Chapter 4

Primes in Arithmetic Progressions — I

1. Additive characters

If $f(z) = \sum_{n=0}^{\infty} c_n z^n$ is a power series, we can restrict our attention to terms for which n has prescribed parity by considering

$$\frac{1}{2}f(z) + \frac{1}{2}f(-z) = \sum_{\substack{n=0 \\ n\equiv 0\ (2)}}^{\infty} c_n z^n$$

or

$$\frac{1}{2}f(z) - \frac{1}{2}f(-z) = \sum_{\substack{n=0 \\ n\equiv 1\ (2)}}^{\infty} c_n z^n.$$

That is, we can express the characteristic function of an arithmetic progression (mod 2) as a linear combination $\frac{1}{2}1^n \pm \frac{1}{2}(-1)^n$ of 1^n and $(-1)^n$. Here 1 and -1 are the square-roots of 1, and we can similarly express the characteristic function of an arithmetic progression (mod q) as a linear combination of the sequences ζ^n where ζ runs over the q different q^{th} roots of unity. We write $e(\theta) = e^{2\pi i\theta}$, and then the q^{th} roots of unity are the numbers $\zeta = e(a/q)$ for $1 \le a \le q$. If $(a,q) = 1$ then the least integer n such that $\zeta^n = 1$ is q, and we say that ζ is a *primitive* q^{th} root of unity. From the formula

$$\sum_{k=0}^{q-1} \zeta^k = \frac{1-\zeta^q}{1-\zeta}$$

for the sum of a geometric progression, we see that if ζ is a q^{th} root of unity then

$$\sum_{k=1}^{q} \zeta^k = 0$$

unless $\zeta = 1$. Hence

$$\frac{1}{q}\sum_{k=1}^{q} e(-ka/q)e(kn/q) = \begin{cases} 1 & \text{if } n \equiv a \pmod q, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

and thus the characteristic function of an arithmetic progression (mod q) can be expressed as a linear combination of the sequences $e(kn/q)$. These functions are called the *additive characters* (mod q) because they are the homomorphisms from the additive group $(\mathbb{Z}/q\mathbb{Z})^+$ of integers (mod q) to the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers.

In the language of linear algebra we see that the arithmetic functions of period q form a vector space of dimension q. For any k, $1 \le k \le q$, the sequence $\{e(kn/q)\}_{n=-\infty}^{\infty}$ has period q, and these q sequences form a basis for the space of q-periodic arithmetic functions. Indeed, the formula (1) expresses the a^{th} elementary vector as a linear combination of the vectors $[e(n/q), e(2n/q), \dots, e((q-1)n/q), 1]$.

If $f(n)$ is an arithmetic function with period q then we define the *finite Fourier transform* of f to be the function

$$\widehat{f}(k) = \frac{1}{q}\sum_{n=1}^{q} f(n)e(-kn/q). \tag{2}$$

To obtain a Fourier representation of f we multiply both sides of (1) by $f(n)$ and sum over n to see that

$$\begin{aligned} f(a) &= \sum_{n=1}^{q} \frac{f(n)}{q} \sum_{k=1}^{q} e(-ka/q)e(kn/q) \\ &= \sum_{k=1}^{q} e(-ka/q)\frac{1}{q}\sum_{n=1}^{q} f(n)e(kn/q) \\ &= \sum_{k=1}^{q} e(-ka/q)\widehat{f}(-k). \end{aligned}$$

Here the exact values that k runs through are immaterial, as long as the set of these values forms a complete residue system modulo q. Hence we may replace k by $-k$ in the above, and so we see that

$$f(n) = \sum_{k=1}^{q} \widehat{f}(k)e(kn/q). \tag{3}$$

This includes (1) as a special case, for if we take f to be the characteristic function of the arithmetic progression a (mod q) then by (2) we have $\widehat{f}(k) = e(-ka/q)/q$, and then (3) coincides with (1). The pair (2), (3) of inversion formulæ are analogous to the formula for the Fourier coefficients and Fourier expansion of a function $f \in L^1(\mathbb{T})$, but the situation here is simpler because our sums have only finitely many terms.

Let $\boldsymbol{v}(h)$ be the vector $\boldsymbol{v}(h) = [e(h/q), e(2h/q), \dots, e((q-1)h/q), 1]$. From (1) we see that two such vectors $\boldsymbol{v}(h_1)$ and $\boldsymbol{v}(h_2)$ are orthogonal unless $h_1 \equiv h_2 \pmod q$. These vectors are not normalized, but they all have the same length $\sqrt{q}$, so apart from some rescaling, the transformation from f to $\widehat{f}$ is an isometry. More precisely, if f has period q and $\widehat{f}$ is given by (2), then by (3),

$$\sum_{n=1}^{q} |f(n)|^2 = \sum_{n=1}^{q} \Big| \sum_{k=1}^{q} \widehat{f}(k)e(kn/q)\Big|^2.$$

By expanding and taking the sum over n inside, we see that this is

$$= \sum_{j=1}^{q} \sum_{k=1}^{q} \widehat{f}(j)\overline{\widehat{f}(k)} \sum_{n=1}^{q} e(jn/q)e(-kn/q).$$

By (1) the innermost sum is q if $j = k$ and is 0 otherwise. Hence

$$\sum_{n=1}^{q} |f(n)|^2 = q \sum_{k=1}^{q} |\widehat{f}(k)|^2. \tag{4}$$

This is analogous to Parseval's identity for functions $f \in L^2(\mathbb{T})$, or to Plancherel's identity for functions $f \in L^2(\mathbb{R})$.

Among the exponential sums that we shall have occasion to consider is *Ramanujan's sum*

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(an/q). \tag{5}$$

We now establish some of the interesting properties of this quantity.

Theorem 1. *As a function of n, $c_q(n)$ has period q. For any given n, $c_q(n)$ is a multiplicative function of q. Also,*

$$\sum_{d|q} c_d(n) = \begin{cases} q & \text{if } q|n, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Finally,

$$c_q(n) = \sum_{d|(q,n)} d\mu(q/d) = \frac{\mu(q/(q,n))}{\varphi(q/(q,n))}\varphi(q). \tag{7}$$

The case $n = 1$ of this last formula is especially memorable:

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(a/q) = \mu(q).$$

Proof. The first assertion is evident, as each term in the sum (5) has period q. As for the second, suppose that $q = q_1q_2$ where $(q_1, q_2) = 1$. By the Chinese Remainder Theorem, for each $a \pmod q$ there is a unique pair a_1, a_2 with a_i determined $(\mod q_i)$, so that

$a \equiv a_1q_2 + a_2q_1 \pmod q$. Moreover, under this correspondence we see that $(a,q) = 1$ if and only if $(a_i, q_i) = 1$ for $i = 1, 2$. Then

$$\begin{aligned} c_q(n) &= \sum_{\substack{a_1=1\\(a_1,q_1)=1}}^{q_1} \sum_{\substack{a_2=1\\(a_2,q_2)=1}}^{q_2} e\big((a_1q_2 + a_2q_1)n/(q_1q_2)\big) \\ &= \Big(\sum_{\substack{a_1=1\\(a_1,q_1)=1}}^{q_1} e(a_1n/q_1)\Big)\Big(\sum_{\substack{a_2=1\\(a_2,q_2)=1}}^{q_2} e(a_2n/q_2)\Big) \\ &= c_{q_1}(n)c_{q_2}(n). \end{aligned}$$

To establish (6), suppose that $d|q$, and consider those a, $1 \le a \le q$, such that $(a,q) = d$. Put $b = a/d$. Then the numbers a are in one-to-one correspondence with those b, $1 \le b \le q/d$, for which $(b, q/d) = 1$. Hence

$$\begin{aligned} \sum_{a=1}^{q} e(na/q) &= \sum_{d|q} \sum_{\substack{a=1\\(a,q)=d}}^{q} e(na/q) \\ &= \sum_{d|q} \sum_{\substack{b=1\\(b,q/d)=1}}^{q/d} e(nb/(q/d)) \\ &= \sum_{d|q} c_{q/d}(n). \end{aligned}$$

By (1), the left hand side above is q if $q|n$, and is 0 otherwise. Thus we have (6).

The first formula in (7) is merely the Möbius inverse of (6). To obtain the second formula in (7), we begin by considering the special case in which q is a prime power, $q = p^k$.

$$\begin{aligned} c_{p^k}(n) &= \sum_{\substack{a=1\\p\nmid a}}^{p^k} e(na/p^k) \\ &= \sum_{a=1}^{p^k} e(na/p^k) - \sum_{a=1}^{p^{k-1}} e(na/p^{k-1}). \end{aligned}$$

Here the first sum is p^k if $p^k|n$, and is 0 otherwise. Similarly, the second sum is p^{k-1} if $p^{k-1}|n$, and is 0 otherwise. Hence the above is

$$\begin{aligned} &= \begin{cases} 0 & \text{if } p^{k-1} \nmid n, \\ -p^{k-1} & \text{if } p^{k-1} \| n, \\ p^k - p^{k-1} & \text{if } p^k | n \end{cases} \\ &= \frac{\mu\big(p^k/(n,p^k)\big)}{\varphi\big(p^k/(n,p^k)\big)}\varphi(p^k). \end{aligned}$$

The general case of (7) now follows because $c_q(n)$ is a multiplicative function of q.

