ON SELBERG'S PROOF OF DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

STEVE FAN

Abstract. It is widely believed that rigorous analytic number theory has begun with Dirichlet's ingenious proof of his theorem on primes in arithmetic progressions using what are now known as the Dirichlet L-functions. Since then, various proofs building on Dirichlet's work have been discovered. Perhaps what is lesser known is an elementary proof due to A. Selberg. The object of this expository note is to present Selberg's original proof of Dirichlet's theorem. Our exposition is based on Selberg's paper [5].

1. Introduction

Dirichlet's theorem on primes in arithmetic progressions asserts that given any integers k, l with $k \geq 1$ and $\gcd(k, l) = 1$, the arithmetic progression $\{kn+l\}_{n=1}^{\infty}$ contains infinitely many primes. A special case of this theorem for $l = 1$ was stated by Euler in 1775. The general form was first conjectured by Legendre who used it without proof in his demonstrations of the law of quadratic reciprocity. The first proof was discovered in 1837 by Dirichlet [3, pp. 411–496] who introduced what is now known as the Dirichlet L-functions, defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for a fixed Dirichlet character $\chi \pmod k$, which plays an analogous role to that of the Riemann zeta function $\zeta(s)$ in Euler's proof of the infinitude of primes. The key step is to show that $L(1, \chi) \neq 0$ for all nonprinciple Dirichlet characters $\chi \pmod k$, which Dirichlet achieved with the aid of his class number formula for quadratic number fields. Dirichlet's work marks the beginning of analytic number theory, and Dirichlet himself was commonly considered as the founder of this branch of mathematics. Since then, various proofs have been discovered, and the proof given by de la Vallée Poussin [2] is arguably one of the most satisfactory ones. One important feature of this proof is that unlike Dirichlet's original proof, it uses the theory of complex analytic functions and does not resort to Dirichlet's class number formula. In 1940 Selberg [5] gave an elementary proof of Dirichlet's theorem that avoids dealing with Dirichlet L-functions and involves only considerations of real characters. In fact, his method allowed him to prove the following quantitative result.

Theorem 1.1. *Let k, l be integers with $k \geq 1$ and $\gcd(k, l) = 1$. Then there exists a positive real number x_0 depending only on k such that the inequality*

$$\sum_{\substack{p \leq x \\ p \equiv l \pmod k}} \frac{\log p}{p} > \frac{\log x}{20^4 \varphi(k)^6}$$

holds for all $x > x_0$, where φ is Euler's totient function.

Before Selberg's proof, many mathematicians, including famously G. H. Hardy, were skeptical that a proof without analyzing the properties of Dirichlet L-functions could ever be found. To the author's knowledge, however, Selberg's proof is lesser known to the math community compared to its analytic counterparts. In the present paper, we give a thorough exposition of Selberg's original proof of Theorem 1.1 following his paper [5].

2. Preliminary Lemmas

In this section, we collect some preliminary results needed for the proof of Theorem 1.1. Lemmas 2.1 and 2.2 below summarize the main results that Selberg proved in Section 2 of his paper [5]. A weaker version of Lemma 2.3 is stated without proof in [5]. The proof presented here was found by the author hismelf. Lemmas 2.4 and 2.5 correspond to Lemmas 1 and 2 in [5], respectively, and we shall present here a detailed proof of the former following Selberg's argument but with some adaptations. Among these results, Lemma 2.2 is perhaps the most crucial part of Selberg's ingenious proof of Theorem 1.1. Though completely elementary, the proof of this lemma is rather intricate, which contributes to the complexity of Selberg's proof of Dirichlet's theorem compared to proofs that take advantage of the power of complex analysis. It is noteworthy that the fundamental ideas in the proof also appeared in Selberg's ingenious elementary proof of the prime number theorem [6].

In what follows, let $\mathbb{R}$ be the set of real numbers, $\mathbb{R}_+$ the set of positive real numbers, $\mathbb{Z}$ the set of integers, $\mathbb{N}_+$ the set of positive integers, and $\mathbb{P}$ the set of prime numbers. For any $x \in \mathbb{R}$, For any $x \in \mathbb{R}$, we denote by $\lfloor x \rfloor$ the integer part of x and by $\lceil x \rceil$ the least integer greater than or equal to x. We shall also reserve the letters p, q, r for primes. Let $\pi(x)$ denote the number of primes up to $x \in \mathbb{R}_+$. Then

$$\pi(x) = O\left(\frac{x}{\log x}\right)$$

for large x by Chebyshev's estimate [4, Theorem 7]. A standard result [4, Theorem 425] in prime number theory states that

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1). \tag{2.1}$$

By partial summation and induction we obtain

$$\sum_{p \le x} \frac{(\log p)^m}{p} = \frac{1}{m}(\log x)^m + O((\log x)^{m-1}) \tag{2.2}$$

for all $m \in \mathbb{N}_+$. Let $\Lambda(n)$ be the von Mangoldt function. It is well known that

$$\Lambda(n) = -\sum_{d \mid n} \mu(d) \log d, \tag{2.3}$$

where μ is the Möbius function. Let us write

$$\theta(x) := \sum_{p \le x} \log p,$$

$$\psi(x) := \sum_{n \le x} \Lambda(n) = \sum_{p^\alpha \le x} \log p.$$

Then we have $\theta(x) = O(x)$ and $\psi(x) = O(x)$ [4, Theorem 414]. It follows by partial summation that

$$\sum_{p\le x} \log p \log\frac{x}{p} = \theta(x)\log x - \sum_{p\le x}(\log p)^2 = \int_1^x \frac{\theta(t)}{t}\,dt = O(x). \tag{2.4}$$

