

# ON A CONJECTURE OF ERDŐS

ADAM TYLER FELIX AND M. RAM MURTY

ABSTRACT. Let  $a$  be an integer different from 0,  $\pm 1$ , or a perfect square. We consider a conjecture of Erdős, which states that  $\#\{p : \ell_a(p) = r\} \ll_\varepsilon r^\varepsilon$  for any  $\varepsilon > 0$  where  $\ell_a(p)$  is the order of  $a$  modulo  $p$ . In particular, we see what this conjecture says about Artin's primitive root conjecture and compare it to the generalized Riemann hypothesis and the ABC conjecture. We also extend work of Goldfeld related to divisors of  $p + a$  and the order of  $a$  modulo  $p$ .

## 1. INTRODUCTION

Let  $p$  be a prime number. We know that  $(\mathbb{Z}/p\mathbb{Z})^* = \langle \bar{a} \rangle$  for  $\varphi(p-1)$  such  $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$  where  $\varphi(n)$  is the Euler totient function. When  $(\mathbb{Z}/p\mathbb{Z})^* = \langle \bar{a} \rangle$  we say that  $a$  is a **primitive root** modulo  $p$ . In 1927, Artin asked a similar question: let  $a$  be a non-zero integer which is not  $\pm 1$  or a square, and define

$$N_a(x) := \#\{p \leq x : (\mathbb{Z}/p\mathbb{Z})^* = \langle \bar{a} \rangle\} = \#\{p \leq x : a \text{ is a primitive root modulo } p\}.$$

Artin asked: what is the growth of  $N_a(x)$  as  $x \rightarrow \infty$ ? He conjectured that

$$(1) \quad N_a(x) \sim A(a)\pi(x),$$

where  $A(a) > 0$  is a constant and  $\pi(x) = \#\{p \leq x : p \text{ is prime}\}$ .

In 1967, Hooley [7] was able to prove the following theorem:

**Theorem 1.1** (Hooley). *Assume GRH holds for the Dedekind zeta-functions of Kummer fields  $\mathbb{Q}(\zeta_n, a^{1/n})$ , where  $\zeta_n$  is a primitive  $n^{\text{th}}$ -root of unity. Then,*

$$(2) \quad N_a(x) = A(a)\pi(x) + O\left(\frac{x \log \log x}{(\log x)^2}\right).$$

It should be noted that  $A(a)$  in equation (1) is not always the same  $A(a)$  in equation (2). This original insight is due to work of D. H. Lehmer.

The best unconditional results about Artin's conjecture are due to Gupta and Murty [5], and Heath-Brown [6] and are of the following nature:

**Theorem 1.2** (Heath-Brown, Gupta and Murty). *One of 2, 3, or 5 is a primitive root modulo  $p$  for infinitely many primes  $p$ .*

---

1991 *Mathematics Subject Classification.* 11N13, 11N56, 11N64.

*Key words and phrases.* primes in arithmetic progression, Artin's conjecture, the order of  $a$  modulo  $p$ .

Research of the first author supported by an NSERC PGS-D.

Research of the second author supported by an NSERC Discovery Grant.

In fact, they have shown that there exists some positive constant  $c$  such that

$$\#\{p \leq x : a \text{ is a primitive root modulo } p\} \geq \frac{cx}{(\log x)^2}$$

where  $a$  is one of 2, 3, or 5.

For  $p \nmid a$ , define

$$\ell_a(p) := \min\{n \in \mathbb{N} : a^n \equiv 1 \pmod{p}\} = |\langle a \pmod{p} \rangle|.$$

We call  $\ell_a(p)$  the **order of  $a$  modulo  $p$** .

Let  $A_a(x, \delta) := \#\{p \leq x : \ell_a(p) > p^\delta\}$  and  $E_a(r) = \#\{p : \ell_a(p) = r\}$ . In 1971, P. Bundschuh [9] proved the following:

$$E_2(r) \leq \frac{r \log 2}{\log r}$$

and for  $\delta < 1/2$ ,

$$A_2(x, \delta) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

and

$$A_2\left(x, \frac{1}{2}\right) \geq (1 - \log 2) \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Bundschuh's techniques can easily be extended to show

$$E_a(r) \leq \frac{r \log a}{\log r}$$

and

$$A_a(x, \delta) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

assuming  $\delta < 1/2$ . The reason his techniques cannot be extended for  $A_a(x, 1/2)$  is  $\log a > 1$  for  $a > 2$ , and this fact is crucial in his proofs.

In 1976, Erdős [2] improved upon this result. Erdős was able to show:

**Theorem 1.3** (Erdős). *As  $x \rightarrow \infty$ , we have*

$$A_2\left(x, \frac{1}{2}\right) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

In order to prove this, Erdős needed a better result for  $E_2(r)$ . He showed

$$(3) \quad E_2(r) \leq \left(\frac{1}{2} + o(1)\right) \frac{r \log 2}{\log r}$$

as  $r \rightarrow \infty$ .