4.1. Exercises

1. Let $U = [u_{kn}]$ be the $q \times q$ matrix with elements $u_{kn} = e(kn/q)/\sqrt{q}$. Show that $UU^* = U^*U = I$, i.e., that U is unitary.

2. (Friedman (1957); cf Reznick (1995)) (a) Show that

$$\int_0^1 \big(ue(\theta/2) + ve(-\theta/2)\big)^{2r}\, d\theta = \binom{2r}{r} u^r v^r$$

for any non-negative integer r and arbitrary complex numbers u, v.
(b) Show that if $u = (x - iy)/2$, $v = (x + iy)/2$, then

$$x\cos\pi\theta + y\sin\pi\theta = ue(\theta/2) + ve(-\theta/2)$$

for all θ.
(c) Show that

$$\int_0^1 \big(x\cos\pi\theta + y\sin\pi\theta\big)^{2r}\, d\theta = \binom{2r}{r} 2^{-2r}(x^2 + y^2)^r$$

for any non-negative integer r and arbitrary real or complex numbers x, y.
(d) Show that

$$\sum_{a=1}^{q} \big(ue^{\pi ia/q} + ve^{-\pi ia/q}\big)^{2r} = q\binom{2r}{r} u^r v^r$$

if r is an integer, $0 \le r < q$.
(e) Show that

$$\sum_{a=1}^{q} \big(x\cos\pi a/q + y\sin\pi a/q\big)^{2r} = q\binom{2r}{r} 2^{-2r}(x^2 + y^2)^r$$

if r is an integer, $0 \le r < q$.

3. Show that $|c_q(n)| \le (q, n)$.

4. (Carmichael (1932)) (a) Show that if $q > 1$ then

$$\sum_{n=1}^{q} c_q(n) = 0.$$

(b) Show that if $q_1 \ne q_2$ and $[q_1, q_2] | N$, then

$$\sum_{n=1}^{N} c_{q_1}(n) c_{q_2}(n) = 0.$$

(c) Show that if $q|N$ then

$$\sum_{n=1}^{N} c_q(n)^2 = N\varphi(q).$$

5. (Grytczuk (1981); cf Redmond (1983)) Show that

$$\sum_{d|q} |c_d(n)| = 2^{\omega(q/(q,n))}(q,n).$$

6. (Ramanujan (1918)) Show that

$$\frac{\varphi(n)}{n} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sum_{q|d} c_q(n) = \sum_{q=1}^{\infty} a_q c_q(n)$$

where

$$a_q = \frac{6\mu(q)}{\pi^2 q^2} \prod_{p|q} \Big(1 - \frac{1}{p^2}\Big)^{-1}.$$

7. (Wintner (1943, §§33–35)) The orthogonality relations of Exercise 4 give us hope that it might be possible to represent an arithmetic function $F(n)$ in the form

$$F(n) = \sum_{q=1}^{\infty} a_q c_q(n) \tag{8}$$

by taking

$$a_q = \frac{1}{\varphi(q)} \lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} F(n) c_q(n)\,. \tag{9}$$

In the following, suppose that $f(r)$ is chosen so that $F(n) = \sum_{r|n} f(r)$ for all n.
(a) Suppose that

$$\sum_{r=1}^{\infty} \frac{|f(r)|}{r} < \infty\,. \tag{10}$$

Let d be a fixed positive integer. Show that

$$\sum_{\substack{n\le x\\ d|n}} F(n) = \frac{x}{d} \sum_{r=1}^{\infty} \frac{f(r)}{r}(d,r) \ + o(x)$$

as $x \to \infty$.
(b) Suppose that (10) holds. Show that

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} F(n)c_q(n) = \varphi(q) \sum_{\substack{r=1\\ q|r}}^{\infty} \frac{f(r)}{r}\,.$$

(c) Put

$$a_q = \sum_{\substack{r=1\\ q|r}}^{\infty} \frac{f(r)}{r}\,.$$

Show that if

$$\sum_{r=1}^{\infty} \frac{|f(r)|d(r)}{r} < \infty \tag{11}$$

then (8) and (9) hold, and moreover that $\sum_{q=1}^{\infty} |a_q c_q(n)| < \infty$.

8. (Ramanujan (1918)) Show that if $q > 1$, then $\sum_{n=1}^{\infty} c_q(n)/n = -\Lambda(q)$. (See also Exercise 8.3.4.)

9. Let $\Phi_q(z)$ denote the q^{th} cyclotomic polynomial, i.e. the monic polynomial whose roots are precisely the primitive q^{th} roots of unity, so that

$$\Phi_q(z) = \prod_{\substack{n=1\\ (n,q)=1}}^{q} (z - e(n/q)).$$

(a) Show that

$$\Phi_q(z) = \prod_{d|q} \left(z^d - 1\right)^{\mu(q/d)}$$

and that $\left(z^d - 1\right)^{\mu(q/d)}$ has a power series expansion, valid when $|z| < 1$, with integer coefficients. Deduce that $\Phi_q(z) \in \mathbb{Z}[z]$.
(b) Suppose that $z \in \mathbb{Z}$ and $p \mid \Phi_q(z)$ and let e denote the order of z modulo p. Show that $e \mid q$ and that if $p \mid (z^d - 1)$ then $e \mid d$.
(c) Choose t so that $p^t \| (z^e - 1)$. Show that for $m \in \mathbb{N}$ with $p \nmid m$ one has $p^t \| (z^{me} - 1)$.
(d) Show that if $p \nmid q$, then $p^{ht} \| \Phi_q(z)$ where $h = \sum_{e|d|q} \mu(q/d)$. Deduce that $e = q$ and that $q \mid (p - 1)$.
(e) By taking z to be a suitable multiple of q, or otherwise, show that there are infinitely many primes p with $p \equiv 1 \pmod{q}$.

2. Dirichlet characters

In the preceding section we expressed the characteristic function of an arithmetic progression as a linear combination of additive characters. For purposes of multiplicative number theory we shall similarly represent the characteristic function of a reduced residue class (mod q) as a linear combination of totally multiplicative functions $\chi(n)$ each one supported on the reduced residue classes and having period q. These are the *Dirichlet characters*. Since $\chi(n)$ has period q we may think of it as mapping from residue classes, and since $\chi(n) \neq 0$ if and only if $(n,q) = 1$, we may think of χ as mapping from the multiplicative group of reduced residue classes to the multiplicative group $\mathbb{C}^\times$ of non-zero complex numbers. As χ is totally multiplicative, $\chi(mn) = \chi(m)\chi(n)$ for all m, n, we see that the map $\chi : \left(\mathbb{Z}/q\mathbb{Z}\right)^\times \longrightarrow \mathbb{C}^\times$ is a homomorphism. The method we use to describe these characters applies when $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ is replaced by an arbitrary finite abelian group G, so we consider the slightly more general problem of finding all homomorphisms $\chi : G \to \mathbb{C}^\times$ from such a group G to $\mathbb{C}^\times$. We call these homomorphisms the characters of G, and let $\widehat{G}$ denote the set of all characters of G. We let χ_0 denote the *principal character*, whose value is identically 1. We note that if $\chi \in \widehat{G}$ then $\chi(e) = 1$ where e denotes the identity in G. Let n denote the order of G. If $g \in G$ and $\chi \in \widehat{G}$, then $g^n = e$, and hence $\chi(g^n) = 1$. Consequently $\chi(g)^n = 1$, and so we see that all values taken by characters are n^{th} roots of unity. In particular, this implies that $\widehat{G}$ is finite, since there can be at most n^n such maps. If χ_1 and χ_2 are two characters of G, then we can define a product character $\chi_1\chi_2$ by $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. For $\chi \in \widehat{G}$, let $\overline{\chi}$ be the character $\overline{\chi(g)}$. Then $\chi \cdot \overline{\chi} = \chi_0$, and we see that $\widehat{G}$ is a finite abelian group with identity χ_0. The following lemmas prepare for a full description of $\widehat{G}$ in Theorem 4.

Lemma 2. *Suppose that G is cyclic of order n, say $G = (a)$. Then there are exactly n characters of G, namely $\chi_k(a^m) = e(km/n)$ for $1 \leq k \leq n$. Moreover,*

$$\sum_{g \in G} \chi(g) = \begin{cases} n & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

and

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n & \text{if } g = e, \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

In this situation, $\widehat{G}$ is cyclic, $\widehat{G} = (\chi_1)$.

Proof. Suppose that $\chi \in \widehat{G}$. As we have observed, $\chi(a)$ is a n^{th} root of unity, say $\chi(a) = e(k/n)$ for some k, $1 \leq k \leq n$. Hence $\chi(a^m) = \chi(a)^m = e(km/n)$. Since the characters are now known explicitly, the remaining assertions are easily verified.

Next we describe the characters of the direct product of two groups in terms of the characters of the factors.

