ON THE NEW BOUND FOR THE NUMBER OF SOLUTIONS OF POLYNOMIAL EQUATIONS IN SUBGROUPS AND THE STRUCTURE OF GRAPHS OF MARKOFF Triples

SERGEI V. KONYAGIN, SERGEY V. MAKARYCHEV, IGOR E. SHPARLINSKI, AND ILYA V. VYUGIN

Abstract. We sharpen the bounds of J. Bourgain, A. Gamburd and P. Sarnak (2016) on the possible number of nodes outside the "giant component" and on the size of individual connected components in the suitably defined functional graph of Markoff triples modulo \( p \). This is a step towards the conjecture that there are no such nodes at all. These results are based on some new ingredients and in particular on a new bound of the number of solutions of polynomial equations in cosets of multiplicative subgroups in finite fields, which generalises previous results of P. Corvaja and U. Zannier (2013).

1. Introduction

1.1. Background and motivation. We recall that the set \( \mathcal{M} \) of Markoff triples \( (x, y, z) \in \mathbb{N}^3 \) is the set of positive integer solutions to the Diophantine equation

\[
\begin{align*}
  x^2 + y^2 + z^2 &= 3xyz, \\
  (x, y, z) &\in \mathbb{Z}^3.
\end{align*}
\]

One easily verifies 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. It is also obvious that so do permutations \( \Pi \in S_3 \) of the components of \( (x, y, z) \).

By a classical result of Markoff [12, 13] one can get all integer solutions to (1.1) starting from the solution \( (1, 1, 1) \) and then applying the above transformations. More formally, let \( \Gamma \) be the group of transformations generated by \( \mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3 \) and permutations \( \Pi \in S_3 \).

2010 Mathematics Subject Classification. 11D25, 11D79, 11T06.

Key words and phrases. Markoff triple, reduction modulo \( p \), connected graph, giant component.
Then the orbit of $(1, 1, 1)$ under $\Gamma$ contains $\mathcal{M}$. Hence, if one defines a functional graph on Markoff triples, where, starting from the “root” $(1, 1, 1)$, the edges $(x_1, y_1, z_1) \rightarrow (x_2, y_2, z_2)$ are governed by $(x_2, y_2, z_2) = T(x_1, y_1, z_1)$, where
\begin{equation}
T = \{R_1, R_2, R_3\} \cup S_3,
\end{equation}
then 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 and the set of non-zero solutions $\mathcal{M}_p$ to (1.1) considered modulo $p$ can be obtained from the set of Markoff triples $\mathcal{M}$ reduced modulo $p$. This conjecture means that the functional graph $\mathcal{X}_p$ associated with the transformation (1.2) remains connected.

Accordingly, if we define by $\mathcal{C}_p \subseteq \mathcal{M}_p$ the set of the triples in 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, 7]. For example, by [2, Theorem 1] we have
\begin{equation}
\#(\mathcal{M}_p \setminus \mathcal{C}_p) = p^{o(1)}, \quad \text{as } p \to \infty,
\end{equation}
and also by [2, Theorem 2] we know that Conjecture 1.1 holds for all but maybe at most $X^{o(1)}$ primes $p \leq X$ as $X \to \infty$.

Here, in Theorem 1.3 below, we obtain a more precise form of the bound (1.3). This result is based on a new bound, given in Theorem 1.2 below, on the total number of zeros in cosets of multiplicative subgroup of $\mathbb{F}_p$ for several polynomials, which generalises a series of previous estimates of similar type that refer to only one polynomial see [5, 8, 9] or to a system of linear equations [14]. We believe that Theorem 1.2 is of independent interest and may find several other applications.

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 $c(\log p)^{1/3}$ for some absolute constant $c > 0$. This bound is based on proving that any component contains a path of length at least $c(\log p)^{1/3}$. Here we use an additional argument and show that a positive proportion of nodes along this path have “secondary” paths attached to them which are not also sufficiently long. Finally, we show that “many” of the elements of these “secondary” paths, have “tertiary” paths that are long as well. This allows us to improve the exponent 1/3 to 7/9, see Theorem 1.4.
1.2. **New results.** For a bivariate irreducible polynomial

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

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

\[ P^\#(X, Y) = \sum_{i+j=d^\#} a_{ij} X^i Y^j. \]

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

\[ \mathcal{P} = \{ P(\lambda X, \mu Y) \mid \lambda, \mu \in \mathbb{F}_p^\ast \}. \]

Define \( g \) as the greatest common divisor of the following set of differences

\[ g = \gcd\{i_1 + j_1 - i_2 - j_2 : a_{i_1,j_1}a_{i_2,j_2} \neq 0\}. \]

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

We now fix \( h \) polynomials

\[ P_k(X, Y) = P(\lambda_k X, \mu_k Y) \in \mathcal{P}, \quad k = 1, \ldots, h, \]

which are \( G \)-independent.

The following result generalises a series of previous estimates of a similar type, see [5, 8, 9, 14] and references therein.

**Theorem 1.2.** Suppose that \( P \) is irreducible,

\[ \deg_X P = m \quad \text{and} \quad \deg_Y P = n \]

and also that \( P^\#(X, Y) \) 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 \( G \subseteq \mathbb{F}_p \) of order \( t = \#G \) satisfying

\[ \frac{1}{2} p^{3/4} h^{1/4} \geq t \geq \max\{h^2, c_0(m, n)\}, \]

and \( G \)-independent polynomials (1.8) we have

\[ \sum_{i=1}^{h} \# \{ (u, v) \in G^2 : P_i(u, v) = 0 \} < 12mngh^{2/3}t^{2/3}. \]

Using Theorem 1.2 we then derive:

**Theorem 1.3.** We have,

\[ \# (\mathcal{M}_p \setminus \mathcal{C}_p) \leq \exp\left( (\log p)^{1/2+o(1)} \right), \quad \text{as} \ p \to \infty. \]
We also obtain the following improvement of a lower bound from [2, 3] on the size of individual components of $\mathcal{X}_p$.