By (2.2) we have

$$\sum_{p\le y} \frac{\log p}{p} \log\frac{x}{p} = \log x \log y - \frac{1}{2}(\log y)^2 + O(\log x), \tag{2.5}$$

$$\sum_{p\le y} \frac{\log p}{p} \left(\log\frac{x}{p}\right)^2 = (\log x)^2 \log y - \log x(\log y)^2 + \frac{1}{3}(\log y)^3 + O((\log x)^2), \tag{2.6}$$

where $1 \le y \le x$. We shall also make use of the identities

$$\sum_{n\le x} \log n = x\log x - x + O(\log x), \tag{2.7}$$

$$\sum_{n\le x} n\log n = \frac{x^2}{2}\log x - \frac{x^2}{4} + O(x\log x). \tag{2.8}$$

Another useful estimate [4, Theorem 423] we shall need is

$$\sum_{n\le x} \left(\log\frac{x}{n}\right)^h = O(x) \tag{2.9}$$

for any $h \in \mathbb{R}_+$.

Lemma 2.1. *For $n \in \mathbb{N}_+$ and $x \in \mathbb{R}_+$, let*

$$\lambda_n(x) := \mu(n)\left(\log\frac{x}{n}\right)^2,$$
$$\Lambda_{2,n}(x) := \sum_{d|n} \lambda_d(x).$$

Then

$$\Lambda_{2,n}(x) = \begin{cases} (\log x)^2 & \text{if } n = 1, \\ \log p \log(x^2/p) & \text{if } n = p^\alpha, \\ 2\log p \log q & \text{if } n = p^\alpha q^\beta, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let

$$\delta(n) := \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

By (2.3) we have

$$\Lambda_{2,n}(x) = \sum_{d|n} \mu(d)\left(\log\frac{x}{d}\right)^2 = \delta(n)(\log x)^2 + 2\Lambda(n)\log x + f(n),$$

where

$$f(n) = \sum_{d|n} \mu(d)(\log d)^2.$$

If $\gcd(n_1, n_2) = 1$, then

$$f(n_1 n_2) = \sum_{d_1|n_1,\, d_2|n_2} \mu(d_1)\mu(d_2)(\log d_1 + \log d_2)^2 = \delta(n_1)f(n_2) + \delta(n_2)f(n_1) + 2\Lambda(n_1)\Lambda(n_2).$$

From this it follows that $f(n) = 0$ if n has at least 3 distinct prime factors. Thus the same holds for $\Lambda_{2,n}(x)$. The remaining cases where n has at most 2 distinct prime factors can be verified easily using the definition of $\Lambda_{2,n}(x)$. □

Remark. In prime number theory, the m-th von Mangoldt function Λ_m is defined by

$$\Lambda_m(n) := \sum_{d|n} \mu(d) \left(\log \frac{n}{d}\right)^m,$$

where $m \geq 0$. Thus $\delta(n) = \Lambda_0(n)$, $\Lambda(n) = \Lambda_1(n)$, and $\Lambda_{2,n}(n) = \Lambda_2(n)$. It is not hard to show that $\Lambda_m(n) \geq 0$, $\Lambda_m(n) = 0$ if n has more than m distinct prime factors and that

$$\Lambda_m(n) = m! \prod_{p|n} \log p$$

if n is the product of m distinct primes. More generally, let $f\colon \mathbb{N}_+ \to \mathbb{C}$ be an additive function, i.e., an arithmetic function with the property that $f(n_1 n_2) = f(n_1) + f(n_2)$ for all $n_1, n_2 \in \mathbb{N}_+$ with $\gcd(n_1, n_2) = 1$. For every integer $m \geq 0$, we define

$$F_m(n) := \sum_{d|n} \mu(d) f(d)^m,$$

$$G_m(n) := \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)^m.$$

Then $F_0(n) = G_0(n) = \delta(n)$. For any $n_1, n_2 \in \mathbb{N}_+$ with $\gcd(n_1, n_2) = 1$, we have

$$F_m(n_1 n_2) = \sum_{k=0}^{m} \binom{m}{k} F_{m-k}(n_1) F_k(n_2),$$

$$G_m(n_1 n_2) = \sum_{k=0}^{m} \binom{m}{k} G_{m-k}(n_1) G_k(n_2).$$

By induction, one can show that $F_m(n) = G_m(n) = 0$ if n has more than m distinct prime factors and that

$$F_m(n) = m! \prod_{p|n} F_1(p^{v_p}) = (-1)^m m! \prod_{p|n} f(p),$$

$$G_m(n) = m! \prod_{p|n} G_1(p^{v_p}) = m! \prod_{p|n} \left(f(p^{v_p}) - f(p^{v_p - 1})\right),$$

whenever n has precisely m distinct prime divisors, where v_p is the exponent of p in n.

Lemma 2.2. *Let $k \in \mathbb{N}_+$. For $x \in \mathbb{R}_+$ and $a \in \mathbb{Z}$, define*

$$Q_a(x) := \frac{1}{\log x} \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} \frac{\log p}{p}.$$

Then there exists $x_1 = x_1(k)$ such that for all $x > x_1$ and $a \in \mathbb{Z}$ with $\gcd(a,k) = 1$, we have

$$Q_a(x) \ge \frac{1}{10\varphi(k)} - \frac{1}{9} \sum_{\substack{m_1, m_2 = 1 \\ m_1 m_2 \equiv a \,(\mathrm{mod}\, k)}}^{k} Q_{m_1}(\sqrt[3]{x}) Q_{m_2}(\sqrt[3]{x}), \tag{2.10}$$

$$Q_a(x) \ge \frac{2}{27} \sum_{\substack{m_1, m_2, m_3 = 1 \\ m_1 m_2 m_3 \equiv a \,(\mathrm{mod}\, k)}}^{k} Q_{m_1}(\sqrt[3]{x}) Q_{m_2}(\sqrt[3]{x}) Q_{m_3}(\sqrt[3]{x}) + O\left(\frac{1}{\log x}\right). \tag{2.11}$$