Lemma 3. *Suppose that G_1 and G_2 are finite abelian groups, and that $G = G_1 \otimes G_2$. If χ_i is a character of G_i, $i = 1, 2$, and $g \in G$ is written $g = (g_1, g_2)$, $g_i \in G_i$, then $\chi(g) = \chi_1(g_1)\chi_2(g_2)$ is a character of G. Conversely, if $\chi \in \widehat{G}$, then there exist unique $\chi_i \in G_i$ such that $\chi(g) = \chi_1(g_1)\chi_2(g_2)$. The identities* 12) *and* 13) *hold for G if they hold for both G_1 and G_2.*

We see here that each $\chi \in \widehat{G}$ corresponds to a pair $(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2$. Thus $G \cong \widehat{G}_1 \otimes \widehat{G}_2$.

Proof. The first assertion is clear. As for the second, put $\chi_1(g_1) = \chi((g_1, e_2))$, $\chi_2(g_2) = \chi((e_1, g_2))$. Then $\chi_i \in \widehat{G}_i$ for $i = 1, 2$, and $\chi_1(g_1)\chi_2(g_2) = \chi(g)$. The χ_i are unique, for if $g = (g_1, e_2)$ then

$$\chi(g) = \chi((g_1, e_2)) = \chi_1(g_1)\chi_2(e_2) = \chi_1(g_1),$$

and similarly for χ_2. If $\chi(g) = \chi_1(g_1)\chi_2(g_2)$, then

$$\sum_{g \in G} \chi(g) = \Big(\sum_{g_1 \in G_1} \chi_1(g_1) \Big) \Big(\sum_{g_2 \in G_2} \chi_2(g_2) \Big),$$

so that 12) holds for G if it holds for G_1 and for G_2. Similarly, if $g = (g_1, g_2)$, then

$$\sum_{\chi \in \widehat{G}} \chi(g) = \Big(\sum_{\chi_1 \in \widehat{G}_1} \chi_1(g_1) \Big) \Big(\sum_{\chi_1 \in \widehat{G}_2} \chi_2(g_2) \Big),$$

so that (13) holds for G if it holds for G_1 and G_2.

Theorem 4. *Let G be a finite abelian group. Then $\widehat{G}$ is isomorphic to G, and* 12) *and* (13) *both hold.*

Proof. Any finite abelian group is isomorphic to a direct product of cyclic groups, say

$$G \cong C_{n_1} \otimes C_{n_2} \otimes \cdots \otimes C_{n_r}.$$

The result then follows immediately from the lemmas.

Though G and $\widehat{G}$ are isomorphic, the isomorphism is not canonical. That is, no particular one-to-one correspondence between the elements of G and those of $\widehat{G}$ is naturally distinguished.

Corollary 5. *The multiplicative group $\big(\mathbb{Z}/q\mathbb{Z}\big)^\times$ of reduced residue classes* (mod q) *has $\varphi(q)$ Dirichlet characters. If χ is such a character, then*

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} \chi(n) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

If $(n,q)=1$ *then*

$$\sum_{\chi}\chi(n)=\begin{cases}\varphi(q) & \text{if } n\equiv 1 \pmod q,\\ 0 & \text{otherwise}\end{cases} \tag{15}$$

where the sum is extended over the $\varphi(q)$ *Dirichlet characters* $\chi \pmod q$.

As we remarked at the outset, for our purposes it is convenient to define the Dirichlet characters (mod q) on all integers; we do this by setting $\chi(n)=0$ when $(n,q)>1$. Thus χ is a totally multiplicative function with period q that vanishes whenever $(n,q)>1$, and any such function is a Dirichlet character (mod q). In this book a character is understood to be a Dirichlet character unless the contrary is indicated.

Corollary 6. *If* χ_i *is a character* (mod q_i) *for* $i=1,2$, *then* $\chi_1(n)\chi_2(n)$ *is a character* (mod $[q_1,q_2]$). *If* $q=q_1q_2$, $(q_1,q_2)=1$, *and* χ *is a character* (mod q), *then there exist unique characters* $\chi_i \pmod q$, $i=1,2$, *such that* $\chi(n)=\chi_1(n)\chi_2(n)$ *for all* n.

Proof. The first assertion follows immediately from the observations that $\chi_1(n)\chi_2(n)$ is totally multiplicative, that it vanishes if $(n,[q_1,q_2])>1$, and that it has period $[q_1,q_2]$. As for the second assertion, we may suppose that $(n,q)=1$. By the Chinese Remainder Theorem we see that

$$\big(\mathbb{Z}/q\mathbb{Z}\big)^\times \cong \big(\mathbb{Z}/q_1\mathbb{Z}\big)^\times \otimes \big(\mathbb{Z}/q_2\mathbb{Z}\big)^\times$$

if $(q_1,q_2)=1$. Thus the result follows from Lemma 2.

Our proof of Theorem 4 depends on Abel's Theorem that any finite abelian group is isomorphic to the direct product of cyclic groups, but we can prove Corollary 5 without appealing to this result, as follows. By the Chinese Remainder Theorem we see that

$$\big(\mathbb{Z}/q\mathbb{Z}\big)^\times \cong \bigotimes_{p^\alpha \| q} \big(\mathbb{Z}/p^\alpha\mathbb{Z}\big)^\times.$$

If p is odd then the reduced residue classes (mod p^α) form a cyclic group; in classical language we say there is a primitive root g. Thus if $(n,p)=1$ then there is a unique ν (mod $\varphi(p^\alpha)$) such that $g^\nu \equiv n \pmod{p^\alpha}$. The number ν is called the index of n, and is denoted $\nu=\operatorname{ind}_g n$. From Lemma 2 it follows that the characters (mod p^α), $p>2$, are given by

$$\chi_k(n)=e\Big(\frac{k\operatorname{ind}_g n}{\varphi(p^\alpha)}\Big) \tag{16}$$

for $(n,p)=1$. We obtain $\varphi(p^\alpha)$ different characters by allowing k to assume integral values in the range $1\le k\le\varphi(p^\alpha)$. By Lemma 3 it follows that if q is odd then the general character (mod q) is given by

$$\chi(n)=e\Big(\sum_{p^\alpha\|q}\frac{k\operatorname{ind}_g n}{\varphi(p^\alpha)}\Big) \tag{17}$$

for $(n,q)=1$, where it is understood that $k=k(p^\alpha)$ is determined (mod $\varphi(p^\alpha)$) and that $g=g(p^\alpha)$ is a primitive root (mod p^α).

The multiplicative structure of the reduced residues (mod 2^α) is more complicated. For $\alpha=1$ or $\alpha=2$ the group is cyclic (of order 1 or 2, respectively), and (16) holds as before. For $\alpha\ge 3$ the group is not cyclic, but if n is odd then there exist unique μ (mod 2) and ν (mod $2^{\alpha-2}$) such that $n\equiv(-1)^\mu 5^\nu \pmod{2^\alpha}$. In group-theoretic terms this means that

$$\big(\mathbb{Z}/2^\alpha\mathbb{Z}\big)^\times \cong C_2\otimes C_{2^{\alpha-2}}$$

when $\alpha\ge 3$. By Lemma 3 the characters in this case take the form

$$\chi(n)=e\Big(\frac{j\mu}{2}+\frac{k\nu}{2^{\alpha-2}}\Big) \tag{18}$$

for odd n where $j=0$ or 1 and $1\le k\le 2^{\alpha-2}$. Thus (17) holds if $8\nmid q$, but if $8|q$ then the general character takes the form

$$\chi(n)=e\Big(\frac{j\mu}{2}+\frac{k\nu}{2^{\alpha-2}}+\sum_{\substack{p^\alpha\|q\\ p>2}}\frac{\ell\,\mathrm{ind}_g\,n}{\varphi(p^\alpha)}\Big) \tag{19}$$

when $(n,q)=1$.

By definition, if $f(n)$ is totally multiplicative, $f(n)=0$ whenever $(n,q)>1$, and $f(n)$ has period q, then f is a Dirichlet character (mod q). It is useful to note that the first condition can be relaxed.

Theorem 7. *If f is multiplicative, $f(n)=0$ whenever $(n,q)>1$, and f has period q, then f is a Dirichlet character modulo q.*

Proof. It suffices to show that f is totally multiplicative. If $(mn,q)>1$ then $f(mn)=f(m)f(n)$ since $0=0$. Suppose that $(mn,q)=1$. Hence in particular $(m,q)=1$, so that the map $k\mapsto n+kq$ (mod m) permutes the residue classes (mod m). Thus there is a k for which $n+kq\equiv 1$ (mod m), and consequently $(m,n+kq)=1$. Then

$$\begin{aligned} f(mn) &= f(m(n+kq)) && \text{(by periodicity)}\\ &= f(m)f(n+kq) && \text{(by multiplicativity)}\\ &= f(m)f(n) && \text{(by periodicity),}\end{aligned}$$

and the proof is complete.

We shall discuss further properties of Dirichlet characters in Chapter 9.

4.2. Exercises

1. Let G be a finite abelian group of order n. Let $g_1,g_2,\dots,g_n$ denote the elements of G, and let $\chi_1(g),\chi_2(g),\dots,\chi_n(g)$ denote the characters of G. Let $U=[u_{ij}]$ be the $n\times n$ matrix with elements $u_{ij}=\chi_i(g_j)/\sqrt{n}$. Show that $UU^*=U^*U=I$, i.e., that U is unitary.

2. Show that for arbitrary real or complex numbers $c_1, \dots, c_q$,

$$\sum_{\chi} \Big| \sum_{n=1}^{q} c_n \chi(n) \Big|^2 = \varphi(q) \sum_{\substack{n=1 \\ (n,q)=1}}^{q} |c_n|^2$$

where the sum on the left hand side runs over all Dirichlet characters $\chi \pmod q$.