**Theorem 1.4.** The size of any connected component of $\mathcal{X}_p$ is at least $c(\log p)^{7/9}$, where $c > 0$ is an absolute constant.

2. Solutions to polynomial equations in subgroups of finite fields

2.1. Stepanov’s method. Consider a polynomial $\Phi \in \mathbb{F}_p[X, Y, Z]$ such that

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

that is,

$$\Phi(X, Y, Z) = \sum_{0 \leq a < A} \sum_{0 \leq b < B} \sum_{0 \leq c < C} \omega_{a,b,c} X^a Y^b Z^c. \quad (2.1)$$

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

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

We now fix some $\mathcal{G}$-independent polynomials (1.8) and define the sets

$$\mathcal{F}_i = (\lambda^{-1}_i \mathcal{G} \times \mu^{-1}_i \mathcal{G}), \quad i = 1, \ldots, h, \quad \text{and} \quad \mathcal{E} = \bigcup_{i=1}^{h} \mathcal{F}_i. \quad (2.2)$$

We also consider the locus of singularity

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

**Lemma 2.1.** Let $P(X, Y)$ be an irreducible polynomial of bi-degree $(\deg_X P, \deg_Y P) = (m, n)$ and let $n \geq 1$. Then for the cardinality of the set $\mathcal{M}_{\text{sing}}$ the following holds:

$$\# \mathcal{M}_{\text{sing}} \leq (m + n)^2.$$
**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 $L \leq (m+n)(m+n-1)$, where $L$ is the number of roots of the system

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

Actually, 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

$$(2.3) \quad P(X,Y) = 0$$

where $P$ is given by (1.4), is less than or equal to $\deg_Y P(X,Y) = n$. The total numbers of such pairs is at most $L + m + n \leq (m+n)^2$. □

Assume that the polynomial $\Psi$ and $\mathcal{G}$-independent polynomials (1.8) satisfy the following conditions:

- all pairs in the set $\{(X,Y) \in \mathcal{E} \setminus \mathcal{M}_{\text{sing}} \mid P(X,Y) = 0\}$ are zeros of orders at least $D$ of the function $\Psi(X,Y)$ on the curve (2.3);
- 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 $D^{-1} \deg \Psi \deg P + \# \mathcal{M}_{\text{sing}}$ for the number of roots $(x,y)$ of the system

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

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

$$P_k(X,Y) = 0, \quad (X,Y) \in \mathcal{G}^2,$$

$$\iff P(u,v) = 0, \quad (u,v) = (\lambda_k^{-1}X,\mu_k^{-1}Y) \in \mathcal{F}_k.$$ 

Therefore, we obtain the bound

$$(2.4) \quad N_h \leq \frac{\deg \Psi \cdot \deg P}{D} + \# \mathcal{M}_{\text{sing}}$$

$$\leq \frac{(m+n)(B+C-1)t}{D} + \# \mathcal{M}_{\text{sing}}$$

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

$$N_h = \sum_{k=1}^{h} \# \{(u,v) \in \mathcal{G}^2 : P_k(u,v) = 0\}.$$
For completeness, we present proofs of several results from \cite{11} 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 irreducible polynomial \( Q(X,Y) \mid \Psi(X,Y) \)
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 \( Q^\sharp(X,Y) \), \( \Psi^\sharp(X,Y) \) are defined as in (1.5) and \( e \) is defined as \( g \) in (1.7).

**Proof.** Consider \( \rho \in \mathcal{G} \) and substitute \( X = \rho \tilde{X} \) and \( Y = \rho \tilde{Y} \) in the polynomials \( Q(X,Y) \) and \( \Psi(X,Y) \). Then
\[
Q(X,Y) \mapsto Q_\rho(\tilde{X}, \tilde{Y}) = Q(\rho \tilde{X}, \rho \tilde{Y}),
\]
and
\[
\Psi(X,Y) = \Psi(\rho \tilde{X}, \rho \tilde{Y}) = (\rho \tilde{Y})^t \Phi((\rho \tilde{X})/(\rho \tilde{Y}), (\rho \tilde{X})^t, (\rho \tilde{Y})^t) = \Psi(\tilde{X}, \tilde{Y}),
\]
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.

Clearly, there exist at least \( s = \lfloor t/e \rfloor \) elements \( \rho_1, \ldots, \rho_s \in \mathcal{G} \) such that
\[
(2.5) \quad Q_{\rho_i}(X,Y)/Q_{\rho_j}(X,Y) \notin \mathbb{F}_p, \quad 1 \leq i < j \leq s.
\]
Obviously the polynomials \( Q_{\rho_1}(X,Y), \ldots, Q_{\rho_s}(X,Y) \) are pairwise relatively prime, because they are irreducible and satisfy (2.5). Polynomials \( Q^\sharp_{\rho_i}(X,Y) \) are homogeneous of degree \( d^2 \) and the following holds
\[
\rho_1^{-d^2} Q^\sharp_{\rho_1}(X,Y) = \ldots = \rho_s^{-d^2} Q^\sharp_{\rho_s}(X,Y).
\]
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
\[
Q^\sharp_{\rho_1}(X,Y) \cdot \ldots \cdot Q^\sharp_{\rho_s}(X,Y) = (\rho_1 \cdot \ldots \cdot \rho_s)^d Q^\sharp(X,Y)^s
\]
we obtain the desired result. \Box

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 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. Let us put \( y = 1 \). 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 [9, Lemma 6] that such a polynomial \( H(X, 1) \) cannot have a nonzero root of order \( s \) and the result follows. \Box

Since the number of monomials of \( \Psi^\#(X, Y) \) does not exceed \( AB \) and we can combine Lemmas 2.3 and 2.2 (applied to irreducible divisors of polynomials \( P_k \)).