Unlike Bundschuh, Erdős's techniques can be used to prove similar bounds for any  $a$ . To see this let's consider  $2^r - 1$ . Write

$$2^r - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{E_2(r)}^{\alpha_{E_2(r)}} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$$

where  $\ell_a(p_i) = r$  and  $\ell_a(q_j) < r$ . Bundschuh made the observation that  $p_i > r$  while Erdős made the observation that  $p_i \equiv 1 \pmod{r}$ , and so, after rearranging  $p_i$ , we have  $p_i > ir$ . This

new observation allows for better control of  $E_2(r)$  by using Stirling's formula, and hence, we can better control  $A_2(x, 1/2)$ . The  $\log 2$  in Equation (3) is dealt with by an appropriate choice of  $\varepsilon$ , and as such,  $\log a$  is of no worry in

$$E_a(r) \leq \left( \frac{1}{2} + o(1) \right) \frac{r \log a}{\log r}.$$

In [2], Erdős made many conjectures related to  $\ell_a(p)$ . The following conjecture is of interest to this article:

**Conjecture** (Erdős's Conjecture). For every  $\varepsilon > 0$ , there exists a constant  $C := C(\varepsilon) > 0$  and an  $r_0 := r_0(\varepsilon) \geq 1$  such that  $E_2(r) \leq Cr^\varepsilon$  for all  $r \geq r_0$ .

Using Vinogradov notation, we can write for every  $\varepsilon > 0$ ,  $E_2(r) \ll_\varepsilon r^\varepsilon$ , where the  $\ll_\varepsilon$  may become  $\ll$  for convenience. For our purposes, we will also assume  $E_a(r) \ll_\varepsilon r^\varepsilon$ . In §5, we refer to this conjecture as Erdős's first conjecture.

We will prove the following theorems.

**Theorem 1.4.** *Let  $a \in \mathbb{Z}$  with  $a \neq 0, \pm 1$  or a perfect square. Suppose Erdős's conjecture holds for  $a$ . Then, there exist infinitely many primes  $p$  for which  $a$  is a primitive root modulo  $p$ .*

In fact, we will show that there are at least  $\gg \frac{x}{(\log x)^2}$  primes  $p \leq x$  which satisfy  $a$  being a primitive root modulo  $p$ .

We call the following statement the **quasi-Riemann hypothesis**: for  $K$  an algebraic number field with Dedekind zeta-function  $\zeta_K(s)$ , there exists some  $\varepsilon \in (0, 1/2]$  such that if  $\Re(s) > 1 - \varepsilon$ , then  $\zeta_K(s) \neq 0$ .

**Theorem 1.5.** *Let  $a \in \mathbb{Z}$  with  $a \neq 0, \pm 1$  or a perfect square. Suppose the quasi-Riemann hypothesis holds for all Kummer fields  $\mathbb{Q}(\zeta_n, a^{1/n})$  for  $n$  prime. Suppose Erdős's conjecture holds for  $a$ . Then,*

$$N_a(x) = A(a) \frac{x}{\log x} + O\left(\frac{x \log \log x}{(\log x)^2}\right).$$

Define  $\text{li}(x) := \int_2^x (\log t)^{-1} dt$ . Using this function, we prove:

**Theorem 1.6.** *Let  $a$  be an integer different from  $0, \pm 1$ . Suppose the quasi-Riemann hypothesis holds for all Kummer fields  $\mathbb{Q}(\zeta_n, a^{1/n})$ . Suppose Erdős's conjecture holds for  $a$ . Then,*

$$\sum_{p \leq x} \log(i_a(p)) = c_a \text{li}(x) + O(x^{1-\frac{\varepsilon}{2}+\theta})$$

for any  $\theta > 0$  and where  $c_a$  is an effectively computable constant and  $\varepsilon \in (0, 1/2]$  is fixed such that if  $\Re(s) > 1 - \varepsilon$ , then  $\zeta_K(s) \neq 0$  with  $K$  ranging over the fields  $\mathbb{Q}(\zeta_n, a^{1/n})$  with  $n \in \mathbb{N}$ .

A weaker version of Theorem 1.6 using some stronger assumptions was proved by Fomenko [3]. In order to state his theorem, we first need to state a conjecture of Hooley [8, Page 112]:

**Conjecture** (Conjecture A of Hooley). Let  $P_b(y; \ell, t)$  be the number of primes  $p \leq y$  such that  $2^t b$  is an  $\ell^{\text{th}}$ -power residue modulo  $p$  and for which  $\ell | p - 1$ . Then, for  $y^{1/4} < \ell < y$ , we have

$$P_b(y; \ell, t) \ll \frac{y}{\varphi(\ell)(\log(2y/\ell))^2}$$

where the implied constant is absolute.

Then, Fomenko showed the following:

**Theorem 1.7** (Fomenko). *Suppose the generalized Riemann hypothesis holds for Dedekind zeta functions for fields of type  $\mathbb{Q}(a^{1/k}, \zeta_k)$  where  $\zeta_k$  is a  $k^{\text{th}}$  root of unity where  $k$  ranges over prime powers. Suppose further Conjecture A of Hooley holds. Then,*

$$\sum_{p \leq x} \log(i_a(p)) = c_a \text{li}(x) + O\left(\frac{x \log \log x}{(\log x)^2}\right)$$

where  $c_a$  is an effectively computable constant dependent on  $a$ .