3. Show that for arbitrary real or complex numbers c_χ,

$$\sum_{n=1}^{q} \Big| \sum_{\chi} c_\chi \chi(n) \Big|^2 = \varphi(q) \sum_{\chi} |c_\chi|^2$$

where the sum over χ is extended over all Dirichlet characters $\pmod q$.

4. Let $(a, q) = 1$, and suppose that k is the order of a in the multiplicative group of reduced residue classes $\pmod q$.
(a) Show that if χ is a Dirichlet character $\pmod q$ then $\chi(a)$ is a k^{th} root of unity.
(b) Show that if z is a k^{th} root of unity then

$$1 + z + \cdots + z^{k-1} = \begin{cases} k & \text{if } z = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(c) Let ζ be a k^{th} root of unity. By taking $z = \chi(a)/\zeta$, show that each k^{th} root of unity occurs precisely $\varphi(q)/k$ times among the numbers $\chi(a)$ as χ runs over the $\varphi(q)$ Dirichlet characters $\pmod q$.

5. Let χ be a Dirichlet character $\pmod q$, and let k denote the order of χ in the character group.
(a) Show that if $(a, q) = 1$ then $\chi(a)$ is a k^{th} root of unity.
(b) Show that each k^{th} root of unity occurs precisely $\varphi(q)/k$ times among the numbers $\chi(a)$ as a runs over the $\varphi(q)$ reduced residue classes $\pmod q$.

6. Let χ be a character $\pmod q$ such that $\chi(a) = \pm 1$ whenever $(a, q) = 1$, and put $S(\chi) = \sum_{n=1}^{q} n\chi(n)$. Thus $S(\chi)$ is an integer.
(a) Show that if $(a, q) = 1$ then $a\chi(a)S(\chi) \equiv S(\chi) \pmod q$.
(b) Show that there is an a such that $(a, q) = 1$ and $(a\chi(a) - 1, q) | 12$.
(c) Deduce that $12S(\chi) \equiv 0 \pmod q$.

In algebraic number fields we encounter not only Dirichlet characters, but also characters of ideal class groups and of Galois groups. In addition, algebraic number fields possessing one or more complex embeddings also have a further kind of character, Hecke's *Grössencharaktere*. In a sequence of exercises, beginning with the one below, we develop the basic properties of these characters for the Gaussian field $\mathbb{Q}(\sqrt{-1})$.

7. Let K be the Gaussian field,

$$K = \mathbb{Q}(\sqrt{-1}) = \{a + bi : a, b \in \mathbb{Q}\},$$

and let $\mathcal{O}_K$ be the ring of algebraic integers in K,

$$\mathcal{O}_K = \{a + bi : a, b \in \mathbb{Z}\}.$$

Elements $\alpha = a + bi \in K$ have a *norm*, $N(\alpha) = a^2 + b^2$, and we observe that $N(\alpha\beta) = N(\alpha)N(\beta)$. An element α of a ring is a *unit* if α has an inverse in the ring. The ring $\mathcal{O}_K$ has precisely 4 units, namely i^k for $k = 0, 1, 2, 3$. Two elements $\alpha, \beta \in \mathcal{O}_K$ are *associates* if $\alpha = u\beta$ for some unit u. For each integer m we define the Hecke Grössencharakter

$$\chi_m(\alpha) = \begin{cases} e^{4mi \arg \alpha} & \text{if } \alpha \neq 0, \\ 0 & \text{if } \alpha = 0. \end{cases}$$

(a) Show that if α and β are associates then $\chi_m(\alpha) = \chi_m(\beta)$.
(b) Show that $\chi_m(\alpha\beta) = \chi_m(\alpha)\chi_m(\beta)$ for all α and β in $\mathcal{O}_K$.

3. Dirichlet L-functions

Let χ be a character (mod q). For $\sigma > 1$ we put

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}. \tag{20}$$

Since χ is totally multiplicative, by Theorem 1.9 we have

$$L(s, \chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1} \tag{21}$$

for $\sigma > 1$. Thus we see that

$$L(s, \chi_0) = \sum_{\substack{n=1 \\ (n,q)=1}}^{\infty} n^{-s} = \zeta(s) \prod_{p|q} \left(1 - p^{-s}\right) \tag{22}$$

for $\sigma > 1$. By (14) we see that if $\chi \neq \chi_0$ then

$$\sum_{1 \leq n \leq kq} \chi(n) = 0$$

for $k = 1, 2, 3, \ldots$. Hence

$$\left| \sum_{n \leq x} \chi(n) \right| \leq q \tag{23}$$

for any x, so that by Theorem 1.3, the series (20) converges for $\sigma > 0$. This result is best possible since the terms in (20) do not tend to 0 when $\sigma = 0$. On the other hand, we shall show in Chapter 10 that the function $L(s, \chi)$ is entire if $\chi \neq \chi_0$. For $\sigma > 1$ we can take logarithms in (21), and differentiate, as in Corollary 1.11, and thus we obtain

Theorem 8. *If $\chi \neq \chi_0$ then $L(s,\chi)$ is analytic for $\sigma > 0$. On the other hand, the function $L(s,\chi_0)$ is analytic in this half plane except for a simple pole at $s = 1$ with residue $\varphi(q)/q$. In either case,*

$$\log L(s,\chi) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n}\chi(n)n^{-s} \tag{24}$$

for $\sigma > 1$, and

$$-\frac{L'}{L}(s,\chi) = \sum_{n=1}^{\infty} \Lambda(n)\chi(n)n^{-s}. \tag{25}$$

In these last formulæ we see how relations for L-functions parallel those for the zeta functions. Indeed, when manipulating Dirichlet series formally, the only property of n^{-s} that is used is that it is totally multiplicative. Hence all such calculations can be made with n^{-s} replaced by $\chi(n)n^{-s}$. For example, we know that $\sum \mu(n)^2 n^{-s} = \zeta(s)/\zeta(2s)$ for $\sigma > 1$. Hence formally

$$\sum_{n=1}^{\infty} \mu(n)^2\chi(n)n^{-s} = L(s,\chi)/L(2s,\chi^2). \tag{26}$$

Since $|\chi(n)n^{-s}| \leq n^{-\sigma}$, this latter series is absolutely convergent whenever the former one is, and by (21) we see that (26) holds for $\sigma > 1$. In fact, by a theorem of Stieltjes (see Exercise 1.3.2), the identity (26) holds for $\sigma > 1/2$ if $\chi \neq \chi_0$.

We now use the identity (15) to capture a prescribed residue class. If $(a,q) = 1$ then

$$\frac{1}{\varphi(q)}\sum_{\chi} \overline{\chi}(a)\chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod q, \\ 0 & \text{otherwise} \end{cases} \tag{27}$$

where the sum is extended over all characters $\chi \pmod q$. This is the multiplicative analogue of (1). Hence if $(a,q) = 1$ then

$$\begin{aligned} \sum_{\substack{n=1 \\ n\equiv a\,(q)}}^{\infty} \Lambda(n)n^{-s} &= \frac{1}{\varphi(q)}\sum_{n=1}^{\infty}\Lambda(n)n^{-s}\sum_{\chi}\overline{\chi}(a)\chi(n) \\ &= \frac{-1}{\varphi(q)}\sum_{\chi}\overline{\chi}(a)\frac{L'}{L}(s,\chi) \end{aligned} \tag{28}$$

for $\sigma > 1$. As $L(s,\chi_0)$ has a simple pole at $s = 1$, the function $\frac{L'}{L}(s,\chi)$ has a simple pole at 1 with residue -1. Thus the term arising from χ_0 on the right hand side above is

$$\frac{1}{\varphi(q)(s-1)} + O_q(1) \tag{29}$$

as $s \to 1^+$. This enables us to prove that there are infinitely many primes $p \equiv a \pmod q$, provided that we can show that the terms from $\chi \neq \chi_0$ on the right hand side of (28) do not interfere with the main term (29). But $L(s,\chi)$ is analytic for $\sigma > 0$, so that $\frac{L'}{L}(s,\chi)$ is analytic except at zeros of $L(s,\chi)$. Hence

$$\lim_{s\to 1^+} \frac{L'}{L}(s,\chi) = \frac{L'}{L}(1,\chi) \tag{30}$$

for $\chi \neq \chi_0$, provided that $L(1,\chi) \neq 0$. Thus the following result lies at the heart of the matter.

