N}$, and $p = P(n)$ such that $n = p^{o(1)}$. Then, $p \equiv 1 \pmod{24}$. Since 2 is a quadratic residue modulo p, we can take $\xi \in \mathbb{F}_p$ such that $\xi^2 = 2$. We consider a group $\mathcal{G}$ generated by ξ. Note that $\#\mathcal{G} = 2n = p^{o(1)}$ as $n \to \infty$. The group $\mathcal{G}$ contains an element ζ_4 of order 4 and an element ζ_6 of order 6. It is easy to check that

$$((\pm\zeta_4 \pm 1)/\xi)^8 = 1.$$

Thus,

$$(\pm\zeta_4 \pm 1)^{2n} = \xi^{6n} = 1.$$

Hence, $\pm\zeta_4 \pm 1 \in \mathcal{G}$. Also,

$$(\pm\zeta_6 - 1)^3 = 1.$$

Hence, similarly $\pm\zeta_6 - 1 \in \mathcal{G}$. Consider a set $\mathcal{D}$ consisting of 9 elements

$$\mathcal{D} = \{(p - 1/2), 1, -2, \zeta_4, -\zeta_4, \zeta_4 - 1, -\zeta_4 - 1, \zeta_6 - 1, -\zeta_6 - 1\}.$$

Clearly, $x \in \mathcal{G}, x + 1 \in \mathcal{G}$ for any $x \in \mathcal{D}$. This shows that probably A in Conjecture 1.3 should be at least 9.

We also observe that in Conjecture 1.3 the value of ε_0 cannot be taken greater than 1/2.

Indeed, suppose that p is a prime and $p - 1$ has a divisor $t = p^{\varepsilon_0 + o(1)}$, as $p \to \infty$ with a fixed $\varepsilon_0 > 1/2$ (the infinitude of such primes follows instantly from [10, Theorem 7]).

Let us fix any $\alpha_{1,1}, \alpha_{1,2}, \alpha_{2,1}, \alpha_{2,2} \in \mathbb{F}_p$. Clearly, the Eq. (12) has $N = p + O(1)$ of solutions $(u, v) \in \left(\mathbb{F}_p^*\right)^2$. Let $\mathcal{G} \subseteq \mathbb{F}_p^*$ be a subgroup of order t. Since $\mathbb{F}_p^*$ is the union of $(p - 1)/t$ cosets $a\mathcal{G}$ of $\mathcal{G}$, the direct product $\mathbb{F}_p^* \times \mathbb{F}_p^*$ is the union of $(p - 1)^2/t^2$ products of cosets of $\mathcal{G}$. By the Dirichlet principle is that there is at least one product $a\mathcal{G} \times b\mathcal{G}$ such that the number of solutions $(u, v) \in a\mathcal{G} \times b\mathcal{G}$ (with some $a, b \in \mathbb{F}_p^*$) is not less than

$$\frac{N}{(p - 1)^2/t^2} \geq (1 + o(1))t^2/p \geq p^{2\varepsilon_0 - 1 + o(1)}$$

and hence is not bounded as $p \to \infty$. Changing the variables $\widetilde{u} = a^{-1}u$, $\widetilde{v} = b^{-1}v$ in (12) we obtain another equation of the same type

$$\frac{\alpha_{1,1}ab^{-1}\widetilde{u} - \alpha_{1,2}b^{-1}}{\alpha_{2,1}a\widetilde{u} - \alpha_{2,2}} = \widetilde{v}$$

with an unbounded number of solutions $(\widetilde{u}, \widetilde{v}) \in \mathcal{G}^2$.

Finally, we note that using [5, Theorem 1.2] one concludes that Conjecture 1.3 holds (in much stronger and general form) for a sequence of primes of relative density 1. However, this does not give any new results for the sets $\mathcal{M}_p$ because, as we mentioned, Bourgain, Gamburd, and Sarnak [2, Theorem 2] have already shown that Conjecture 1.1 holds for an overwhelming majority of primes $p \leq X$ as $X \to \infty$.

