



Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

A note on the two variable Artin's conjecture [☆]S.G. Hazra ^a, M. Ram Murty ^{b,*}, J. Sivaraman ^c^a Chennai Mathematical Institute, H1, SIPCOT IT Park, Siruseri, Kelambakkam, 603103, India^b Department of Mathematics, Jeffery Hall, 99 University Avenue, Queen's University, Kingston, Ontario, K7L 3N6, Canada^c School of Mathematics, Indian Institute of Science Education and Research (IISER), Maruthamala P.O., Vithura, Thiruvananthapuram, Kerala 695551, India

ARTICLE INFO

Article history:

Received 19 September 2023

Received in revised form 1 March 2024

Accepted 1 March 2024

Available online 23 April 2024

Communicated by S.J. Miller

MSC:

primary 11A07, 11N36

secondary 11A25, 11A41, 11N13

Keywords:

Primitive roots

Artin's conjecture

ABSTRACT

In 1927, Artin conjectured that any integer a which is not -1 or a perfect square is a primitive root for a positive density of primes p . While this conjecture still remains open, there has been a lot of progress in last six decades. In 2000, Moree and Stevenhagen proposed what is known as the two variable Artin's conjecture and proved that for any multiplicatively independent rational numbers a and b , the set

$$\{p \leq x : p \text{ prime, } a \bmod p \in \langle b \rangle \bmod p\}$$

has positive density under the Generalised Riemann Hypothesis for certain Dedekind zeta functions. While the infinitude of such primes is known, the only unconditional lower bound for the size of the above set is due to Ram Murty, Séguin and Stewart who in 2019 showed that for infinitely many pairs (a, b)

$$\#\{p \leq x : p \text{ prime, } a \bmod p \in \langle b \rangle \bmod p\} \gg \frac{x}{\log^2 x}.$$

In this paper we improve this lower bound. In particular we show that given any three multiplicatively independent integers $S = \{m_1, m_2, m_3\}$ such that

[☆] Research of the second author was partially supported by an NSERC Discovery grant.

* Corresponding author.

E-mail addresses: suhita@cmi.ac.in (S.G. Hazra), murty@queensu.ca (M. Ram Murty), joythsnas@gmail.com (J. Sivaraman).

$$m_1, m_2, m_3, -3m_1m_2, -3m_2m_3, -3m_1m_3, m_1m_2m_3$$

are not squares, there exists a pair of elements $a, b \in S$ such that

$$\#\{p \leq x : p \text{ prime, } a \bmod p \in \langle b \rangle \bmod p\} \gg \frac{x \log \log x}{\log^2 x}.$$

Further, under the assumption of a level of distribution greater than $x^{\frac{2}{3}}$ in a theorem of Bombieri, Friedlander and Iwaniec (as modified by Heath-Brown), we prove the following conditional result. Given any two multiplicatively independent integers $S = \{m_1, m_2\}$ such that

$$m_1, m_2, -3m_1m_2$$

are not squares, there exists a pair of elements $a, b \in \{m_1, m_2, -3m_1m_2\}$ such that

$$\#\{p \leq x : p \text{ prime, } a \bmod p \in \langle b \rangle \bmod p\} \gg \frac{x \log \log x}{\log^2 x}.$$

© 2024 Elsevier Inc. All rights reserved.

Contents

1. Introduction and statement of the theorem	162
2. Preliminaries	166
3. Some sieve theoretic lemmas	169
4. Proof of Theorem 1	178
5. Consequences of higher levels of distribution	180
Data availability	184
Acknowledgments	185
References	185

1. Introduction and statement of the theorem

A well known conjecture of Artin [1] from 1927 states that any integer a , which is neither -1 nor a perfect square, is a primitive root for a positive density of primes p . Further, Artin conjectured the density of the set of such primes. If h is the largest integer such that a is a perfect h -th power then Artin proposed that the number of primes $p \leq x$ such that a is a primitive root modulo p (denoted $N_a(x)$) is asymptotic to

$$C(a) \text{Li}(x)$$

where

$$C(a) = \prod_{p|h} \left(1 - \frac{1}{p(p-1)}\right) \prod_{p|h} \left(1 - \frac{1}{p-1}\right).$$

However, calculations later revealed that the value of the density, $C(a)$, was incorrect for certain values of a and a correction factor was required. In 1967, Hooley [6] proved a corrected form of Artin’s conjecture, under the assumption of the Generalised Riemann Hypothesis for certain Dedekind zeta functions. Let a_1 be the squarefree part of a and h as before. Then,

$$N_a(x) \sim C_1(a) \frac{x}{\log x}$$

where

$$C_1(a) = \begin{cases} C(a), & \text{if } a_1 \not\equiv 1 \pmod{4} \\ \left(1 - \mu(|a_1|) \prod_{p|(a_1, h)} \frac{1}{p-2} \prod_{\substack{p|a_1 \\ p \nmid h}} \frac{1}{p^2 - p - 1}\right) C(a), & \text{otherwise.} \end{cases}$$

However, unconditionally the problem is still intractable but there has been some progress in this direction. Several variants, generalisations and weaker conjectures connected to Artin’s primitive root conjecture have appeared and have been studied. An obvious restatement of Artin’s conjecture is as follows. Consider the set

$$L = \{p : \mathbb{F}_p^* = \langle a \rangle \pmod{p}\}.$$

Artin’s conjecture gives an explicit asymptotic for the growth of this set. In particular, it states that this set has positive density. We may consider the following weaker problem. Let

$$L = \{p : \mathbb{F}_p^* = \langle a, b \rangle \pmod{p}\}$$

for two multiplicatively independent integers a and b which are not perfect squares. Then, is the set L infinite? In 1984, Gupta and Ram Murty [4] proved that the above problem can be successfully resolved if one replaces two multiplicatively independent elements by three primes. Further, they used linear algebraic tools to isolate a set of 13 elements from the monoid generated by these three elements and showed that at least one of these 13 elements is a primitive root for at least $cx/\log^2 x$ primes $p \leq x$, for some positive constant c .

In 1985, this argument was refined by Heath-Brown [5] to show the following. Given three multiplicatively independent integers q, r and s , suppose that none of $q, r, s, -3qr, -3qs, -3rs$ or qrs is a square. Then the number of primes $p \leq x$ for which at

least one of q, r and s is a primitive root is at least $cx/\log^2 x$, for some positive constant c . In particular, if q, r and s are primes, at least one of them is a primitive root for infinitely many primes.

In 1997, Ram Murty used a zero free region hypothesis to show that at least one of q, r and s is a primitive root for a positive density of primes $p \leq x$. Here, once again, q, r and s are multiplicatively independent integers such that none of $q, r, s, -3qr, -3qs, -3rs$ or qrs is a square.

However, note that, till date we do not know a single integer which is a primitive root for infinitely many primes.

We are now interested in a variant of Artin’s conjecture and would like to apply the techniques of these papers to deduce new results about this variant. Before we state this variant, let us rephrase Artin’s conjecture once again. Given any integer a let

$$P_a = \{p \text{ prime} : b \bmod p \in \langle a \rangle \bmod p \cup \{0 \bmod p\} \text{ for every } b \in \mathbb{Z}\}.$$

Artin’s conjecture states that for an integer a which is not -1 or a perfect square, P_a is infinite. Note that this set P_a is independent of b . Let us, once again, pose a weaker question which we may be able to answer more easily. In order to do so, for any two multiplicatively independent rational numbers a and b , we define the set

$$P_{a,b} = \{p \text{ prime} : b \bmod p \in \langle a \rangle \bmod p\}.$$

We now ask the question: Given any two multiplicatively independent rational numbers a and b , is $P_{a,b}$ infinite? This has been termed the “Two variable Artin’s conjecture” by Moree and Stevenhagen [9] and it has been proved unconditionally. This conjecture is known as a special case of a result of Pólya [11]. Moree and Stevenhagen give an alternate proof in [9] and go on to pose the following question. Given any two multiplicatively independent rational numbers a and b , does $P_{a,b}$ have positive density? They answer this question in the affirmative under the assumption of the Generalised Riemann Hypothesis for certain Dedekind zeta functions. More precisely they prove that

$$\#\{p \leq x : p \in P_{a,b}\} \sim \left[c_{a,b} \prod_p \left(1 - \frac{p}{p^3 - 1} \right) \right] \text{Li } x$$

for some positive constant $c_{a,b}$. Moreover when $\mathbb{Q}^*/\langle -1, a, b \rangle$ is torsion free they compute the value of the constant $c_{a,b}$. In 2019, Ram Murty, Séguin and Stewart [14] unconditionally proved that for non-zero integers a and b with $|b| \neq 1$

$$\#\{p \leq x : p \in P_{a,b}\} \gg \log x.$$

In the same paper they show the following disjunction theorem. For a, b integers which are not -1 or perfect squares with $(a, b) = 1$,

$$\#\{p \leq x : p \in P_{a,b} \cup P_b\} \gg \frac{x}{\log^2 x}.$$

In particular they show that for any two co-prime integers a, b which are not -1 or perfect squares,

$$\#\{p \leq x : p \in P_{a,b} \cup P_{b,a}\} \gg \frac{x}{\log^2 x}.$$

Therefore by pigeon hole principle, this gives us the existence of infinitely many pairs of integers (a, b) for which

$$\#\{p \leq x : p \in P_{a,b}\} \gg \frac{x}{\log^2 x}.$$

In this paper, we improve this result to show the following.