Theorem 9. (Dirichlet) *If χ is a character* (mod q)*, $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.*

Suppose that $(a,q) = 1$. Then the above, with (28), (29), and (30) give the estimate

$$\sum_{\substack{n=1\\ n\equiv a\,(q)}}^{\infty} \Lambda(n) n^{-s} = \frac{1}{\varphi(q)(s-1)} + O_q(1)$$

as $s \to 1^+$. Consequently

$$\sum_{\substack{n=1\\ n\equiv a\,(q)}}^{\infty} \frac{\Lambda(n)}{n} = \infty.$$

Here the contribution of the proper prime powers is

$$\sum_{\substack{p^k\equiv a\,(q)\\ k\geq 2}} \frac{\log p}{p^k} \leq \sum_p \log p \sum_{k=2}^{\infty} p^{-k} = \sum_p \frac{\log p}{p(p-1)} < \infty, \tag{31}$$

and thus we have

Corollary 10. (Dirichlet's Theorem) *If $(a,q) = 1$ then there are infinitely many primes $p \equiv a \pmod q$, and indeed*

$$\sum_{p\equiv a\,(q)} \frac{\log p}{p} = \infty.$$

We call a character *real* if all its values are real (i.e., $\chi(n) = 0$ or ± 1 for all n). Otherwise a character is *complex*. A character is *quadratic* if it has order 2 in the character group: $\chi^2 = \chi_0$ but $\chi \neq \chi_0$. Thus a quadratic character is real, and a real character is either principal or quadratic. In Chapter 9 we shall express quadratic characters in terms of the Kronecker symbol $\left(\frac{d}{n}\right)$.

Proof of Theorem 9. We treat quadratic and complex characters separately.

Case 1: Complex χ. From (24) we have

$$\prod_{\chi} L(s,\chi) = \exp\Big(\sum_{\chi}\sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n}\chi(n) n^{-s}\Big)$$

for $\sigma > 1$. By (15) this is

$$= \exp\Big(\varphi(q) \sum_{\substack{n=2 \\ n\equiv 1\ (q)}}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}\Big).$$

If we take $s = \sigma > 1$ then the sum above is a non-negative real number, and hence we see that

$$\prod_{\chi} L(\sigma, \chi) \geq 1 \tag{32}$$

for $\sigma > 1$. Now $L(s, \chi_0)$ has a simple pole at $s = 1$, but the other $L(s, \chi)$ are analytic at s = 1. Thus $L(1, \chi) = 0$ can hold for at most one χ, since otherwise the product in (32) would tend to 0 as $\sigma \to 1^+$. If χ is a character (mod q) then $\overline{\chi}$ is a character (mod q), and $\chi \neq \overline{\chi}$ if χ is complex. Moreover $\overline{L(s, \chi)} = L(\overline{s}, \overline{\chi})$ by the Schwarz reflection principle, so that $L(1, \overline{\chi}) = 0$ if $L(1, \chi) = 0$. Consequently $L(1, \chi) \neq 0$ for complex χ.

Case 2: Quadratic χ. Let $r(n) = \sum_{d|n} \chi(d)$. Thus $\sum_{n=1}^{\infty} r(n) n^{-s} = \zeta(s) L(s, \chi)$ for $\sigma > 1$, $r(n)$ is multiplicative, and

$$r(p^\alpha) = \begin{cases} 1 & \text{if } p \mid q, \\ \alpha + 1 & \text{if } \chi(p) = 1, \\ 1 & \text{if } \chi(p) = -1 \text{ and } 2 \mid \alpha, \\ 0 & \text{if } \chi(p) = -1 \text{ and } 2 \nmid \alpha. \end{cases}$$

Hence $r(n) \geq 0$ for all n, and $r(n^2) \geq 1$ for all n. Suppose that $L(1, \chi) = 0$. Then $\zeta(s) L(s, \chi)$ is analytic for $\sigma > 0$, and by Landau's Theorem (Theorem 1.7) the series $\sum r(n) n^{-s}$ converges for $\sigma > 0$. But this is false, since

$$\sum_{n=1}^{\infty} r(n) n^{-1/2} \geq \sum_{n=1}^{\infty} r(n^2) n^{-1} \geq \sum_{n=1}^{\infty} n^{-1} = +\infty.$$

Hence $L(1, \chi) \neq 0$. Since $L(\sigma, \chi) > 0$ for $\sigma > 1$ when χ is quadratic, we see in fact that $L(1, \chi) > 0$ in this case.

By using the techniques of Chapter 2 we can prove more than the mere divergence of the series in Corollary 10.

Theorem 11. *Suppose that χ is a non-principal Dirichlet character. Then for $x \geq 2$,*

$$\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} \ll_\chi 1, \tag{a}$$

$$\sum_{p \leq x} \frac{\chi(p) \log p}{p} \ll_\chi 1, \tag{b}$$

$$\sum_{p \leq x} \frac{\chi(p)}{p} = b(\chi) + O_\chi\Big(\frac{1}{\log x}\Big), \tag{c}$$

$$\prod_{p \leq x} \Big(1 - \frac{\chi(p)}{p}\Big)^{-1} = L(1, \chi) + O_\chi\Big(\frac{1}{\log x}\Big) \tag{d}$$

where

$$b(\chi) = \log L(1,\chi) - \sum_{\substack{p^k \\ k>1}} \frac{\chi(p^k)}{kp^k}.$$

Proof. We show first that

$$\sum_{n\le x} \frac{\chi(n)\log n}{n} = -L'(1,\chi) + O_q\Big(\frac{\log x}{x}\Big). \tag{33}$$

To this end we put $S(x) = \sum_{n\le x}\chi(n)$. Then from (23) we see that $S(x) \ll_\chi 1$. Thus the error term above is

$$\begin{aligned}\sum_{n>x} \frac{\chi(n)\log n}{n} &= \int_x^\infty \frac{\log u}{u}\, dS(u)\\ &= -\frac{S(x)\log x}{x} - \int_x^\infty S(u)(1-\log u)u^{-2}\, du\\ &\ll_\chi \frac{\log x}{x}.\end{aligned}$$

As $\log n = \sum_{d|n}\Lambda(d)$, the left hand side of (33) is

$$\sum_{md\le x} \frac{\Lambda(d)\chi(md)}{md} = \sum_{d\le x}\frac{\Lambda(d)\chi(d)}{d}\sum_{m\le x/d}\frac{\chi(m)}{m}. \tag{34}$$

Here the inner sum is of the form

$$\sum_{m\le y}\frac{\chi(m)}{m} = L(1,\chi) - \sum_{m>y}\frac{\chi(m)}{m},$$

and this last sum is

$$\int_y^\infty u^{-1}\, dS(u) = -\frac{S(y)}{y} + \int_y^\infty S(u)u^{-2}\, du \ll_\chi y^{-1}.$$

Hence the right hand side of (34) is

$$L(1,\chi)\sum_{d\le x}\frac{\Lambda(d)\chi(d)}{d} + O_\chi\Big(\frac{1}{x}\sum_{d\le x}\Lambda(d)\Big).$$

This last error term is $\ll_\chi 1$, and then (a) follows from (33) and the fact that $L(1,\chi)\ne 0$. The derivation of (b) from (a), and of (c) from (b) proceeds as in the proof of Theorem 2.7. Continuing as in that proof, we see from (c) that

$$\sum_{1<n\le x}\frac{\Lambda(n)\chi(n)}{n\log n} = c(\chi) + O_\chi\Big(\frac{1}{\log x}\Big)$$

where

$$c(\chi) = b(\chi) + \sum_{\substack{p^k \\ k>1}} \frac{\chi(p^k)}{kp^k}.$$

We let $s \to 1^+$ in (24), and deduce by Theorem 1.1 that $c(\chi) = \log L(1,\chi)$. To complete the derivation of (d) it suffices to argue as in the proof of Theorem 2.7.

By forming a linear combination of these estimates as in (27) we obtain

Corollary 12. *If $(a,q) = 1$ and $x \geq 2$ then*

(a) $$\sum_{\substack{n\leq x \\ n\equiv a\,(q)}} \frac{\Lambda(n)}{n} = \frac{1}{\varphi(q)} \log x + O_q(1),$$

(b) $$\sum_{\substack{p\leq x \\ p\equiv a\,(q)}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O_q(1),$$

(c) $$\sum_{\substack{p\leq x \\ p\equiv a\,(q)}} \frac{1}{p} = \frac{1}{\varphi(q)} \log\log x + b(q,a) + O_q\Big(\frac{1}{\log x}\Big),$$

(d) $$\prod_{\substack{p\leq x \\ p\equiv a\,(q)}} \Big(1-\frac{1}{p}\Big)^{-1} = c(q,a)(\log x)^{1/\varphi(q)}\Big(1+O_q\Big(\frac{1}{\log x}\Big)\Big)$$

where

$$b(q,a) = \frac{1}{\varphi(q)}\Big(C_0 + \sum_{p|q} \log\Big(1-\frac{1}{p}\Big) + \sum_{\chi\neq\chi_0} \overline{\chi}(a) \log L(1,\chi)\Big) - \sum_{\substack{p^k\equiv a\,(q) \\ k>1}} \frac{1}{kp^k}$$

and

$$c(q,a) = \Big(e^{C_0}\frac{\varphi(q)}{q} \prod_{\chi\neq\chi_0} \Big(L(1,\chi)^{\overline{\chi}(a)} \prod_p \Big(1-\frac{1}{p}\Big)^{-\chi(p)}\Big(1-\frac{\chi(p)}{p}\Big)\Big)\Big)^{1/\varphi(q)}.$$

Proof. To derive (a) from Theorem 11(a) we use (27) and the estimate

$$\sum_{n\leq x} \frac{\Lambda(n)\chi_0(n)}{n} = \log x + O_q(1),$$

which follows from Theorem 2.7(a) since

$$\sum_{\substack{p^k \\ p|q}} \frac{\log p}{p^k} = \sum_{p|q} \frac{\log p}{p-1} \ll_q 1.$$