Acknowledgments The authors are very grateful to William Chen for clarifying discussion concerning his work [6] and to the referee for the careful reading of the manuscript and valuable remarks.

This work was supported by the Australian Research Council Grants DP180100201 and DP200100355 (Shparlinski) and by the Russian Science Foundation Grant 19-11-00001 (Vyugin).

References

1. Baragar, A.: The Markoff equation and equations of Hurwitz. Ph.D. Thesis, Brown University, 1991
2. Bourgain, J., Gamburd, A., Sarnak, P.: Markoff triples and strong approximation. C. R. Acad. Sci. Paris, Ser. I **354**, 131–135 (2016)
3. Bourgain, J., Gamburd, A., Sarnak, P.: Markoff surfaces and strong approximation, I. Preprint (2016). http://arxiv.org/abs/1607.01530
4. Cerbu, A., Gunther, E., Magee, M., Peilen, L.: The cycle structure of a Markoff automorphism over finite fields. J. Number Theory **211**, 1–27 (2020)
5. Chang, M.-C., Kerr, B., Shparlinski, I., Zannier, U.: Elements of large order on varieties over prime finite fields. J. Théor. Nombres Bordeaux **26**, 579–593 (2014)
6. Chen, W.: Nonabelian level structures, Nielsen equivalence, and Markoff triples. Preprint (2020). http://arxiv.org/abs/2011.12940
7. Corvaja, P., Zannier, U.: Greatest common divisors of $u - 1$, $v - 1$ in positive characteristic and rational points on curves over finite fields. J. Eur. Math. Soc. **15**, 1927–1942 (2013)
8. de Courcy-Ireland, M., Lee, S.: Experiments with the Markoff surface. Experimental Math. (2018), (to appear)
9. de Courcy-Ireland, M., Magee, M.: Kesten-McKay law for the Markoff surface mod$p$. Annales Henri Lebesgue (to appear)
10. Ford, K.: The distribution of integers with a divisor in a given interval. Annals Math. **168**, 367–433 (2008)
11. Gamburd, A., Magee, M. and Ronan, R.: An asymptotic formula for integer points on Markoff-Hurwitz varieties. Annals Math., **190**, 751–809 (2019)
12. Garcia, A., Voloch, J.F.: Fermat curves over finite fields. J. Number Theory **30**, 345–356 (1988)
13. Granville, A.: Smooth numbers: Computational number theory and beyond. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, pp. 267–322. Cambridge University Press (2008)
14. Heath-Brown, D.R., Konyagin, S.V.: New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. Quart. J. Math. **51**, 221–235 (2000)
15. Hildebrand, A., Tenenbaum, G.: Integers without large prime factors. J. Théorie des Nombres de Bordeaux **5**, 411–484 (1993)
16. Konyagin, S.V., Makarychev, S.V., Shparlinski, I.E., Vyugin, I.V.: On the structure of graphs of Markoff triples. Quart. J. Math. **71**, 637–648 (2020)
17. Makarychev, S.V., Vyugin, I.V.: Solutions of polynomial equations in subgroups of $\mathbb{F}_p$. Arnold Math J. **5**, 105–121 (2019)
18. Markoff, A.: Sur les formes quadratiques binaires indéfinies. Math. Ann. **15**, 381–409 (1879)
19. Markoff, A.: Sur les formes quadratiques binaires indéfinies. Math. Ann. **17**, 379–399 (1880)
20. Shkredov, I.D., Vyugin, I.V.: On additive shifts of multiplicative subgroups. Mat. Sb. **203**, 81–100 (2012) (in Russian)
21. Stewart, C.L.: On divisors of Lucas and Lehmer numbers. Acta Math. **211**, 291–314 (2013)
22. Tenenbaum, G.: Introduction to analytic and probabilistic number theory. Grad. Studies Math., vol. 163. Amer. Math. Soc. (2015)