Proof. Let $a \in \mathbb{Z}$ be an arbitrary integer coprime to k. By Lemma 2.1 we have

$$\sum_{\substack{n \le x \\ n \equiv a \,(\mathrm{mod}\, k)}} \Lambda_{2,n}(x) = \sum_{\substack{p^\alpha \le x \\ p^\alpha \equiv a \,(\mathrm{mod}\, k)}} \log p \log \frac{x^2}{p} + \sum_{\substack{p^\alpha q^\beta \le x \\ p^\alpha q^\beta \equiv a \,(\mathrm{mod}\, k)}} \log p \log q + O((\log x)^2).$$

By (2.4) we have

$$\sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} \log p \log \frac{x^2}{p} = \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} (\log p)^2 + 2 \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} \log p \log \frac{x}{p} = \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} (\log p)^2 + O(x).$$

Note that

$$\sum_{\substack{p^\alpha \le x,\, \alpha \ge 2 \\ p^\alpha \equiv a \,(\mathrm{mod}\, k)}} \log p \log \frac{x^2}{p} \le 2 \log x \sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \log p \ll (\log x)^2 \sum_{p \le \sqrt{x}} 1 \ll \sqrt{x} \log x,$$

$$\sum_{\substack{p^\alpha q^\beta \le x,\, \alpha \ge 2 \\ p^\alpha q^\beta \equiv a \,(\mathrm{mod}\, k)}} \log p \log q \le \sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \log p \sum_{q^\beta \le x/p^\alpha} \log q \ll x \sum_{\substack{p^\alpha \le x \\ \alpha \ge 2}} \frac{\log p}{p^\alpha} \ll x \sum_{p} \frac{\log p}{p(p-1)} \ll x.$$

Thus we have

$$\sum_{\substack{n \le x \\ n \equiv a \,(\mathrm{mod}\, k)}} \Lambda_{2,n}(x) = \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} (\log p)^2 + \sum_{\substack{pq \le x \\ pq \equiv a \,(\mathrm{mod}\, k)}} \log p \log q + O(x). \tag{2.12}$$

On the other hand, we see that

$$\sum_{\substack{n \le x \\ n \equiv a \,(\mathrm{mod}\, k)}} \Lambda_{2,n}(x) = \sum_{\substack{d \le x \\ \gcd(d,k) = 1}} \lambda_d(x) \sum_{\substack{m \le x/d \\ md \equiv a \,(\mathrm{mod}\, k)}} 1 = \frac{x}{k} \sum_{\substack{d \le x \\ \gcd(d,k) = 1}} \frac{\lambda_d(x)}{d} + O\left(\sum_{d \le x} |\lambda_d(x)|\right).$$

By (2.9) we have

$$\sum_{d \le x} |\lambda_d(x)| \le \sum_{d \le x} \left(\log \frac{x}{d}\right)^2 = O(x).$$

It follows that

$$\sum_{\substack{n\le x\\ n\equiv a\,(\mathrm{mod}\,k)}}\Lambda_{2,n}(x)=\frac{x}{k}\sum_{\substack{d\le x\\ \gcd(d,k)=1}}\frac{\lambda_d(x)}{d}+O(x).$$

Combining this with (2.12) we obtain

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}(\log p)^2+\sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\log p\log q=\frac{x}{k}\sum_{\substack{d\le x\\ \gcd(d,k)=1}}\frac{\lambda_d(x)}{d}+O(x). \tag{2.13}$$

Note that

$$\sum_{\substack{b=1\\ \gcd(b,k)>1}}^{k}\sum_{\substack{p\le x\\ p\equiv b\,(\mathrm{mod}\,k)}}(\log p)^2\le\sum_{p\le x}(\log p)^2\sum_{\substack{b=1\\ p\mid b}}^{k}1\le k\sum_{p\le x}\frac{(\log p)^2}{p}=O((\log x)^2)$$

by (2.2) and

$$\begin{aligned}\sum_{\substack{b=1\\ \gcd(b,k)>1}}^{k}\sum_{\substack{pq\le x\\ pq\equiv b\,(\mathrm{mod}\,k)}}\log p\log q&\le 2\sum_{pq\le x}\log p\log q\sum_{\substack{b=1\\ p\mid b}}^{k}1\\ &\le 2k\sum_{p\le x}\frac{\log p}{p}\sum_{q\le x/p}\log q\\ &\ll x\sum_{p\le x}\frac{\log p}{p^2}\\ &\ll x.\end{aligned}$$

Since the right-hand side of (2.13) does not depend on a, we have

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}(\log p)^2+\sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\log p\log q=\frac{1}{\varphi(k)}\left(\sum_{p\le x}(\log p)^2+\sum_{pq\le x}\log p\log q\right)+O(x).$$

By partial summation we have

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\frac{(\log p)^2}{p}&=\frac{1}{x}\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}(\log p)^2+\int_1^x\sum_{\substack{p\le t\\ p\equiv a\,(\mathrm{mod}\,k)}}(\log p)^2\cdot\frac{1}{t^2}\,dt,\\ \sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}&=\frac{1}{x}\sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\log p\log q+\int_1^x\sum_{\substack{pq\le t\\ pq\equiv a\,(\mathrm{mod}\,k)}}\log p\log q\cdot\frac{1}{t^2}\,dt.\end{aligned}$$

Adding up these two identities and using partial summation again, we obtain

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\frac{(\log p)^2}{p}+\sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}=\frac{1}{\varphi(k)}\left(\sum_{p\le x}\frac{(\log p)^2}{p}+\sum_{pq\le x}\frac{\log p\log q}{pq}\right)+O(\log x).$$