Theorem 1. *Let $W = \{m_1, m_2, m_3\}$ be a set of three multiplicatively independent integers such that none of $m_1, m_2, m_3, -3m_1m_2, -3m_2m_3, -3m_3m_1, m_1m_2m_3$ is a perfect square. Then, there is at least one pair of distinct elements $a, b \in W$ such that*

$$\#\{p \leq x : p \in P_{a,b}\} \gg \frac{x \log \log x}{\log^2 x}.$$

As a consequence we now have the following corollary.

Corollary 2. *There is at most one prime m_1 such that*

$$\#\{p \leq x : p \in P_{m_1, m_2} \cup P_{m_2, m_1}\} = o\left(\frac{x \log \log x}{\log^2 x}\right)$$

for all primes m_2 distinct from m_1 .

The proof of this main theorem employs the use of well-factorable weights and the following theorem of Bombieri, Friedlander and Iwaniec [2] (as modified by Heath-Brown [5]).

Theorem 3. [Heath-Brown; Bombieri, Friedlander and Iwaniec (see [2], [5])] *Let a, k be positive natural numbers with $(a, k) = 1$. For any positive natural number q with $(q, k) = 1$, let*

$$u_q \equiv a \pmod{k} \quad \text{and} \quad u_q \equiv 1 \pmod{q}.$$

Fix a positive integer $A > 0$ and a real number $\theta < 4/7$. For every well-factorable function λ of level x^θ , one has

$$\sum_{(q,k)=1} \lambda(q) \left(\pi(x, qk, u_q) - \frac{\text{Li}(x)}{\varphi(qk)} \right) \ll \frac{x}{\log^A x}.$$

The constant in \ll depends on a, A, k and θ .

The second theorem of this paper proves a conditional result assuming a level of distribution of x^μ with $\mu > \frac{2}{3}$ in the above.

Theorem 4. *Assume the above result of Bombieri, Friedlander, Iwaniec and Heath-Brown with a level of distribution x^μ with $\mu > \frac{2}{3}$. Let m_1, m_2 be two multiplicatively independent integers such that $m_1, m_2, -3m_1m_2$ are not perfect squares. Then, there exist elements $a, b \in \{m_1, m_2, -3m_1m_2\}$ such that*

$$\#\{p \leq x : p \in P_{a,b}\} \gg \frac{x \log \log x}{\log^2 x}.$$

Suppose we use $\text{EH}(\alpha)$ to denote the assumption of a level of distribution of x^α in the Bombieri-Vinogradov theorem, we note that $\text{EH}(\alpha)$ with $\alpha > 2/3$ implies the Bombieri, Friedlander, Iwaniec and Heath-Brown theorem with a level of distribution as required by Theorem 4. Thus, our assumption is substantially weaker than the Elliott-Halberstam conjecture. It is conceivable that such a hypothesis is within reach of current sieve technology.

In section 2 we introduce some preliminaries required for our proof. In section 3 we prove some sieve theoretic lemmas and in the penultimate section we prove our main theorem. This is followed by the last section where we show the conditional Theorem 4.

2. Preliminaries

In this section we introduce some of the preliminaries required for the proofs of our theorems. We begin with some definitions and notations. Let

$$\begin{aligned} \pi(x) &:= \#\{p \leq x : p \text{ prime}\}, \\ \pi(x, d, e) &:= \#\{p \leq x : p \text{ prime}, p \equiv e \pmod{d}\} \end{aligned}$$

and μ denote the Möbius function given by

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is squarefree and a product of } r \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

We will now briefly discuss some notations required for the statement of the Rosser-Iwaniec sieve which we will use to find the lower bounds. Let \mathcal{A} be a set of integers, \mathcal{P} be a set of primes and $z \geq 2$ be a real number. We define

$$S(\mathcal{A}; \mathcal{P}, z) := \#\{n : n \in \mathcal{A}, (n, P(z)) = 1\} \text{ where } P(z) = \prod_{\substack{p \leq z \\ p \in \mathcal{P}}} p.$$

For q square free we define

$$\mathcal{A}_q := \{a \in \mathcal{A} : a \equiv 0 \pmod q\}$$

and let ω_0 be a function such that $\frac{\omega_0(p)}{p}X$ will give an estimate of $\#\mathcal{A}_p$ for p prime where X denotes the size of the set \mathcal{A} . For any prime p we define another function ω as

$$\omega(p) = \begin{cases} \omega_0(p) & \text{if } p \in \mathcal{P} \\ 0 & \text{if } p \notin \mathcal{P}. \end{cases}$$

We set $\omega(1) = 1$. For any square free number q , $\omega(q) = \prod_{p|q} \omega(p)$. Further, for any square free number q , define

$$R_q := \#\mathcal{A}_q - \frac{\omega(q)}{q}X \quad \text{and let} \quad V(z) = \prod_{\substack{p < z \\ p \in \mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right).$$

We further assume that by the choice of ω , we have

$$\frac{V(z_1)}{V(z_2)} \leq \frac{\log z_2}{\log z_1} \left(1 + \frac{C}{\log z_1}\right) \text{ for } z_2 \geq z_1 \geq 2 \tag{1}$$

where C is some constant > 1 . We now introduce a few definitions required to introduce the Rosser-Iwaniec sieves.

Definition 5. An arithmetical function λ is said to be of level Q and order k if

$$Q = \min\{q \in \mathbb{N} : \lambda(q) = 0\} \text{ and } k = \min\{u \in \mathbb{N} : |\lambda(q)| \leq d_u(q) \forall q \in \mathbb{N}\}.$$

Here $d_u(n)$ denotes the number of ordered ways of writing a natural number n as a product of u natural numbers.

We now introduce the notion of well-factorable weights

Definition 6. An arithmetical function λ of level Q is said to be well-factorable if for any Q_1, Q_2 with $Q_1 Q_2 = Q$, there exist two arithmetical functions λ_1, λ_2 of levels at most Q_1, Q_2 and of bounded order such that $\lambda = \lambda_1 * \lambda_2$.

Remark 7. Note that given two arithmetical functions λ, λ' of levels Q, Q' and orders k, k' the function $\lambda * \lambda'$ has level at most QQ' and order $k + k'$.

We now state the Rosser-Iwaniec upper and lower bound sieves. The novice can find a gentle introduction to the lower bound sieve in Chapter 10 of [3].

Theorem 8. (Rosser - Iwaniec [7], [8]) *Let $0 < \tau < \frac{1}{8}$, $2 \leq z \leq Q^{\frac{1}{2}}$. Under the above notation, we have*

$$S(\mathcal{A}, \mathcal{P}, z) \leq XV(z)(F(\log Q/\log z) + E) + \sum_{l < L} \sum_{q|P(z)} \lambda_l^+(q)R_q,$$

$$S(\mathcal{A}, \mathcal{P}, z) \geq XV(z)(f(\log Q/\log z) - E) - \sum_{l < L} \sum_{q|P(z)} \lambda_l^-(q)R_q.$$

Here, L depends only on τ and λ_l^+, λ_l^- are well-factorable functions of order 1 and of level Q . The constant E satisfies

$$E = O\left(\tau + \tau^{-8}e^C / \log^{\frac{1}{3}} Q\right).$$

Here C is the constant appearing in (1). The continuous functions $F(s)$ and $f(s)$ are defined recursively by

$$F(s) = 2e^\gamma/s, \quad f(s) = 0 \quad \text{for } s \leq 2,$$

$$(sF(s))' = f(s - 1), \quad (sf(s))' = F(s - 1) \quad \text{for } s > 2,$$

and γ denotes the Euler-Mascheroni constant.