Lemma 2.4. If \( AB < t/g \) then for polynomial (1.4) we have

\[ P(X, Y) \nmid \Psi(X, Y). \]

2.3. Derivatives on some curves. There we study derivatives on the algebraic curve and define some special differential operators. Thought this section we use

\[ \frac{\partial}{\partial X}, \quad \frac{\partial}{\partial Y} \quad \text{and} \quad \frac{d}{dX} \]

for standard partial derivatives with respect to \( X \) and \( Y \) and for a derivative with respect to \( X \) along the curve (2.3). In particular

\[ \frac{d}{dX} = \frac{\partial}{\partial X} + \frac{dY}{dX} \frac{\partial}{\partial Y}, \quad (2.6) \]

where by the implicit function theorem from the equation (2.3) 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 (2.3).

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

\[ q_1(X, Y) = -\frac{\partial}{\partial X} P(X, Y), \quad r_1(X, Y) = \frac{\partial}{\partial Y} P(X, Y), \]
and
\[ q_{k+1}(X, Y) = \frac{\partial q_k}{\partial X} \left( \frac{\partial P}{\partial Y} \right)^2 - \frac{\partial q_k}{\partial Y} \frac{\partial P}{\partial X} \frac{\partial P}{\partial Y} - (2k - 1)q_k(X, Y) \frac{\partial^2 P}{\partial X \partial Y} \frac{\partial P}{\partial Y} + (2k - 1)q_k(X, Y) \frac{\partial^2 P}{\partial Y^2} \frac{\partial P}{\partial X}, \]
\[ r_{k+1}(X, Y) = r_k(X, Y) \left( \frac{\partial P}{\partial Y} \right)^2 = \left( \frac{\partial P}{\partial Y} \right)^{2k+1}. \]

We now show by induction that
\[ \frac{d^k}{dX^k} Y = \frac{q_k(X, Y)}{r_k(X, Y)}, \quad k \in \mathbb{N}. \]

The base of induction is
\[ \frac{d}{dX} Y = -\frac{\partial}{\partial X} \frac{P(X, Y)}{r_1(X, Y)} = \frac{q_1(X, Y)}{r_1(X, Y)}. \]

One can now easily verifies that assuming (2.8) and (2.6) 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 (2.7), which concludes the induction and proves the formula (2.8).

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 (2.3), 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
\[ \deg_X q_k \leq (2k - 1)m - k, \quad \deg_Y q_k \leq (2k - 1)n - 2k + 2, \]
\[ \deg_X r_k \leq (2k - 1)m, \quad \deg_Y r_k \leq (2k - 1)(n - 1). \]

**Proof.** Direct calculations show that
\[ \deg_X q_1 \leq m - 1 \quad \text{and} \quad \deg_Y q_1 \leq n, \]
and using (2.7) (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. \( \Box \)

**Lemma 2.6.** Let \( Q(X,Y) \in \mathbb{F}_p[X,Y] \) be a polynomial such that
\[
\deg_X Q(X,Y) \leq \mu, \quad \deg_Y Q(X,Y) \leq \nu,
\]
and \( P(X,Y) \in \mathbb{F}_p[X,Y] \) be a polynomial such that
\[
\deg_X P(X,Y) \leq m, \quad \deg_Y P(X,Y) \leq n.
\]
Then the divisibility condition
\[
P(X,Y) \mid Q(X,Y)
\]
on the coefficients of the polynomial \( Q(X,Y) \) is equivalent to a certain system of \( n((\nu - n + 2)m + \mu) \leq (\mu + \nu + 1)mn \) 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 (2.9) is equal to \( (\mu + 1)(\nu + 1) \). Let us call the vector subspace of polynomials \( Q(X,Y) \) that satisfy (2.9) and (2.10) by \( \tilde{\mathcal{L}} \). Because \( Q(X,Y) = P(X,Y)R(X,Y) \) where the polynomial \( R(X,Y) \) is such that
\[
\deg_X R(X,Y) \leq \mu - m \quad \text{and} \quad \deg_Y R(X,Y) \leq \nu - n,
\]
then the vector space \( \tilde{\mathcal{L}} \) isomorphic to the vector space of the coefficients of the polynomials \( R(x,y) \) satisfying (2.11). The dimension of the vector space \( \tilde{\mathcal{L}} \) is equal to
\[
\dim \tilde{\mathcal{L}} = (\mu - m + 1)(\nu - n + 1).
\]
It means that the subspace \( \tilde{\mathcal{L}} \) of the space \( \mathcal{L} \) is given by a system of
\[
(\mu + 1)(\nu + 1) - (\mu - m + 1)(\nu - n + 1)
= \mu n + \nu m - mn + m + n + 1 \leq (\mu + \nu + 1)mn
\]
homogeneous linear algebraic equations. \( \Box \)

As in [11], we now consider the differential operators:

\[
D_k = \left( \frac{\partial P}{\partial Y} \right)^{2k-1} X^k Y^k \frac{d^k}{dX^k}, \quad k \in \mathbb{N},
\]
where, as before, \( \frac{d^k}{dX^k} \) denotes the \( k \)-th derivative on the algebraic curve (2.3) 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 (2.8) for derivatives on the algebraic curve (2.3) we obtain by induction the following relations

\[
D_k \left( \frac{X}{Y} \right)^a X^{bt} Y^{(c+1)t} = R_{k,a,b,c}(X,Y) \left( \frac{X}{Y} \right)^a X^{bt} Y^{(c+1)t},
\]

(2.13)

\[
D_k \Psi(X,Y)|_{x,y \in \mathcal{F}} = R_{k,i}(X,Y)|_{x,y \in \mathcal{F}_i},
\]

where \( \mathcal{F}_i \) from formula (2.2),

\[
R_{k,i}(X,Y) = \sum_{0 \leq a < A} \sum_{0 \leq b < B} \sum_{0 \leq c < C} \omega_{a,b,c} R_{k,a,b,c}(X,Y) \left( \frac{X}{Y} \right)^a \lambda_i^{bt} \mu_i^{(c+1)t}, \tag{2.14}
\]

for some coefficients \( \omega_{a,b,c} \in \mathbb{F}_p, a < A, b < B, c < C, \) and \( \lambda_i, \mu_i \) from (2.2).