The proofs of Theorems 1.5 and 1.6 will follow [7] in many aspects.

## 2. PROOF OF THEOREM 1.4

Before we can prove Theorem 1.4 we need the following result of Gupta and Murty [5]. For a fixed  $\alpha > 0$ , define

$$P_r(\alpha) := \{n \in \mathbb{N} : n \text{ is prime or } \Omega(n) \leq r \text{ and if } p|n, \text{ then } p \geq n^\alpha\}$$

where  $\Omega(n)$  is the number of prime factors of  $n$  counted with multiplicity.

**Proposition 2.1.** (Gupta and Murty) *Let  $a$  be a non-zero integer different from 0,  $\pm 1$  or a perfect square. Then, there exists  $\alpha \in (\frac{1}{4}, \frac{1}{2})$  such that*

$$A(x) := \#\left\{p \leq x : \ell_a(p) \neq \frac{p-1}{2} \in P_2(\alpha)\right\} \gg \frac{x}{(\log x)^2}.$$

This result is established using techniques developed by Bombieri, Friedlander, and Iwaniec [1].

To see how this result coupled with Erdős's conjecture yields Theorem 1.4, let us consider

$$B(x) = \#\left\{p \in \mathcal{A}(x) : \ell_a(p) < \frac{p-1}{2}\right\},$$

where  $\mathcal{A}(x)$  is the underlying set corresponding to  $A(x)$ . We are going to show that  $B(x) \ll x^\delta$  for some  $0 < \delta < 1$ .

If the prime number  $p$  contributes to  $B(x)$ , then  $p-1 = 2q_1 q_2$  is the prime factorization of

$p - 1$ . Since  $\ell_a(p) < \frac{p-1}{2}$ , we have  $\ell_a(p) \leq x^{\frac{3}{4}}$ . Hence, by Erdős's conjecture, we have

$$\begin{aligned} B(x) &\leq \sum_{r < x^{\frac{3}{4}}} \#\{p : \ell_a(p) = r\} \\ &\ll \sum_{r < x^{\frac{3}{4}}} r^\varepsilon \leq x^{\frac{3(1+\varepsilon)}{4}}. \end{aligned}$$

Choosing  $\varepsilon < \frac{1}{3}$  gives us  $B(x) \ll x^\delta$  for some  $\delta < 1$ . Thus,  $B(x) = o(x/(\log x)^2)$ . Since no element of  $\mathcal{A}(x)$  has  $\ell_a(p) = \frac{p-1}{2}$ , we have

$$\#\{p \in \mathcal{A}(x) : \ell_a(p) = p - 1\} \geq \frac{Cx}{(\log x)^2} + O_\varepsilon(x^\delta)$$

by Proposition 2.1. That is, the number of primes of  $p \leq x$  for which  $a$  is a primitive root modulo  $p$  is at least  $\frac{Cx}{(\log x)^2}$  for sufficiently large  $x$ , and hence, Theorem 1.4 holds.

### 3. PROOFS OF THEOREM 1.5 AND 1.6

**3.1. Proof of Theorem 1.5.** Following the argument of Hooley [7], for any prime  $q$  define  $L_q := \mathbb{Q}\left(a^{\frac{1}{q}}, \zeta_q\right)$  where  $\zeta_q$  is a primitive  $q^{\text{th}}$  root of unity. For any squarefree  $k \in \mathbb{N}$ , define  $L_k$  to be the smallest field containing  $L_q$  for all primes  $q$  which divide  $k$ . For  $q$  prime, define  $\Pi_q$  to be the set of primes which split completely in  $L_q$ , and for squarefree  $k$ , define

$$\pi_k(x) := \#\left\{p \leq x : p \in \bigcap_{q|k} \Pi_q\right\}.$$

Recall  $N_a(x)$  is the number of primes  $p \leq x$  for which  $a$  is a primitive root modulo  $p$ . We have

$$N_a(x) \leq \sum_{d|k} \mu(d) \pi_d(x)$$

where  $k = \prod_{p < z} p$  for some  $z$  to be specified later.

Also, if we define

$$M(x; z, w) := \#\left\{p \leq x : \exists q \in (z, w) \text{ with } p \equiv 1 \pmod{q}, \text{ and } a^{\frac{p-1}{q}} \equiv 1 \pmod{p}\right\},$$

then clearly

$$N_a(x) \geq \sum_{d|k} \mu(d) \pi_d(x) - M(x; z, x).$$

For  $z = (\log x)^\eta$  for some fixed  $\eta > 0$ , we have

$$\sum_{d|k} \mu(d) \pi_d(x) = A(a) \text{li}(x) + o(\text{li}(x))$$

using techniques from Hooley [7] and the effective Chebotarev Density Theorem of Lagarias and Odlyzko [10]: for any  $d$  squarefree, we have

$$\pi_d(x) = \frac{\text{li}(x)}{[L_d : \mathbb{Q}]} + O\left(x \exp\left(-\kappa \sqrt{\frac{\log x}{[L_d : \mathbb{Q}]}}\right)\right)$$

for some fixed constant  $\kappa > 0$ . Here we would also need to assume  $\eta \leq 1/7$  to ensure that a potential exceptional zero ( $\beta_0$  in [10]) does not contribute significantly to the error term. Hooley [7] has shown that  $[L_d : \mathbb{Q}] \asymp d\varphi(d)$ .