We derive (b) and (c) similarly from the corresponding parts of Theorem 11. In the latter case we use the estimate

$$\sum_{p\le x}\frac{\chi_0(p)}{p} = \log\log x + b(\chi_0) + O_q\Big(\frac{1}{\log x}\Big)$$

where

$$b(\chi_0) = C_0 + \sum_{p\mid q}\log\Big(1-\frac{1}{p}\Big) - \sum_{\substack{p^k\\ k>1}}\frac{\chi_0(p^k)}{kp^k}.$$

To derive (d) we observe first that

$$\prod_{p\le x}\Big(1-\frac{\chi_0(p)}{p}\Big)^{-1} = \prod_{\substack{p\le x\\ p\mid q}}\Big(1-\frac{1}{p}\Big)\prod_{p\le x}\Big(1-\frac{1}{p}\Big)^{-1},$$

which by Theorem 2.7(e) is

$$= \frac{\varphi(q)}{q}\Big(\prod_{\substack{p\mid q\\ p>x}}\Big(1-\frac{1}{p}\Big)\Big)^{-1} e^{-C_0}(\log x)\Big(1+O\Big(\frac{1}{\log x}\Big)\Big).$$

Here each term in the product is $1+O(1/x)$, and the number of factors is $\le \omega(q)$, so the product is $1+O_q(1/x)$, and hence the above is

$$= e^{C_0}\frac{\varphi(q)}{q}(\log x)\Big(1+O_q\Big(\frac{1}{\log x}\Big)\Big).$$

To complete the proof it suffices to combine this with Theorem 11(d) in (27).

4.3. Exercises

1. Let χ be a Dirichlet character (mod q). Show that if $\sigma > 1$ then

(a) $$\sum_{n=1}^{\infty}(-1)^{n-1}\chi(n)n^{-s} = \big(1-\chi(2)2^{1-s}\big)L(s,\chi);$$

(b) $$\sum_{n=1}^{\infty} d(n)^2\chi(n)n^{-s} = \frac{L(s,\chi)^4}{L(2s,\chi^2)}.$$

2. (Mertens (1895a,b)) Let $r(n) = \sum_{d\mid n}\chi(d)$.
(a) Show that if χ is a non-principal character (mod q), then

$$\sum_{n>x}\frac{\chi(n)}{\sqrt{n}} \ll_\chi \frac{1}{\sqrt{x}}.$$

(b) Show that if χ is a non-principal character (mod q), then

$$\sum_{n\le x}\frac{r(n)}{n^{1/2}} = 2x^{1/2}L(1,\chi)+O_\chi(1).$$

(c) Recall that if χ is quadratic then $r(n)\ge 0$ for all n, and that $r(n^2)\ge 1$. Deduce that if χ is a quadratic character, then the left hand side above is $\gg \log x$.
(d) Conclude that if χ is a quadratic character, then $L(1,\chi)>0$.

3. (Mertens (1897), (1899)) For $u\ge 0$, put $f(u)=\sum_{m\le u}(1-m/u)$.
(a) Show that $f(u)\ge 0$, that $f(u)$ is continuous, and that if u is not an integer, then

$$f'(u)=\frac{[u]([u]+1)}{2u^2};$$

deduce that f is increasing.
(b) Show also that

$$f(u)=\frac{u}{2}-\frac{1}{u}\int_0^u\{v\}\,dv=\frac{u}{2}-\frac{1}{2}+O(1/u)\,.$$

(c) Let $r(n)=\sum_{d|n}\chi(d)$, and assume that χ is non-principal. Show that

$$\sum_{n\le x}r(n)(1-n/x)=\sum_{d\le x}\chi(d)f(x/d)\,.$$

(d) Write $\sum_{d\le x}=\sum_{d\le y}+\sum_{y<d\le x}=S_1+S_2$ where $1\le y\le x$. Use part (b) to show that $S_1=\frac12 xL(1,\chi)+O_\chi(x/y)+O\big(y^2/x\big)$.
(e) Use the results of part (a) to show that $S_2\ll_\chi f(x/y)$.
(f) By making an appropriate choice of y, deduce that if χ is a non-principal character, then

$$\sum_{n\le x}r(n)(1-n/x)=\frac{x}{2}L(1,\chi)+O_\chi\big(x^{1/3}\big)\,.$$

(g) Argue that if χ is a quadratic character, then the left hand side above is $\gg x^{1/2}$; deduce that $L(1,\chi)>0$.

4. (Ingham (1929)) Let $f_1(n)$ and $f_2(n)$ be totally multiplicative functions, and suppose that $|f_i(n)|\le 1$ for all n.
(a) Show that if $\sigma>1$ then

$$\begin{aligned}\sum_{n=1}^\infty\Big(\sum_{d|n}f_1(d)\Big)\Big(\sum_{d|n}f_2(d)\Big)n^{-s}&\\ =\frac{\zeta(s)\Big(\sum_{n=1}^\infty f_1(n)n^{-s}\Big)\Big(\sum_{n=1}^\infty f_2(n)n^{-s}\Big)\Big(\sum_{n=1}^\infty f_1(n)f_2(n)n^{-s}\Big)}{\sum_{n=1}^\infty f_1(n)f_2(n)n^{-2s}}&\\ =\frac{\prod_p\Big(1-\frac{f_1(p)f_2(p)}{p^{2s}}\Big)}{\prod_p\Big(1-\frac{1}{p^s}\Big)\Big(1-\frac{f_1(p)}{p^s}\Big)\Big(1-\frac{f_2(p)}{p^s}\Big)\Big(1-\frac{f_1(p)f_2(p)}{p^s}\Big)}.&\end{aligned}$$

(b) By considering

$$F(s) = \sum_{n=1}^{\infty} \Big| \sum_{d|n} \chi(d) d^{-iu} \Big|^2 n^{-s},$$

show that $L(1+iu, \chi) \neq 0$.

5. Let $\pi(x; q, a)$ denote the number of primes $p \equiv a \pmod q$ with p not exceeding x. Similarly, let

$$\vartheta(x; q, a) = \sum_{\substack{p \le x \\ p \equiv a\,(q)}} \log p, \qquad \psi(x; q, a) = \sum_{\substack{n \le x \\ n \equiv a\,(q)}} \Lambda(n).$$

(a) Show that

$$\vartheta(x; q, a) = \psi(x; q, a) + O\big(x^{1/2}\big).$$

(b) Show that

$$\pi(x; q, a) = \frac{\vartheta(x; q, a)}{\log x} + O\Big(\frac{x}{(\log x)^2}\Big).$$

(c) Show that if $x \ge C$, $C \ge 2$, and $(a, q) = 1$ then

$$\sum_{\substack{x/C < p \le x \\ p \equiv a\,(q)}} \frac{\log p}{p} = \frac{\log C}{\varphi(q)} + O_q(1).$$

(d) Show that for any positive integer q there is a small number c_q and a large number C_q such that if $x \ge 2C_q$ and $(a, q) = 1$ then

$$\sum_{\substack{x/C_q < p \le x \\ p \equiv a\,(q)}} \frac{\log p}{p} > c_q.$$

(e) Show that for any positive integer q there is a C_q such that if $(a, q) = 1$ then

$$\pi(x; q, a) \gg_q \frac{x}{\log x}$$

uniformly for $x \ge C_q$.
(f) Show that if $(a, q) = 1$ then

$$\liminf_{x\to\infty} \frac{\pi(x; q, a)}{x/\log x} \le \frac{1}{\varphi(q)}, \qquad \limsup_{x\to\infty} \frac{\pi(x; q, a)}{x/\log x} \ge \frac{1}{\varphi(q)}.$$

6. (a) Show that

$$\vartheta(x) \le \pi(x) \log x \le \vartheta(x) + O\Big(\frac{x}{\log x}\Big)$$

for $x \geq 2$.
(b) Let $\mathcal{P}$ denote a set of prime numbers, and put

$$\pi_{\mathcal{P}}(x) = \sum_{\substack{p \leq x \\ p \in \mathcal{P}}} 1, \qquad \vartheta_{\mathcal{P}}(x) = \sum_{\substack{p \leq x \\ p \in \mathcal{P}}} \log p.$$

Show that

$$\vartheta_{\mathcal{P}}(x) = \pi_{\mathcal{P}}(x) \log x + O\Big(\frac{x}{\log x}\Big)$$

for $x \geq 2$, where the implicit constant is absolute.
(c) Let

$$n = \prod_{\substack{p \leq y \\ p \in \mathcal{P}}} p\,.$$

Show that $\log n = \omega(n) \log y + O(y/\log y)$ for $y \geq 2$.
(d) From now on, assume that $\vartheta_{\mathcal{P}}(x) \gg x$ for all sufficiently large x, where the implicit constant may depend on $\mathcal{P}$. Show that $\log\log n = \log y + O_{\mathcal{P}}(1)$.
(e) Deduce that

$$d(n) = n^{(\log 2 + o(1))/\log\log n}$$

as $y \to \infty$.