We now define

\[
\tilde{R}_{k,i}(X,Y) = Y^{A-1} R_{k,i}(X,Y). \tag{2.15}
\]

**Lemma 2.7.** The rational functions \( R_{k,a,b,c}(X,Y) \) and \( \tilde{R}_{k,i}(X,Y) \), given by (2.13) and (2.15), are polynomials of degrees

\[
\deg_X R_{k,a,b,c} \leq 4km, \quad \deg_Y R_{k,a,b,c} \leq 4kn,
\]

and

\[
\deg_X \tilde{R}_{k,i} \leq A + 4km, \quad \deg_Y \tilde{R}_{k,i} \leq A + 4kn.
\]

**Proof.** We have

\[
\frac{d^k}{dX^k} X^{a+bt} Y^{(c+1)t-a} = \sum_{(\ell_1, \ldots, \ell_s)} C_{\ell_1, \ldots, \ell_s} X^{a+bt-k+\sum_{i=1}^s \ell_i} Y^{(c+1)t-a-s} \left( \frac{d^\ell_1 Y}{dX^{\ell_1}} \right) \cdots \left( \frac{d^\ell_s Y}{dX^{\ell_s}} \right), \tag{2.16}
\]

where \( (\ell_1, \ldots, \ell_s) \) runs through the all \( s \)-tuples of positive integers with \( \ell_1 + \ldots + \ell_s \leq k, s = 0, \ldots, k \) and \( C_{\ell_1, \ldots, \ell_s} \) are some constant coefficients.
By the formula (2.16) and the form of the operator (2.12) 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 (2.16) and (2.8) 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 $(\frac{\partial P}{\partial Y}(X,Y))^{2k-1}$. We obtain that $R_{k,a,b,c}(X,Y)$ are polynomials. From the formula (2.14) we obtain that $R_{k,i}$ is a rational function with denominator divided by $Y^{A-1}$. Consequently, $\tilde{R}_{k,i}$ are polynomials.

The result now follows from Lemma 2.5 and the formulas (2.12) and (2.13). \qed

2.4. Multiplicities points on some curves.

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 (2.3);
- or $(x,y) \in M_{\text{sing}}$.

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

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

where, as before, $\frac{d^j}{dX^j}$ is $j$-th derivative on the algebraic curve (2.3) with the local parameter $X$, or

$$
xy = 0,
$$

or

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

on the curve (2.3).

If we have (2.17) 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 (2.18) or (2.19) on the curve (2.3) then the pair $(x,y)$ satisfies the second case of conditions of Lemma 2.8. \qed
3. Multiplicative orders and divisors

3.1. Multiplicative orders and binary recurrences. For $x \in \mathbb{F}_p^*$ we define

\begin{equation}
(3.1) \quad t(x) = \text{ord} \xi
\end{equation}

as the order of $\xi \in \mathbb{F}_p^*$ which satisfies the equation $3x = \xi + \xi^{-1}$ (it is easy to see that this is correctly defined and does not depend on the particular choice of $\xi$).

Throughout the paper, as usual, we use the expressions $F \ll G$, $G \gg F$ and $F = O(G)$ to mean that $|F| \leq cG$ for some constant $c > 0$.

**Lemma 3.1.** For any nonzero triple $(x, y, z) \in \mathbb{M}_p$, we have

$$t(x)t(y)t(z) \gg \log p.$$ 

**Proof.** As in [2, 3] we note that the inequality between the arithmetic and geometric means implies that the equation (1.1), considered over $\mathbb{C}$ has no non-zero solution $(x, y, z)$ where

$$3x = \xi + \xi^{-1}, \quad 3y = \zeta + \zeta^{-1}, \quad 3z = \eta + \eta^{-1}$$

with the roots of unity $\xi, \zeta, \eta$ (or more generally with any $|\xi| = |\zeta| = |\eta| = 1$).

Thus if we denote by $\Phi_k$ the $k$th cyclotomic polynomial, and also define

$$F(U, V, W) = (U + U^{-1})^2 + (V + V^{-1})^2 + (W + W^{-1})^2 - (U + U^{-1})(V + V^{-1})(W + W^{-1})$$

then for any positive integers $r, s, t$, the system of polynomials equations

$$U^2V^2W^2F(U, V, W) = \Phi_r(U) = \Phi_s(V) = \Phi_t(W) = 0$$

has no solutions (unless $r = s = t = 4$). Using the effective Hilbert’s Nullstellensatz in the form given by D’Andrea, Krick and Sombra [6, Theorem 1] we see that for some polynomials $g_i(U, V, W) \in \mathbb{Z}[U, V, W]$, $i = 1, \ldots, 4$ we have

$$U^2V^2W^2F(U, V, W)g_1(U, V, W) + \Phi_r(U)g_2(U, V, W) + \Phi_s(V)g_3(U, V, W) + \Phi_t(W)g_4(U, V, W) = A$$

with some positive integer $A$ with $\log A \ll rst$. This immediately implies the result. $\Box$
We also use the following result which follows immediately from the explicit form of solutions to binary recurrence equations and a result [5, Theorem 2].

