Mathematika 58 (2012) 275–289 © University College London
doi:10.1112/S0025579311008205

ON A CONJECTURE OF ERDŐS

ADAM TYLER FELIX AND M. RAM MURTY

Abstract. Let a be an integer different from 0, ± 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 $(\mathbb{Z}/p\mathbb{Z})^* = \langle \overline{a} \rangle$ for $\varphi(p-1)$ such $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, where $\varphi(n)$ is the Euler totient function. When $(\mathbb{Z}/p\mathbb{Z})^* = \langle \overline{a} \rangle$ 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 ± 1 or a square, and define

$$\begin{aligned} N_a(x) &:= \#\{p \leqslant x : (\mathbb{Z}/p\mathbb{Z})^* = \langle \overline{a} \rangle\} \\ &= \#\{p \leqslant x : a \text{ is a primitive root modulo } p\}. \end{aligned}$$

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

$$N_a(x) \sim A(a)\pi(x), \tag{1}$$

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

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

THEOREM 1.1 (Hooley). *Assume that* GRH *holds for the Dedekind zeta functions of Kummer fields $\mathbb{Q}(\zeta_n, a^{1/n})$, where ζ_n is a primitive nth root of unity as n ranges over all positive squarefree integers. Then*

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

It should be noted that $A(a)$ in equation (1) is not always the same as $A(a)$ 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.

Received 20 August 2011, published online 23 February 2012.
MSC (2010): 11N13, 11N56, 11N64 (primary).
The first author's research was supported by an NSERC PGS-D and the second author's research was supported by an NSERC Discovery Grant.

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.

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

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

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

For $p \nmid a$, define

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

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

Let

$$A_a(x, \delta) := \#\{p \leqslant x : \ell_a(p) > p^\delta\} \quad \text{and} \quad E_a(r) = \#\{p : \ell_a(p) = r\}.$$

In 1971, P. Bundschuh [9] proved the following:

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

and, for $\delta < 1/2$,

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

and

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

Bundschuh's techniques can easily be extended to show that

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

and

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

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

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

THEOREM 1.3 (Erdős). *As* $x \to \infty$,

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

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

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

as $r \to \infty$.

Unlike Bundschuh, Erdős's techniques can be used to prove similar bounds for any a. To see this, let us 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 $\ell_2(p_i) = r$ and $\ell_2(q_j) < r$. Bundschuh made the observation that $p_i > r$, while Erdős made the observation that $p_i \equiv 1 \bmod r$, 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 better control of $A_2(x, 1/2)$. The $\log 2$ in equation (3) is dealt with by an appropriate choice of ε, and as such, $\log a$ is of no worry in

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

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

CONJECTURE (Erdős's conjecture). *For every $\varepsilon > 0$, there exist a constant $C := C(\varepsilon) > 0$ and an $r_0 := r_0(\varepsilon) \geqslant 1$ such that $E_2(r) \leqslant Cr^{\varepsilon}$ for all $r \geqslant r_0$.*

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 that $E_a(r) \ll_{\varepsilon} r^{\varepsilon}$. 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 that 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 $\gg x/(\log x)^2$ primes $p \leqslant x$ 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 that 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 $\mathrm{li}(x) := \int_2^x (\log t)^{-1}\, dt$. Using this function, we prove the following theorem.

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

$$\sum_{p \leqslant x} \log(i_a(p)) = c_a \mathrm{li}(x) + O(x^{1-\varepsilon/2+\theta})$$

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 $\mathbb{Q}(\zeta_n, a^{1/n})$ as n ranges over prime powers.

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, p. 112].

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

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

where the implied constant is absolute.

Then, Fomenko showed the following theorem.

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

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

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

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

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*

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

This result is established using techniques developed by Bombieri *et al* [**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 will show that $B(x) \ll x^{\delta}$ for some $0 < \delta < 1$.