7. Let $R(n)$ denote the number of ordered pairs a, b such that $a^2 + b^2 = n$ with $a \geq 0$ and $b > 0$. Also, let $r(n)$ denote the number of such pairs for which $(a, b) = 1$. Finally, let $\chi_{-4} = \left(\frac{-4}{n}\right)$ be the non-principal character (mod 4). We recall that if the prime factorization of n is written in the form

$$n = 2^\alpha \prod_{\substack{p^\beta \| n \\ p \equiv 1\,(4)}} p^\beta \prod_{\substack{q^\gamma \| n \\ q \equiv 3\,(4)}} q^\gamma$$

then $r(n) > 0$ if and only if $\gamma = 0$ for all primes q and $\alpha \leq 1$. We also recall that

$$R(n) = \sum_{d^2 | n} r(n/d^2) = \sum_{d | n} \chi_{-4}(d) = \begin{cases} \prod_p (\beta + 1) & \text{if } 2|\gamma \text{ for all } q, \\ 0 & \text{otherwise.} \end{cases}$$

(a) Show that $\sum_{n=1}^\infty R(n) n^{-s} = \zeta(s) L(s, \chi_{-4})$ for $\sigma > 1$.
(b) Show that $\sum_{n=1}^\infty r(n) n^{-s} = \zeta(s) L(s, \chi_{-4})/\zeta(2s)$ for $\sigma > 1$.
(c) Show that if $x \geq 0$ and $y \geq 2$ then

$$\operatorname{card}\{n \in (x, x+y] : r(n) > 0\} \ll \frac{y}{\sqrt{\log y}}.$$

(d) Show that

$$\operatorname{card}\{n \leq x : R(n) > 0\} \ll \frac{x}{\sqrt{\log x}}$$

for $x \geq 2$.
(e) Suppose that n is of the form

$$n = \prod_{\substack{p \leq y \\ p \equiv 1 \ (4)}} p.$$

Thus $\log n = \vartheta(y;, 4, 1) \asymp y$ for $y \geq 5$, and hence $\log y = \log\log n + O(1)$. Show that for such n,

$$R(n) = n^{(\log 2 + o(1))/\log\log n}.$$

In the above it is noteworthy that although $R(n) \leq d(n)$ for all n, that $R(n)$ is usually 0 and has a smaller average value (cf Exercise 2.1.9) than $d(n)$ (cf Theorem 2.3), the maximum order of magnitude of $R(n)$ is the same as for $d(n)$.

8. Let $K = \mathbb{Q}(\sqrt{-1})$ be the Gaussian field, $\mathcal{O}_K = \{a + ib : a, b \in \mathbb{Z}\}$ the ring of integers in K. Ideals $\mathfrak{a}$ in $\mathcal{O}_K$ are principal, $\mathfrak{a} = (a + ib)$, and have norm $N(\mathfrak{a}) = a^2 + b^2$.
(a) Explain why the number of ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq x$ is $\frac{\pi}{4}x + O\big(x^{1/2}\big)$.
(b) For $\sigma > 1$, let $\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ be the Dedekind zeta function of K. Show that $\zeta_K(s) = \zeta(s)L\big(s, \chi_{-4}\big)$.
(c) For the Gaussian field K, show that $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. (This is true in any algebraic number field.)
(d) Assume that ideals in K factor uniquely into prime ideals. (This is true in any algebraic number field, and is particularly easy to establish for the Gaussian field since it has a division algorithm.) Deduce that if $\sigma > 1$, then

$$\zeta_K(s) = \prod_{\mathfrak{p}} \Big(1 - \frac{1}{N(\mathfrak{p})}\Big)^{-1}$$

where the product runs over all prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$.
(e) Define a function $\mu(\mathfrak{a}) = \mu_K(\mathfrak{a})$ in such a way that

$$\frac{1}{\zeta_K(s)} = \sum_{\mathfrak{a}} \frac{\mu(\mathfrak{a})}{N(\mathfrak{a})^s}$$

for $\sigma > 1$.
(f) Let $\mathfrak{a}$ and $\mathfrak{b}$ be given ideals. Show that

$$\sum_{\substack{\mathfrak{d} \mid \mathfrak{a} \\ \mathfrak{d} \mid \mathfrak{b}}} \mu(\mathfrak{d}) = \begin{cases} 1 & \text{if } \gcd(\mathfrak{a}, \mathfrak{b}) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(g) Among pairs $\mathfrak{a}$, $\mathfrak{b}$ of ideals with $N(\mathfrak{a}) \leq x$, $N(\mathfrak{b}) \leq x$, show that the probability that $\gcd(\mathfrak{a}, \mathfrak{b}) = 1$ is

$$\frac{1}{\zeta_K(2)} + O\big(x^{-1/2}\big) = \frac{6}{\pi^2 L\big(2, \chi_{-4}\big)} + O\big(x^{1/2}\big).$$

9. (Erdős (1946), Saffari (unpublished), Bateman, Pomerance & Vaughan (1981); cf Exercise 2.3.7) Let $\Phi_q(z) = \prod_{d|q}(z^d - 1)^{\mu(q/d)}$ denote the q^{th} cyclotomic polynomial. Suppose that

$$q = \prod_{\substack{p \le y \\ p \equiv \pm 2 \ (5)}} p$$

where y is chosen so that $\omega(q)$ is odd.
(a) Show that if $d|q$ and $\omega(d)$ is even, then $|e(d/5) - 1| = |e(1/5) - 1|$.
(b) Show that if $d|q$ and $\omega(d)$ is odd, then $|e(d/5) - 1| = |e(2/5) - 1|$.
(c) Deduce that $|\Phi_q(e(1/5))| = |e(1/5) + 1|^{d(q)/2}$.
(d) Deduce that $\Phi_q(z)$ has a coefficient whose absolute value is at least

$$\exp\left(q^{(\log 2 - \varepsilon)/\log\log q}\right)$$

if $y > y_0(\varepsilon)$.

10. Grössencharaktere for $\mathbb{Q}(\sqrt{-1})$, continued from Exercise 4.2.7.
(a) For $\sigma > 1$ put

$$L(s, \chi_m) = \sum_{\alpha \in \mathcal{O}_K}{}' \chi_m(\alpha) N(\alpha)^{-s} = \frac{1}{4} \sum_{\substack{a,b \in \mathbb{Z} \\ (a,b) \neq (0,0)}} \chi_m(a+bi)(a^2+b^2)^{-s}$$

where $\sum'_\alpha$ denotes a sum over unassociated members of $\mathcal{O}_K$. Show that the above sum is absolutely convergent in this half-plane.
(b) We recall that members of $\mathcal{O}_K$ factor uniquely into Gaussian primes. Also, the Gaussian primes are obtained by factoring the rational primes: The prime 2 ramifies, $2 = i^3(1+i)^2$, the rational primes $p \equiv 1 \pmod 4$ split into two distinct Gaussian primes, $p = (a+bi)(a-bi)$, and the rational primes $q \equiv 3 \pmod 4$ are inert. Show that

$$L(s, \chi_m) = \prod_{\mathfrak{p}} \left(1 - \chi_m(\mathfrak{p}) N(\mathfrak{p})^{-s}\right)^{-1}$$

for $\sigma > 1$ where the product is over an unassociated family of Gaussian primes $\mathfrak{p}$.
(c) By grouping associates together, show that if $4 \nmid m$ then the sum

$$\sum_{\substack{a,b \in \mathbb{Z} \\ (a,b) \neq (0,0)}} e^{mi \arg(a+bi)} (a^2+b^2)^{-s}$$

vanishes identically for $\sigma > 1$.
(d) For $0 \le \theta \le 2\pi$, put $N(x;\theta) = \text{card}\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 \le x, 0 < \arg(a+bi) \le \theta\}$. Show that for $x \ge 1$,

$$N(x;\theta) = \frac{\theta}{2} x + O(x^{1/2})$$

uniformly in θ.
(e) Show that if $m \neq 0$ then

$$\sum_{\substack{a^2+b^2\le x\\ a>0,b\ge 0}} \chi_m(a+bi) = \int_0^{\pi/2} e^{4mi\theta}\, dN(x;\theta) \ll |m|x^{1/2}.$$

(f) Show that if $m \neq 0$ then the Dirichlet series $L(s,\chi_m)$ is convergent for $\sigma > 1/2$.
(g) Show that $L(s,\chi_m)$ and $L(s,\chi_{-m})$ are identically equal, and hence that $L(\sigma,\chi_m) \in \mathbb{R}$ for $\sigma > 1/2$.

4. Notes

§1. Ramanujan's sum was introduced by Ramanujan (1918). Incredibly, both Hardy and Ramanujan missed the fact that $c_q(n)$ be be written in closed form: The formula on the extreme right of (7) is due to Hölder (1936). Normally one would say that a function f is even if $f(x) = f(-x)$. However, in the present context, an arithmetic function f with period q is said to be *even* if $f(n)$ is a function only of (n,q). Thus $c_q(n)$ is an even function. The space of almost-even functions is rather small, but includes several arithmetic functions of interest. For such functions one may hope for a representation in the form $f(n) = \sum_{q=1}^{\infty} a_q c_q(n)$, called a *Ramanujan expansion*. For a survey of the theory of such expansions, see Schwarz (1988). Hildebrand (1984) established definitive results concerning the pointwise convergence of Ramanujan expansions. An appropriate Parseval identity has been established for mean-square summable almost-even functions; see Hildebrand, Schwarz & Spilker (1988).