Lemma 3.2. For two distinct elements \( x_1, x_2 \in \mathbb{F}_p \) we consider the binary recurrence sequences

\[
  u_{i,n+2} = 3x_i u_{i,n+1} - u_{i,n}, \quad n = 1, 2, \ldots,
\]

with nonzero initial values, \((u_{i,1}, u_{i,2}) \in \mathbb{F}_p, i = 1, 2\). Then

\[
  \# \left( \{u_{1,1}, \ldots, u_{1,t(x_1)}\} \cap \{u_{2,1}, \ldots, u_{2,t(x_2)}\} \right) \lesssim \frac{t(x_1)t(x_2)}{p} + (t(x_1)t(x_2))^{1/3}.
\]

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 integer positive divisors \( d \mid n \) with \( d \leq z \). 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 3.3. For any fixed real positive \( \gamma < 1 \), if \( z \geq \exp\left((\log n)^{\gamma+o(1)}\right) \) then

\[
  \tau_z(n) \leq z^{1-\gamma+o(1)}
\]
as \( n \to \infty \).

Proof. 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 that are up to \( x \). Let \( s \) be the number of all distinct prime divisors of \( n \) and let \( p_1, \ldots, p_s \) be the first \( s \) primes. We note that

\[
  \tau_z(n) \leq \psi(z, p_s).
\]

By the prime number theorem we have \( n \geq p_1 \ldots p_s = \exp(s + o(s)) \) and thus

\[
  p_s \ll s \log s \leq (\log n)^{1+o(1)} \leq (\log z)^{1/\gamma+o(1)}.
\]

We now recall that for any fixed \( \alpha > 1 \) we have

\[
  \Psi(x, (\log x)^{\alpha}) = x^{1-1/\alpha+o(1)}
\]
as \( x \to \infty \), see, for example, [10, Equation (1.14)]. Combining this with (3.2) and (3.3) we conclude the proof. \( \square \)
4. Proofs of main results

4.1. Proof of Theorem 1.2. We define the following parameters:

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

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

\[ D_k \Psi(x, y) = 0, \quad (x, y) \in \bigcup_{i=1}^{h} F_i, \]

with the operators (2.12), where the sets \( F_i \) are as in (2.2), is given by the 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 (4.1) for some \( k \) we have to make sure that the polynomials \( \tilde{R}_{k,i}(X,Y) \), \( i = 1, \ldots, h \), given by (2.15), vanish identically on the curve (2.3). The bi-degree of \( \tilde{R}_{k,i}(X,Y) \) is given by Lemma 2.7:

\[ \deg_X \tilde{R}_{k,i} \leq A + 4km, \quad \deg_Y \tilde{R}_{k,i} \leq A + 4kn. \]

The number of equations on the coefficients that give us the vanishing of polynomial \( \tilde{R}_{k,i}(X,Y) \) on the curve (2.3) is given by Lemma 2.6 and is equal to \((\mu + \nu + 1)mn\), where \( \mu, \nu \) are as Lemma 2.6 and

\[ \mu \leq A + 4km, \quad \nu \leq A + 4kn. \]

Finally, the condition (4.1) for some \( k \) is given by \( h(\mu + \nu + 1)mn \leq mnh(2A + 4k(m + n)) \) linear algebraic homogeneous equations. Consequently, the condition (4.1) 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 \( \kappa_{a,b,c} \). Now it is easy to see that

\[ L = h ((2A + 1)Dmn + 2nm(m + n)D(D - 1)) \leq 2hADmn + 2hmn(m + n)D^2 = 2hmn(AD + (m + n)D^2). \]

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

\[ 2hmn(AD + (m + n)D^2) < ABC, \]
as we have $ABC$ variables. It is easy to get an upper bound for the left hand side of (4.2). For sufficiently large $t > c_0(m, n)$, where $c_0(m, n)$ is some constant depending only on $m$ and $n$, we have

$$2hmn(AD + (m + n)D^2) < 2hmn\left(\frac{h^{-1/3}t^{2/3}}{g} + (m + n)\frac{h^{-2/3}t^{4/3}}{16m^2n^2g^2}\right)$$

$$< \frac{3h^{1/3}t^{4/3}}{4g^2}.$$  (4.3)

On the other hand, assuming that $c_0(m, n)$ is large enough, we obtain

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

which together with (4.3) implies (4.2).

It is clearly that

$$gAB \leq t.$$  

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

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

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 2.1 and 2.8 and the inequality (2.4) we obtain that $N_h$ satisfies the inequality

$$N_h \leq \#M_{\text{sing}} + (m + n)\frac{(B + C - 1)t}{D}$$

$$< (m + n)^2 + \frac{2h^{1/3}t^{4/3}}{[h^{-1/3}t^{2/3}/(4mng)]} < 12mngh^{2/3}t^{2/3}$$

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

### 4.2. Proof of Theorem 1.3.

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 $\Gamma$ 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

$$u_{n+2} = 3xu_{n+1} - u_n, \quad n = 1, 2, \ldots,$$

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 $\xi, \xi^{-1} \in \mathbb{F}_p^*$ be the roots of the characteristic polynomial $Z^2 - 3xZ + 1$ of the recurrence relation (4.4). 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 $\xi$ in $\mathbb{F}_p^*$ as given by (3.1).

