Characters

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 $a \pmod q$ 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 $f \in L^2(\mathbb{R})$.

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. (a) Let

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

Show that

$$\sum_{d|q} f(d) = \sum_{a=1}^{q} e(a/q) = \begin{cases} 1 & (q = 1), \\ 0 & (q > 1). \end{cases}$$

(b) Deduce that

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

for all positive integers q.

3. 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 $(\bmod\ q)$ 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 1. *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 $1 \le k \le n$. Moreover,*

$$\sum_{g \in G} \chi(g) = \begin{cases} n & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise}, \end{cases} \tag{5}$$

and

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} n & \text{if } g = e, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

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, $1 \le k \le n$. 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 2. *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* 5) *and* 6) *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 (5) 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 (6) holds for G if it holds for G_1 and G_2.

Theorem 3. *Let G be a finite abelian group. Then $\widehat{G}$ is isomorphic to G, and* (5) *and* (6) *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 4. *The multiplicative group $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ of reduced residue classes* (mod q) *has $\varphi(q)$ Dirichlet characters. If χ is such a character, then*

$$\sum_{\substack{n=1 \\ (n,q)=1}}^{q} \chi(n) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

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

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(q) & \text{if } n \equiv 1 \pmod q, \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

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).

Corollary 5. *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 $q = q_1 q_2$, $(q_1, q_2) = 1$, 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

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

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

Our proof of Theorem 3 depends on Abel's Theorem that any finite abelian group is isomorphic to the direct product of cyclic groups, but we can prove Corollary 4 without appealing to this result, as follows. By the Chinese Remainder Theorem we see that

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

Characters

If p is odd then the reduced residue classes $(\mathrm{mod}\ p^\alpha)$ 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 $(\mathrm{mod}\ \varphi(p^\alpha))$ such that $g^\nu \equiv n \pmod{p^\alpha}$. The number ν is called the index of n, and is denoted $\nu = \mathrm{ind}_g\, n$. From Lemma 2 it follows that the characters $(\mathrm{mod}\ p^\alpha)$, $p>2$, are given by

$$\chi_k(n) = e\Big(\frac{k\,\mathrm{ind}_g\, n}{\varphi(p^\alpha)}\Big) \tag{9}$$

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 2 it follows that if q is odd then the general character $(\mathrm{mod}\ q)$ is given by

$$\chi(n) = e\Big(\sum_{p^\alpha \| q} \frac{k\,\mathrm{ind}_g\, n}{\varphi(p^\alpha)}\Big) \tag{10}$$

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

The multiplicative structure of the reduced residues $(\mathrm{mod}\ 2^\alpha)$ is more complicated. For $\alpha=1$ or $\alpha=2$ the group is cyclic (of order 1 or 2, respectively), and (9) 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 $(\mathrm{mod}\ 2^{\alpha-2})$ 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 2 the characters in this case take the form

$$\chi(n) = e\Big(\frac{j\mu}{2} + \frac{k\nu}{2^{\alpha-2}}\Big) \tag{11}$$

for odd n where $j=0$ or 1 and $1 \le k \le 2^{\alpha-2}$. Thus (10) holds if $8 \nmid q$, but if $8|q$ then the general character takes the form

$$\chi(n) = e\Big(\frac{j\mu}{2} + \frac{k\nu}{2^{\alpha-2}} + \sum_{\substack{p^\alpha\|q\\ p>2}} \frac{\ell\,\mathrm{ind}_g\, n}{\varphi(p^\alpha)}\Big) \tag{12}$$

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 $(\mathrm{mod}\ q)$. It is useful to note that the first condition can be relaxed.

Theorem 6. *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 $k \mapsto n + kq \pmod{m}$ permutes the residue classes (mod m). Thus there is a k for which $n + kq \equiv 1 \pmod{m}$, 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.

2. Exercises

1. Let G be a finite abelian group of order n. Let $g_1, g_2, \ldots, g_n$ denote the elements of G, and let $\chi_1(g), \chi_2(g), \ldots, \chi_n(g)$ 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 $c_1, \ldots, c_q$,

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

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 (mod q).

4. Let $(a, q) = 1$, and suppose that k is the order of a in the multiplicative group of reduced residue classes (mod q).
(a) Show that if χ is a Dirichlet character (mod 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 (mod q).