If the prime number p contributes to $B(x)$, then $p - 1 = 2q_1q_2$ is the prime factorization of $p - 1$. Since $\ell_a(p) < (p-1)/2$, we have $\ell_a(p) \leqslant x^{\frac{3}{4}}$. Hence, by Erdős's conjecture,

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

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 $\ell_a(p) = (p-1)/2$,

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

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

§3. *Proofs of Theorems 1.5 and 1.6.*

3.1. *Proof of Theorem 1.5.* Following the argument of Hooley [**7**], for any prime q define $L_q := \mathbb{Q}(a^{1/q}, \zeta_q)$ where ζ_q is a primitive qth 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 Π_q to be the set of primes which split completely in L_q, and for squarefree k, define

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

Recall that $N_a(x)$ is the number of primes $p \leqslant x$ for which a is a primitive root modulo p. Then

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

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

Also, if we define

$$M(x; z, w) := \#\{p \leqslant x : \exists q \in (z, w) \text{ with } p \equiv 1 \bmod q, \text{ and } a^{(p-1)/q} \equiv 1 \bmod p\},$$

then clearly

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

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

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

using techniques from Hooley [7] and the effective Chebotarev density theorem of Lagarias and Odlyzko [10]: for any d squarefree,

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

for some fixed constant $\kappa > 0$. Here we would also need to assume $\eta \leqslant 1/7$ to ensure that a potential exceptional zero (β_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 $M(x; z, x) \leqslant M(x; z, x^\varepsilon) + M(x; x^\varepsilon, x)$. In fact, if the prime number $p \leqslant x$ contributes to $M(x; x^\varepsilon, x)$, then clearly $\ell_a(p) < x^{1-\varepsilon}$. Thus,

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

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

So, since $x^{1-\varepsilon_2} = o(\mathrm{li}(x))$, if we can show that $M(x; z, x^\varepsilon) = o(\mathrm{li}(x))$, 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:

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

Using this instead of the GRH will give us the result. To see this, note that

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

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

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

it follows that

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

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

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

Hence, Theorem 1.5 holds.

3.2. *Proof of Theorem 1.6.* We observe that

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

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

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

Now, the quasi-Riemann hypothesis implies that

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

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

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

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

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

We note that

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

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

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

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

Thus,

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

Also

$$\sum_{\substack{x^\delta < q^\alpha \leqslant x \\ \alpha \geqslant 2}} (\log q)\pi_{q^\alpha}(x) \leqslant x \sum_{\substack{q^\alpha > x^\delta \\ \alpha \geqslant 2}} \frac{\log q}{q^\alpha} \ll x \sum_{\substack{q^\alpha \geqslant x^\delta \\ \alpha \geqslant 2}} \frac{\log q}{q^2} \ll x^{1-\delta}.$$

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

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

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

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

for any $\theta > 0$. Therefore,

$$\sum_{p \leqslant x} \log(i_a(p)) = c_a \mathrm{li}(x) + O(x^{1-(\varepsilon/2)+\theta})$$

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

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

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 $MR < x/(\log x)^B$,

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

where

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

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

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

for some B dependent on A.

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

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

and subsequently that

$$\sum_{p \leqslant x} \sum_{\substack{\sqrt{x} < q \leqslant x \\ q \mid \ell_a(p)}} \log q = \frac{x}{2} + O\left(\frac{x \log\log x}{\log x} \right).$$

Define

$$N_a(x, y) := \#\{p \leqslant x : q \mid p + a \text{ for some } q > y\}.$$

Immediate corollaries (Goldfeld [4]) of these results are that

$$N_a(x, \sqrt{x}) \geqslant \frac{1}{2} \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2} \right),$$

$$\sum_{p \leqslant x} \sum_{\substack{\sqrt{x} < q \leqslant x \\ q \mid \ell_a(p)}} 1 \geqslant \frac{1}{2} \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2} \right),$$

and

$$\sum_{p \leqslant x} \ell_a(p) \geqslant \frac{1}{2} \frac{x^{\frac{3}{2}}}{\log x} + O\left(\frac{x^{\frac{3}{2}} \log\log x}{(\log x)^2} \right).$$

Stephens [13] was able to show that by the GRH for Kummerian fields,

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

where $c_a > 0$ is a constant.

From this we obtain

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

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

We have the following theorem.

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

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

Proof. Following Goldfeld [4], let us consider

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

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

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

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

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

since

$$\sum_{\substack{m\leqslant y\\ \gcd(m,a)=1}}\frac{\Lambda(m)}{\varphi(m)} = \log y + O_a(1)$$

by Mertens' theorem.

Therefore, letting $y = x^\theta$ yields

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

Hence,

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

Rewriting the above summation leads to

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

However, by the Brun–Titchmarsh theorem,

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

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

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

So the result holds. □

An immediate corollary is that

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

We also have the following theorem.