We now fix some $\varepsilon > 0$ and denote

$$M_0 = \exp((\log p)^{1/2+\varepsilon}), \quad M_1 = M_0^{1/6}/2 > \exp((\log p)^{1/2+\varepsilon/2}).$$

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 $\Pi(x, y, z) \in \mathcal{R}$ for every $\Pi \in S_3$. Therefore, there are more that $M_0^{1/3}$ 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 $\xi \in \mathbb{F}_p^*$ of order at most $T$ we conclude that there is a triple $(x^*, y^*, z^*) \in \mathcal{R}$ with

$$t(x^*) > \sqrt{M_0^{1/3}} = 2M_1.$$

Then the orbit $\Gamma(x^*, y^*, z^*)$ of this triple has at least $2M_1$ elements. Let $M$ be the cardinality of the set $\mathcal{M}$ 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

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

where the sequence $u_n$ is defined as in (4.4) with respect to $(x^*, y^*, z^*)$, produce the same projection no more than twice we obtain

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

Recalling (4.5), we obtain

$$M \geq M_1 > \exp((\log p)^{1/2+\varepsilon/2}).$$

We also notice, that by the bound (1.3) we also have

$$M = p^{\alpha(1)}.$$
By Lemma 3.3, applied with $\gamma = 1/2 + \varepsilon/2$ and the inequalities (4.7) we have

$$\sum_{t \leq M^{2/3+\varepsilon/3}/5} t \leq M^{2/3+\varepsilon/5} \tau_{M^{2/3+\varepsilon/5}}(p^2 - 1)$$

$$= M^{2/3+\varepsilon/5} M^{(2/3+\varepsilon/5)(1/2-\varepsilon/2)+o(1)}$$

$$= M^{1-\varepsilon/30-\varepsilon^2/10+o(1)} = o(M).$$

For $t \mid p^2 - 1$ we denote $g(t)$ the number of $x \in \mathcal{M}$ with $t(x) = t$. Since

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

and $g(t) < t$ for any $t$, we conclude that

$$\sum_{t > M^{2/3+\varepsilon/3}/5} g(t) = M + o(M)$$

Next, the same argument as used in the bound (4.6) implies that $g(t) = 0$ for $t > 2M$. Applying Lemma 3.3 and the inequalities (4.7) again we see that for some integer $t_0 \mid p^2 - 1$ with

$$2M \geq t_0 > M^{2/3+\varepsilon/3}$$

we have

$$g(t_0) \geq \frac{1}{\tau_{2M}(p^2 - 1)} \sum_{t > M^{2/3+\varepsilon/3}/5} g(t)$$

$$\geq \frac{M + o(M)}{\tau_{2M}(p^2 - 1)} \geq M^{1/2+\varepsilon/2+o(1)} \geq M^{1/2+\varepsilon/3},$$

provided that $p$ is large enough.

Let $\mathcal{L}$ be the set of $x \in \mathcal{M}$ with $t(x) = t_0$ thus

$$\# \mathcal{L} = g(t_0).$$

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 (4.4) and of period $t(x) = t_0$, so we consider the set

$$Z(x) = \{u_n : n = 1, \ldots, t_0\}$$

Let $\mathcal{H}$ be the subgroup of $\mathbb{F}_p^*$ of order $t_0$, 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
\[ Z(x) = \left\{ \alpha(x)u + \frac{r(x)}{\alpha(x)u} : u \in \mathcal{H} \right\}, \]
where
\[ r(x) = \frac{(\xi(x)^2 + 1)^2}{9(\xi(x)^2 - 1)^2}, \]
and \( \alpha(x) \in \mathbb{F}_p^* \). If \( \xi = \xi_0 \) 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 at most two values whose sum is 0. Since every value is taken at most twice among the elements of the sequence \( u_n, n = 1, \ldots, t_0 \), we have
\[ \#Z(x) \geq \frac{1}{2}t_0. \]

If we have \( x_1, x_2 \in \mathcal{L} \) with \( x_1 \neq \pm x_2 \) (the last condition guarantees that the orbits \( Z(x_1) \) and \( Z(x_2) \) do not coincide), then \( \#(Z(x_1) \cap Z(x_2)) \) is the number of solutions of the equation
\[ \alpha(x_1)u + \frac{r(x_1)}{\alpha(x_1)u} = \alpha(x_2)v + \frac{r(x_2)}{\alpha(x_2)v} \quad u, v \in \mathcal{H}, \]
or, equivalently,
\[ P_{x_1, x_2}(u, v) = 0, \quad u, v \in \mathcal{H}, \]
where
\[ P_{x_1, x_2}(X, Y) = \alpha(x_1)^2\alpha(x_2)X^2Y - \alpha(x_1)\alpha(x_2)^2XY^2 - \alpha(x_1)r(x_2)X + \alpha(x_2)r(x_1)Y. \]

We now use Theorem 1.2 to estimate the size of these intersections, for different choices of pairs \( (x_1, x_2), (x_1, x_3) \in \mathcal{L}^2 \) (sharing the first component). For this, we need to show that for \( x_1, x_2, x_3 \in \mathcal{L} \) with \( x_1 \neq \pm x_2, x_1 \neq \pm x_3 \) and \( x_2 \neq x_3 \), the polynomials \( P_{x_1, x_2} \) and \( P_{x_1, x_3} \) are \( \mathcal{H} \)-independent. Indeed, assume that
\[ P_{x_1, x_2}(X, Y) = \gamma P_{x_1, x_3}(uX, vY). \]
We then derive
\[ \alpha(x_1)X + \frac{r(x_1)}{\alpha(x_1)X} - \alpha(x_2)Y + \frac{r(x_2)}{\alpha(x_2)Y} \]
\[ = \gamma \left( \alpha(x_1)uX + \frac{r(x_1)}{\alpha(x_1)uX} - \alpha(x_3)vY + \frac{r(x_3)}{\alpha(x_3)vY} \right). \]
Hence, we have \((\gamma, u) = (\pm 1, \pm 1)\), and in fact we can assume that \(\gamma = u = 1\). Then we obtain \(\alpha(x_2)/\alpha(x_3) = v/u \in \mathcal{H}\). However this means that \(\mathcal{Z}(x_2) = \mathcal{Z}(x_3)\), which by Lemma 3.2 contradicts our choice of \(x_2\) and \(x_3\).

