DISTRIBUTION OF PRIME NUMBERS

W W L CHEN

Chapter 4

PRIMES IN ARITHMETIC PROGRESSIONS

4.1. Dirichlet's Theorem

The purpose of this chapter is to prove the following remarkable result of Dirichlet, widely regarded as one of the greatest achievements in mathematics.

THEOREM 4A. (DIRICHLET) *Suppose that $q \in \mathbb{N}$ and $a \in \mathbb{Z}$ satisfy $(a,q) = 1$. Then there are infinitely many primes $p \equiv a \pmod{q}$.*

Note that the requirement $(a,q) = 1$ is crucial. If $n \equiv a \pmod{q}$, then clearly $(a,q) \mid n$. It follows that if $(a,q) > 1$, then the residue class $n \equiv a \pmod{q}$ of natural numbers contains at most one prime. In other words, Dirichlet's theorem asserts that any residue class $n \equiv a \pmod{q}$ of natural numbers must contain infinitely many primes if there is no simple reason to support the contrary.

It is easy to prove Theorem 4A by elementary methods for some special values of a and q.

Examples. (i) There are infinitely many primes $p \equiv -1 \pmod{4}$. Suppose on the contrary that $p_1, \ldots, p_r$ represent all such primes. Then $4p_1 \ldots p_r - 1$ must have a prime factor $p \equiv -1 \pmod{4}$. But p cannot be any of $p_1, \ldots, p_r$.

(ii) There are infinitely many primes $p \equiv 1 \pmod{4}$. Suppose on the contrary that $p_1, \ldots, p_r$ represent all such primes. Consider the number $4(p_1 \ldots p_r)^2 + 1$. Suppose that a prime p divides $4(p_1 \ldots p_r)^2 + 1$. Then $4(p_1 \ldots p_r)^2 + 1 \equiv 0 \pmod{p}$. It follows that -1 is a quadratic residue modulo p, so that we must have $p \equiv 1 \pmod{4}$. Clearly p cannot be any of $p_1, \ldots, p_r$.

4.2. A Special Case

The idea of Dirichlet is to show that if $(a,q)=1$, then the series

$$\sum_{p\equiv a \pmod q} \frac{1}{p}$$

is divergent. For technical reasons, it is easier to show that if $(a,q)=1$, then

$$\sum_{p\equiv a \pmod q} \frac{\log p}{p^\sigma} \to +\infty \quad \text{as } \sigma\to 1+.$$

Let us illustrate the idea of Dirichlet by studying the case $n\equiv 1 \pmod 4$.

First of all, we need a function that distinguishes between integers $n\equiv 1 \pmod 4$ and the others. Suppose that n is odd. Then it is easy to check that

$$\frac{1+(-1)^{\frac{n-1}{2}}}{2} = \begin{cases} 1 & \text{if } n\equiv 1 \pmod 4,\\ 0 & \text{if } n\equiv -1 \pmod 4;\end{cases}$$

so that

$$\sum_{p\equiv 1 \pmod 4} \frac{\log p}{p^\sigma} = \frac{1}{2}\sum_{p \text{ odd}} \frac{\log p}{p^\sigma}\left(1+(-1)^{\frac{p-1}{2}}\right).$$

Now the series

$$\sum_{p \text{ odd}} \frac{\log p}{p^\sigma} \to +\infty \quad \text{as } \sigma\to 1+,$$

so it suffices to show that the series

$$\sum_{p \text{ odd}} \frac{(-1)^{\frac{p-1}{2}}\log p}{p^\sigma}$$

converges as $\sigma\to 1+$.

The next idea is to show that if we consider the series

$$\sum_{\substack{n=1\\ n \text{ odd}}}^{\infty} \frac{(-1)^{\frac{n-1}{2}}\Lambda(n)}{n^\sigma} \tag{1}$$

instead, then the contribution from the terms corresponding to non-prime odd natural numbers n is convergent. It therefore suffices to show that the series (1) converges as $\sigma\to 1+$.