By (2.2) we have

$$\begin{aligned}\sum_{pq\le x}\frac{\log p\log q}{pq}&=\sum_{p\le x}\frac{\log p}{p}\sum_{q\le x/p}\frac{\log q}{q}\\&=\sum_{p\le x}\frac{\log p}{p}\log\frac{x}{p}+O(\log x)\\&=(\log x)^2-\sum_{p\le x}\frac{(\log p)^2}{p}+O(\log x).\end{aligned}$$

It follows that

$$A(x;a):=\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\frac{(\log p)^2}{p}+\sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}=\frac{1}{\varphi(k)}(\log x)^2+O(\log x).\tag{2.14}$$

Now we deduce from (2.14) that

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\frac{(\log p)^2}{p}\le\frac{1}{\varphi(k)}(\log x)^2+O(\log x),$$

from which it follows by partial summation that

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p}{p}\le\frac{2}{\varphi(k)}\log x+O(\log\log x).\tag{2.15}$$

This together with (2.5) implies

$$\begin{aligned}\sum_{\sqrt[3]{x}<p\le x}\frac{\log p}{p}\sum_{\substack{q\le x/p\\ q\equiv\bar{p}a\,(\mathrm{mod}\,k)}}\frac{\log q}{q}&\le\frac{2}{\varphi(k)}\sum_{\sqrt[3]{x}<p\le x}\frac{\log p}{p}\log\frac{x}{p}+O(\log x\log\log x)\\&\le\frac{4}{9\varphi(k)}(\log x)^2+O(\log x\log\log x).\end{aligned}$$

Thus we have

$$\begin{aligned}\sum_{\substack{pq\le x\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}&\le\sum_{\substack{p,q\le\sqrt[3]{x}\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}+2\sum_{\sqrt[3]{x}<p\le x}\frac{\log p}{p}\sum_{\substack{q\le x/p\\ q\equiv\bar{p}a\,(\mathrm{mod}\,k)}}\frac{\log q}{q}\\&\le\sum_{\substack{p,q\le\sqrt[3]{x}\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}+\frac{8}{9\varphi(k)}(\log x)^2+O(\log x\log\log x).\end{aligned}$$

Inserting this in (2.14) we obtain

$$\sum_{\substack{p\le x\\ p\equiv a\,(\mathrm{mod}\,k)}}\frac{(\log p)^2}{p}\ge\frac{1}{9\varphi(k)}(\log x)^2-\sum_{\substack{p,q\le\sqrt[3]{x}\\ pq\equiv a\,(\mathrm{mod}\,k)}}\frac{\log p\log q}{pq}+O(\log x\log\log x).$$

Thus there exists $x_1 = x_1(k)$ such that

$$\begin{aligned} Q_a(x) &> \frac{1}{10\varphi(k)} - \frac{1}{(\log x)^2} \sum_{\substack{p,q\le \sqrt[3]{x} \\ pq\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q}{pq} \\ &= \frac{1}{10\varphi(k)} - \frac{1}{9} \sum_{\substack{m_1,m_2=1 \\ m_1m_2\equiv a \,(\mathrm{mod}\, k)}}^{k} Q_{m_1}(\sqrt[3]{x}) Q_{m_2}(\sqrt[3]{x}) \end{aligned}$$

for all $x > x_1$. This establishes (2.10).

Now by (2.14) and partial summation we have

$$\begin{aligned} \sum_{\substack{p\le x \\ p\equiv a \,(\mathrm{mod}\, k)}} \frac{(\log p)^3}{p} + \sum_{\substack{pq\le x \\ pq\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q}{pq} \log pq &= A(x;a)\log x - \int_1^x \frac{A(t;a)}{t}\, dt \\ &= \frac{2}{3\varphi(k)} (\log x)^3 + O((\log x)^2). \end{aligned}$$

Note that

$$\sum_{\substack{pq\le x \\ pq\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q}{pq} \log pq = 2 \sum_{\substack{pq\le x \\ pq\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p (\log q)^2}{pq} = 2 \sum_{\substack{p\le x \\ p\mid k}} \frac{\log p}{p} \sum_{\substack{q\le x/p \\ q\equiv \bar{p}a \,(\mathrm{mod}\, k)}} \frac{(\log q)^2}{q},$$

where $\bar{p}$ is an integer such that $p\bar{p} \equiv 1 \,(\mathrm{mod}\, k)$. By (2.14) we have

$$\sum_{\substack{q\le x/p \\ q\equiv \bar{p}a \,(\mathrm{mod}\, k)}} \frac{(\log q)^2}{q} = A(x/p;\bar{p}a) - \sum_{\substack{qr\le x \\ qr\equiv \bar{p}a \,(\mathrm{mod}\, k)}} \frac{\log q \log r}{qr} + O(\log x).$$

Since

$$\sum_{\substack{p\le x \\ p\mid k}} \frac{\log p}{p} A(x/p;\bar{p}a) = \frac{1}{\varphi(k)} \sum_{p\le x} \frac{\log p}{p} \left(\log \frac{x}{p}\right)^2 + O((\log x)^2) = \frac{1}{3\varphi(k)} + O((\log x)^2)$$

by (2.6), we have

$$\sum_{\substack{pq\le x \\ pq\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q}{pq} \log pq = \frac{2}{3\varphi(k)} (\log x)^3 - 2 \sum_{\substack{pqr\le x \\ pqr\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q \log r}{pqr} + O((\log x)^2).$$

Hence we have

$$\sum_{\substack{p\le x \\ p\equiv a \,(\mathrm{mod}\, k)}} \frac{(\log p)^3}{p} = 2 \sum_{\substack{pqr\le x \\ pqr\equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q \log r}{pqr} + O((\log x)^2).$$

