A NOTE ON THE TWO VARIABLE ARTIN'S CONJECTURE.

S. G. HAZRA, M. RAM MURTY AND J. SIVARAMAN

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

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

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)

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

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

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

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

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

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

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

CONTENTS

2020 *Mathematics Subject Classification.* Primary: 11A07, 11N36; Secondary: 11A25, 11A41, 11N13.
Key words and phrases. Primitive roots, Artin's conjecture.
Research of the second author was partially supported by an NSERC Discovery grant.

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 conjectured that the number of primes $p \leqslant x$ such that a is a primitive root modulo p (denoted $N_a(x)$) is asymptotic to

$$C(a)\,\mathrm{Li}(x)$$

where

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

However, calculations later revealed that the conjectured density 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

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

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

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

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

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

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 $p \leqslant x$, 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 $p \leqslant x$ 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 $p \leqslant x$. 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. Artin's conjecture states that given any integer a which is not -1 or a perfect square,

$$\text{there exists an infinite set of primes } \ P_a \ \text{ such that for every}$$
$$b \in \mathbb{Z},\ b \bmod p \in \langle a\rangle \bmod p \cup \{0 \bmod p\} \text{ for all } p \in P_a.$$

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. Given any two multiplicatively independent rational numbers a and b, does there exist

$$P_{a,b}, \ \text{ an infinite set of primes such that } \ b \bmod p \in \langle a\rangle \bmod p \text{ for all } p \in P_{a,b}?$$

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 there exist

$$P_{a,b}, \text{ a set of primes of positive density such that } b \bmod p \in \langle a \bmod p \rangle \text{ for all } p \in P_{a,b}?$$

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

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

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 $|b| \neq 1$

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

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

$$\#\{p \leqslant x : p \text{ prime }, a \bmod p \in \langle b \bmod p \rangle \text{ or } \langle a \bmod p \rangle = \mathbb{F}_p^*\} \gg \frac{x}{\log^2 x}.$$

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

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

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

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

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

Theorem 1. *Let $S = \{m_1, m_2, m_3\}$ 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 $a, b \in S$ such that*

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

As a consequence we now have the following corollary.

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

$$\#\{p \leqslant x : p \text{ prime with } m_1 \bmod p \in \langle m_2 \rangle \bmod p \text{ or } m_2 \bmod p \in \langle m_1 \rangle \bmod p\} = o\left(\frac{x \log\log x}{\log^2 x}\right)$$

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*

$$u_q \equiv a \bmod k \qquad \text{and} \qquad u_q \equiv 1 \bmod q.$$

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

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

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*

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

Suppose we use EH(α) to denote the assumption of a level of distribution of x^α in the Bombieri-Vinogradov theorem, we note that EH(α) 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

$$\begin{aligned} \pi(x) &:= \#\{p \leqslant x : p \text{ prime}\}, \text{ and} \\ \pi(x, d, e) &:= \#\{p \leqslant x : p \text{ prime}, \ p \equiv e \bmod d\}. \end{aligned}$$

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 $z \geqslant 2$ be a real number. We define

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

For q square free we define

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

and choose a function ω_0 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, $\omega(q) = \Pi_{p|q}\omega(p)$. Further, for any square free number q, define

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

We also suppose that

$$\frac{V(z_1)}{V(z_2)} \leqslant \frac{\log z_2}{\log z_1} \left(1 + \frac{C}{\log z_1}\right) \text{ for } z_2 \geqslant z_1 \geqslant 2$$

where C is some constant > 1. We now state the Rosser-Iwaniec upper and lower bound sieves.

Theorem 5. (Rosser - Iwaniec [7], [8]) *Let $0 < \epsilon < \frac{1}{8}$, $2 \leqslant z \leqslant Q^{\frac{1}{2}}$. Under the above notation, we have*

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

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

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

The continuous functions $F(s)$ and $f(s)$ are defined recursively by

$$F(s) = 2e^\gamma/s, \qquad f(s) = 0 \qquad \text{for } s \leqslant 2,$$
$$(sF(s))' = f(s-1), \quad (sf(s))' = F(s-1) \quad \text{for } s > 2,$$

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 6. [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*

$$u_q \equiv a \bmod k \qquad \text{and} \qquad u_q \equiv 1 \bmod q.$$

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

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

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

Theorem 7. [Pan [10]] *Let*

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

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

$$\sum_{n \leqslant x} |f(n)| \ll x \log^{a_1} x, \qquad \sum_{n \leqslant x} \sum_{d|n} |f(d)| \ll x \log^{a_2} x$$

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

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

and $0 < \epsilon < 1$.