Note now that the function

$$\chi(n) = \begin{cases} (-1)^{\frac{n-1}{2}} & \text{if } n \text{ is odd},\\ 0 & \text{if } n \text{ is even},\end{cases}$$

is totally multiplicative; in other words, $\chi(mn)=\chi(m)\chi(n)$ for every $m,n\in\mathbb{N}$. Write

$$L(\sigma) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^\sigma}, \tag{2}$$

and note that for every $n \in \mathbb{N}$, we have

$$\chi(n)\log n = \chi(n)\sum_{m|n}\Lambda(m) = \sum_{m|n}\chi(m)\Lambda(m)\chi\left(\frac{n}{m}\right).$$

It follows from Theorems 3B and 3E that for $\sigma > 1$, we have

$$L'(\sigma) = -\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n^\sigma} = -\left(\sum_{n=1}^{\infty}\frac{\chi(n)\Lambda(n)}{n^\sigma}\right)\left(\sum_{n=1}^{\infty}\frac{\chi(n)}{n^\sigma}\right).$$

Hence

$$\sum_{\substack{n=1\\ n \text{ odd}}}^{\infty}\frac{(-1)^{\frac{n-1}{2}}\Lambda(n)}{n^\sigma} = \sum_{n=1}^{\infty}\frac{\chi(n)\Lambda(n)}{n^\sigma} = -\frac{L'(\sigma)}{L(\sigma)}.$$

Now as $\sigma \to 1+$, we expect

$$L(\sigma) \to L(1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots > 0 \qquad \text{and} \qquad L'(\sigma) \to \frac{\log 3}{3} - \frac{\log 5}{5} + \frac{\log 7}{7} - \ldots$$

which converges by the Alternating series test. We therefore expect the series (1) to converge to a finite limit.

4.3. Dirichlet Characters

Dirichlet's most crucial discovery is that for every $q \in \mathbb{N}$, there is a family of $\phi(q)$ functions $\chi : \mathbb{N} \to \mathbb{C}$, known nowadays as the Dirichlet characters modulo q, which generalize the function χ in the special case and satisfy

$$\frac{1}{\phi(q)}\sum_{\chi \bmod q}\frac{\chi(n)}{\chi(a)} = \begin{cases} 1 & \text{if } n \equiv a \pmod{q}, \\ 0 & \text{if } n \not\equiv a \pmod{q}, \end{cases}$$

where the summation is over the $\phi(q)$ distinct Dirichlet characters modulo q.

To understand Dirichlet's ideas, we shall first of all study group characters. Our treatment here is slightly more general than is necessary, but easier to understand.

Let G be a finite abelian group of order h and with identity element e. A character on G is a non-zero complex-valued function χ on G for which $\chi(uv) = \chi(u)\chi(v)$ for every $u, v \in G$. It is easy to check the following simple results.

Remark. We have

(i) $\chi(e) = 1$;

(ii) for every $u \in G$, $\chi(u)$ is an h-th root of unity;

(iii) the number c of characters is finite; and

(iv) the characters form an abelian group.

Slightly less trivial is the following.

REMARK. If $u \in G$ and $u \neq e$, then there exists a character χ on G such that $\chi(u) \neq 1$. To see this, note that G can be expressed as a direct product of cyclic groups $G_1, \ldots, G_s$ of orders $h_1, \ldots, h_s$ respectively, where $h = h_1 \ldots h_s$. Suppose that for each $j = 1, \ldots, s$, the cyclic group G_j is generated by v_j. Then we can write $u = v_1^{y_1} \ldots v_s^{y_s}$, where $y_j \pmod{h_j}$ is uniquely determined for every $j = 1, \ldots, s$. Since $u \neq e$, there exists $k = 1, \ldots, s$ such that $y_k \not\equiv 0 \pmod{h_k}$. Let $\chi(v_k) = e(1/h_k)$, and let $\chi(v_j) = 1$ for every $j = 1, \ldots, s$ such that $j \neq k$. Clearly $\chi(u) = e(y_k/h_k) \neq 1$.

We shall denote by χ_0 the principal character on G. In other words, $\chi_0(u) = 1$ for every $u \in G$. Also, $\sum_\chi$ denotes a summation over all the distinct characters on G.