We note that  $M(x; z, x) \leq M(x; z, x^\varepsilon) + M(x; x^\varepsilon, x)$ . In fact, if the prime number  $p \leq x$  contributes to  $M(x; x^\varepsilon, x)$ , then clearly  $\ell_a(p) < x^{1-\varepsilon}$ . So,

$$\begin{aligned} M(x; x^\varepsilon, x) &\leq \#\{p \leq x : \ell_a(p) < x^{1-\varepsilon}\} \\ &\leq \sum_{r < x^{1-\varepsilon}} \#\{p : \ell_a(p) = r\} \\ &\leq (x^{\varepsilon_1}) \sum_{r < x^{1-\varepsilon}} 1 \leq x^{1-\varepsilon_2}. \end{aligned}$$

for some  $0 < \varepsilon_2 < 1$  by Erdős's conjecture.

So, since  $x^{1-\varepsilon_2} = o(\text{li}(x))$ , if we can show that  $M(x; z, x^\varepsilon) = o(\text{li}(x))$ , then Theorem 1.5 will follow. This is where we employ a quasi-Riemann hypothesis. The quasi-generalized Riemann hypothesis that we will be using is the following. There exists  $\theta \in [\frac{1}{2}, 1)$  such that the Dedekind zeta functions for every field  $\mathbb{Q}(\zeta_d, a^{1/d})$  as  $d$  ranges over the squarefree positive integers have no zeros in the region  $\Re(s) > \theta$ . This has the following implication:

$$\pi_d(x) = \frac{\text{li}(x)}{[L_d : \mathbb{Q}]} + O(x^\theta \log d a x).$$

Using this instead of the generalized Riemann hypothesis will give us the result. To see this note

$$\begin{aligned} M(x; z, x^\varepsilon) &\leq \sum_{z < q < x^\varepsilon} \pi_q(x) \\ &\ll \sum_{z < q < x^\varepsilon} \left( \frac{\text{li}(x)}{q(q-1)} + x^\theta \log q a x \right) \\ &\leq \sum_{q > z} \frac{\text{li}(x)}{q(q-1)} + \sum_{q < x^\varepsilon} x^\theta \log q a x. \end{aligned}$$

Since  $z \rightarrow \infty$  as  $x \rightarrow \infty$  and since

$$\sum_{q \geq 2} \frac{1}{q(q-1)} < \infty,$$

we have

$$\sum_{q > z} \frac{\text{li}(x)}{q(q-1)} = o(\text{li}(x)).$$

Also, since Erdős's conjecture holds for all  $\varepsilon > 0$ , choose  $\varepsilon > 0$  such that  $\theta + \varepsilon < 1$ . Then, we have

$$\begin{aligned} \sum_{q < x^\varepsilon} x^\theta \log q a x &\ll_{\varepsilon, a} x^\theta \log x \sum_{q < x^\varepsilon} 1 \\ &\ll_{\varepsilon, a} x^{\theta + \varepsilon} = o(\text{li}(x)). \end{aligned}$$

Hence, Theorem 1.5 holds.

**3.2. Proof of Theorem 1.6.** We have

$$\sum_{p \leq x} \log(i_a(p)) = \sum_{d \leq x} \Lambda(d) \pi_d(x) = \sum_{d \leq x^\delta} \Lambda(d) \pi_d(x) + \sum_{x^\delta < d \leq x} \Lambda(d) \pi_d(x)$$

for some  $\delta \in (0, \varepsilon)$  to be chosen later and

$$\pi_d(x) := \#\{p \leq x : d | i_a(p)\}.$$

Now, the quasi-Riemann hypothesis implies

$$\pi_d(x) = \frac{\text{li}(x)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]} + O(x^{1-\varepsilon} \log(dx)).$$

Hooley [7, Equation (12)] has shown  $[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}] \asymp n\varphi(n)$  for  $n$  squarefree. For generic  $n \in \mathbb{N}$ , see [15, Proposition 4.1]. It can be shown that

$$\sum_{d \leq y} \Lambda(d) \ll y$$

by the prime number theorem or Chebychev's theorem. Thus,

$$\begin{aligned} \sum_{d \leq x^\delta} \Lambda(d) \pi_d(x) &= \text{li}(x) \sum_{d \leq x^\delta} \frac{\Lambda(d)}{[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]} + O\left(x^{1-\varepsilon} \log x \sum_{d \leq x^\delta} \Lambda(d)\right) \\ &= c_a \text{li}(x) + O(x^{1-\delta}) + O(x^{1-\varepsilon+\delta} \log x). \end{aligned}$$

We note that

$$\sum_{x^\delta < q \leq x} \pi_q(x) \ll \#\{p \leq x : f_a(p) < x^{1-\delta}\}.$$

To see this, we suppose that the prime number  $p$  contributes to the left-hand summation  $n$  times. Therefore, there exist  $q_1, q_2, \dots, q_n \in (x^\delta, x]$  such that  $q_i | i_a(p)$ . Hence,

$$x^{n\delta} < q_1 q_2 \cdots q_n \leq i_a(p) < x.$$

Therefore,  $n \leq \delta^{-1}$ .