We will now state two important theorems required to estimate the error terms in the application of the Rosser-Iwaniec sieve in our context. These are the well known theorem of Bombieri, Friedlander and Iwaniec, as modified by Heath-Brown and a mean value theorem due to Pan.

Theorem 9. [Heath-Brown; Bombieri, Friedlander and Iwaniec (see [2], [5])] *Let a, k be positive natural numbers with $(a, k) = 1$. For any positive natural number q with $(q, k) = 1$, let*

$$u_q \equiv a \pmod k \quad \text{and} \quad u_q \equiv 1 \pmod q.$$

Fix a positive integer $A > 0$ and a real number $\theta < 4/7$. For every well-factorable function λ of level x^θ , one has

$$\sum_{(q,k)=1} \lambda(q) \left(\pi(x, qk, u_q) - \frac{\text{Li}(x)}{\varphi(qk)} \right) \ll \frac{x}{\log^A x}.$$

The constant in \ll depends on a, A, k and θ .

Theorem 10. [Pan [10]] *Let*

$$\pi(X; a, d, l) = \sum_{\substack{ap \leq X \\ ap \equiv l \pmod{d} \\ p \text{ prime}}} 1$$

and let $j(a)$ be a real valued function satisfying the conditions

$$\sum_{n \leq x} |j(n)| \ll x \log^{a_1} x, \quad \sum_{n \leq x} \sum_{d|n} |j(d)| \ll x \log^{a_2} x$$

where a_1, a_2 are positive constants. Given $A > 0$ there is a $B = B(A, a_1, a_2)$ such that

$$\sum_{d \leq \frac{\sqrt{X}}{\log^B X}} \max_{y \leq X} \max_{(l,d)=1} \left| \sum_{\substack{a \leq X^{1-\epsilon} \\ (a,d)=1}} j(a) \left(\pi(y; a, d, l) - \frac{\pi(y; a, 1, 1)}{\phi(d)} \right) \right| \ll \frac{X}{\log^A X}$$

and $0 < \epsilon < 1$.

We add here a standard result in analytic number theory which we use in our proof.

Lemma 11 (See Exercise 2.5.1 of [13]). *Let $d_k(n)$ denote the number of ordered ways of writing a natural number n as a product of k natural numbers. We have*

$$\sum_{n \leq x} d_k(n) \ll x \log^{k-1} x$$

for every natural number $k \geq 2$.

Finally, we conclude this section with a result from [12] due to Ram Murty (see also Gupta and Ram Murty [4]).

Lemma 12. (Gupta and Ram Murty [4], Ram Murty [12]) *Suppose that $\{q_1, \dots, q_n\}$ is a set of n multiplicatively independent integers. Let $\Gamma = \{q_1^{a_1} \cdots q_n^{a_n} : a_i \in \mathbb{N}\}$ and $\Gamma_p = \{b \pmod{p} : b \in \Gamma\}$. Then*

$$\#\{p : p \text{ is prime and } |\Gamma_p| \leq y\} \ll y^{\frac{n+1}{n}}.$$

3. Some sieve theoretic lemmas

In this section, we prove some sieve-theoretic lemmas required to prove our main theorem. Throughout the discussion, $\epsilon, \epsilon_1, \epsilon_2, \epsilon_3, \eta$ will denote sufficiently small positive real numbers.

Lemma 13. Let $K = 2^k$ for some $k \in \{1, 2, 3\}$. Fix u, v such that $(u, v) = 1$, $K|(u - 1)$, $16|v$ and $(\frac{u-1}{K}, v) = 1$. Further, let α be a positive real number greater than $1/4$ and

$$c_1 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|v \\ p>2}} \left(\frac{p-1}{p-2}\right).$$

There exists an $\eta > 0$ and a set $\mathcal{M}(x, \eta)$ of primes $p \leq x$ of size

$$\#\mathcal{M}(x, \eta) \geq \frac{(1 + o(1))2e^{-\gamma}c_1f(4/7\alpha) \operatorname{Li}(x) \log \log x^\eta}{\alpha\phi(v) \log x},$$

such that for all $p \in \mathcal{M}(x, \eta)$, we have:

- (a) $p \equiv u \pmod v$;
- (b) there exists exactly one odd prime $\ell_p \leq x^\eta$ such that $\ell_p|(p - 1)$;
- (c) any odd prime $p_1|(p - 1)$ with $p_1 \neq \ell_p$ satisfies $p_1 > x^\alpha$;
- (d) $(p - 1)/K\ell_p$ has at most three prime factors.

Here f is the function introduced in Theorem 8.

Proof. Fix a prime $\ell \leq x^\eta$, where η is a positive quantity to be chosen later. Define

$$\mathcal{A}_\ell := \left\{ \frac{p-1}{K\ell} : p \leq x, \quad p \equiv u \pmod v, \quad p \equiv 1 \pmod \ell \right\}.$$

Let $\mathcal{P}_\ell = \{2 < p : p \text{ prime}, (p, v\ell) = 1\}$. Now for any square free integer q such that $(q, 2v\ell) = 1$, define

$$\mathcal{A}_{\ell q} := \{a \in \mathcal{A}_\ell : q|a\}.$$

We note that

$$\#\mathcal{A}_{\ell q} = \#\{p \leq x : p \text{ prime}, p \equiv u \pmod v, p \equiv 1 \pmod \ell q\} = \pi(x, v\ell q, e_{\ell q})$$

for some $e_{\ell q}$ (such $e_{\ell q}$ exists by the Chinese remainder theorem as v, ℓ, q are pairwise coprime). We know that

$$\#\mathcal{A}_{\ell q} = \frac{\operatorname{Li}(x)}{\phi(v\ell q)} + R_q = X_1 \frac{\omega(q)}{q} + R_q$$

where $X_1 = \frac{\operatorname{Li}(x)}{\phi(v\ell)}$ and

$$r_{\ell q} := R_q = \pi(x, v\ell q, e_{\ell q}) - \frac{\operatorname{Li}(x)}{\phi(v\ell q)}.$$

For any square free integer q ,

$$\omega(q) = \begin{cases} \frac{q}{\phi(q)} & \text{if } q \text{ is supported on the primes in } \mathcal{P}_\ell \\ 0 & \text{otherwise.} \end{cases}$$

We apply the lower bound sieve in Theorem 8 with $z = x^\alpha$ and $Q = x^\mu$ to deduce, for ϵ sufficiently small

$$S(\mathcal{A}_\ell, \mathcal{P}_\ell, x^\alpha) \geq X_1 \prod_{p \leq x^\alpha, p \nmid v\ell} \left(1 - \frac{1}{p-1}\right) \{f(\mu/\alpha) - \epsilon\} - \sum_{d < L} \sum_{q | P(x^\alpha)} \lambda_d^-(q) r_{q\ell}. \tag{2}$$

Here the λ_d^- are well-factorable functions of level $Q = x^\mu$ and order 1 as in Theorem 8 and Theorem 9. We choose $\mu = \frac{4}{7} - \epsilon_1$ and $\alpha = 1/4 + \epsilon_2$. By the argument on Page 33 of [5], we have

$$\prod_{p \leq x^\alpha, p \nmid v\ell} \left(1 - \frac{1}{p-1}\right) = (1 + o(1)) \frac{2e^{-\gamma}}{\alpha \log x} \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p | v\ell \\ p > 2}} \left(\frac{p-1}{p-2}\right). \tag{3}$$

We now sum over all odd primes $\ell \leq x^\eta$. Let us first consider the inner sum of the second term in (2), on summing over all $\ell \leq x^\eta$ we get

$$\sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \sum_{\substack{q | P(x^\alpha) \\ q < x^\mu, (q, \ell) = 1}} \lambda_d^-(q) r_{q\ell} = \sum_{b \leq x^{\mu+\eta}} r_b \sum_{\substack{b = \ell q \\ \ell \leq x^\eta, q < x^\mu, (q, \ell) = 1 \\ \ell \text{ odd prime, } q | P(x^\alpha)}} \lambda_d^-(q).$$