It follows that

$$Q_a(x) \geq \frac{2}{(\log x)^3} \sum_{\substack{p,q,r \leq \sqrt[3]{x} \\ pqr \equiv a \,(\mathrm{mod}\, k)}} \frac{\log p \log q \log r}{pqr} + O\left(\frac{1}{\log x}\right)$$

$$= \frac{2}{27} \sum_{\substack{m_1,m_2,m_3=1 \\ m_1 m_2 m_3 \equiv a \,(\mathrm{mod}\, k)}}^{k} Q_{m_1}(\sqrt[3]{x}) Q_{m_2}(\sqrt[3]{x}) Q_{m_3}(\sqrt[3]{x}) + O\left(\frac{1}{\log x}\right).$$

This proves (2.11). □

Lemma 2.3. *Let $k \in \mathbb{N}_+$ and χ a real nonprinciple character modulo k. Then there exists $D \in \mathbb{Z}$ which is not a perfect square, such that $|D| < k^2$, $16 \nmid D$, $p^3 \nmid D$ for all odd $p \in \mathbb{P}$, $D \not\equiv -1 \pmod 8$, and*

$$\chi(p) = \left(\frac{D}{p}\right)$$

for all $p \in \mathbb{P}$, where $(\frac{\cdot}{\cdot})$ is the Kronecker symbol. Furthermore, if

$$P := \prod_{(u,v) \in E} |u^2 - Dv^2|,$$

where

$$E := \left\{(u,v) \in \mathbb{Z}^2 \setminus \{(0,0)\} \colon |u| \leq \sqrt{x/2},\ |v| \leq \sqrt{x/(2|D|)}\right\},$$

then

$$\log P \geq \frac{5x}{4\sqrt{|D|}} \log x + O(x)$$

for sufficiently large $x \in \mathbb{R}_+$.

Proof. Suppose that χ is induced by a real primitive character $\chi_1 \,(\mathrm{mod}\, k_1)$, where $k_1 > 1$ is a divisor of k. Then $\chi_1(n) = (d/n)$ for some $d = 2^\alpha m$ with $|d| = k_1$, where $0 \leq \alpha \leq 3$ and m is odd and square-free with the property that $m \equiv 1 \pmod 4$ if $\alpha = 0$ (see for instance [1, §5]). Let $D := dd'$, where

$$d' := \prod_{q \mid k,\, q \nmid k_1} q^2.$$

Then D is not a perfect square, $|D| < k^2$, $16 \nmid D$, $p^3 \nmid D$ for all odd $p \in \mathbb{P}$, and $D \not\equiv -1 \pmod 8$. Moreover, we have

$$\left(\frac{d}{p}\right) = \chi_1(p) \left(\frac{d'}{p}\right) = \chi(p)$$

for all $p \in \mathbb{P}$, since $\chi_1(n) = \chi(n)$ whenever $\gcd(n,k) = 1$ and

$$\left(\frac{d'}{p}\right) = \begin{cases} 1 & \text{if } p \nmid d', \\ 0 & \text{otherwise.} \end{cases}$$

We now estimate $\log P$. Let $E_+ := E \cap \mathbb{N}_+^2$. Then

$$\sum_{(u,v) \in E_+} \log|u^2 - |D|v^2| \geq \sum_{\substack{(u,v) \in E_+ \\ \left|u - \sqrt{|D|}v\right| \geq 1}} \log\left(u + \sqrt{|D|}v\right) + \sum_{\substack{(u,v) \in E_+ \\ \left|u - \sqrt{|D|}v\right| \geq 1}} \log\left|u - \sqrt{|D|}v\right|.$$

Since

$$\sum_{\substack{(u,v)\in E_+\\ \left|u-\sqrt{|D|}v\right|<1}} \log\left(u+\sqrt{|D|}v\right) \ll \sum_{u\le\sqrt{x}} \sum_{\frac{u-1}{\sqrt{|D|}}<v<\frac{u+1}{\sqrt{|D|}}} \log x \ll \sqrt{x}\log x,$$

we have by (2.7) that

$$\begin{aligned}\sum_{\substack{(u,v)\in E_+\\ \left|u-\sqrt{|D|}v\right|\ge1}} \log\left(u+\sqrt{|D|}v\right) &= \sum_{(u,v)\in E_+} \log\left(u+\sqrt{|D|}v\right) + O(\sqrt{x}\log x)\\ &\ge \sum_{u\le\sqrt{x/2}} \left\lfloor\sqrt{\frac{x}{2|D|}}\right\rfloor \log u + O(\sqrt{x}\log x)\\ &= \sqrt{\frac{x}{2|D|}} \sum_{u\le\sqrt{x/2}} \log u + O(\sqrt{x}\log x)\\ &= \frac{x}{4\sqrt{|D|}}\log x + O(x).\end{aligned}$$

On the other hand, we have by (2.7) and (2.8) that

$$\begin{aligned}\sum_{\substack{(u,v)\in E_+\\ \left|u-\sqrt{|D|}v\right|\ge1}} \log\left|u-\sqrt{|D|}v\right| &\ge \sum_{2\sqrt{|D|}\le u\le\sqrt{x/2}} \sum_{v\le\frac{u}{2\sqrt{|D|}}} \log\frac{u}{2}\\ &= \frac{1}{2\sqrt{|D|}} \sum_{2\sqrt{|D|}\le u\le\sqrt{x/2}} u\log\frac{u}{2} + O(\sqrt{x}\log x)\\ &= \frac{1}{2\sqrt{|D|}} \sum_{u\le\sqrt{x/2}} u\log u + O(x)\\ &= \frac{x}{16\sqrt{|D|}}\log x + O(x).\end{aligned}$$

Hence we have

$$\sum_{(u,v)\in E_+} \log|u^2-|D|v^2| \ge \frac{5x}{16\sqrt{|D|}}\log x + O(x).$$