THEOREM 4B. *Suppose that G is a finite abelian group of order h and with identity element e. Suppose further that χ_0 is the principal character on G.*

(i) For every character χ on G, we have

$$\sum_{u \in G} \chi(u) = \begin{cases} h & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

(ii) For every $u \in G$, we have

$$\sum_{\chi} \chi(u) = \begin{cases} c & \text{if } u = e, \\ 0 & \text{if } u \neq e, \end{cases}$$

where c denotes the number of distinct characters on G.

(iii) We have $c = h$.

(iv) For every $u, v \in G$, we have

$$\frac{1}{h} \sum_{\chi} \frac{\chi(u)}{\chi(v)} = \begin{cases} 1 & \text{if } u = v, \\ 0 & \text{if } u \neq v. \end{cases}$$

PROOF. (i) If $\chi = \chi_0$, then the result is obvious. If $\chi \neq \chi_0$, then there exists $v \in G$ such that $\chi(v) \neq 1$, and so

$$\chi(v) \sum_{u \in G} \chi(u) = \sum_{u \in G} \chi(u)\chi(v) = \sum_{u \in G} \chi(uv) = \sum_{u \in G} \chi(u),$$

the last equality following from the fact that uv runs over all the elements of G as u runs over all the elements of G. Hence

$$(1 - \chi(v)) \sum_{u \in G} \chi(u) = 0.$$

The result follows since $\chi(v) \neq 1$.

(ii) If $u = e$, then the result is obvious. If $u \neq e$, then we have already shown that there exists a character χ_1 such that $\chi_1(u) \neq 1$, and so

$$\chi_1(u) \sum_{\chi} \chi(u) = \sum_{\chi} \chi_1(u)\chi(u) = \sum_{\chi} (\chi_1\chi)(u) = \sum_{\chi} \chi(u),$$

the last equality following from noting that the characters on G form an abelian group so that $\chi_1\chi$ runs through all the characters on G as χ runs through all the characters on G. Hence

$$(1 - \chi_1(u)) \sum_{\chi} \chi(u) = 0.$$

The result follows since $\chi_1(u) \neq 1$.

(iii) Note that

$$h = \sum_{\chi} \sum_{u \in G} \chi(u) = \sum_{u \in G} \sum_{\chi} \chi(u) = c.$$

(iv) Note that

$$\frac{1}{h} \sum_{\chi} \frac{\chi(u)}{\chi(v)} = \frac{1}{h} \sum_{\chi} \chi(u)\chi(v^{-1}) = \frac{1}{h} \sum_{\chi} \chi(uv^{-1}) = \begin{cases} c/h & \text{if } uv^{-1} = e, \\ 0 & \text{if } uv^{-1} \neq e. \end{cases}$$

The result follows since $h = c$. ○

We are now in a position to introduce Dirichlet characters. Let $q \in \mathbb{N}$ be given. Then there are exactly $\phi(q)$ residue classes $n \equiv a \pmod{q}$ satisfying $(a, q) = 1$. Under multiplication of residue classes, they form an abelian group of order $\phi(q)$. Suppose that these residue classes are represented by $a_1, \ldots, a_{\phi(q)}$ modulo q. Let $G = \{a_1, \ldots, a_{\phi(q)}\}$. We can now define a character χ on the group G as described earlier, interpreting the group elements as residue classes. Furthermore, we can extend the definition to cover the remaining residue classes. Precisely, for every $n \in \mathbb{N}$, let

$$\chi(n) = \begin{cases} \chi(a_j) & \text{if } n \equiv a_j \pmod{q} \text{ for some } j = 1, \ldots, \phi(q), \\ 0 & \text{if } (n, q) > 1. \end{cases} \tag{3}$$

A function $\chi : \mathbb{N} \to \mathbb{C}$ of the form (3) is called a Dirichlet character modulo q. Note that χ is totally multiplicative. Also, clearly there are exactly $\phi(q)$ Dirichlet characters modulo q. Furthermore, the principal Dirichlet character χ_0 modulo q is defined by

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n, q) = 1, \\ 0 & \text{if } (n, q) > 1. \end{cases}$$

The following theorem follows immediately from these observations and Theorem 4B.