5. Let χ be a Dirichlet character (mod 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 (mod q).

3. Dirichlet L-functions

For real $s > 1$ we define the Riemann zeta function $\zeta(s)$ to be

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,. \tag{13}$$

By the integral test we note that

$$\frac{1}{s-1} = \int_1^{\infty} x^{-s}\,dx < \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \int_1^{\infty} x^{-s}\,dx = \frac{s}{s-1}\,. \tag{14}$$

Hence in particular, $\zeta(s) \to \infty$ as $s \to 1^+$. A second formula for the zeta function, known as the Euler product formula, asserts that

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \tag{15}$$

for $s > 1$. To understand why this holds, suppose that y is given, and let $\mathcal{N} = \mathcal{N}(y)$ denote the set of those positive integers composed entirely of primes not exceeding y. By the unique factorization theorem it follows that

$$\sum_{n\in\mathcal{N}} \frac{1}{n^s} = \prod_{p\le y} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_{p\le y}\left(1 - \frac{1}{p^s}\right)^{-1}.$$

Here the reordering of the summands is justified by absolute convergence, and we obtain (15) by letting y tend to infinity.

Similarly, if χ is a character (mod q), then for $s > 1$ we put

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}. \tag{16}$$

Since χ is totally multiplicative, it follows that

$$L(s,\chi) = \prod_p \left(1-\chi(p)p^{-s}\right)^{-1} \tag{17}$$

for $s>1$. In particular, we see that

$$L(s,\chi_0) = \sum_{\substack{n=1\\(n,q)=1}}^{\infty} n^{-s} = \zeta(s)\prod_{p|q}\left(1-p^{-s}\right) \tag{18}$$

for $s>1$.

The zeta function is differentiable for $s>1$, since the differentiated series

$$-\sum_{n=1}^{\infty}\frac{\log n}{n^s}$$

is uniformly convergent for $s \ge 1+\delta$. Indeed, since $(\log n)/n$ is monotonically decreasing for $n \ge 3$, it follows by the integral test that

$$\zeta'(s) = -\sum_{n=1}^{\infty}\frac{\log n}{n^s} = -\int_1^{\infty}\frac{\log x}{x^s}\,dx + O(1) = \frac{-1}{(s-1)^2} + O(1) \tag{19}$$

uniformly for $s>1$. By taking logarithms of both sides of the Euler product identity (15), we find that

$$\log\zeta(s) = \sum_p \log\left(1-p^{-s}\right)^{-1} = \sum_p\sum_{k=1}^{\infty}\frac{1}{kp^{ks}}$$

in view of the power series expansion $\log(1-w)^{-1} = \sum_{k=1}^{\infty} w^k/k$. We can differentiate the above term-by-term, since the differentiated series is uniformly convergent for $s \ge 1+\delta$. Thus we find that

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p\sum_{k=1}^{\infty}\frac{\log p}{p^{ks}} = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} \tag{20}$$

where $\Lambda(n)$ is the von Mangoldt lambda function,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \\ 0 & \text{otherwise.}\end{cases}$$

We note that

$$\sum_{d|n}\Lambda(d) = \sum_{p^a\|n}\sum_{b=1}^{a}\log p = \sum_{p^a\|n} a\log p = \log n, \tag{21}$$

which is an elementary way of expressing the relation

$$\Big(- \frac{\zeta'(s)}{\zeta(s)}\Big) \cdot \zeta(s) = -\zeta'(s)\,.$$

By taking logarithms in (18), and then differentiating, we deduce that

$$\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \frac{\zeta'(s)}{\zeta(s)} + \sum_{p|q} \frac{\log p}{p^s - 1}$$

for $s > 1$. On combining this with the estimates (14) and (19), we deduce that

$$\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \frac{-1}{s-1} + O_q(1) \tag{22}$$

for $s > 1$.

For $\chi \ne \chi_0$ we proceed somewhat differently. First we recall Dirichlet's test, which asserts that if a_n is a sequence of real or complex numbers such that the sums $\sum_{n=1}^N a_n$ are uniformly bounded, and if b_n are positive real numbers decreasing monotonically to 0, then the series $\sum_{n=1}^\infty a_n b_n$ converges. From (7) we see that if $\chi \ne \chi_0$, then