Finally, we see that

$$\begin{aligned}\sum_{0<|u|\le\sqrt{x/2}} \log u^2 &\ll \sqrt{x}\log x,\\ \sum_{0<|v|\le\sqrt{x/(2|D|)}} \log|D|v^2 &\ll \sqrt{x}\log x.\end{aligned}$$

It follows that

$$\log P = 4 \sum_{(u,v)\in E_+} \log|u^2 - |D|v^2| + \sum_{0<|u|\le\sqrt{x/2}} \log u^2 + \sum_{0<|v|\le\sqrt{x/(2|D|)}} \log|D|v^2$$
$$\ge \frac{5x}{4\sqrt{|D|}} \log x + O(x)$$

for sufficiently large $x > 0$. □

Lemma 2.4. *Let $k \in \mathbb{N}_+$ and let χ be a real nonprinciple character modulo k. Then there exists $x_2 = x_2(k)$ such that*

$$\sum_{\substack{p\le x\\ \chi(p)=1}} \frac{\log p}{p} > \frac{1}{4}\log x$$

for all $x > x_2$.

Proof. By Lemma 2.3, there exists $D \in \mathbb{Z}$ which is not a perfect square, such that $|D| < k^2$, $p^4 \nmid D$ for all $p \in \mathbb{P}$, $D \not\equiv -1 \pmod 8$, and $\chi(p) = (D/p)$ for all $p \in \mathbb{P}$. Let $p \in \mathbb{P}$ be an odd prime and let $\alpha \in \mathbb{N}_+$. Put $e_p(x) := \lfloor \log x/\log p \rfloor$. Consider the solutions $(u, v) \in E$ to the congruence equation

$$u^2 - Dv^2 \equiv 0 \pmod{p^\alpha}, \tag{2.16}$$

where E is the set defined in Lemma 2.3. In order for (2.16) to have a solution $(u, v) \in E$, we may assume $p \le x$ and $\alpha \le e_p(x)$, since $0 < |u^2 - Dv^2| \le x$. We now estimate the number of solutions $(u, v) \in E$ to (2.16), which will allow us to estimate the highest power of p dividing the number P defined in Lemma 2.3.

If $(D/p) = -1$, then $p \ge 3$ and any solution $(u, v) \in E$ to (2.16) must satisfy $p^\beta \mid u$ and $p^\beta \mid v$ for some $\beta \in \mathbb{N}_+$ with $\beta \ge \alpha/2$. Hence the number of pairs $(u, v) \in E$ for which (2.16) holds is at most $O(x/p^\alpha)$ for even α and at most $O(x/p^{\alpha+1})$ for odd α. Thus the highest power of p dividing P is less than

$$2\sum_{m=1}^{\infty} \frac{x}{p^{2m}} = \frac{2x}{p^2-1} = O\left(\frac{x}{p^2}\right).$$

Consider now the case $(D/p) = 1$. For sufficiently large x, there exists a primitive solution $(u_0, v_0) \in E$ to (2.16), namely, a solution satisfying $p \nmid u_0v_0$. If $(u, v) \in E$ is any solution to (2.16), then we have

$$v_0u \pm u_0v \equiv 0 \pmod{p^\alpha}. \tag{2.17}$$

The number of choices for $(u, v) \in E$ for which (2.17) holds is at most

$$2\left(\frac{2\sqrt{x/2}}{p^\alpha} + O(1)\right)\left(2\sqrt{\frac{x}{2|D|}} + O(1)\right) = \frac{4x}{p^\alpha\sqrt{|D|}} + O(\sqrt{x}).$$

Thus the highest power of p dividing P is at most

$$\sum_{m=1}^{e_p(x)} \left(\frac{4x}{p^m\sqrt{|D|}} + O(\sqrt{x})\right) \le \frac{4x}{(p-1)\sqrt{|D|}} + O\left(\frac{\sqrt{x}\log x}{\log p}\right).$$

If $p > \sqrt{2x}$, then $\alpha = 1$. Moreover, for each $m \in \mathbb{Z}$, there are at most two pairs $(u, v) \in E$ satisfying the equation

$$v_0 u \pm u_0 v = mp,$$

since $p > 2\sqrt{x/2}$. Note that

$$|m| = \frac{|v_0 u \pm u_0 v|}{p} \leq \frac{x}{p\sqrt{|D|}}.$$

Thus there are at most

$$2\left(\frac{2x}{p\sqrt{|D|}} + 1\right) = \frac{4x}{p\sqrt{|D|}} + O(1)$$

choices for $(u, v) \in E$ that satisfy (2.17). This implies that when $p > \sqrt{2x}$, the highest power of p dividing P is at most

$$\frac{4x}{p\sqrt{|D|}} + O(1).$$

If $(D/p) = 0$, then $p \mid D$. Suppose that $p^\beta \parallel D$. Then $1 \leq \beta \leq 3$. If $\beta = 1$, then any solution $(u, v) \in E$ to (2.16) satisfy the condition $p^{\lceil \alpha/2 \rceil} \mid u$ and $p^{\lfloor \alpha/2 \rfloor} \mid v$. It follows that the number of pairs $(u, v) \in E$ for which (2.16) holds is at most $O(x/p^\alpha)$. Hence the highest power of p dividing P is less than

$$\sum_{m=1}^{\infty} \frac{x}{p^m} = \frac{x}{p-1} = O\left(\frac{x}{p}\right).$$

Suppose now that $\beta = 3$. Then for any solution $(u, v) \in E$ to (2.16), we have $p \mid u$ if $\alpha = 1$ and $p^{\lceil \alpha/2 \rceil} \mid u$ and $p^{\lfloor \alpha/2 \rfloor - 1} \mid v$ if $\alpha \geq 2$. Thus the highest power of p dividing P is less than

$$\frac{x}{p} + \sum_{m=2}^{\infty} \frac{x}{p^{m-1}} = O\left(\frac{x}{p}\right).$$