Thus,

$$\sum_{x^\delta < q \leq x} \pi_q(x) \ll \#\{p \leq x : f_a(p) < x^{1-\delta}\}.$$

We also have

$$\begin{aligned} \sum_{\substack{x^\delta < q^\alpha \leq x \\ \alpha \geq 2}} (\log q) \pi_{q^\alpha}(x) &\leq x \sum_{\substack{q^\alpha > x^\delta \\ \alpha \geq 2}} \frac{\log q}{q^\alpha} \ll x \sum_{\substack{q^\alpha \geq x^\delta \\ \alpha \geq 2}} \frac{\log q}{q^2} \\ &\ll x^{1-\delta}. \end{aligned}$$

Now, Erdős's conjecture says  $\#\{p : f_a(p) = r\} \ll r^\theta$  for any  $\theta > 0$ . Thus,

$$\begin{aligned} \sum_{x^\delta < d \leq x} \Lambda(d) \pi_d(x) &= \sum_{x^\delta < q \leq x} (\log q) \pi_q(x) + \sum_{\substack{x^\delta < q^\alpha \leq x \\ \alpha \geq 2}} (\log q) \pi_{q^\alpha}(x) \\ &\ll \log x \sum_{x^\delta < q \leq x} \pi_q(x) + O(x^{1-\delta}) \\ &\ll \log x \#\{p \leq x : f_a(p) < x^{1-\delta}\} + O(x^{1-\delta}) \\ &\ll \log x \sum_{r < x^{1-\delta}} E_a(r) + O(x^{1-\delta}) \\ &\ll \log x \sum_{r < x^{1-\delta}} r^\theta + O(x^{1-\delta}) \\ &\ll x^\Theta \log x + O(x^{1-\delta}) \end{aligned}$$

for any  $\Theta > 1 - \delta$ . Thus,

$$\sum_{x^\delta < d \leq x} \Lambda(d) \pi_d(x) \ll x^{1-\delta+\theta}$$

for any  $\theta > 0$ . Therefore,

$$\sum_{p \leq x} \log(i_a(p)) = c_a \text{li}(x) + O(x^{1-\frac{\varepsilon}{2}+\theta})$$

upon choosing  $\delta = \varepsilon/2$ .

#### 4. THE PRIMES $p$ FOR WHICH $p + a$ AND $\ell_a(p)$ HAVE LARGE PRIME FACTORS

Throughout this section  $q$  will denote a prime. For  $m \in \mathbb{N}$ , we let

$$\pi(x; m, a) = \#\{p \leq x : p \equiv a \pmod{m}\}.$$

Then, [1, Theorem 9] states the following: let  $a \neq 0$ ,  $\lambda < 1/10$  and  $R < x^\lambda$ . For any  $A > 0$ , there exists  $B = B(a)$  such that provided  $MR < x/(\log x)^B$ , we have

$$\sum_{\substack{r \leq R \\ \gcd(r, a) = 1}} \left| \sum_{\substack{m \leq M \\ \gcd(m, a) = 1}} \left( \psi(x; mr, a) - \frac{x}{\varphi(mr)} \right) \right| \ll_{a, A, \lambda} \frac{x}{(\log x)^A}$$



where

$$\psi(x; k, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod k}} \Lambda(n)$$

where  $\Lambda(n) = \log p$  if  $n = p^\alpha$  where  $p \in \mathbb{N}$  is prime and  $\alpha \geq 1$  and 0 otherwise. This can be viewed as an extension of the famous Bombieri-Vinogradov Theorem:

$$\sum_{m \leq \frac{x^{1/2}}{(\log x)^B}} \max_{\gcd(a, m)=1} \max_{y \leq x} \left| \pi(y; m, a) - \frac{\text{li}(y)}{\varphi(m)} \right| \ll \frac{x}{(\log x)^A}$$

for some  $B$  dependent on  $A$ .

Goldfeld [4] was able to show using the Bombieri-Vinogradov theorem that

$$\sum_{p \leq x} \sum_{\substack{\sqrt{x} < q \leq x \\ q|p+a}} \log q = \frac{x}{2} + O\left(\frac{x \log \log x}{\log x}\right)$$

and subsequently

$$\sum_{p \leq x} \sum_{\substack{\sqrt{x} < q \leq x \\ q|l_a(p)}} \log q = \frac{x}{2} + O\left(\frac{x \log \log x}{\log x}\right).$$

Define  $N_a(x, y) := \#\{p \leq x : q|p+a \text{ for some } q > y\}$ . Immediate corollaries (Goldfeld [4]) of these results are

$$\begin{aligned} N_a(x, \sqrt{x}) &\geq \frac{1}{2} \frac{x}{\log x} + O\left(\frac{x \log \log x}{(\log x)^2}\right) \\ \sum_{p \leq x} \sum_{\substack{\sqrt{x} < q \leq x \\ q|l_a(p)}} 1 &= \frac{1}{2} \frac{x}{\log x} + O\left(\frac{x \log \log x}{(\log x)^2}\right), \end{aligned}$$

and

$$\sum_{p \leq x} l_a(p) \geq \frac{1}{2} \frac{x^{\frac{3}{2}}}{\log x} + O\left(\frac{x^{\frac{3}{2}} \log \log x}{(\log x)^2}\right).$$

Stephens [13] was able to show that on GRH for Kummerian fields, we have

$$\sum_{p \leq x} \frac{l_a(p)}{p-1} = c_a \pi(x) + O\left(\frac{x \log \log x}{(\log x)^2}\right)$$

where  $c_a > 0$  is a constant.