Let us use $\mathbf{1}_{p \leq x^\eta}$ to denote the indicator function of the odd primes less than x^η and $\mathbf{1}_{a | P(x^\alpha), a < x^\mu}$ to denote the indicator function of square free $q | P(x^\alpha)$ and less than x^μ . Then,

$$\sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \sum_{\substack{q | P(x^\alpha) \\ q < x^\mu, (q, \ell) = 1}} \lambda_d^-(q) r_{q\ell} = \sum_{\substack{b \leq x^{\mu+\eta} \\ b | P(x^\alpha)}} r_b \sum_{b = \ell q} \lambda_d^-(q) \mathbf{1}_{p \leq x^\eta}(\ell).$$

It is now obvious that the inner sum is a convolution of two functions. We know that λ_d^- is a well-factorable function of level x^μ and we claim that

$$\lambda_d^- * \mathbf{1}_{p \leq x^\eta}$$

is a well-factorable function of level $x^{\mu+2\eta}$. Since the convolution of a well-factorable functions of level Q_1 and Q_2 is a well-factorable function of level $Q_1 Q_2$, it suffices to show that $\mathbf{1}_{p \leq x^\eta}$ is well-factorable of level $x^{2\eta}$. This follows from the following decomposition. Let M and N be two positive real numbers such that $MN = x^{2\eta}$. Without loss of generality we assume $M \geq x^\eta$. This implies that

$$\mathbf{1}_{p \leq x^\eta}(m) = \sum_{a \leq M} \sum_{\substack{b \leq N \\ ab=m}} \delta(b) \mathbf{1}_{p \leq x^\eta}(a)$$

where $\delta(b)$ is 1 iff $b = 1$ and zero otherwise. Now by Theorem 9, for some $\eta > 0$ satisfying $\mu + 2\eta < 4/7$, we get

$$\begin{aligned} \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell; \mathcal{P}_\ell, x^\alpha) &\geq \frac{(1 + o(1))2c_1 e^{-\gamma}}{\alpha} \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \frac{\text{Li}(x)}{\phi(v)(\ell - 2) \log x} \{f(\mu/\alpha) - \epsilon\} \\ &+ O\left(\frac{x}{\log^3 x}\right) \end{aligned}$$

where

$$c_1 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|v \\ p>2}} \left(\frac{p-1}{p-2}\right).$$

For ϵ_1 and ϵ_2 sufficiently small we have $2 < \mu/\alpha < 4$. Further by continuity of f in the interval $[2, 4]$, we get

$$f(\mu/\alpha) \geq f(4/7\alpha) - \epsilon.$$

This implies

$$\sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell; \mathcal{P}_\ell, x^\alpha) \geq \frac{(1 + o(1))2c_1 e^{-\gamma} \text{Li}(x) \log \log x^\eta}{\alpha \phi(v) \log x} \{f(4/7\alpha) - 2\epsilon\}. \tag{4}$$

Let us now define for a prime $\ell \leq x^\eta$

$$\mathcal{A}'_\ell := \left\{ \frac{p-1}{K\ell} : p \leq x, \quad p \equiv u \pmod v \quad p \equiv 1 \pmod{\ell^2} \right\}.$$

For $(q, v\ell) = 1$, let $\mathcal{A}'_{\ell q} = \{a \in \mathcal{A}'_\ell : q \mid a\}$. Therefore, we have for $(q, v\ell) = 1$,

$$\#\mathcal{A}'_{\ell q} = \#\{p \leq x : p \text{ prime}, p \equiv 1 \pmod{\ell^2 q}, p \equiv u \pmod v\} = \pi(x, v\ell^2 q, e_{\ell^2 q}),$$

and

$$\#\mathcal{A}'_{\ell q} = \frac{\text{Li}(x)}{\phi(v\ell^2 q)} + R'_q = X'_1 \frac{\omega(q)}{q} + R'_q$$

where $X'_1 = \frac{\text{Li}(x)}{\phi(v\ell^2)}$ and

$$r'_{\ell^2 q} := R'_q = \pi(x, v\ell^2 q, e_{\ell^2 q}) - \frac{\text{Li}(x)}{\phi(v\ell^2 q)}.$$

We now apply the upper bound Rosser-Iwaniec sieve (Theorem 8) with $z = Q = x^\mu$, to get

$$S(\mathcal{A}'_\ell; \mathcal{P}_\ell, x^\mu) \ll \frac{\text{Li}(x)}{\phi(v\ell^2)} \prod_{\substack{p \leq x^\mu \\ p \in \mathcal{P}_\ell}} \left(1 - \frac{1}{p-1}\right) + \sum_{d < L} \sum_{\substack{q | P(x^\mu) \\ (q, \ell v) = 1}} \lambda_d^+(q) r'_{\ell^2 q}. \tag{5}$$

Summing both sides of (5) over $\ell \leq x^\eta$ for the same η as before and arguing as before in the lower bound, we get by Theorem 9

$$\sum_{\ell \leq x^\eta} S(\mathcal{A}'_\ell; \mathcal{P}_\ell, x^\mu) \ll \sum_{\ell \leq x^\eta} \frac{\text{Li}(x)}{\phi(v\ell^2)} \prod_{\substack{p \leq x^\mu \\ p \in \mathcal{P}_\ell}} \left(1 - \frac{1}{p-1}\right) + O\left(\frac{x}{\log^3 x}\right)$$

By (3), we get

$$\sum_{\ell \leq x^\eta} S(\mathcal{A}'_\ell; \mathcal{P}_\ell, x^\mu) \ll \frac{x}{\log^2 x}. \tag{6}$$

Then

$$\#\mathcal{M}(x, \eta) \geq \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell; \mathcal{P}_\ell, x^\alpha) - \sum_{\ell \leq x^\eta} S(\mathcal{A}'_\ell; \mathcal{P}_\ell, x^\mu)$$

By (4) and (6), there exists an $\eta > 0$ such that for every $\epsilon > 0$

$$\#\mathcal{M}(x, \eta) \geq \frac{(1 + o(1))2e^{-\gamma}c_1 \text{Li}(x) \log \log x^\eta}{\alpha\phi(v) \log x} \{f(4/7\alpha) - 2\epsilon\}. \quad \square \tag{7}$$

Lemma 14. *Let $K = 2^k$ for some $k \in \{1, 2, 3\}$. Fix u, v such that $(u, v) = 1$, $K|(u-1)$, $16|v$ and $(\frac{u-1}{K}, v) = 1$. There exists an $\eta > 0$ and a set $\mathcal{T}^*(x, \eta)$ of primes $p \leq x$ of size*

$$\gg_\eta \frac{x \log \log x}{\log^2 x}$$

such that for all $p \in \mathcal{T}^*(x, \eta)$, we have:

- (a) $p \equiv u \pmod v$;
- (b) there exists exactly one odd prime $\ell_p \leq x^\eta$ such that $\ell_p | (p-1)$;
- (c) any odd prime $p_1 | (p-1)$ with $p_1 \neq \ell_p$ satisfies $p_1 > x^\alpha$ with $\alpha > 1/4$;
- (d) $(p-1)/K\ell_p$ has at most two prime factors.

Proof. We now use the Chen-Iwaniec switching method to remove those primes with exactly three prime factors from the set $\mathcal{M}(x, \eta)$. To this end, we apply the upper bound sieve as indicated in Theorem 8. Let

$$\mathcal{B}_\ell = \left\{ 1 + K\ell p_1 p_2 p_3 \leq x : p_i \geq x^\alpha, \quad 1 + K\ell p_1 p_2 p_3 \equiv u \pmod v \right\}.$$

This is a multiset and the six different orderings of p_1, p_2, p_3 are to be counted as distinct. If $(q, \ell v) = 1$, then

$$\#\mathcal{B}_{\ell q} = \#\{b \in \mathcal{B}_\ell : q|b\} = \#\{p_1 p_2 p_3 \leq y : p_i \geq x^\alpha, \quad p_1 p_2 p_3 \equiv t_q \pmod{qv/K}\},$$

where $y = (x - 1)/K\ell$ and t_q is the common solution of

$$K\ell t_q + 1 \equiv u \pmod v, \quad K\ell t_q + 1 \equiv 0 \pmod q. \tag{8}$$