THEOREM 4C. *Suppose that $q \in \mathbb{N}$. Suppose further that χ_0 is the principal Dirichlet character modulo q.*

(i) For every Dirichlet character χ modulo q, we have

$$\sum_{n \pmod{q}} \chi(n) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

(ii) For every $n \in \mathbb{N}$, we have

$$\sum_{\chi \pmod{q}} \chi(n) = \begin{cases} \phi(q) & \text{if } n \equiv 1 \pmod{q}, \\ 0 & \text{if } n \not\equiv 1 \pmod{q}. \end{cases}$$

(iii) For every $a \in \mathbb{Z}$ satisfying $(a, q) = 1$ and for every $n \in \mathbb{N}$, we have

$$\frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \frac{\chi(n)}{\chi(a)} = \begin{cases} 1 & \text{if } n \equiv a \pmod{q}, \\ 0 & \text{if } n \not\equiv a \pmod{q}. \end{cases}$$

4.4. Some Dirichlet Series

Our next task is to introduce the functions analogous to the function (2) earlier. Let $s = \sigma + it \in \mathbb{C}$, where $\sigma, t \in \mathbb{R}$. For $\sigma > 1$, let

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}; \tag{4}$$

furthermore, for any Dirichlet character χ modulo q, let

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}. \tag{5}$$

The functions (4) and (5) are called the Riemann zeta function and Dirichlet L-functions respectively. Note that the series are Dirichlet series and converge absolutely for $\sigma > 1$ and uniformly for $\sigma > 1 + \delta$ for any $\delta > 0$. Furthermore, the coefficients are totally multiplicative. It follows from Theorem 3G that for $\sigma > 1$, the series (4) and (5) have the Euler product representations

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} \qquad \text{and} \qquad L(s,\chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}$$

respectively. The following are some simple properties of these functions.

THEOREM 4D. *Suppose that $\sigma > 1$. Then $\zeta(s) \neq 0$. Furthermore, $L(s,\chi) \neq 0$ for any Dirichlet character χ modulo q.*

PROOF. Since $\sigma > 1$, we have

$$|\zeta(s)| = \left| \prod_p (1 - p^{-s})^{-1} \right| \geq \prod_p (1 + p^{-\sigma})^{-1} = \prod_p \frac{1 - p^{-\sigma}}{1 - p^{-2\sigma}} = \frac{\zeta(2\sigma)}{\zeta(\sigma)} > 0$$

and

$$|L(s,\chi)| = \left| \prod_p (1 - \chi(p) p^{-s})^{-1} \right| \geq \prod_{p \nmid q} (1 + p^{-\sigma})^{-1} \geq \prod_p (1 + p^{-\sigma})^{-1} > 0.$$

This completes the proof. ○

THEOREM 4E. *Suppose that χ_0 is the principal Dirichlet character modulo q. Then for $\sigma > 1$, we have*

$$L(s,\chi_0) = \zeta(s) \prod_{p \mid q} (1 - p^{-s}).$$

PROOF. Since $\sigma > 1$, we have

$$L(s,\chi_0) = \prod_p (1 - \chi_0(p) p^{-s})^{-1} = \prod_{p \nmid q} (1 - p^{-s})^{-1} = \frac{\displaystyle\prod_p (1 - p^{-s})^{-1}}{\displaystyle\prod_{p \mid q} (1 - p^{-s})^{-1}} = \zeta(s) \prod_{p \mid q} (1 - p^{-s}).$$

This completes the proof. ○

THEOREM 4F. *Suppose that $\sigma > 1$. Then*

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$

Furthermore, for every Dirichlet character χ modulo q, we have

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

PROOF. Since $\sigma > 1$, it follows from Theorem 3B that

$$-\zeta'(s) = \sum_{n=1}^{\infty} (\log n) n^{-s}.$$

It now follows from Theorem 3E and

$$\log n = \sum_{m \mid n} \Lambda(m)$$

that

$$-\zeta'(s) = \left(\sum_{n=1}^{\infty} \Lambda(n) n^{-s}\right)\left(\sum_{n=1}^{\infty} n^{-s}\right).$$

The first assertion follows. On the other hand, it also follows from Theorem 3B that

$$-L'(s,\chi) = \sum_{n=1}^{\infty} \chi(n)(\log n) n^{-s}.$$

It now follows from Theorem 3E and

$$\chi(n)\log n = \sum_{m \mid n} \chi(m)\Lambda(m)\chi\left(\frac{n}{m}\right)$$

that

$$-L'(s,\chi) = \left(\sum_{n=1}^{\infty} \chi(n)\Lambda(n) n^{-s}\right)\left(\sum_{n=1}^{\infty} \chi(n) n^{-s}\right).$$