Now we consider \(x_1, \ldots, x_h \in \mathcal{L}\) with \(x_i \neq \pm x_j\) for \(1 \leq i < j \leq h\). We take \(h = \lfloor c_0 t_0^{1/2} \rfloor\) for an appropriate small \(c_0 > 0\). We can do it due to (4.10) and (4.11). We now recall Theorem 1.2, which applies due to the upper and lower bounds (4.6), (4.8) and (4.9). Hence, for an appropriate choice of \(c_0\), we conclude that for \(i = 1, \ldots, h\) we have

\[
\# \left( \mathcal{Z}(x_i) \setminus \bigcup_{j=1}^{i-1} \mathcal{Z}(x_j) \right) \geq \frac{1}{2} \# \mathcal{Z}(x_i) \geq t_0/4.
\]

Therefore,

\[
\# \bigcup_{i=1}^{h} \mathcal{Z}(x_i) \geq t_0 h/4 \gg t_0^{3/2}
\]

and thus, by (4.9), we have

\[
\# \bigcup_{i=1}^{h} \mathcal{Z}(x_i) > M
\]

provided that \(t\) is large enough. This contradicts the choice of \(M\).

### 4.3. Proof of Theorem 1.4

We assume that consider that \(p\) is large enough and fix a connected component \(C\) of \(\mathcal{M}_p\).

Let \(\mathcal{X}\) be the set of \(x \in \mathbb{F}_p\) such that \((x, y, z) \in C\) for some \(y, z\). If \(t(x) > (\log p)^{7/9}\) for some \(x \in \mathcal{X}\), then \(C\) contains at least \(t(x)\) triples \((x, y, z)\) and the desired result easily follows. Thus, we assume that \(t(x) \leq (\log p)^{7/9}\) for all \(x \in \mathcal{X}\). In particular, for \(x_1, x_2 \in \mathcal{X}\) the bound of Lemma 3.2 becomes \(O\left( (t(x_1)t(x_2))^{1/3} \right)\).

We consider first the case where there exists \(x_0 \in \mathcal{X}\) such that (4.12)

\[
(\log p)^{0.15} \leq t(x_0) \leq (\log p)^{1/3}
\]

(one can see from the argument below that the exponent 0.15 can be replaced by any constant in the open interval \((1/7, 1/6)\)).

With every \(x_0\) satisfying (4.12), we associate the \(t(x_0)\)-periodic sequence \(\{u_j\}\) as in (4.4). By Lemma 3.1 for any \(j = 1, 2, \ldots\) we have

\[
\max\{t(u_j), t(u_{j+1})\} \geq \sqrt[3]{t(u_j)t(u_{j+1})} \gg (\log p)^{1/2} t(x_0)^{-1/2}.
\]
Hence, if we define
\[ \vartheta(x_0) = c(\log p)^{1/2} t(x_0)^{-1/2} \gg (\log p)^{1/3} \]
for an appropriate constant \( c > 0 \), then for any \( j = 1, 2, \ldots \) we have
\[ \max\{t(u_j), t(u_{j+1})\} \geq \vartheta(x_0). \]
Therefore, there are at least \( t(x_0)/2 \) values \( j, 1 \leq j \leq t(x_0) \), such that \( t(u_j) \geq \vartheta(x_0) \). Since there are at most two \( j \) with the same \( t(u_j) \), there is a set \( \mathcal{Y}(x_0) \) \( \subset \{u_1, \ldots, u_{t(x_0)}\} \) with \( \#\mathcal{Y}(x_0) \geq t(x_0)/4 \) and \( t(y) \geq \vartheta(x_0) \) for \( y \in \mathcal{Y}(x_0) \).

We say that \( y \) is associated with \( x \) if \((x, y, z) \in \mathcal{C}\) for some \( z \). By our construction, all elements of \( \mathcal{Y}(x_0) \) are associated with \( x_0 \).

Let
\[ s = \left\lfloor c_0(\vartheta(x_0))^{1/3} \right\rfloor \]
where \( c_0 \) is a small positive constant. By the first inequality from (4.12) we have \( s \leq t(x_0)/4 \) (provided \( c_0 \) is small enough). Hence we can choose elements \( y_1, \ldots, y_s \in \mathcal{Y}(x_0) \). We order them so that
\[ t(y_1) \leq \ldots \leq t(y_s). \]

For \( i = 1, \ldots, s \), there is a set \( \mathcal{Z}(y_i) \) of elements associated with \( y_i \) such that \( \#\mathcal{Z}(y_i) \geq t(y_i)/4 \) and
\[ t(z) \gg (\log p)^{1/2} t(y_i)^{-1/2} \]
for \( z \in \mathcal{Z}(y_i) \).

Now we use that due to Lemma 3.2 for any \( 1 \leq j < i \leq s \) we have
\[ \#(\mathcal{Z}(y_i) \cap \mathcal{Z}(y_j)) \ll (t(y_i) t(y_j))^{1/3} \ll t(x_i) \vartheta(x_0)^{-1/3}. \]
Taking into account the choice of \( s \) we conclude that
\[ \sum_{j < i} \#(\mathcal{Z}(y_i) \cap \mathcal{Z}(y_j)) \leq \frac{1}{2} \mathcal{Z}(y_i), \]
provided that \( c_0 \) is small enough. Hence, there are subsets \( \mathcal{W}(y_i) \subseteq \mathcal{Z}(y_i) \) such that
\[ \#\mathcal{W}(y_i) \geq \frac{1}{2} \#\mathcal{Z}(y_i) \geq t(y_i)/8 \]
which are pairwise disjoined, that is
\[ \mathcal{W}(y_i) \cap \mathcal{W}(y_j) = \emptyset, \quad 1 \leq j < i \leq s. \]

For any \( i = 1, \ldots, s \) and \( z \in \mathcal{W}(y_i) \) we have \( t(z) \) triples \((x, y, z)\) from \( \mathcal{C} \). Summing up the bound (4.13) over \( z \in \mathcal{W}(y_i) \) we get
\[ \sum_{z \in \mathcal{W}(y_i)} t(z) \gg (\log p)^{1/2} (t(y_i)^{1/2}) \geq (\log p)^{1/2} \vartheta(x_0)^{1/2} \]
triples from $C$. So,
\[
\#C \gg s(\log p)^{1/2} \vartheta(x_0)^{1/2} \gg (\log p)^{1/2} \vartheta(x_0)^{5/6} \gg (\log p)^{7/9}
\]
as required.