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

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

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

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

By the Brun–Titchmarsh theorem, we have

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

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

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

Then

$$\begin{aligned}\sum_{p\leqslant x}\sum_{\substack{\sqrt{x}\log x<q\leqslant x\\ q\mid p-1\\ q\nmid \ell_a(p)}}\log q &\leqslant \log x\sum_{p\leqslant x}\sum_{\substack{\sqrt{x}\log x<q\leqslant x\\ q\mid p-1\\ q\nmid \ell_a(p)}}1\ll(\log x)\log(2^{M_a(x)})\\ &\ll(\log x)\log\Bigg(\prod_{m\leqslant\sqrt{x}/\log x}a^{2m}-1\Bigg)\\ &\ll\log x\sum_{m\leqslant\sqrt{x}/\log x}m\ll\frac{x}{\log x}.\end{aligned}$$

Therefore, the result holds. □

An immediate corollary is as follows.

COROLLARY 4.1. *The following statements hold:*

$$\sum_{p\leqslant x}\sum_{\substack{x^\theta<q\leqslant x\\ q\mid \ell_a(p)}}1\geqslant\frac{(1-\theta)x}{\log x}+O\bigg(\frac{x\log\log x}{(\log x)^2}\bigg)$$

and

$$\sum_{p\leqslant x}\ell_a(p)\geqslant\frac{(1-\theta)x^{1+\theta}}{\log x}+O\bigg(\frac{x^{1+\theta}\log\log x}{(\log x)^2}\bigg).$$

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

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

However, as above,

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

after choosing $\varepsilon < 1 - \theta$, and

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

Thus,

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

assuming that Erdős's conjecture is true. Thus,

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

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

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

So based on the problem of evaluating

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

we could say that Erdős's conjecture is "easier" than the GRH. However, this can only be said for 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 ε 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 that $B_n \ll a^{\varepsilon_2 n}$ 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 that $P(a^n - 1) > n^{2-\varepsilon}$ for all $\varepsilon > 0$. This resolves another conjecture of Erdős, which states that

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

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

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

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

Now Erdős's first conjecture and ABC imply that $P(a^n - 1) \geqslant a^{n^{1-\varepsilon}}$. 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 an abuse of notation and where $d(n) = \sum_{d|n} 1$.

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

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

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

References

1. E. Bombieri, J. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli. *Acta Math.* **156** (1986), 203–251.
2. P. Erdős, Bemerkungen zu einer Aufgabe in den Elementen. *Arch. Math. (Basel)* **27** (1976), 159–163.
3. O. M. Fomenko, Class number of indefinite binary quadratic forms and the residual indices of integers modulo p. *J. Math. Sci.* **122**(6) (2004), 3685–3698.
4. D. M. Goldfeld, On the number of primes p for which $p + a$ has a large prime factor. *Mathematika* **16** (1969), 23–27.
5. R. Gupta and M. R. Murty, A remark on Artin's conjecture. *Invent. Math.* **78** (1984), 127–130.
6. D. R. Heath-Brown, Artin's conjecture for primitive roots. *Q. J. Math. Oxford* **37** (1986), 27–38.
7. C. Hooley, On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220.
8. C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press (Cambridge, 1976).
9. G. Jaeschke, Aufgaben: Aufgabe 618. *Elem. Math.* **26** (1971), 43–44.
10. J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem. In *Algebraic Number Fields* (ed. A. Frohlich), Academic Press (New York, 1977), 409–464.
11. M. R. 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)*, AK Peters (Natick, MA, 2002), 43–54.
12. J. Silverman, Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30** (1988), 226–237.
13. P. J. Stephens, Prime divisors of second-order linear recurrences. I. *J. Number Theory* **8** (1976), 313–332.

14. C. L. Stewart, On divisors of Lucas and Lehmer numbers. *Preprint*, 2011, arXiv:1008.1274[math.NT], pp. 1–18.
15. S. S. Wagstaff Jr, Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.* **41** (1982), 141–150.

Adam Tyler Felix,
Max Planck Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn,
Germany
E-mail: felix@mpim-bonn.mpg.de

M. Ram Murty,
Department of Mathematics & Statistics,
Queen's University,
Jeffery Hall, University Avenue, Kingston,
Ontario,
Canada K7L 3N6
E-mail: murty@mast.queensu.ca