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

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

$$\Big| \sum_{n\le x} \chi(n) \Big| \le q \tag{23}$$

for all $x/ge1$. Thus by Dirichlet's test, the series (16) that defines $L(s,\chi)$ is convergent for all $s > 0$, when $\chi \ne \chi_0$. The usual proof of Dirichlet's test can be modified to show further that if the sums $\sum_{n=1}^N a_n$ are uniformly bounded, and $b_n(x)$ are functions such that $b_n(x) \ge b_{n+1}(x)$ for all $x \in [a,b]$, with $0 \le b_n(x) \le B_n$ for all $x \in [a,b]$, and $B_n \to 0$ as $n \to \infty$, then $\sum a_n b_n(x)$ is uniformly convergent. By applying this to the differentiated series $-\sum \chi(n)(\log n)n^{-s}$, we deduce that

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

is a continuous function for $s > 0$. For $s > 1$ we apply (21), and thus find that the above is

$$= -\sum_{n=1}^\infty \frac{\chi(n)}{n^s} \sum_{d|n} \Lambda(d).$$

On putting $n = md$, and inverting the order of summation, we find that the above is

$$\begin{aligned} &= -\sum_{d=1}^{\infty} \frac{\chi(d)\Lambda(d)}{d^s} \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} \\ &= -L(s,\chi) \sum_{m=1}^{\infty} \frac{\chi(m)\Lambda(m)}{m^s}. \end{aligned}$$

That is,

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{m=1}^{\infty} \frac{\chi(m)\Lambda(m)}{m^s} \tag{24}$$

for $s > 1$. Suppose that $(a, q) = 1$. If we multiply both sides of the above by $\overline{\chi}(a)$, sum over χ (mod q), and divide both sides by $\varphi(q)$, then we find that

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

for $s > 1$. Our intent is to show that the above tends to infinity as $s \to 1^+$. From (22) we see that the contribution made by the principal character on the right hand side tends to infinity. The other terms on the right hand side tend to finite limits, provided that $L(1,\chi) \ne 0$. That is, if $L(1,\chi) \ne 0$ for all $\chi \ne \chi_0$, then

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

Since

$$\sum_p \sum_{k>1} \frac{\log p}{p^k} = \sum_p \frac{\log p}{p^2 - p} < \infty,$$

it follows that

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

Thus our approach has the following logical structure:

Lemma 7. (Dirichlet) *Let χ be a Dirichlet character modulo q, $\chi \ne \chi_0$. Then $L(1,\chi) \ne 0$.*

Characters

Theorem 8. (Dirichlet) *Suppose that $(a,q)=1$. Then there exist infinitely many primes p such that $p\equiv a \pmod q$, and indeed*

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

Our proof of Lemma 7 depends on the nature of the character involved. 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 $\chi\ne\chi_0$. Thus a quadratic character is real, and a real character is either principal or quadratic. If χ is quadratic, then $\chi^2=\chi_0$, and hence χ is its own inverse in the character group. If χ is complex, then $\overline{\chi}$ is also a character, $\chi\ne\overline{\chi}$, and $\chi\overline{\chi}=\chi_0$, so that $\overline{\chi}$ is the inverse of χ in the character group.

To prove Lemma 7 for complex characters, we first show that

$$\prod_\chi L(s,\chi)\ge 1 \tag{25}$$

for all $s>1$. To this end we take logarithms on both sides of the Euler product formula (17) for $L(s,\chi)$ to see that

$$\log L(s,\chi)=\sum_p \log\big(1-\chi(p)p^{-s}\big)^{-1}=\sum_p\sum_{k=1}^\infty \frac{\chi(p^k)}{kp^{ks}}=\sum_{n=2}^\infty \frac{\Lambda(n)}{\log n}\cdot\frac{\chi(n)}{n^s}\,.$$

We sum over χ and use the orthogonality relation (8) to see that

$$\sum_\chi \log L(s,\chi)=\varphi(q)\sum_{\substack{n=2\\ n\equiv 1\ (q)}}^\infty \frac{\Lambda(n)}{\log n}\cdot\frac{\chi(n)}{n^s}\,.$$

On exponentiating, we deduce that

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

On the right hand side we are exponentiating a non-negative real number, and hence the right hand side is at least 1, which is to say we have (25).