Let

$$g_\ell(a) = \#\{\ell p_2 p_3 = a : p_2, p_3 \geq x^\alpha\}.$$

By the definition of u and v we only count a such that $(a, v/K) = 1$. Note that $g_\ell(a) \leq d_3(a)$ where $d_3(a)$ is the number of ordered ways of writing a as a product of three natural numbers. We now write

$$X_2 := \frac{1}{\phi(v/K)} \sum_{\substack{a \leq y\ell x^{-\alpha} \\ (a, v/K)=1}} g_\ell(a)(\pi(y\ell/a) - \pi(x^\alpha)).$$

Further for any prime q co-prime to ℓv ,

$$\#\mathcal{B}_{\ell q} = \frac{\omega(q)X_2}{q} + R_q,$$

where $\omega(q) = q/(q - 1)$ and

$$R_q = \sum_{\substack{a_1 \leq yx^{-\alpha} \\ (a_1, qv/K)=1}} g_\ell(a_1\ell)[E(y; a_1, qv/K, t_q) - E(a_1x^\alpha; a_1, qv/K, t_q)]$$

with

$$E(y; a_1, qv/K, t_q) = \pi(y; a_1, qv/K, t_q) - \frac{\pi(y/a_1)}{\phi(qv/K)}.$$

By partial summation and the prime number theorem, we have

$$\sum_{\substack{a \leq y\ell x^{-\alpha} \\ (a, qv/K)=1}} g_\ell(a)(\pi(y\ell/a) - \pi(x^\alpha)) \sim - \int_2^{\frac{y\ell}{x^\alpha}} \sum_{a \leq t} g_\ell(a) \frac{d(y\ell/t)}{\log(y\ell/t)}.$$

Putting $z = y\ell/t$ and writing the asymptotics for $\sum_{a \leq t} g_\ell(a)$

$$\sum_{\substack{a \leq y\ell x^{-\alpha} \\ (a, qv/K)=1}} g_\ell(a)(\pi(y\ell/a) - \pi(x^\alpha)) \sim \int_{x^\alpha}^{y\ell/2} \frac{dz}{\log z} \int_{x^\alpha}^{y/(zx^\alpha)} \int_{x^\alpha}^{y/(p_2z)} \frac{dp_2 dp_3}{\log p_2 \log p_3}.$$

Changing the order of integration

$$\sum_{\substack{a \leq y\ell x^{-\alpha} \\ (a, qv/K)=1}} g_\ell(a)(\pi(y\ell/a) - \pi(x^\alpha)) \sim \int_{x^\alpha}^{y/x^{2\alpha}} \frac{dp_2}{\log p_2} \int_{x^\alpha}^{y/(p_2x^\alpha)} \frac{dp_3}{\log p_3} \int_{x^\alpha}^{y/(p_2p_3)} \frac{dz}{\log z}.$$

Putting $p_2 = x^\theta$, $p_3 = x^\psi$ and using the main term of $\text{Li}(x)$ we get

$$\begin{aligned} & \sum_{\substack{a \leq y\ell x^{-\alpha} \\ (a, qv/K)=1}} g_\ell(a)(\pi(y\ell/a) - \pi(x^\alpha)) \\ & \sim \int_\alpha^{1-2\alpha-\log_x \ell} \frac{p_2 d\theta}{\theta} \int_\alpha^{1-\alpha-\theta-\log_x \ell} \frac{p_3 d\psi}{\psi} \cdot \frac{y/(p_2p_3)}{\log(y/(p_2p_3))} \\ & \sim \frac{y}{\log x} \int_\alpha^{1-2\alpha-\log_x \ell} \int_\alpha^{1-\alpha-\theta-\log_x \ell} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\log_x \ell}. \\ X_2 & \sim \frac{y}{\phi(v/K) \log x} \int_\alpha^{1-2\alpha-\log_x \ell} \int_\alpha^{1-\alpha-\theta-\log_x \ell} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\log_x \ell} = I^* \frac{(x-1)/\ell}{\phi(v) \log x} \end{aligned}$$

where

$$I^* = \int_\alpha^{1-2\alpha-\log_x \ell} \int_\alpha^{1-\alpha-\theta-\log_x \ell} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\log_x \ell}.$$

Note that if $2^{k_1} \parallel v$, then

$$\phi(v/K) \cdot K = \phi(v/2^{k_1}) \cdot \phi(2^{k_1}/K) \cdot K = \phi(v/2^{k_1}) \cdot 2^{k_1-k-1} \cdot 2^k = \phi(v).$$

Now consider the integral

$$\int_\alpha^{1-2\alpha-\log_x \ell} \int_{1-\alpha-\theta-\eta}^{1-\alpha-\theta-\log_x \ell} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\log_x \ell} \leq \frac{1}{\alpha^3} \int_\alpha^{1-2\alpha-\log_x \ell} \int_{1-\alpha-\theta-\eta}^{1-\alpha-\theta-\log_x \ell} d\theta d\psi$$

Therefore

$$\int_{\alpha}^{1-2\alpha-\log_x \ell} \int_{1-\alpha-\theta-\eta}^{1-\alpha-\theta-\log_x \ell} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\log_x \ell} \leq \frac{(1-3\alpha)\eta}{\alpha^3}.$$

Similarly if we consider

$$\int_{1-2\alpha-\eta}^{1-2\alpha-\log_x \ell} \int_{\alpha}^{1-\alpha-\theta-\eta} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\log_x \ell} \leq \frac{(1-2\alpha)\eta}{\alpha^3}.$$

Let

$$I = \int_{\alpha}^{1-2\alpha-\eta} \int_{\alpha}^{1-\alpha-\theta-\eta} \frac{d\theta d\psi}{\theta\psi} \cdot \frac{1}{1-\theta-\psi-\eta}.$$

Then for η sufficiently small

$$I^* = I + O(\eta).$$

Further

$$I = 2 \int_{\alpha}^{1-2\alpha-\eta} \frac{d\theta}{\theta(1-\theta-\eta)} \log \left(\frac{1-\alpha-\theta-\eta}{\alpha} \right).$$

On the other hand, by the Rosser-Iwaniec upper bound sieve (Theorem 8) for $z = y^{1/2-\epsilon_3}$ we have

$$S(\mathcal{B}_\ell, \mathcal{P}_\ell, y^{1/2-\epsilon_3}) \leq X_2(F(1) + \epsilon) \prod_{\substack{p \leq y^{1/2-\epsilon_3} \\ p \in \mathcal{P}_\ell}} \left(1 - \frac{1}{p-1} \right) + L \sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q, \ell v) = 1}} d_2(q) \mu^2(q) |R_q| \tag{9}$$

where $F(1) = 2e^\gamma$ and $d_2(q)$ is the number of divisors of q . To estimate the error we use Cauchy-Schwarz inequality. We now get

$$\sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q, \ell v) = 1}} d_2(q) \mu^2(q) |R_q| \ll \left(\sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q, \ell v) = 1}} |R_q| \right)^{\frac{1}{2}} \cdot \left(\sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q, \ell v) = 1}} (d_2(q))^2 \mu^2(q) |R_q| \right)^{\frac{1}{2}}$$

Therefore we now need to estimate

$$\sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q, \ell v) = 1}} |R_q| \leq \sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q, \ell v) = 1}} \sum_{\substack{a_1 \leq yx^{-\alpha} \\ (a_1, qv/K) = 1}} d_3(a_1 \ell) |E(y; a_1, qv/K, t_q) - E(a_1 x^\alpha; a_1, qv/K, t_q)|.$$

We now observe that the hypothesis of Theorem 10 holds for $j(n) = d_3(n)$ by Lemma 11 and the fact that

$$\sum_{m|n} d_3(m) = d_4(n) \text{ and } d_3(a_1\ell) \leq 3d_3(a_1).$$

By Theorem 10, we have for $\ell \leq x^\eta$,

$$\sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q,\ell v)=1}} |R_q| \ll \frac{y}{\log^A y} \ll \frac{x/\ell}{\log^A x}.$$

For the other sum, we get

$$\begin{aligned} \sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q,\ell v)=1}} (d_2(q))^2 \mu^2(q) |R_q| &\ll \sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q,\ell v)=1}} (d_2(q))^2 \mu^2(q) \cdot \frac{y}{\phi(qv/K)} \sum_{\substack{a \leq yx^{-\alpha} \\ (a,qv/K)=1}} d_3(a) \\ &\ll \frac{y \log^2 y}{\phi(v/K)} \sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q,\ell v)=1}} (d_2(q))^2 \mu^2(q) \cdot \frac{1}{\phi(q)} \\ &\ll \frac{y \log^2 y}{\phi(v/K)} \prod_{q \leq y^{1/2-\epsilon_3}} \left(1 + \frac{4}{p-1}\right) \ll \frac{y \log^6 y}{\phi(v/K)}. \end{aligned}$$