The second assertion follows. ○

THEOREM 4G. *If $\sigma > 1$, then for every Dirichlet character χ modulo q, we have*

$$\log L(s,\chi) = \sum_{p} \sum_{m=1}^{\infty} m^{-1} \chi(p^m) p^{-ms}.$$

PROOF. Taking logarithms on the Euler product representation, we have

(6) $$\log L(s,\chi) = \log \prod_{p} (1-\chi(p)p^{-s})^{-1} = \sum_{p} \log(1-\chi(p)p^{-s})^{-1},$$

so that

$$-\log L(s,\chi) = \sum_p \log(1-\chi(p)p^{-s}).$$

The justification for (6) is that the series on the right hand side converges uniformly for $\sigma > 1+\delta$, as can be deduced from the Weierstrass M-test on noting that

$$|\log(1-\chi(p)p^{-s})| \le 2|\chi(p)p^{-s}| \le 2p^{-1-\delta}.$$

The proof is now completed by expanding $\log(1-\chi(p)p^{-s})$. ○

4.5. Analytic Continuation

Our next task is to extend the definition of $\zeta(s)$ and $L(s,\chi)$ to the half plane $\sigma > 0$. This is achieved by analytic continuation.

An example of analytic continuation is the following: Consider the geometric series

$$f(s) = \sum_{n=0}^\infty s^n.$$

This series converges absolutely in the set $\{s \in \mathbb{C} : |s| < 1\}$ and uniformly in the set $\{s \in \mathbb{C} : |s| < 1-\delta\}$ for any $\delta > 0$ to the sum $1/(1-s)$. Now let

$$g(s) = \frac{1}{1-s}$$

in $\mathbb{C}$. Then g is analytic in the set $\mathbb{C} \setminus \{1\}$, $g(s) = f(s)$ in the set $\{s \in \mathbb{C} : |s| < 1\}$, and g has a pole at $s = 1$. So g can be viewed as an analytic continuation of f to $\mathbb{C}$ with a pole at $s = 1$.

Returning to the functions $\zeta(s)$ and $L(s,\chi)$, we shall establish the following results on analytic continuation.

THEOREM 4H. *The function $\zeta(s)$ admits an analytic continuation to the half plane $\sigma > 0$, and is analytic in this half plane except for a simple pole at $s = 1$ with residue 1.*

THEOREM 4J. *Suppose that $q \in \mathbb{N}$ and χ_0 is the principal Dirichlet character modulo q. Then the function $L(s,\chi_0)$ admits an analytic continuation to the half plane $\sigma > 0$, and is analytic in this half plane except for a simple pole at $s = 1$ with residue $\phi(q)/q$.*

THEOREM 4K. *Suppose that $q \in \mathbb{N}$ and χ is a non-principal Dirichlet character modulo q. Then the function $L(s,\chi)$ admits an analytic continuation to the half plane $\sigma > 0$, and is analytic in this half plane.*

The proofs of these three theorems depend on the following two simple technical results. The first of these is basically a result on partial summation.

THEOREM 4L. *Suppose that $a(n) = O(1)$ for every $n \in \mathbb{N}$. For every $x > 0$, write*

$$S(x) = \sum_{n \le x} a(n).$$

Suppose further that for $\sigma > 1$, we have

$$F(s) = \sum_{n=1}^{\infty} a(n)n^{-s}.$$

Then for every $X > 0$ and $\sigma > 1$, we have

$$\sum_{n \le X} a(n)n^{-s} = S(X)X^{-s} + s\int_1^X S(x)x^{-s-1}\,\mathrm{d}x. \tag{7}$$

Furthermore, for $\sigma > 1$, we have

$$F(s) = s\int_1^{\infty} S(x)x^{-s-1}\,\mathrm{d}x. \tag{8}$$

Proof. To prove (7), simply note that

$$\begin{aligned}\sum_{n \le X} a(n)n^{-s} - S(X)X^{-s} &= \sum_{n \le X} a(n)(n^{-s} - X^{-s}) = \sum_{n \le X} a(n)\int_n^X sx^{-s-1}\,\mathrm{d}x \\ &= s\int_1^X \left(\sum_{n \le x} a(n)\right) x^{-s-1}\,\mathrm{d}x = s\int_1^X S(x)x^{-s-1}\,\mathrm{d}x.\end{aligned}$$

Also, (8) follows from (7) on letting $X \to \infty$. ◯

The second technical result, standard in complex function theory, will be stated without proof.