We note that the argument just completed involves taking logarithms of complex numbers. This can be avoided by the following alternative line of reasoning: On the left hand side of (25) we express each L-function by its Euler product formula. The contribution of a particular prime p is then

$$\prod_\chi\Big(1-\frac{\chi(p)}{p^s}\Big)^{-1}.$$

Suppose that p has order 4 in the multiplicative group of reduced residue classes (mod q). By Exercise 2.4 we know that the numbers $\chi(p)$ are k^{th} roots of unity, each one with multiplicity $\varphi(q)/k$. Also, we note the polynomial factorization $z^k - 1 = \prod_{a=1}^k (z - e(a/k))$. Hence the above is

$$= \prod_{a=1}^{k} \Big(1 - \frac{e(a/k)}{p^s}\Big)^{-\varphi(q)/k} = \Big(1 - \frac{1}{p^{ks}}\Big)^{-\varphi(q)/k}.$$

Since this last expression is clearly > 1, we again have (25).

We now consider the asymptotic behavior of the left hand side of (25) as $s \to 1^+$. From (14) and (18) we see that

$$L(s, \chi_0) \sim \frac{\varphi(q)/q}{s-1}$$

as $s \to 1^+$. Suppose that $\chi \ne \chi_0$. Then $L(s, \chi)$ is continuous for $s > 0$, and hence $\lim_{s\to 1^+} L(s, \chi) = L(1, \chi)$. Suppose now that $L(1, \chi) = 0$. Since $L'(s, \chi)$ is continuous for $s > 0$, the number

$$C_\chi = \max_{1 \le s \le 2} |L'(s, \chi)|$$

is finite, and by Rolle's theorem $|L(s, \chi)| \le C_\chi (s-1)$ for $1 < s \le 2$. We note that the factor $s - 1$ cancels the effect of the factor $1/(s-1)$ contributed by $L(s, \chi_0)$. Suppose now that $L(1, \chi) = 0$ for n different characters (mod q). Then the left hand side of (25) is $< C(s-1)^{n-1}$ as $s \to 1^+$, which contradicts (25) if $n > 1$. That is, $L(1, \chi) = 0$ for at most one character (mod q). However, if χ is a complex character, then $L(s, \overline{\chi}) = \overline{L(s, chi)})$. Hence if $L(1, \chi) = 0$, then also $L(1, \overline{\chi}) = 0$. Since this we now have two different characters that vanish at $s = 1$, we deduce that $L(1, \chi) \ne 0$ when χ is complex.

We now see that the heart of the matter is to show that $L(1, \chi) \ne 0$ when χ is a quadratic character. Dirichlet achieved this by relating $L(1, \chi)$ to the number of equivalence classes of binary quadratic forms. To prepare for our more elementary approach, we first establish two subsidiary estimates.

Lemma 9. *There is a real number C such that*

$$\sum_{m \le y} \frac{1}{\sqrt{m}} = 2y^{1/2} + C + O\big(y^{-1/2}\big)$$

for $y \ge 1$.

The constant C here is $\zeta(1/2) = -1.4603545\ldots$, but this is a bit nonsensical, since we have only defined the zeta function for real $s > 1$.

Proof. Suppose that f has continuous derivative on an interval $[a, b]$. Then by integration by parts we see that

$$\int_a^b f(x)\, dx = \frac{b-a}{2}(f(a) + f(b)) - \int_a^b (x - \tfrac{a+b}{2}) f'(x)\, dx\,.$$

Here the first term on the right hand side is the area of a trapezoid, and the integral on the right represents the error introduced when approximating to an integral by the trapezoid rule. (For purposes of numerical integration, one would usually integrate this latter integral by parts to obtain an estimate in terms of $f''(x)$.) By taking $a = m$, $b = m+1$, $f(x) = x^{-1/2}$, we find that

$$\frac{1}{2}\Big(\frac{1}{\sqrt{m}} + \frac{1}{\sqrt{m+1}}\Big) = \int_m^{m+1} x^{-1/2}\,dx - \frac{1}{2}\int_m^{m+1}(x-m-1/2)x^{-3/2}\,dx\,.$$

By summing this over $m = 1, 2, \ldots, M-1$, we find that

$$\begin{aligned}\sum_{m=1}^{M}\frac{1}{\sqrt{m}} &= \frac{1}{2} + \frac{1}{2\sqrt{M}} + \int_1^M x^{-1/2}\,dx - \frac{1}{2}\int_1^M(\{x\}-1/2)x^{-3/2}\,dx \\ &= 2M^{1/2} - \frac{3}{2} - \frac{1}{2}\int_1^\infty(\{x\}-1/2)x^{-3/2}\,dx + \frac{1}{2\sqrt{M}} + \frac{1}{2}\int_M^\infty(\{x\}-1/2)x^{-3/2}\,dx \\ &= 2M^{1/2} + C + O\big(M^{-1/2}\big)\end{aligned}$$