Now summing over the primes $\ell \leq x^\eta$, we get

$$\sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \sum_{\substack{q \leq y^{1/2-\epsilon_3} \\ (q,\ell v)=1}} d_2(q) \mu^2(q) |R_q| \ll \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \frac{x/\ell}{\log^A x} \ll \frac{x}{\log^{A-1} x}. \tag{10}$$

For the upper bound, we get by (9) and (10)

$$\begin{aligned} \frac{1}{6} \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} S(\mathcal{B}_\ell, \mathcal{P}_\ell, x^{1/2-\epsilon_3}) &\leq \frac{1}{6} \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \frac{\ell-1}{\ell-2} \cdot (1+o(1)) 4e^{-\gamma} c_1 \cdot F(1) \\ &\quad \cdot 2(I+O(\eta)) \frac{x/\ell}{\phi(v) \log^2 x} + O\left(\frac{x}{\log^{A-1} x}\right) \\ &\leq (1+o(1)) e^{-\gamma} c_1 \cdot F(1) \cdot \frac{4}{3} (I+O(\eta)) \frac{x \log \log x^\eta}{\phi(v) \log^2 x}. \end{aligned}$$

Therefore, we have

$$\begin{aligned} \#\mathcal{T}^*(x, \eta) &\geq \#\mathcal{M}(x, \eta) - \frac{1}{6} \sum_{\ell \leq x^\eta} S(\mathcal{B}_\ell, \mathcal{P}_\ell, x^{1/2-\epsilon_3}) \\ &\geq c_1(1 + o(1))e^{-\gamma} \frac{x \log \log x^\eta}{\phi(v) \log^2 x} \left(2\alpha^{-1} f\left(\frac{4}{7\alpha}\right) - \frac{4}{3}(I + O(\eta))F(1) \right), \end{aligned} \tag{11}$$

and for η sufficiently small

$$I \leq 2 \int_{1/4+\epsilon_2}^{1/2-2\epsilon_2-\eta} \frac{\log(3-4\theta)}{\theta(1-\theta-\eta)} d\theta \leq 2 \int_{1/4}^{1/2} \frac{\log(3-4\theta)}{\theta(1-\theta-\eta)} d\theta = 2 \log \frac{16}{9} + O(\eta).$$

Since $f(u) = 2e^\gamma u^{-1} \log(u-1)$ for $2 \leq u \leq 4$, we get the following lower bound for the left hand side of (11)

$$\begin{aligned} &c_1(1 + o(1)) \frac{x \log \log x^\eta}{\log^2 x} \left(7 \log\left(\frac{4}{7\alpha} - 1\right) - \frac{8}{3}(I + O(\eta)) \right) \\ &\geq (0.225 + O(\eta))c_1(1 + o(1)) \frac{x \log \log x^\eta}{\log^2 x} \end{aligned}$$

for the choice $\alpha = \frac{1}{4} + \epsilon_2$. This completes the proof. \square

4. Proof of Theorem 1

In this section we give the proof of our main theorem.

Lemma 15. *With notation as in the previous lemma, there exists a $\delta = \delta(\eta)$ such that $0 < \eta < \delta$ and a subset $\mathcal{T}(x, \eta)$ of $\mathcal{T}^*(x, \eta)$ with size*

$$\gg \frac{x \log \log x}{\log^2 x}$$

such that if $p \in \mathcal{T}(x, \eta)$ and $(p-1)/K\ell_p$ has exactly two prime factors $\ell_0 \leq \ell_1$ then, $\ell_0 < x^{1/2-\delta}$.

Proof. Clearly $\ell_0^2 \leq x$. Fix $\ell < x^\eta$ and $x^{1/2-\delta} < \ell_0 \leq x^{1/2}$. By Brun’s sieve, the number of primes $p \equiv 1 \pmod{K\ell\ell_0}$ such that $(p-1)/K\ell\ell_0$ is free of prime factors less than x^α is bounded by

$$\ll \frac{\pi(x)}{\phi(\ell\ell_0) \log x}.$$

We sum this over $\ell \leq x^\eta$ and ℓ_0 satisfying $x^{1/2-\delta} \leq \ell_0 < x^{1/2}$. The sum is

$$\ll \delta \frac{x \log \log x}{\log^2 x}$$

and choosing $\delta > \eta > 0$ sufficiently small shows that we can discard these primes from our set $\mathcal{T}^*(x, \eta)$ to deduce the desired estimate. \square

Theorem 16. *Let $W = \{m_1, m_2, m_3\}$ be a set of three multiplicatively independent integers such that none of $m_1, m_2, m_3, -3m_1m_2, -3m_2m_3, -3m_3m_1, m_1m_2m_3$ is a perfect square. Then, there is at least one pair of distinct elements $a, b \in W$ such that*

$$\#\{p \leq x : p \in P_{a,b}\} \gg \frac{x \log \log x}{\log^2 x}.$$

Proof. The conditions on m_1, m_2, m_3 ensure that there is a v determined by m_1, m_2, m_3 and an arithmetic progression of primes $p \equiv u \pmod{v}$ such that m_1, m_2, m_3 are non-residues \pmod{p} (see section 5 of [5]). The argument further ensures that such a class, denoted $u \pmod{v}$ satisfies $(u, v) = 1, K|(u-1), 16|v$ and $((u-1)/K, v) = 1$ where $K = 2^k$ with $k = 1, 2$ or 3 . Let $\mathcal{T}(x, \eta)$ be as in Lemma 15. Now consider the multiplicative group Γ generated by $\{m_1, m_2, m_3\}$. For each prime $p \in \mathcal{T}(x, \eta)$, we consider the index $[\mathbb{F}_p^* : \Gamma_p]$. If this index is divisible by a prime greater than x^α with $\alpha > 1/4$, then by Lemma 12, the number of such primes is $O(x^{4(1-\alpha)/3})$. This is negligible compared to the size of $\mathcal{T}(x, \eta)$ and so discarding these primes, we obtain a subset $\mathcal{T}^{**}(x, \eta)$ of $\mathcal{T}(x, \eta)$ with size

$$\gg_\eta \frac{x \log \log x}{\log^2 x}$$

such that the index of Γ_p is coprime to $(p-1)/K\ell_p$. As m_1, m_2, m_3 are non-residues \pmod{p} , the orders of each of $m_1, m_2, m_3 \pmod{p}$ are all divisible by K . We consider two cases.

- (1) Case 1: $\lambda := (p-1)/K\ell_p$ is prime. Then, we can assume that the order of each of m_1, m_2, m_3 is divisible by λ . This is because if λ divides the indices of $\langle m_1 \rangle, \langle m_2 \rangle, \langle m_3 \rangle$ then by Lemma 12 the number of such primes is $O(x^{2\eta})$ which we can ignore when η is sufficiently small. If the orders of m_1, m_2, m_3 are coprime to ℓ_p , then clearly $\langle m_1 \rangle, \langle m_2 \rangle$ are contained in $\langle m_3 \rangle$. If all these orders are divisible by ℓ_p , we are also done. If some are and some are not, then among the list of orders, there will be a pair with orders $\lambda, \ell_p\lambda$ respectively and so we are done.
- (2) Case 2: $(p-1)/K\ell_p$ is a product of two primes $\ell_0\ell_1$ with $x^\alpha < \ell_0 < \ell_1$. Note that $\ell_0 \leq x^{1/2-\delta}$. If m_1, m_2, m_3 have orders coprime to ℓ_1 , then the group generated by each of them will have order at most $K\ell_0\ell_p \leq 8x^{1/2+\eta-\delta}$ and the Lemma 12 (applied in the rank 1 case) implies that the number of such primes is negligible for $\eta < \delta$ sufficiently small. Thus, the orders of m_1, m_2, m_3 are all divisible by ℓ_1 . Also note that $\ell_0\ell_1$ divides the order of Γ_p for otherwise Γ_p would have index divisible by a prime greater than x^α . So at least one of m_1, m_2, m_3 has order divisible by $\ell_0\ell_1$. Without any loss of generality, suppose that m_3 has order divisible by $\ell_0\ell_1$. Thus, the orders of m_1, m_2, m_3 are divisible by

$$K\ell_0^{n_1}\ell_1, \quad K\ell_0^{n_2}\ell_1, \quad K\ell_0\ell_1, \quad n_1, n_2 \in \{0, 1\}$$

respectively. For each of the four possibilities for (n_1, n_2) , we easily see that at least two of the elements in the above list are identical. Let a, b be such a pair taken from $\{m_1, m_2, m_3\}$. If ℓ_p is coprime to the orders of a, b , then we are done. If ℓ_p divides both the orders, we are also done. If ℓ_p divides only one of them, we are also done in this case too.