From this we get

$$\sum_{p \leq x} l_a(p) = \frac{c_a}{2} \frac{x^2}{\log x} + O\left(\frac{x^2 \log \log x}{(\log x)^2}\right).$$

We will see that [1, Theorem 9] allows us to push the  $\sqrt{x}$  to  $x^\theta$  for  $\frac{1}{2} < \theta < 1$ .

We have the following theorem:

**Theorem 4.1.** *Let  $\theta \in [1/2, 1)$ . Then,*

$$\sum_{p \leq x} \sum_{\substack{x^\theta < q \leq x \\ q|p+a}} \log q = (1 - \theta)x + O\left(\frac{x}{\log x}\right).$$

*Proof.* Following Goldfeld [4], let us consider

$$\begin{aligned} \sum_{m \leq x} \pi(x; m, -a) \Lambda(m) &= \sum_{m \leq x} \sum_{\substack{p \leq x \\ p \equiv -a \pmod{m}}} \Lambda(m) = \sum_{p \leq x} \sum_{\substack{m \leq x \\ m|p+a}} \Lambda(m) \\ &= \sum_{p \leq x} \log(p + a) + O((\log x)^2) \\ &= x + O\left(\frac{x}{\log x}\right). \end{aligned}$$

Let  $y \leq x/(\log x)^B$ . Then,

$$\begin{aligned} \sum_{m \leq y} \pi(x; m, -a) \Lambda(m) &= \sum_{\substack{m \leq y \\ \gcd(m, a) = 1}} \Lambda(m) \left( \pi(x; m, -a) - \frac{\text{li}(x)}{\varphi(m)} + \frac{\text{li}(x)}{\varphi(m)} \right) \\ &\quad + \sum_{\substack{m \leq y \\ \gcd(m, a) \neq 1}} \pi(x; m, -a) \Lambda(m) \\ &= \text{li}(x) \sum_{\substack{m \leq y \\ \gcd(m, a) = 1}} \frac{\Lambda(m)}{\varphi(m)} + O\left( \left| \sum_{\substack{m \leq y \\ \gcd(m, a) = 1}} \Lambda(m) \left( \pi(x; m, -a) - \frac{\text{li}(x)}{\varphi(m)} \right) \right| \right) \\ &\quad + O\left( \sum_{\substack{m \leq y \\ \gcd(m, a) \neq 1}} \Lambda(m) \right) \end{aligned}$$

since for  $\gcd(m, a) \neq 1$ , we have  $\pi(x, m, -a) \leq 1$ . Noticing that  $\Lambda(m) \ll \log x$  and choosing  $r = R = 1$  in [1, Theorem 9] after applying partial summation, we have

$$\begin{aligned} \sum_{m \leq y} \pi(x; m, -a) \Lambda(m) &= \text{li}(x) \sum_{m \leq x^\theta} \frac{\Lambda(m)}{\varphi(m)} + O\left(\frac{x}{(\log x)^{B-1}}\right) \\ &= \text{li}(x) \log y + O\left(\frac{x}{\log x}\right) \end{aligned}$$

since

$$\sum_{m \leq y} \frac{\Lambda(m)}{\varphi(m)} = \log y + O_a(1)$$

by Mertens' Theorem.

Therefore, letting  $y = x^\theta$  gives us

$$\sum_{m \leq x^\theta} \pi(x; m, -a) \Lambda(m) = \theta(\log x) \text{li}(x) + O\left(\frac{x}{\log x}\right) = \theta x + O\left(\frac{x}{\log x}\right).$$

Hence,

$$\sum_{x^\theta < m \leq x} \pi(x; m, -a) \Lambda(m) = (1 - \theta)x + O\left(\frac{x}{\log x}\right).$$

Rewriting the above summation we have

$$\sum_{x^\theta < q \leq x} \pi(x; q, -a) \log q + \sum_{\substack{x^\theta < q^k \leq x \\ k > 1}} \pi(x; q^k, -a) \log q = (1 - \theta)x + O\left(\frac{x}{\log x}\right).$$

However, by the Brun-Titchmarsh theorem, we have

$$\sum_{\substack{x^\theta < q^k \leq x^{\frac{3}{4}} \\ k > 1}} \pi(x; q^k, -a) \log q \ll \frac{x}{\log x} \sum_{\substack{x^\theta < q^k \leq x \\ k > 1}} \frac{\log q}{q^k} = o\left(\frac{x}{\log x}\right)$$

since the above right-hand summation is a tail of a convergent series, and thus  $o(1)$ . Also,

$$\sum_{\substack{x^{\frac{3}{4}} < q^k \leq x \\ k > 1}} \pi(x; q^k, -a) \log q \ll x^{\frac{1}{4}} \sum_{\substack{x^{\frac{3}{4}} < q^k \leq x \\ k > 1}} \log q \ll x^{\frac{1}{4}} (\log x)^2.$$