Now we consider the case where no element $x_0 \in X$ satisfies (4.12). By Lemma 3.1 there exists $x_1 \in X$ with $t(x_1) \gg (\log p)^{1/3}$. There are at least $t(x_1)/2$ elements $y \in X$ associated with $x_1$. Among them there are at most $(\log p)^{0.3}$ elements $y$ with $t(y) < (\log p)^{0.15}$. Hence, there is a set $\mathcal{Y}(x_1)$ of elements associated with $x_1$ such that $\#\mathcal{Y}(x_1) \geq t(x_1)/3 \gg (\log p)^{1/3}$ and $t(y) > (\log p)^{1/3}$ for any $y \in \mathcal{Y}(x_1)$. We now define
\[
s = \left\lfloor c_1(\log p)^{1/9} \right\rfloor,
\]
where $c_1$ is a small positive constant, and take elements $y_1, \ldots, y_s$ from $\mathcal{Y}(x_1)$. The same argument as in the first case shows again that
\[
\#C \gg s(\log p)^{2/3} \gg (\log p)^{7/9}.
\]
This completes the proof.

**Acknowledgement**

The authors would like to thank Peter Sarnak for the encouragement and useful comments.

This work was supported by the Program of the Presidium of the Russian Academy of Sciences no.01 “Fundamental Mathematics and its Applications”, Grant PRAS-18-01 (Konyagin), by the Russian Fund of Fundamental Research, Grants RFBR 17-01-00515 (Makarychev and Vyugin), and RFBR-CNRS 16-51-150005 (Vyugin), the Australian Research Council, Grant DP170100786 (Shparlinski) and by the Simons-IUM fellowship (Vyugin).

**References**

[1] A. Baragar, The Markoff equation and equations of Hurwitz, Ph.D. Thesis, Brown University, 1991. (p. 2)

[2] J. Bourgain, A. Gamburd and P. Sarnak, ‘Markoff triples and strong approximation’, *C. R. Acad. Sci. Paris, Ser. I*, 354 (2016), 131–135. (pp. 2, 4, and 12)

[3] J. Bourgain, A. Gamburd and P. Sarnak, ‘Markoff surfaces and strong approximation, I’, Preprint, 2016, [http://arxiv.org/abs/1607.01530](http://arxiv.org/abs/1607.01530). (pp. 2, 4, and 12)

[4] A. Cerbu, E. Gunther, M. Magee and L. Peilen, ‘The cycle structure of a Markoff automorphism over finite fields’, Preprint, 2016, (see [http://arxiv.org/abs/1610.07077](http://arxiv.org/abs/1610.07077)). (p. 2)
[5] P. Corvaja and U. Zannier, ‘Greatest common divisors of $u - 1, v - 1$ in positive characteristic and rational points on curves over finite fields’, J. Eur. Math. Soc., 15 (2013), 1927–1942. (pp. 2, 3, and 13)

[6] C. D’Andrea, T. Krick and M. Sombra, ‘Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze’, Ann. Sci. Éc. Norm. Supér. 46 (2013), 549–627. (p. 12)

[7] A. Gamburd, M. Magee and R. Ronan ‘An asymptotic for Markoff-Hurwitz tuples’, Preprint, 2016, (see http://arxiv.org/abs/1603.06267. (p. 2)

[8] A. Garcia and J. F. Voloch, ‘Fermat curves over finite fields’, J. Number Theory, 30 (1988), 345–356. (pp. 2 and 3)

[9] D. R. Heath-Brown and S. V. Konyagin, ‘New bounds for Gauss sums derived from $k$th powers, and for Heilbronn’s exponential sum’, Quart. J. Math., 51 (2000), 221–235. (pp. 2, 3, and 7)

[10] A. Hildebran and G. Tenenbaum, ‘Integers without large prime factors’, J. Théorie des Nombres de Bordeaux, 5 (1993), 411–484. (p. 13)

[11] S. Makarychev and I. Vyugin, ‘Solutions of polynomial equation over $\mathbb{F}_p$ and new bounds of additive energy’, Preprint, 2016, (see http://arxiv.org/abs/1504.01354). (pp. 6 and 9)

[12] A. Markoff, ‘Sur les formes quadratiques binaires indéfinies’, Math. Ann., 15 (1879), 381–409. (p. 1)

[13] A. Markoff, ‘Sur les formes quadratiques binaires indéfinies’, Math. Ann., 17 (1880), 379–399. (p. 1)

[14] I. D. Shkredov and I. V. Vyugin, ‘On additive shifts of multiplicative subgroups’, Mat. Sb., 203 (2012), 81–100 (in Russian). (pp. 2 and 3)

Steklov Mathematical Institute, 8, Gubkin Street, Moscow, 119991, Russia

E-mail address: konyagin@mi.ras.ru

Skolkovo Institute of Science and Technology, Skolkovo Innovation Center, Building 3, Moscow, 143026, Russia

E-mail address: svmakarychev@yandex.ru

Department of Pure Mathematics, University of New South Wales, 2052 NSW, Australia.

E-mail address: igor.shparlinski@unsw.edu.au

Institute for Information Transmission Problems RAS, 19, Bolshoy Karetny per., Moscow, 127051, Russia, and, Department of Mathematics, Higher School of Economics, 6, Usacheva Street, Moscow, 119048, Russia.

E-mail address: vyugin@gmail.com