THEOREM 4M. *Suppose that the path Γ is defined by $w(t) = u(t) + \mathrm{i}v(t)$, where $u(t), v(t) \in \mathbb{R}$ for every $t \in [0, 1]$. Suppose further that $u'(t)$ and $v'(t)$ are continuous on $[0, 1]$. Let D be a domain in $\mathbb{C}$. For every $s \in D$, let*

$$F(s) = \int_{\Gamma} f(s, w)\,\mathrm{d}w,$$

where
- *$f(s, w)$ is continuous for every $s \in D$ and every $w \in \Gamma$; and*
- *for every $w \in \Gamma$, the function $f(s, w)$ is analytic in D.*

Then $F(s)$ is analytic in D.

Proof of Theorem 4H. Let $F(s) = \zeta(s)$. In the notation of Theorem 4L, we have $a(n) = 1$ for every $n \in \mathbb{N}$, so that $S(x) = [x]$ for every $x > 0$. It follows from (8) that

$$\zeta(s) = s\int_1^{\infty} [x]x^{-s-1}\,\mathrm{d}x = s\int_1^{\infty} x^{-s}\,\mathrm{d}x - s\int_1^{\infty} \{x\}x^{-s-1}\,\mathrm{d}x = 1 + \frac{1}{s-1} - s\int_1^{\infty} \{x\}x^{-s-1}\,\mathrm{d}x.$$

We shall show that the last term on the right hand side represents an analytic function for $\sigma > 0$. We can write

$$\int_1^{\infty} \{x\}x^{-s-1}\,\mathrm{d}x = \sum_{n=1}^{\infty} F_n(s),$$

where for every $n \in \mathbb{N}$,

$$F_n(s) = \int_n^{n+1} \{x\} x^{-s-1} \, \mathrm{d}x.$$

It remains to show that (i) for every $n \in \mathbb{N}$, the function $F_n(s)$ is analytic in $\mathbb{C}$; and (ii) for every $\delta > 0$, the series $\sum_{n=1}^{\infty} F_n(s)$ converges uniformly for $\sigma > \delta$. To show (i), note that by a change of variable,

$$F_n(s) = \int_0^1 t(n+t)^{-s-1} \, \mathrm{d}t = \int_0^1 t\mathrm{e}^{-(s+1)\log(n+t)} \, \mathrm{d}t,$$

and (i) follows from Theorem 4M. To show (ii), note that for $\sigma > \delta$, we have

$$|F_n(s)| = \left| \int_n^{n+1} \{x\} x^{-s-1} \, \mathrm{d}x \right| \le n^{-\sigma-1} < n^{-1-\delta},$$

and (ii) follows from the Weierstrass M-test. ○

Proof of Theorem 4J. Suppose that $\sigma > 1$. Recall Theorem 4E, that

$$L(s, \chi_0) = \zeta(s) \prod_{p \mid q} \left(1 - \frac{1}{p^s} \right).$$

Clearly the right hand side is analytic for $\sigma > 0$ except for a simple pole at $s = 1$. Furthermore, at $s = 1$, the function $\zeta(s)$ has a simple pole with residue 1, while

$$\prod_{p \mid q} \left(1 - \frac{1}{p} \right) = \frac{\phi(q)}{q}.$$

The result follows. ○

The proof of Theorem 4K is left as an exercise.

4.6. Proof of Dirichlet's Theorem

We now attempt to prove Theorem 4A. The result below will enable us to consider the analogue of (1).