where

$$C = -\frac{1}{2}\int_1^\infty(\{x\}-1/2)x^{-3/2}\,dx\,.$$

Lemma 10. *Let χ be a non-principal character modulo q. If $s > 0$ and $x \ge 1$, then*

$$\sum_{n\le x}\frac{\chi(n)}{n^s} = L(s,\chi) + O\big(qx^{-s}\big)\,.$$

We have already made the qualitative observation that the series defining $L(s,\chi)$ converges for $s > 0$. In the above, we are making a more specific claim concerning the rate of this convergence.

Proof. Let $S(x) = \sum_{n\le x}\chi(n)$. Then

$$\begin{aligned}\sum_{n=M+1}^{M+N}\frac{\chi(n)}{n^s} &= \sum_{n=M+1}^{M+N}\frac{S(n)-S(n-1)}{n^s} \\ &= \sum_{n=M+1}^{M+N-1}S(n)\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big) + \frac{S(M+N)}{(M+N)^s} - \frac{S(M)}{(M+1)^s}\end{aligned}$$

We have already observed that $|S(x)| \le q$ for all x. Thus the above has absolute value not exceeding

$$q\Big(\sum_{n=M+1}^{M+N}\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big) + \frac{1}{(M+1)^s} + \frac{1}{(M+N)^s}\Big) = \frac{2q}{(M+1)^s}\,.$$

Thus we have the stated result.

We now complete the proof of Lemma 7. Suppose that χ is a quadratic character modulo q, and put $r(n) = \sum_{d|n} \chi(d)$. Since χ is multiplicative, it follows that $r(n)$ is also multiplicative, and indeed if $n = \prod_p p^\alpha$ where $\alpha = \alpha(p)$, then

$$r(n) = \prod_p \big(1 + \chi(p) + \chi(p^2) + \cdots + \chi(p^\alpha)\big)\,.$$

We note that

$$1 + \chi(p) + \chi(p^2) + \cdots + \chi(p^\alpha) = \begin{cases} 1 & \text{if } p|q, \\ \alpha + 1 & \text{if } \chi(p) = 1, \\ 1 & \text{if } \chi(p) = -1 \text{ and } 2|\alpha, \\ 0 & \text{if } \chi(p) = -1 \text{ and } 2 \nmid \alpha. \end{cases} \tag{26}$$

Next we show that

$$\sum_{n \le x} \frac{r(n)}{\sqrt{n}} = 2x^{1/2} L(1, \chi) + O\big(\sqrt{q}\big) \tag{27}$$

for $x \ge q$. For $d|n$ we write $n = md$, we let y be a parameter to be chosen later, $1 \le y \le x$, and we distinguish between $d \le y$ and $d > y$ to see that the above is

$$\begin{aligned} \sum_{n \le x} n^{-1/2} \sum_{d|n} \chi(d) &= \sum_{\substack{m,d \\ md \le x}} \frac{\chi(d)}{\sqrt{md}} \\ &= \sum_{d \le y} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le x/d} \frac{1}{\sqrt{m}} \\ &\quad + \sum_{m \le x/y} \frac{1}{\sqrt{m}} \sum_{y < d \le x/m} \frac{\chi(d)}{\sqrt{d}} \end{aligned}$$

which by Lemmas 9 and 10 is

$$\begin{aligned} &= \sum_{d \le y} \frac{\chi(d)}{\sqrt{d}} \Big(2\sqrt{x/d} + C + O\big(\sqrt{d/x}\big)\Big) + O\Big(\sum_{m \le x/y} \frac{q}{\sqrt{my}}\Big) \\ &= 2\sqrt{x} \sum_{d \le y} \frac{\chi(d)}{d} + C \sum_{d \le y} \frac{\chi(d)}{\sqrt{d}} + O\big(y/\sqrt{x}\big) + O\big(q\sqrt{x}/y\big)\,. \end{aligned}$$

By two further applications of Lemma 10 we see that this is

$$= 2\sqrt{x} L(1, \chi) + C L(1/2, \chi) + O\big(y/\sqrt{x}\big) + O\big(q\sqrt{x}/y\big)\,.$$

By taking $x = q$ and $s = 1/2$ in Lemma 10, and estimating the sum on the left hand side trivially, we deduce that $L(1/2, \chi) = O\big(\sqrt{q}\big)$. On inserting this in the above, and taking $y = \sqrt{qx}$, we obtain the estimate (27).