Thus, for each prime p in our set, we have shown that $\langle a \rangle \subseteq \langle b \rangle \pmod p$ for at least one pair of elements from $\{m_1, m_2, m_3\}$. As there are only 3 pairs, we see that at least for one pair, the number of primes satisfies the lower bound as claimed. \square

We now state the following corollary.

Corollary 17. *There is at most one prime m_1 such that*

$$\#\{p \leq x : p \in P_{m_1, m_2} \cup P_{m_2, m_1}\} = o\left(\frac{x \log \log x}{\log^2 x}\right)$$

for all primes m_2 distinct from m_1 .

5. Consequences of higher levels of distribution

Theorem 18. *Assume Theorem 9 with a level of distribution x^μ with $\mu > \frac{2}{3}$. Let m_1, m_2 be two multiplicatively independent integers such that $m_1, m_2, -3m_1m_2$ are not perfect squares. Then, there exist elements $a, b \in \{m_1, m_2, -3m_1m_2\}$ such that*

$$\#\{p \leq x : p \in P_{a, b}\} \gg \frac{x \log \log x}{\log^2 x}.$$

Lemma 19. *Assume Theorem 9 with a level of distribution x^μ with $\mu > \frac{2}{3}$. Let $K = 2^k$ for some $k \in \{1, 2, 3\}$. Fix u, v such that $(u, v) = 1, K|(u - 1), 16|v$ and $(\frac{u-1}{K}, v) = 1$. There exists an $\eta > 0, \epsilon_1 > 0$ and a set $\mathcal{T}^*(x, \eta, \epsilon_1)$ of primes $p \leq x$ of size*

$$\gg_{\epsilon_1, \eta} \frac{x \log \log x}{\log^2 x}$$

such that for all $p \in \mathcal{T}^*(x, \eta, \epsilon_1)$, we have:

- (a) $p \equiv u \pmod v$;
- (b) there exists exactly one odd prime $\ell_p \leq x^\eta$ such that $\ell_p|(p - 1)$;
- (c) any odd prime $p_1|(p - 1)$ with $p_1 \neq \ell_p$ satisfies $p_1 > x^\alpha$ with $\alpha = 1/3 + \epsilon_1$;
- (d) $(p - 1)/K\ell_p$ has at most two prime factors.

Proof. The proof of this theorem closely follows that of Lemma 14. Therefore we quickly sketch an outline of the proof here. Let $\mathcal{A}_\ell, \mathcal{P}_\ell$ and $r_{q\ell}$ be as defined in the proof of Lemma 14. We now apply the lower bound sieve in Theorem 8 with $z = x^\alpha$ and $Q = x^\mu$ to deduce

$$S(\mathcal{A}_\ell, \mathcal{P}_\ell, x^\alpha) \geq X \prod_{p \leq x^\alpha, p \nmid v\ell} \left(1 - \frac{1}{p-1}\right) \{f(\mu/\alpha) - \epsilon\} - \sum_{d < L} \sum_{q|P(x^\alpha)} \lambda_d^-(q)r_{q\ell}$$

where the λ_d^- are well-factorable functions of level $Q > x^{\frac{2}{3}}$. Let $\epsilon_1 > 0$ be a sufficiently small constant such that $\frac{2}{3} + 4\epsilon_1 < Q$. We now choose $\mu = \frac{2}{3} + 3\epsilon_1$ and $\alpha = \frac{1}{3} + \epsilon_1$. We may assume that the ϵ in Theorem 8 satisfies

$$f\left(2 + \frac{\epsilon_1}{1/3 + \epsilon_1}\right) > \epsilon.$$

As seen in the Lemma 14, we have

$$\prod_{p \leq x^\alpha, p \nmid v\ell} \left(1 - \frac{1}{p-1}\right) = (1 + o(1)) \frac{2e^{-\gamma}}{\alpha \log x} \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|v\ell} \left(\frac{p-1}{p-2}\right). \tag{12}$$

Now by Theorem 9, for some $\eta > 0$ satisfying

$$\eta < \min \left[\frac{(1 + o(1))2e^{-\gamma}c_1}{4\alpha\phi(v)} \left(f\left(2 + \frac{\epsilon_1}{1/3 + \epsilon_1}\right) - \epsilon \right), \frac{1}{3} + 2\epsilon_1 - \frac{\mu}{2} \right],$$

we get

$$\begin{aligned} \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell; \mathcal{P}_\ell, x^\alpha) &\geq \frac{(1 + o(1))2c_1e^{-\gamma}}{\alpha} \sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} \frac{\text{Li}(x)}{\phi(v)(\ell - 2) \log x} \{f(\mu/\alpha) - \epsilon\} \\ &\quad + O\left(\frac{x}{\log^3 x}\right) \end{aligned}$$

where

$$c_1 = \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|v} \left(\frac{p-1}{p-2}\right).$$

This implies

$$\sum_{\substack{\ell \leq x^\eta \\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell; \mathcal{P}_\ell, x^\alpha) \gg_{\epsilon_1} \frac{\text{Li}(x) \log \log x^\eta}{\phi(v) \log x}. \tag{13}$$

Arguing as before and removing those primes for which $p \equiv 1 \pmod{\ell^2}$ from (13), we now have a set $\mathcal{M}(x, \eta)$ such that for all $p \in \mathcal{M}(x, \eta)$:

- (a) $p \equiv u \pmod v$;
- (b) there exists exactly one odd prime $\ell_p \leq x^\eta$ such that $\ell_p | (p - 1)$;
- (c) any odd prime $p_1 | (p - 1)$ with $p_1 \neq \ell_p$ satisfies $p_1 > x^\alpha$ with $\alpha > 1/3$;
- (d) $(p - 1)/K\ell_p$ has at most two prime factors.

There exists an $\eta > 0$ such that

$$\#\mathcal{M}(x, \eta) \gg_{\epsilon_1, \eta} \frac{\text{Li}(x) \log \log x}{\phi(v) \log x}. \quad \square$$

We recall here Lemma 15 used in the proof of Theorem 1. We apply it again in this context. The proof however is identical and has been omitted.

Lemma 20. *Assume Theorem 9 with a level of distribution x^μ with $\mu > \frac{2}{3}$. With notation as in the previous lemma, there exists a $\delta = \delta(\eta, \epsilon_1)$ such that $0 < \eta < \delta$ and a subset $\mathcal{T}(x, \eta, \epsilon_1)$ of $\mathcal{T}^*(x, \eta, \epsilon_1)$ with size*

$$\gg_{\eta, \epsilon_1} \frac{x \log \log x}{\log^2 x}$$

such that if $p \in \mathcal{T}(x, \eta, \epsilon_1)$ and $(p - 1)/K\ell_p$ has exactly two prime factors $\ell_0 \leq \ell_1$ then $\ell_0 < x^{1/2-\delta}$.

Theorem 21. *Assume Theorem 9 with a level of distribution x^μ with $\mu > \frac{2}{3}$. Let $W = \{m_1, m_2\}$ be a set of two multiplicatively independent integers such that none of $m_1, m_2, -3m_1m_2$ is a perfect square. Then, there is at least one pair of distinct elements $a, b \in \{m_1, m_2, -3m_1m_2\}$ such that*

$$\#\{p \leq x : p \in P_{a,b}\} \gg \frac{x \log \log x}{\log^2 x}.$$

Proof. As seen in the proof of Theorem 16

- there is a v determined by m_1, m_2 and an arithmetic progression $u \pmod v$ such that $-3, m_1, m_2$ are non-residues $\pmod p$ for all $p \equiv u \pmod v$.
- we may further ensure that $(u, v) = 1, K|(u - 1), 16|v$ and $((u - 1)/K, v) = 1$ where $K = 2^k$ with $k = 1, 2$ or 3 .