§2. The first instance of characters of a non-cyclic group occurs in Gauss's analysis of the genus structure of the class group of binary quadratic forms. The quotient of the class group by the principal genus is isomorphic to $C_2 \otimes C_2 \otimes \cdots \otimes C_2$, and the associated characters are given by Kronecker's symbol. Dirichlet (1939) defined the Dirichlet characters for the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ of reduced residues modulo q, and the same technique suffices to construct the characters for any finite abelian group. More generally, if G is a group, then a homomorphism $h : G \longrightarrow GL(n,\mathbb{C})$ is called a *group representation*, and the trace of $h(g)$ is a *group character*. Note that if a and b are conjugate elements of G, say $a = gbg^{-1}$, then $h(a)$ and $h(b)$ are similar matrices. Hence they have the same eigenvalues, and in particular $\operatorname{tr} h(a) = \operatorname{tr} h(b)$. Thus a group character is constant on conjugacy classes. In the case of a finite abelian group it suffices to take $n = 1$, and in this case the representation and its trace are essentially the same. For an introduction to characters in a wider setting, see Serre (1977).

§3. Dirichlet (1837a,b,c) first proved Corollary 10 in the case that q is prime. The definition of the Dirichlet characters is not difficult in that case, since the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of reduced residues is cyclic. The most challenging part of the proof is to show that $L(1,\chi)$ when χ is the Legendre symbol (mod p). If $p \equiv 3 \pmod 4$, then

$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) \equiv \sum_{a=1}^{p-1} a = \frac{p(p-1)}{2} \equiv 1 \pmod 2,$$

and hence the sum on the left is non-zero. It follows by (9.9) that $L(1,\chi_p) \neq 0$ in this case. If $p \equiv 1 \pmod 4$, then one has the identity of Exercise 9.3.7(c), and thus to show that $L(1,\chi_p) \neq 0$ it suffices to show that $Q \neq 1$. Dirichlet established this by means of Gauss's theory of cyclotomy. Accounts of this are found in Davenport (2000, §§1–3), and in Narkiewicz (2000, pp. 64–65). An alternative proof that $Q \neq 1$ was given more recently by Chowla & Mordell (1961) (cf Exercise 9.3.8). Dirichlet (1839) defined the Dirichlet characters in the general case. In order to prove that $L(1,\chi) \neq 0$ when χ is quadratic, Dirichlet related $L(1,\chi)$ to the class number of binary quadratic forms. Suppose that d is a fundamental quadratic discriminant, and put $\chi_d(n) = \left(\frac{d}{n}\right)$, the Kronecker symbol (as discussed in §9.3). Suppose first that $d > 0$. Among the solutions of Pell's equation $x^2 - dy^2 = 4$, let (x_0, y_0) be the solution with $x_0 > 0$, $y_0 > 0$, and y_0 minimal, and put $\eta = \frac{1}{2}(x_0 + y_0\sqrt{d})$. Dirichlet showed that

$$L(1,\chi_d) = \frac{h \log \eta}{\sqrt{d}} \tag{35}$$

where h is the number of equivalences classes of binary quadratic forms with discriminant d. Since $h \geq 1$ and $y_0 \geq 1$, it follows that $L(1,\chi_d) \gg (\log d)/\sqrt{d}$ in this case. Now suppose that $d < 0$ and that w denotes the number of automorphs of the positive definite binary quadratic forms of discriminant d (i.e., $w = 6$ if $d = -3$, $w = 4$ if $d = -4$, and $w = 2$ if $d < -4$). Dirichlet showed that

$$L(1,\chi_d) = \frac{2\pi h}{w\sqrt{-d}}\,. \tag{36}$$

Thus $L(1,\chi_d) \geq \pi/\sqrt{-d}$ when $d < -4$.

Our treatment of quadratic characters in the proof of Theorem 9 is due to Landau (1906). Mertens (1895a,b), (1897), (1899) gave two elementary proofs that $L(1,\chi) > 0$ when χ is quadratic; cf Exercises 2 and 3. For a definitive account of Mertens' methods, see Bateman (1959). Other proofs have been given by Teege (1901), Gelfond & Linnik (1962, Chapter 3§2), Bateman (1966), (1997), Pintz (1971), and Monsky (1993). See also Baker, Birch & Wirsing (1973).

4. Literature

A. Baker, B. J. Birch & E. A. Wirsing (1973). *On a problem of Chowla*, J. Number Theory **5**, 224–236.

P. T. Bateman (1959). *Theorems implying the non-vanishing of* $\sum \chi(m)m^{-1}$ *for real residue-characters*, J. Indian Math. Soc. **23**, 101–115.

——— (1966). *Lower bounds for* $\sum h(m)/m$ *for arithmetical function* h *similar to real residue characters*, J. Math. Anal. Appl. **15**, 2–20.

——— (1997). *A theorem of Ingham implying that Dirichlet's L-functions have no zeros with real part one*, Enseignement Math. (2) **43**, 281–284.

P. T. Bateman, C. Pomerance, R. C. Vaughan (1981). *On the size of the coefficients of the cyclotomic polynomial*, Coll. Math. Soc. J. Bolyai, pp. 171–202.

R. Carmichael (1932). *Expansions of arithmetical functions in infinite series*, Proc. London Math. Soc. (2) **34**, 1–26.

H. Davenport (2000). *Multiplicative number theory*, Graduate Texts Math. 74, Springer-Verlag (New York), xiv+177 pp.

H. Delange (1976). *On Ramanujan expansions of certain arithmetical functions*, Acta Arith. **31**, 259–270.

P. Erdős (1946). *On the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **52**, 179–184.

A. Friedman (1957). *Mean-values and polyharmonic polynomials*, Michigan Math. J. **4**, 67–74.

A. O. Gelfond & Ju. V. Linnik (1962). *Elementary methods in analytic number theory*, Gosudarstv. Izdat. Fiz.-Mat. Lit. (Moscow), 272 pp.; English translation, Rand McNally (Chicago), 1965, xii+242 pp; English translation, M. I. T. Press (Cambridge), 1966, xi+229 pp.

A. Grytczuk (1981). *An identity involving Ramanujan's sum*, Elem. Math. **36**, 16–17.

A. Hildebrand (1984). *Über die punkweise Konvergenz von Ramanujan-Entwicklungen zahlentheoretischer Funktionen*, Acta Arith. **44**, 108–140.

A. Hildebrand, W. Schwarz & J. Spilker (1988). *Still another proof of Parseval's equation for almost-even arithmetical functions*, Aequationes Math. **35**, 132–139.

O. Hölder (1936). *Zur Theorie der Kreisteilungsgleichung*, Prace Mat.–Fiz. **43**, 13–23.

A. E. Ingham (1929). *Note on Riemann's ζ-function and Dirichlet's L-functions*, J. London Math. Soc. **5**, 107–112.

E. Landau (1906). *Über das Nichtverschwinden einer Dirichletschen Reihe*, Sitzungsber. Akad. Wiss. Berlin **11**, 314–320; Collected Works, Vol. 2, Thales (Essen), 1986, pp. 230–236.

F. Mertens (1895a). *Über Dirichletsche Reihen*, Sitzungsber. Kais. Akad. Wiss. Wien **104**, 2a, 1093–1153.

——— (1895b). *Über das Nichtverschwinden Dirichletscher Reihen mit reelen Gliedern*, Sitzber. Kais. Akad. Wiss. Wien **104**, 2a, 1158–1166.

——— (1897). *Über Multiplikation und Nichtverschwinden Dirichlet'scher Reihen*, J. Reine Angew. Math. **117**, 169–184.

——— (1899). *Eine asymptotische Aufgabe*, Sitzber. Kais. Akad. Wiss. Wien **108**, 2a, 32–37.

P. Monsky (1993). *Simplifying the proof of Dirichlet's theorem*, Amer. Math. Monthly **100**, 861–862.

J. Pintz (1971). *On a certain point in the theory of Dirichlet's L-functions, I,II*, Mat. Lapok **22**, 143–148; 331–335.

S. Ramanujan (1918). *On certain trigonometrical sums and their applications in the theory of numbers*, Trans. Cambridge Philos. Soc. **22**, 259–276; Collected papers, Cambridge University Press (Cambridge), 1927, pp. 179–199.

D. Redmond (1983). *A remark on a paper: "An identity involving Ramanujan's sum" by A. Grytczuk*, Elem. Math. **38**, 17–20.

B. Reznick (1995). *Some constructions of spherical* 5*-designs*, Linear Algebra Appl., 226/228, 163–196.

W. Schwarz (1988). *Ramanujan expansions of arithmetical functions*, Ramanujan revisited, Proc. Centenary Conference (Urbana, June 1987), Academic Press (Boston), pp. 187–214.

J.–P. Serre (1977). *Linear representation of finite groups*, Graduate Texts Math. 42, Springer-Verlag (New York), x+170 pp.

H. Teege (1901). *Beweis, daß die unendliche Reihe* $\sum_{n=1}^{n=\infty} \left(\frac{p}{n}\right) \frac{1}{n}$ *einen positiven von Null verschiedenen Wert hat*, Mitt. Math. Ges. Hamburg **4**, 1–11.

A. Wintner (1943). *Eratosthenian averages*, Waverly Press (Baltimore), vi+81 pp.