So the result holds.  $\square$

As an immediate corollary we have

$$N(x, x^\theta) \geq (1 - \theta) \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

We also have the following theorem:

**Theorem 4.2.** *Let  $\theta \in [1/2, 1)$ . Then,*

$$\sum_{p \leq x} \sum_{\substack{x^\theta < q \leq x \\ q | \ell_a(p)}} \log q = (1 - \theta)x + O\left(\frac{x \log \log x}{\log x}\right).$$

*Proof.* From the previous theorem, all we need to show is that

$$\sum_{p \leq x} \sum_{\substack{x^\theta < q \leq x \\ q | p-1 \\ q | \ell_a(p)}} \log q \ll \frac{x \log \log x}{\log x}.$$

By the Brun-Titchmarsh theorem, we have

$$\sum_{p \leq x} \sum_{\substack{\sqrt{x} < q \leq \sqrt{x} \log x \\ q|p-1 \\ q \nmid \ell_a(p)}} \log q \ll \frac{x}{\log x} \sum_{\sqrt{x} < q \leq \sqrt{x} \log x} \frac{\log q}{q} \ll \frac{x \log \log x}{\log x}.$$

The final sum is estimated by an idea of Hooley [7]. Let

$$M_a(x) := \sum_{p \leq x} \sum_{\substack{\sqrt{x} \log x < q \leq x \\ q|p-1 \\ q \nmid \ell_a(p)}} 1.$$

We have

$$\begin{aligned} \sum_{p \leq x} \sum_{\substack{\sqrt{x} \log x < q \leq x \\ q|p-1 \\ q \nmid \ell_a(p)}} \log q &\leq \log x \sum_{p \leq x} \sum_{\substack{\sqrt{x} \log x < q \leq x \\ q|p-1 \\ q \nmid \ell_a(p)}} 1 \ll (\log x) \log (2^{M_a(x)}) \\ &\ll (\log x) \log \left( \prod_{m \leq \frac{\sqrt{x}}{\log x}} a^{2^m} - 1 \right) \\ &\ll \log x \sum_{m \leq \frac{\sqrt{x}}{\log x}} m \ll \frac{x}{\log x}. \end{aligned}$$

Therefore, the result holds. □

As an immediate corollary, we have

**Corollary 4.1.** *We have*

$$\sum_{p \leq x} \sum_{\substack{x^\theta < q \leq x \\ q|\ell_a(p)}} 1 = \frac{(1-\theta)x}{\log x} + O\left(\frac{x \log \log x}{(\log x)^2}\right)$$

and

$$\sum_{p \leq x} \ell_a(p) \geq \frac{(1-\theta)x^{1+\theta}}{\log x} + O\left(\frac{x^{1+\theta} \log \log x}{(\log x)^2}\right).$$

*Proof.* The first statement follows from partial summation, and the second statement follows from the first statement. □

An immediate corollary of Erdős's conjecture is the following:

$$\begin{aligned}
\sum_{p \leq x} \ell_a(p) &= \sum_{\ell_a(p) \leq x^\theta} \ell_a(p) + \sum_{\ell_a(p) > x^\theta} \ell_a(p) \\
&= O\left(x^\theta \sum_{r \leq x^\theta} E_a(r)\right) + \sum_{\ell_a(p) > x^\theta} \ell_a(p) \\
&= O(x^{2\theta+\varepsilon}) + \sum_{\ell_a(p) > x^\theta} \ell_a(p).
\end{aligned}$$

However, as above,

$$\begin{aligned}
\#\{p \leq x : \ell_a(p) > x^\theta\} &= \pi(x) - \#\{p \leq x : \ell_a(p) \leq x^\theta\} \\
&= \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right) + O(x^{\theta+\varepsilon}) \\
&= \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)
\end{aligned}$$

after choosing  $\varepsilon < 1 - \theta$ .

$$\sum_{\ell_a(p) > x^\theta} \ell_a(p) > x^\theta \sum_{\ell_a(p) > x^\theta} 1 = \frac{x^{1+\theta}}{\log x} + O\left(\frac{x^{1+\theta}}{(\log x)^2}\right).$$

Thus,

$$\sum_{p \leq x} \ell_a(p) > \frac{x^{1+\theta}}{\log x} + O\left(\frac{x^{1+\theta}}{(\log x)^2}\right)$$

assuming Erdős's conjecture is true. Thus, we have the following:

$$\sum_{p \leq x} \ell_a(p) = \frac{c_a}{2} \frac{x^2}{(\log x)} + O\left(\frac{x^2 \log \log x}{(\log x)^2}\right) \quad (\text{assuming GRH})$$

$$\sum_{p \leq x} \ell_a(p) > \frac{x^{1+\theta}}{\log x} + O\left(\frac{x^{1+\theta}}{(\log x)^2}\right) \quad (\text{assuming Erdős's conjecture})$$

$$\sum_{p \leq x} \ell_a(p) \geq \frac{(1-\theta)x^{1+\theta}}{\log x} + O\left(\frac{x^{1+\theta} \log \log x}{(\log x)^2}\right) \quad (\text{unconditionally}).$$

So based on the problem of evaluating

$$\sum_{p \leq x} \ell_a(p)$$

we could say that Erdős's conjecture is "easier" than GRH. However, this can only be said towards this problem.