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

Lemma 8. (Gupta and Ram Murty [4], Ram Murty [12]) *Suppose that $\{q_1, \ldots, q_n\}$ 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 $\Gamma_p = \{b \bmod p : b \in \Gamma\}$. Then*

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

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 9. *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 $\left(\frac{u-1}{K}, v\right) = 1$. There exists an $\eta > 0$ and a set $\mathcal{T}^*(x,\eta)$ of primes $p \leqslant x$ 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) $p \equiv u \bmod v$;
(b) *there exists exactly one odd prime $\ell_p \leqslant x^\eta$ 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. Fix a prime $\ell \leqslant x^\eta$, where η is a positive quantity to be chosen later. Define

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

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

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

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

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

where $X = \frac{\mathrm{Li}(x)}{\phi(v\ell)}$ and

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

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 5 with $z = x^\alpha$ and $Q = x^\mu$ to deduce

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

where the λ_d^- are well-factorable functions of level $Q = x^\mu$ in Theorem 6. We choose $\mu = \frac{4}{7} - \epsilon_1$ and $\alpha = 1/4 + \epsilon_2$. By the argument on Page 33 of [5], we have

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

We now sum over all odd primes $\ell \leqslant x^\eta$. Let us first consider the inner sum of the second term in (1), on summing over all $\ell \leqslant x^\eta$ we get

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

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

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

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

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

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_1Q_2, it suffices to show that $\mathbf{1}_{p\leqslant x^\eta}$ 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 $M \geqslant x^\eta$. This implies that

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

where $\delta(b)$ is 1 iff $b = 1$ and zero otherwise. Now by Theorem 6, for some $\eta > 0$ satisfying $\mu + 2\eta < 4/7$, we get

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

where

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

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

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

This implies

$$\sum_{\substack{\ell \leqslant x^{\eta} \\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell; \mathcal{P}_\ell, x^{\alpha}) \geqslant \frac{(1+o(1))2c_1 e^{-\gamma} \operatorname{Li}(x) \log\log x^{\eta}}{\alpha \phi(v) \log x} \{f(4/7\alpha) - 2\epsilon\}. \tag{3}$$

We now note that if we consider for a prime $\ell \leqslant x^{\eta}$, then

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

We have for $(q, v\ell) = 1$,

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

and

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

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

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

We now apply the upper bound Rosser-Iwaniec sieve Theorem 5 with $z = Q = x^{\mu}$, to get

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

Summing over $\ell \leqslant x^{\eta}$ for the same η as before and arguing as before in the lower bound, we get by Theorem 6

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

By (2), we get

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

Removing these primes from our enumeration in (3), we now have a set $\mathcal{S}(x, \eta)$ such that for all $p \in \mathcal{S}(x, \eta)$:

(a) $p \equiv u \bmod v$;
(b) there exists exactly one odd prime $\ell_p \leqslant x^{\eta}$ 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 three prime factors.

There exists an $\eta > 0$ such that

$$\#S(x, \eta) \geqslant \frac{(1+o(1))2e^{-\gamma} c_1 \operatorname{Li}(x) \log\log x^{\eta}}{\alpha \phi(v) \log x} \{f(4/7\alpha) - 2\epsilon\}.$$

We now use the Chen-Iwaniec switching method to remove those primes with exactly three prime factors. To this end, we apply the upper bound sieve as indicated in Theorem 5. Let

$$\mathcal{B}_\ell = \Big\{1 + K\ell p_1p_2p_3 \leqslant x : \quad p_i \geqslant x^\alpha, \quad 1 + K\ell p_1p_2p_3 \equiv u \bmod v\Big\}.$$