THEOREM 4N. *Suppose that $\sigma > 1$. Then*

$$\sum_{p \equiv a \pmod{q}} \frac{\log p}{p^\sigma} = \sum_{n \equiv a \pmod{q}} \frac{\Lambda(n)}{n^\sigma} + O(1).$$

Proof. Note first of all that the sum on the left hand side does not exceed the first term on the right hand side. On the other hand, we have

$$\sum_{n \equiv a \pmod{q}} \frac{\Lambda(n)}{n^\sigma} - \sum_{p \equiv a \pmod{q}} \frac{\log p}{p^\sigma} \le \sum_p \sum_{m=2}^{\infty} \frac{\log p}{p^{m\sigma}}$$
$$\le \sum_p \sum_{m=2}^{\infty} \frac{\log p}{p^m} = \sum_p \frac{\log p}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1).$$

The result follows. ○

Combining Theorems 4N, 4C and 4F, we have

$$(9)\qquad \sum_{p\equiv a \pmod q} \frac{\log p}{p^\sigma} = \sum_{n\equiv a \pmod q} \frac{\Lambda(n)}{n^\sigma} + O(1) = \sum_{n=1}^\infty \left(\frac{1}{\phi(q)} \sum_{\chi \pmod q} \frac{\chi(n)}{\chi(a)} \right) \frac{\Lambda(n)}{n^\sigma} + O(1)$$

$$= \frac{1}{\phi(q)} \sum_{\chi \pmod q} \frac{1}{\chi(a)} \sum_{n=1}^\infty \frac{\chi(n)\Lambda(n)}{n^\sigma} + O(1) = -\frac{1}{\phi(q)} \sum_{\chi \pmod q} \frac{1}{\chi(a)} \frac{L'(\sigma,\chi)}{L(\sigma,\chi)} + O(1).$$

Suppose now that

$$(10)\qquad \sum_{\substack{\chi \pmod q\\ \chi\neq\chi_0}} \frac{1}{\chi(a)} \frac{L'(\sigma,\chi)}{L(\sigma,\chi)} = O(1) \quad \text{as } \sigma \to 1+.$$

Then combining (9) and (10), we have

$$\sum_{p\equiv a \pmod q} \frac{\log p}{p^\sigma} = -\frac{1}{\phi(q)} \frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} + O(1) = \frac{1}{\phi(q)} \frac{1}{\sigma-1} + O(1) \to \infty \quad \text{as } \sigma \to 1+.$$

since the function $L'(s,\chi_0)/L(s,\chi_0)$ has a simple pole at $s=1$ with residue -1 by Theorem 4J. To complete the proof of Dirichlet's theorem, it remains to prove (10). Clearly (10) will follow if we can show that for every non-principal Dirichlet character $\chi \pmod q$, we have $L(1,\chi)\neq 0$. Here we need to distinguish two cases, represented by the next two theorems.

THEOREM 4P. *Suppose that $q\in\mathbb{N}$ and χ is a non-real Dirichlet character modulo q. Then we have $L(1,\chi)\neq 0$.*

Proof. For $\sigma>1$, we have, in view of Theorem 4G, that

$$\sum_{\chi \pmod q} \log L(\sigma,\chi) = \sum_{\chi \pmod q} \sum_p \sum_{m=1}^\infty \chi(p^m) m^{-1} p^{-m\sigma}$$

$$= \sum_p \sum_{m=1}^\infty \left(\sum_{\chi \pmod q} \chi(p^m) \right) m^{-1}p^{-m\sigma} = \phi(q) \sum_p \sum_{\substack{m=1\\ p^m\equiv 1 \pmod q}}^\infty m^{-1}p^{-m\sigma} > 0,$$

where the change of order of summation is justified since

$$\sum_{\chi \pmod q} \sum_p \sum_{m=1}^\infty |\chi(p^m)m^{-1}p^{-m\sigma}|$$

is finite. It follows that

$$(11)\qquad \left| \prod_{\chi \pmod q} L(\sigma,\chi) \right| > 1.$$

Suppose that χ_1 is a non-real Dirichlet character modulo q, and $L(1,\chi_1)=0$. Then $\chi_1\neq\overline{\chi_1}$, and $L(1,\overline{\chi_1}) = \overline{L(1,\chi_1)} = 0$ also. It follows that these two zeros more than cancel the simple pole of $L(\sigma,\chi_0)$ at $\sigma=1$, so that the product on the left hand side of (11) has a zero at $\sigma=1$. This gives a contradiction. ○

Clearly this approach does not work when χ is real.