Consider now the case $\beta = 2$. If $(u, v) \in E$ is a solution to (2.16), then $p \mid u$. This implies that if $\alpha \in \{1, 2\}$, then the number of pairs $(u, v) \in E$ satisfying (2.16) is at most $O(x/p)$. Suppose now that $\alpha \geq 3$. Writing $D = p^2 D'$ and $u = pu'$, we have $|u'| \leq \sqrt{x/2}/p$ and

$$u'^2 - D'v^2 \equiv 0 \pmod{p^{\alpha-2}}.$$

By the same argument, we see that the highest power of p dividing P is at most $O(x/p^3)$ if $(D'/p) = -1$ and at most $O(x/p^2)$ if $(D'/p) = 1$.

Collecting the results we just proved, we have

$$\log P \leq \frac{4x}{\sqrt{|D|}} \sum_{\substack{p \leq \sqrt{2x} \\ \chi(p)=1}} \frac{\log p}{p-1} + \frac{4x}{\sqrt{|D|}} \sum_{\substack{\sqrt{2x} < p \leq x \\ \chi(p)=1}} \frac{\log p}{p} + R(x),$$

where

$$R(x) = O\left(\sqrt{x} \log x \cdot \pi(\sqrt{2x})\right) + O(x) + O\left(x \sum_{p \leq x} \frac{\log p}{p^2}\right) + O\left(x \sum_{p \mid D} \frac{\log p}{p}\right) = O(x).$$

Since

$$\sum_{\substack{p\le\sqrt{2x}\\ \chi(p)=1}}\frac{\log p}{p-1}=\sum_{\substack{p\le\sqrt{2x}\\ \chi(p)=1}}\frac{\log p}{p}+O\left(\sum_{p\le x}\frac{\log p}{p(p-1)}\right)=\sum_{\substack{p\le\sqrt{2x}\\ \chi(p)=1}}\frac{\log p}{p}+O(1),$$

we obtain

$$\log P\le\frac{4x}{\sqrt{|D|}}\sum_{\substack{p\le x\\ \chi(p)=1}}\frac{\log p}{p}+O(x).$$

Combining this with Lemma 2.3 gives

$$\frac{4x}{\sqrt{|D|}}\sum_{\substack{p\le x\\ \chi(p)=1}}\frac{\log p}{p}\ge\frac{5x}{4\sqrt{|D|}}\log x+O(x).$$

This implies

$$\sum_{\substack{p\le x\\ \chi(p)=1}}\frac{\log p}{p}\ge\frac{5}{16}\log x+O(1)$$

Hence there exists $x_2=x_2(k)$ such that

$$\sum_{\substack{p\le x\\ \chi(p)=1}}\frac{\log p}{p}>\frac{1}{4}\log x$$

for all $x>x_2$. □

Lemma 2.5. *Let $k\in\mathbb{N}_+$ and H a subset of $G:=(\mathbb{Z}/k\mathbb{Z})^\times$ with $\#H=h\ge\varphi(k)/2$. Suppose that to every real nonprinciple character χ modulo k, there exists $m\in H$ with $\chi(m)=1$. Let $l\in G$, and suppose that there exists a pair $(m,m')\in H^2$ for which $mm'=l$. Then there exists a triple $(m_1,m_2,m_3)\in H^3$ for which $m_1m_2m_3=l$.*

Proof. Assume to the contrary that $m_1m_2m_3\ne l$ for all $(m_1,m_2,m_3)\in H^3$. Then $m_1m_2\ne lm_3^{-1}$ for all $(m_1,m_2,m_3)\in H^3$. Since $\{m_1m_2\}_{m_1,m_2\in H}$ contains $h'\ge h$ distinct elements in G and $\{lm_3^{-1}\}_{m_3\in H}$ contains precisely h distinct elements in G, we get at least $h'+h$ distinct elements in G. Thus $h'+h\le\varphi(k)$. Since $h\ge\varphi(k)/2$, we have $h'=h=\varphi(k)/2$.

Now fix $m_0\in H$ and let $K:=m_0^{-1}H$. If $m_1,m_2\in H$, then there exists $m_3\in H$ for which $m_0m_1=m_2m_3$ holds in G, since $h'=h$ implies $\{m_2m\}_{m\in H}=\{mm'\}_{m,m'\in H}$. It follows that

$$(m_0^{-1}m_1)(m_0^{-1}m_2)^{-1}=m_1m_2^{-1}=m_0^{-1}m_3\in K.$$

This shows that K is a subgroup of G. Now we define $\chi\colon G\to\mathbb{R}$ by $\chi(n)=1$ for all $n\in K$ and $\chi(n)=-1$ for all $n\in G\setminus K$. Note that if $n\in G\setminus K$, then $\{nn'\}_{n'\in K}=G\setminus K$ and thus $\{nn'\}_{n'\in G\setminus K}=K$. Using this we see that χ defines a real nonprinciple character modulo k satisfying $\chi(m)=\chi(m_0)$ for all $m\in H$. Since $1\in\chi(H)$, we have $\chi(m)=1$ for all $m\in H$. Thus $H\subseteq K$. Since $\#K=\#H=h$, we have $H=K$. On the other hand, we can find $(m,m')\in H^2$ for which $mm'=l$. This implies that $\chi(l)=\chi(m)\chi(m')=1$. Hence $l\in K=H$. As a consequence, we have $1\cdot1\cdot l=l$ with $1,l\in H$, a contradiction. □