Let $\mathcal{T}(x, \eta, \epsilon_1)$ be as in Lemma 20. Now consider the multiplicative group Γ generated by $\{m_1, m_2\}$. By Lemma 12, we may assume that the index of the image of Γ in \mathbb{F}_p^* , denoted Γ_p , is not divisible by a prime greater than x^α with $\alpha > 1/3$, by discarding a small set of primes. We now obtain a subset $\mathcal{T}^{**}(x, \eta, \epsilon_1)$ of $\mathcal{T}(x, \eta, \epsilon_1)$ of size

$$\gg_{\epsilon_1, \eta} \frac{x \log \log x}{\log^2 x}$$

such that the index of Γ_p is coprime to $(p - 1)/K\ell_p$. As m_1, m_2 are non-residues (mod p), the orders of each of m_1, m_2 (mod p) are all divisible by K . We consider two cases.

- (1) Case 1: $\lambda := (p - 1)/K\ell_p$ is prime. In this case, by an argument identical to the one presented in the proof of Theorem 1 it follows that

$$\text{either } m_1 \text{ mod } p \in \langle m_2 \rangle \text{ mod } p \quad \text{or} \quad m_2 \text{ mod } p \in \langle m_1 \rangle \text{ mod } p.$$

- (2) Case 2: $(p - 1)/K\ell_p$ is a product of two primes $\ell_0\ell_1$ with $x^\alpha < \ell_0 < \ell_1$. Recall from Lemma 20 that $\ell_0 \leq x^{1/2-\delta}$. Since $K\ell_0\ell_p \leq 8x^{1/2+\eta-\delta}$ (note $\eta < \delta$), an application of Lemma 12 implies that the orders of m_1 and m_2 are divisible by ℓ_1 . Also note that $\ell_0\ell_1$ divides the order of Γ_p so at least one of m_1, m_2 has order divisible by $\ell_0\ell_1$. Without any loss of generality, suppose that m_2 has order divisible by $\ell_0\ell_1$. Thus, the orders of m_1, m_2 are divisible by

$$K\ell_0^m\ell_1, \quad K\ell_0\ell_1, \quad m \in \{0, 1\}$$

respectively. For one of the two possibilities for m , we easily see that both the elements in the above list are identical. In this case, if ℓ_p is coprime to the orders of m_1, m_2 , then we are done. If ℓ_p divides both the orders, we are also done. If ℓ_p divides only one of them, we are also done in this case too. We are now left with the case where the orders of m_1 and m_2 are given by

$$K\ell_p\ell_1 \text{ and } K\ell_0\ell_1.$$

In this case, we consider the element $-3m_1m_2$. Since $-3m_1m_2$ is also a quadratic non-residue modulo p , the order of this element in the group \mathbb{F}_p^* is divisible by K . Further an application of Lemma 12, gives us, for any $\epsilon > 0$

$$\#\{p : \#\langle -3m_1m_2 \rangle \text{ mod } p\} \leq x^{\frac{1}{2}-\epsilon} \ll x^{1-\epsilon}.$$

If the order of $-3m_1m_2$ is not divisible by ℓ_1 then it is atmost $K\ell_0\ell_p \ll x^{\frac{1}{2}-\delta+\eta}$ where $\eta < \delta$. Hence we may assume, by discarding a small set of primes from $\mathcal{T}^{**}(x, \eta, \epsilon_1)$, that the order of $-3m_1m_2$ is divisible by ℓ_1 . The order of $-3m_1m_2$ must therefore be

$$K\ell_1\ell_0^{n_1}\ell_p^{n_2}, \quad n_1, n_2 \in \{0, 1\}.$$

In each of the four cases listed above we see that there exists a pair of distinct elements $a, b \in \{m_1, m_2, -3m_1m_2\}$ such that

$$\#\{p \leq x : p \in P_{a,b}\} \gg \frac{x \log \log x}{\log^2 x}. \quad \square$$

Remark 22. Suppose m_1 and m_2 are multiplicatively independent elements coprime to 6 and congruent to 1 mod 4. By the Chinese remainder theorem and Dirichlet’s theorem on primes in arithmetic progression, we may choose a prime p_0 such that

$$p_0 \equiv 3 \pmod{4} \quad \text{and} \quad \left(\frac{p_0}{m_1}\right) = \left(\frac{p_0}{m_2}\right) = 1.$$

For every prime $\ell \mid m_1 m_2$, let

$$u_\ell = \begin{cases} p_0 & \text{if } \ell \nmid p_0 - 1 \\ 4p_0 & \text{otherwise.} \end{cases}$$

For $\ell = 2$, we set $u_2 = p_0$. Consider the congruences

$$u_\ell \pmod{\ell} \quad \text{for all } \ell \mid m_1 m_2 \quad \text{and} \quad u_2 \pmod{4}.$$

Now there exists a choice of residue class $u \pmod{16m_1 m_2}$ such that $\left(\frac{u-1}{2}, 16m_1 m_2\right) = 1$ and any prime $p \equiv u \pmod{v}$ satisfies

$$\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right) = 1.$$

We may now directly apply Lemma 19 and Lemma 20. Finally we consider the set $\{m_1, m_2, m_1 m_2\}$. Since all the three elements are quadratic residues, none of the orders are divisible by 2 (which is the highest power of 2 dividing $p - 1$ for all $p \in \mathcal{T}(x, \eta, \epsilon_1)$). By Lemma 12 (applied in the rank 1 case) all the orders are divisible by ℓ_1 . By Lemma 12 (applied in the rank 2 case) at least two of the orders are divisible by ℓ_0 . Let two of these elements be denoted by a and b respectively. We now claim

$$\#\{p \leq x : p \in P_{a,b} \cup P_{b,a}\} \gg \frac{x \log \log x}{\log^2 x}.$$

If the orders of both a and b are divisible by ℓ_p or if both are not divisible by ℓ_p , the orders are the same. If only one of them is divisible by ℓ_p , then the orders are $\ell_0 \ell_1 \ell_p$ and $\ell_0 \ell_1$ and the claim holds.

Data availability

No data was used for the research described in the article.

Acknowledgments

We would like to thank Sanoli Gun for suggesting the question. We would also like to thank Sanoli Gun and Purusottam Rath for helpful suggestions and encouragement. It is our pleasure to thank the Chennai Mathematical Institute, the Indian Statistical Institute, Bangalore and the National Board for Higher Mathematics for support. Finally, we are grateful to the referee for her/his suggestions which improved the exposition of the article.

References

- [1] E. Artin, *The Collected Papers of Emil Artin* (S. Lang and J. Tate, Eds.), Addison-Wesley, Reading, Mass., 1965.
- [2] E. Bombieri, J.B. Friedlander, H. Iwaniec, Primes in arithmetic progressions to large moduli, *Acta Math.* 156 (3–4) (1986) 203–251.
- [3] A. Cojocaru, M. Ram Murty, *An Introduction to Sieve Methods and Their Applications*, London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 2005.
- [4] R. Gupta, M. Ram Murty, A remark on Artin’s conjecture, *Invent. Math.* 78 (1) (1984) 127–130.
- [5] D.R. Heath-Brown, Artin’s conjecture for primitive roots, *Quart. J. Math. Oxford Ser. (2)* 37 (145) (1986) 27–38.
- [6] C. Hooley, On Artin’s conjecture, *J. Reine Angew. Math.* 226 (1967) 209–220.
- [7] H. Iwaniec, Rosser’s sieve, *Acta Arith.* 36 (1980) 171–202.
- [8] H. Iwaniec, A new form of the error term in the linear sieve, *Acta Arith.* 37 (1980) 307–320.
- [9] P. Moree, P. Stevenhagen, A two-variable Artin conjecture, *J. Number Theory* 85 (2) (2000) 291–304.
- [10] C.D. Pan, A new mean value theorem and its applications, in: *Recent Progress in Analytic Number Theory*, vol. 1, Academic Press, 1981, pp. 275–287.
- [11] G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. Reine Angew. Math.* 151 (1921) 1–31.
- [12] M. Ram Murty, Artin’s conjecture and elliptic analogues in Sieve Methods, in: G.R.H. Greaves, G. Harman, M.N. Huxley (Eds.), *Exponential Sums, and their Applications in Number Theory*, Cambridge University Press, 1996, pp. 325–344.
- [13] M. Ram Murty, *Problems in Analytic Number Theory*, Graduate Texts in Mathematics, vol. 206, Springer Science and Business Media, 2008.
- [14] M. Ram Murty, F. Séguin, C. Stewart, A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences, *J. Number Theory* 194 (2019) 8–29.