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

$$\#\mathcal{B}_{\ell q} = \#\{b \in \mathcal{B}_\ell : q|b\} = \#\{p_1p_2p_3 \leqslant y : \quad p_i \geqslant x^\alpha, \quad p_1p_2p_3 \equiv t_q \bmod qv/K\},$$

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

$$K\ell t_q + 1 \equiv u \bmod v, \qquad K\ell t_q + 1 \equiv 0 \bmod q. \tag{4}$$

Let

$$g_\ell(a) = \#\{\ell p_2p_3 = a \ : \ p_2, p_3 \geqslant x^\alpha\}.$$

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

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

Further for any prime q co-prime to ℓv,

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

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

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

with

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

By partial summation and the prime number theorem, we have

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

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

$$\sum_{\substack{a \leqslant y\ell x^{-\alpha} \\ (a, qv/K)=1}} g_\ell(a)(\pi(y\ell/a) - \pi(x^\alpha)) \quad \sim \quad \int_{x^\alpha}^{y\ell/2} \frac{dz}{\log z} \int_{x^\alpha}^{y/(zx^\alpha)} \int_{x^\alpha}^{y/(p_2z)} \frac{dp_2dp_3}{\log p_2 \log p_3}.$$

Changing the order of integration

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

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

$$\begin{aligned}\sum_{\substack{a\leqslant y\ell x^{-\alpha}\\(a,qv/K)=1}} g_\ell(a)(\pi(y\ell/a)-\pi(x^\alpha)) &\sim \int_\alpha^{1-2\alpha-\log_x\ell}\frac{p_2d\theta}{\theta}\int_\alpha^{1-\alpha-\theta-\log_x\ell}\frac{p_3d\psi}{\psi}\cdot\frac{y/(p_2p_3)}{\log(y/(p_2p_3))}\\ &\sim \frac{y}{\log x}\int_\alpha^{1-2\alpha-\log_x\ell}\int_\alpha^{1-\alpha-\theta-\log_x\ell}\frac{d\theta d\psi}{\theta\psi}\cdot\frac{1}{1-\theta-\psi-\log_x\ell}.\end{aligned}$$

$$X\sim\frac{y}{\phi(v/K)\log x}\int_\alpha^{1-2\alpha-\log_x\ell}\int_\alpha^{1-\alpha-\theta-\log_x\ell}\frac{d\theta d\psi}{\theta\psi}\cdot\frac{1}{1-\theta-\psi-\log_x\ell}=I^*\frac{x/\ell}{\phi(v)\log x}$$

where

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

Now consider the integral

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

Therefore

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

Similarly if we consider

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

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

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

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 5) for $z=y^{1/2-\epsilon_3}$ we have

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

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

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

Therefore we now need to estimate

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

We now observe that the hypothesis of Theorem 7 holds for $f(n) = d_3(n)$ (see Exercise 2.5.1, page 29 of [13]) By Theorem 7 , we have for $\ell \leqslant x^{\eta}$,

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

For the other sum, we get

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

Now summing over the primes $\ell \leqslant x^{\eta}$, we get

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

For the main term of the upper bound, we get

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

Therefore, we have

$$\sum_{\ell\leqslant x^{\eta}} \left\{S(\mathcal{A}_\ell,\mathcal{P}_\ell,x^{\alpha}) - \frac{1}{6}S(\mathcal{B}_\ell,\mathcal{P}_\ell,x^{1/2-\epsilon_3})\right\} \geqslant c_1(1+o(1))e^{-\gamma}\frac{x\log\log x^{\eta}}{\phi(v)\log^2 x}\left(2\alpha^{-1}f\left(\frac{4}{7\alpha}\right) - \frac{4}{3}(I+\mathrm{O}(\eta))F(1)\right),$$

and for η suffciently small

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

Since $f(u) = 2e^{\gamma}u^{-1}\log(u-1)$ for $2 \leqslant u \leqslant 4$, we get a lower bound of

$$\geqslant c_1(1+o(1))\frac{x\log\log x^{\eta}}{\log^2 x}\left(7\log\left(\frac{4}{7\alpha}-1\right) - \frac{8}{3}(I+\mathrm{O}(\eta))\right) \geqslant (0.225+\mathrm{O}(\eta))c_1(1+o(1))\frac{x\log\log x^{\eta}}{\log^2 x}$$

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

4. Proof of Theorem 1

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

Lemma 10. *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 $\ell_0 \leqslant \ell_1$ then, $\ell_0 < x^{1/2-\delta}$.