## 5. THE ABC-CONJECTURE AND ERDŐS'S CONJECTURES

The ABC-conjecture of Masser and Oesterlé states the following: let  $A, B, C \in \mathbb{Z}$  be relatively prime integers satisfying  $A + B + C = 0$ . Then, for every  $\varepsilon > 0$ ,

$$\max\{|A|, |B|, |C|\} \ll \left( \prod_{p|ABC} p \right)^{1+\varepsilon},$$

where the implied constant is dependent only on  $\varepsilon$  and independent of  $A, B, C$ .

For each  $n \in \mathbb{N}$  write  $a^n - 1 = A_n B_n$  where  $A_n$  is the squarefree part of  $a^n - 1$ . Silverman [12] has shown that the ABC-conjecture implies  $B_n \ll a^{\varepsilon_2 n}$  for any  $\varepsilon_2 > 0$ . For  $n \in \mathbb{N}$ , let  $P(n)$  be the largest prime factor of  $n$ . Then, the second author and Wong [11] have shown that the ABC-conjecture implies  $P(a^n - 1) > n^{2-\varepsilon}$  for all  $\varepsilon > 0$ . This resolves another conjecture of Erdős, which states

$$\frac{P(a^n - 1)}{n} \rightarrow \infty$$

as  $n \rightarrow \infty$ . We refer to this as Erdős's second conjecture. This has been unconditionally proven by Stewart [14]. In fact, Stewart has shown

$$P(a^n - b^n) > n \exp\left(\frac{\log n}{104 \log \log n}\right)$$

for sufficiently large  $n$  (see [14, Equation (8)]).

Now Erdős's first conjecture and ABC imply  $P(a^n - 1) \geq a^{n^{1-\varepsilon}}$ . To see this we note that

$$\begin{aligned} \omega(a^n - 1) &:= \#\{p|a^n - 1\} = \sum_{d|n} E_a(d) \\ &\ll \sum_{d|n} d^\varepsilon \ll d(n)n^\varepsilon \ll n^{\varepsilon'} = n^\varepsilon, \end{aligned}$$

by abuse of notation and where  $d(n) = \sum_{d|n} 1$ .

Now  $P(a^n - 1) \geq P(A_n)$  and so

$$P(A_n)^{Cn^\varepsilon} \geq P(A_n)^{\omega(a^n - 1)} \geq A_n = \frac{a^n - 1}{B_n} \gg a^{n(1-\varepsilon)}.$$

Thus,  $P(A_n) \gg a^{n^{1-\varepsilon}}$ .

## REFERENCES

- [1] Enrico Bombieri, John Friedlander, and Henryk Iwaniec. Primes in arithmetic progressions to large moduli. *Acta Math.*, 156:203–251, 1986.
- [2] Pál Erdős. Bemerkungen zu einer Aufgabe in den Elementen. *Arch. Math. (Basel)*, 27:159–163, 1976.
- [3] O. M. Fomenko. Class number of indefinite binary quadratic forms and the residual indices of integers modulo  $p$ . *J. of Math. Sci.*, 122(6):3685–3698, 2004.
- [4] Dorian M. Goldfeld. On the number of primes  $p$  for which  $p + a$  has a large prime factor. *Mathematika*, 16:23–27, 1969.
- [5] Rajiv Gupta and M. Ram Murty. A remark on Artin's conjecture. *Inv. Math.*, 78:127–130, 1984.

- [6] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford*, 37:27–38, 1986.
- [7] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
- [8] Christopher Hooley. *Applications of sieve methods to the theory of numbers*. Cambridge University Press, Cambridge, Great Britain, 1976.
- [9] Gerhard Jaeschke. Aufgaben: Aufgabe 618. *Elem. Math.*, 26:43–44, 1971.
- [10] Jeffrey Lagarias and Andrew Odlyzko. Effective versions of the Chebotarev density theorem. In Albrecht Frohlich, editor, *Algebraic Number Fields*, pages 409–464, New York, 1977. Academic Press Inc.
- [11] M. Ram Murty and S. Wong. The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences. In *Number theory for the millennium, III (Urbana, IL, 2000)*, pages 43–54, Natick, MA, 2002. A K Peters.
- [12] Joseph Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30:226–237, 1988.
- [13] P. J. Stephens. Prime divisors of second-order linear recurrences. I. *J. Number Theory*, 8:313–332, 1976.
- [14] C. L. Stewart. On divisors of Lucas and Lehmer numbers. *preprint: arXiv:1008.1274[math.NT]*, pages 1–18, 2011.
- [15] Samuel S. Wagstaff, Jr. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.*, 41:141–150, 1982.

DEPARTMENT OF MATHEMATICS & STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO  
*E-mail address:* felix@mast.queensu.ca

DEPARTMENT OF MATHEMATICS & STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, ONTARIO  
*E-mail address:* murty@mast.queensu.ca