THEOREM 4Q. *Suppose that $q \in \mathbb{N}$ and χ is a real, non-principal Dirichlet character modulo q. Then we have $L(1,\chi) \neq 0$.*

Proof. Suppose that the result is false, so that there exists a real Dirichlet character χ modulo q such that $L(1,\chi) = 0$. Then the function $F(s) = \zeta(s)L(s,\chi)$ is analytic for $\sigma > 0$. Note that for $\sigma > 1$, we have

$$F(s) = \sum_{n=1}^{\infty} f(n)n^{-s},$$

where for every $n \in \mathbb{N}$,

$$f(n) = \sum_{m \mid n} \chi(m).$$

Let the function $g : \mathbb{N} \to \mathbb{R}$ be defined by

$$g(n) = \begin{cases} 1 & \text{if } n \text{ is a perfect square,} \\ 0 & \text{otherwise.} \end{cases}$$

We shall first of all show that for every $n \in \mathbb{N}$, we have

$$f(n) \geq g(n). \tag{12}$$

Since χ is totally multiplicative, it suffices to prove (12) when $n = p^k$, where p is a prime and $k \in \mathbb{N}$. Indeed, since χ assumes only the values ± 1 and 0, we have

$$f(p^k) = 1 + \chi(p) + (\chi(p))^2 + \ldots + (\chi(p))^k = \begin{cases} 1 & \text{if } \chi(p) = 0, \\ k+1 & \text{if } \chi(p) = 1, \\ 1 & \text{if } \chi(p) = -1 \text{ and } k \text{ is even,} \\ 0 & \text{if } \chi(p) = -1 \text{ and } k \text{ is odd,} \end{cases}$$

so that

$$f(p^k) \geq g(p^k) = \begin{cases} 1 & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

Suppose now that $0 < r < 3/2$. Since $F(s)$ is analytic for $\sigma > 0$, we must have the Taylor expansion

$$F(2-r) = \sum_{\nu=0}^{\infty} \frac{F^{(\nu)}(2)}{\nu!}(-r)^{\nu}.$$

Now by Theorem 3B, we have

$$F^{(\nu)}(2) = \sum_{n=1}^{\infty} f(n)(-\log n)^{\nu} n^{-2}.$$

It follows that for every $\nu \in \mathbb{N} \cup \{0\}$, we have, in view of (12),

$$\begin{aligned} \frac{F^{(\nu)}(2)}{\nu!}(-r)^{\nu} &= \frac{r^{\nu}}{\nu!} \sum_{n=1}^{\infty} f(n)(\log n)^{\nu} n^{-2} \geq \frac{r^{\nu}}{\nu!} \sum_{n=1}^{\infty} g(n)(\log n)^{\nu} n^{-2} = \frac{r^{\nu}}{\nu!} \sum_{k=1}^{\infty} (\log k^2)^{\nu} (k^2)^{-2} \\ &= \frac{(2r)^{\nu}}{\nu!} \sum_{k=1}^{\infty} (\log k)^{\nu} k^{-4} = \frac{(-2r)^{\nu}}{\nu!} \sum_{k=1}^{\infty} (-\log k)^{\nu} k^{-4} = \frac{(-2r)^{\nu}}{\nu!} \zeta^{(\nu)}(4) \end{aligned}$$

by Theorem 3B. It follows that for $0 < r < 3/2$, we have

$$F(2-r) \geq \sum_{\nu=0}^{\infty} \frac{(-2r)^{\nu}}{\nu!} \zeta^{(\nu)}(4) = \zeta(4-2r).$$

Now as $r \to 3/2-$, we must therefore have $F(2-r) \to +\infty$. This contradicts our assertion that $F(s)$ is analytic for $\sigma > 0$ and hence continuous at $s = 1/2$. ○

Problems for Chapter 4

1. Suppose that $q \in \mathbb{N}$, and that χ is a non-principal character modulo q.
   (i) Show that for every $X > 0$, we have

$$\left| \sum_{n \le X} \chi(n) \right| \le q.$$

   (ii) Noting that the function

$$S(X) = \sum_{n \le X} \chi(n)$$

   is constant between consecutive natural numbers, prove Theorem 4K.