Proof. Clearly $\ell_0^2 \leqslant x$. Fix $\ell < x^{\eta}$ and $x^{1/2-\delta} < \ell_0 \leqslant x^{1/2}$. By Brun's sieve, the number of primes $p \equiv 1 \bmod K\ell\ell_0$ 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 $\ell \leqslant x^{\eta}$ and ℓ_0 satisfying $x^{1/2-\delta} \leqslant \ell_0 < x^{1/2}$. 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. □

Theorem 11. *Let $S = \{m_1, m_2, m_3\}$ 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 $a, b \in S$ such that*

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

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 (mod p) (see section 5 of [5]). The argument further ensures that such a class, denoted $u \bmod v$ 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 10. 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 8, the number of such primes is $O(x^{4(1-\alpha)/3})$ 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 $\mathcal{T}(x,\eta)$ wth 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 (mod p), the orders of each of m_1, m_2, m_3 (mod 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 8 the number of such primes is $O(x^{2\eta})$ which we can ignore when η is suffficiently 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 $\ell_0 \leqslant x^{1/2-\delta}$. 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 $K\ell_0\ell_p \leqslant 8x^{1/2+\eta-\delta}$ and the Lemma 8 (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

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

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 $\langle a\rangle \subseteq \langle b\rangle \bmod p$ 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. □

We now state the following corollary.

Corollary 12. *There is at most one prime m_1 such that*

$$\#\{p \leqslant x : p \text{ prime with } m_1 \bmod p \in \langle m_2\rangle \bmod p \text{ or } m_2 \bmod p \in \langle m_1\rangle \bmod p\} = o\left(\frac{x\log\log x}{\log^2 x}\right)$$

for all primes m_2 distinct from m_1.

5. Consequences of higher levels of distribution

Theorem 13. *Assume Theorem 6 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*

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

Lemma 14. *Assume Theorem 6 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 $\left(\frac{u-1}{K}, v\right) = 1$. There exists an $\eta > 0, \epsilon_1 > 0$ and a set $\mathcal{T}^*(x, \eta, \epsilon_1)$ of primes $p \leqslant x$ 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) $p \equiv u \bmod v$;
(b) *there exists exactly one odd prime $\ell_p \leqslant x^\eta$ 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 9. 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 9. We now apply the lower bound sieve in Theorem 5 with $z = x^\alpha$ and $Q = x^\mu$ to deduce

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

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 5 satisfies

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

As seen in the Lemma 9, we have

$$\prod_{p \leqslant x^\alpha, p \nmid v\ell} \left(1 - \frac{1}{p-1}\right) = (1 + o(1)) \frac{2e^{-\gamma}}{\alpha \log x} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|v\ell} \left(\frac{p-1}{p-2}\right). \tag{5}$$

Now by Theorem 6, 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

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

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

$$\sum_{\substack{\ell\leqslant x^{\eta}\\ \ell \text{ odd prime}}} S(\mathcal{A}_\ell;\mathcal{P}_\ell,x^{\alpha}) \gg_{\epsilon_1} \frac{\mathrm{Li}(x)\log\log x^{\eta}}{\phi(v)\log x}. \tag{6}$$

Arguing as before and removing those primes for which $p\equiv 1 \bmod \ell^2$ from (6), we now have a set $\mathcal{S}(x,\eta)$ such that for all $p\in\mathcal{S}(x,\eta)$:

(a) $p\equiv u \bmod v$;
(b) there exists exactly one odd prime $\ell_p\leqslant x^{\eta}$ 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

$$\#S(x,\eta)\gg_{\epsilon_1,\eta}\frac{\mathrm{Li}(x)\log\log x}{\phi(v)\log x}.$$

□

We recall here Lemma 10 used in the proof of Theorem 1. We apply it again in this context. The proof however is identical and has been omitted.

Lemma 15. *Assume Theorem 6 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 $\ell_0\leqslant\ell_1$ then $\ell_0<x^{1/2-\delta}$.