3. Proof of Theorem 1.1

We are now ready to prove Theorem 1.1 stated in Section 1. Let us fix $k \in \mathbb{N}_+$. We need to prove that there exists $x_0 = x_0(k)$ such that for all $x > x_0$ and any $l \in \mathbb{Z}$ with $\gcd(k, l) = 1$, we have

$$Q_l(x) > \frac{1}{20^4\varphi(k)^6}.$$

We need only to prove this for all sufficiently large x for which

$$Q_l(x) < \frac{1}{30\varphi(k)}. \tag{3.1}$$

Let

$$H_x := \#\left\{1 \le m \le k\colon \ \gcd(m,k) = 1 \text{ and } Q_m(\sqrt[3]{x}) > \frac{1}{20\varphi(k)^2}\right\}$$

and $h_x := \#H_x$. Observe that

$$\sum_{\substack{m=1\\ \gcd(m,k)=1}}^{k} Q_m(\sqrt[3]{x}) = \sum_{m=1}^{k} Q_m(\sqrt[3]{x}) + O\left(\frac{1}{\log x}\right) = 1 + O\left(\frac{1}{\log x}\right)$$

by (2.1). By (2.15) we have

$$Q_m(x) \le \frac{2}{\varphi(k)} + O\left(\frac{\log\log x}{\log x}\right) \tag{3.2}$$

for any $m \in \mathbb{Z}$ with $\gcd(m, k) = 1$. It follows that

$$1 + O\left(\frac{1}{\log x}\right) \le \frac{2h_x}{\varphi(k)} + \frac{\varphi(k) - h_x}{20\varphi(k)^2} + O\left(\frac{\log\log x}{\log x}\right),$$

which implies

$$h_x \ge \frac{\varphi(k)}{2} \cdot \frac{40\varphi(k) - 2}{40\varphi(k) - 1} + O\left(\frac{\log\log x}{\log x}\right).$$

Since $h_x \in \mathbb{Z}$ and

$$\frac{\varphi(k)}{2} \cdot \frac{40\varphi(k) - 2}{40\varphi(k) - 1} = \frac{\varphi(k)}{2}\left(1 - \frac{1}{40\varphi(k) - 1}\right) > \frac{\varphi(k)}{2}\left(1 - \frac{1}{2\varphi(k)}\right) = \frac{\varphi(k) - 1/2}{2},$$

we have $h_x \ge \varphi(k)/2$ for all sufficiently large x. On the other hand, it follows from Lemma 2.4 that for any real nonprinciple character $\chi \pmod k$, we have

$$\sum_{\substack{m=1\\ \chi(m)=1}}^{k} Q_m(\sqrt[3]{x}) = \frac{1}{\log\sqrt[3]{x}} \sum_{\substack{p \le \sqrt[3]{x}\\ \chi(p)=1}} \frac{\log p}{p} > \frac{1}{9}$$

for all sufficiently large x. Thus for every sufficiently large x, there exists $1 \le m_0 = m_0(k, x) \le k$ with $\chi(m_0) = 1$ such that

$$Q_{m_0}(\sqrt[3]{x}) > \frac{1}{18\varphi(k)}.$$

By (2.10) we have

$$\sum_{\substack{m_1,m_2=1\\ m_1m_2\equiv l\,(\mathrm{mod}\,k)}}^{k} Q_{m_1}(\sqrt[3]{x})Q_{m_2}(\sqrt[3]{x}) \geq \frac{1}{10\varphi(k)} - Q_l(\sqrt[3]{x}) > \frac{1}{15\varphi(k)}$$

for all sufficiently large x for which (3.1) holds. Hence for every such x, there exists a pair (m_1, m_2) depending only on k and x with $m_1m_2 \equiv l\,(\mathrm{mod}\,k)$ such that

$$Q_{m_1}(\sqrt[3]{x})Q_{m_2}(\sqrt[3]{x}) > \frac{1}{15\varphi(k)}.$$

From (3.2) it follows that

$$Q_{m_1}(\sqrt[3]{x}), Q_{m_2}(\sqrt[3]{x}) > \frac{1}{31\varphi(k)} > \frac{1}{20\varphi(k)^2}.$$

We have thus proved that for every sufficiently large x satisfying (3.1), the set H_x satisfies the conditions of Lemma 2.5. Hence there exists $(m_3, m_4, m_5) \in H_x^3$ for which $m_3m_4m_5 \equiv l\,(\mathrm{mod}\,k)$. It follows from (2.11) that

$$Q_l(x) \geq \frac{2}{27}\,Q_{m_3}(\sqrt[3]{x})Q_{m_4}(\sqrt[3]{x})Q_{m_5}(\sqrt[3]{x}) + O\left(\frac{1}{\log x}\right) > \frac{1}{20^4\varphi(k)^6}.$$

This completes the proof of Theorem 1.1.

References

[1] H. Davenport, *Multiplicative Number Theory*, 3rd. ed., Grad. Texts in Math., vol. 74, Springer-Verlag, New York, 2000. Revised and with a preface by H. L. Montgomery.

[2] C. de la Vallée Poussin, *Recherches analytiques de la théorie des nombres premiers*, Deuxième partie. Ann. Soc. Sci. Bruxelles, **20** (1896), 281–362.

[3] P. G. L. Dirichlet and L. Kronecker (ed.), *G. Lejeune Dirichlet's Werke*, vol. 1, Cambridge Univ. Press, Cambridge, 2012.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th. ed., Oxford Univ. Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman; With a forward by A. J. Wiles.

[5] A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. of Math. **50** (2) (1949), 297–304.

[6] A. Selberg, *An elementary proof of the prime number theorem*, Ann. of Math. **50** (2) (1949), 305–313.

Department of Mathematics, Dartmouth College, Hanover, NH 03755, USA
Email address: steve.fan.gr@dartmouth.edu