Theorem 16. *Assume Theorem 6 with a level of distribution x^{μ} with $\mu>\frac{2}{3}$. Let $S=\{m_1,m_2\}$ 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*

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

Proof. As seen in the proof of Theorem 11

- 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 (mod p) for all $p \equiv u \bmod v$.
- 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 15. Now consider the multiplicative group Γ generated by $\{m_1, m_2\}$. By Lemma 8, 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

$$\text{either} \qquad m_1 \bmod p \in \langle m_2 \rangle \bmod p \qquad \text{or} \qquad m_2 \bmod p \in \langle m_1 \rangle \bmod p.$$

(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 15 that $\ell_0 \leqslant x^{1/2-\delta}$. Since $K\ell_0\ell_p \leqslant 8x^{1/2+\eta-\delta}$ (note $\eta < \delta$), an application of Lemma 8 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

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

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 8, gives us, for any $\epsilon > 0$

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

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

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

□

Remark 17. *Suppose m_1 and m_2 are multiplicatively independent elements coprime to 6 and congruent to $1 \bmod 4$. By the Chinese remainder theorem and Dirichlet's theorem on primes in arithmetic progression, we may choose a prime p_0 such that*

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

For every prime $\ell \mid m_1m_2$, 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

$$u_\ell \bmod \ell \text{ for all } \ell \mid m_1m_2 \text{ and } u_2 \bmod 4.$$

Now there exists a choice of residue class $u \bmod 16m_1m_2$ such that $(\frac{u-1}{2}, 16m_1m_2) = 1$ and any prime $p \equiv u \bmod v$ satisfies

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

We may now directly apply Lemma 14 and Lemma 15. Finally we consider the set $\{m_1, m_2, m_1m_2\}$. 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 8 (applied in the rank 1 case) all the orders are divisble by ℓ_1. By Lemma 8 (applied in the rank 2 case) atleast two of the orders are divisible by ℓ_0. Let two of these elements be denoted by a and b respectively. We now claim

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

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.

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.

REFERENCES

[1] E. Artin, The Collected Papers of Emil Artin (S. Lang and J. Tate, Eds.), *Reading, Mass.: Addison- Wesley* (1965).

[2] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. **156** (1986), no. 3-4, 203–251.

[3] A. Cojocaru and M. Ram Murty, An Introduction to Sieve Methods and Their Applications, London Mathematical Society Student Texts, *Cambridge: Cambridge University Press* (2005).

[4] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130.

[5] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2), **37** (1986), no. 145, 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 and P. Stevenhagen, *A two-variable Artin conjecture*, J. Number Theory, **85** (2000), no. 2, 291-304.

[10] C. D. Pan, *A new mean value theorem and its applications*, Recent Progress in Analytic Number Theory, **1**, Academic Press, (1981), 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*, Exponential Sums, and their Applications in Number Theory, (eds. G.R.H. Greaves, G. Harman, and M.N. Huxley), Cambridge University Press, (1996), 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 and C. Stewart, *A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences*, J. Number Theory, **194** (2019), 8-29.

[15] J. Sivaraman, *Primitive roots for Pjateckiĭ-Šapiro primes*, J. Théor. Nombres Bordeaux **33** (2021), no. 1, 83–94.

[16] P. J. Stephens, *Prime divisors of second order linear recurrences*, J. Number Theory, **8** (1976), 313–332.

(S. G. Hazra) CHENNAI MATHEMATICAL INSTITUTE, H1, SIPCOT IT PARK, SIRUSERI, KELAMBAKKAM, 603103, INDIA.

(M. Ram Murty) DEPARTMENT OF MATHEMATICS, JEFFERY HALL, 99 UNIVERSITY AVENUE, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO, K7L 3N6, CANADA.

(J. Sivaraman) STATISTICS AND MATHEMATICS UNIT, INDIAN STATISTICAL INSTITUTE, 8TH MILE, MYSORE RD, RVCE POST, BENGALURU, KARNATAKA 560059

Email address: suhita@cmi.ac.in

Email address: murty@queensu.ca

Email address: jyothsnaa.s@gmail.com