If $L(1, \chi) = 0$, then the right hand side of (27) remains bounded as x tends to infinity. On the other hand, from (26) we see that $r(n) \ge 0$ for all n, and that $r\big(n^2\big) \ge 1$. Thus the left hand side of (27) is $\ge \sum_{m \le \sqrt{x}} 1/m$, which tends to infinity with x. Thus $L(1, \chi) > 0$, and so Lemma 7 is proved, and with it, Theorem 8.

4. Gauss sums

In the additive characters $e(an/q)$ we have a basis for the vector space of arithmetic functions with period q. Let $\chi(n)$ be a Dirichlet character modulo q. Since $\chi(n)$ has period q, it follows that the multiplicative character χ can be written as a linear combination of additive characters. This can be done for arbitrary q, but we restrict our attention here to a prime modulus. Let χ be a non-principal character (mod p). We define the Gauss sum of χ to be

$$\tau(\chi) = \sum_{n=1}^{p} \chi(n) e(n/p)\,. \tag{28}$$

Note that this is the inner product of χ with the particular additive character $e(n/p)$. We may consider similar inner products with other characters, say by setting

$$G(a, \chi) = \sum_{n=1}^{p} \chi(n) e(an/p).$$

By (7) we see that

$$G(0, \chi) = 0. \tag{29}$$

On the other hand, if $(a, p) = 1$, then

$$\chi(a) G(a, \chi) = \sum_{n=1}^{p} \chi(an) e(an/p)\,.$$

Since an runs through a complete residue system (mod p) as n does, the right hand side above is $\tau(\chi)$. That is,

$$G(a, \chi) = \overline{\chi}(a) \tau(\chi) \tag{30}$$

for $a \not\equiv 0 \pmod{p}$. From (29) we see that the above also holds when $a \equiv 0 \pmod{p}$; thus it holds for all a.

In the notation (2) of the finite Fourier transform,

$$\widehat{\chi}(k) = \frac{1}{p} G(-k, \chi)\,.$$

We recall that the Parseval identity (4) for the finite Fourier transform asserts that

$$\sum_{n=1}^{p} |\chi(n)|^2 = p \sum_{k=1}^{p} |\widehat{\chi}(k)|^2.$$

Here the left hand side is $p - 1$, and by (30) the right hand side is $(p-1)|\tau(\chi)|^2/p$. Consequently,

$$|\tau(\chi)| = \sqrt{p} \tag{31}$$

for each non-principal character character $\chi \pmod p$. The Gauss sum (28) could also be defined similarly for the principal character χ_0; by (7) we find that $\tau(\chi_0) = -1$. This is a special case of Exercise 1.2.

By taking complex conjugates in the definition (28) of the Gauss sum, we find that

$$\overline{\tau(\chi)} = \sum_{n=1}^{p} \overline{\chi}(n) e(-n/p),$$

which by (30) is

$$= \chi(-1)\tau(\overline{\chi}).$$

The only quadratic character modulo p is the Legendre symbol $\left(\frac{n}{p}\right)$. When the above is applied to this particular character, we find that

$$\tau\big(\big(\frac{\cdot}{p}\big)\big) = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p} & \text{if } p \equiv -1 \pmod 4\,. \end{cases} \tag{32}$$

Gauss noticed empirically—and eventually proved—that only the plus sign occurs. For complex characters the location of $\tau(\chi)$ on the circle $|z| = \sqrt{p}$ is less predictable, and indeed Deligne showed that the numbers $\tau(\chi)$ are asymptotically uniformly distributed on this circle, as $p \to \infty$.

On the additive group of real numbers we have additive characters $x \mapsto e^{-ax}$, which is to say homomorphisms into the multiplicative group $\mathbb{C}^\times$ of non-zero of complex numbers. On the multiplicative group of positive real numbers—which may be construed as analogous to the reduced residues modulo q—we have multiplicative characters $x \mapsto x^s$ where s is a complex number. The inner product of these, with respect to the multiplicatively invariant measure dx/x, is

$$\int_0^\infty e^{-ax}x^s\,\frac{dx}{x} = a^{-s}\int_0^\infty e^{-x}x^s\,\frac{dx}{x} = a^{-s}\Gamma(s)$$

for $\Re s > 0$. This is Euler's integral for the Gamma function. Although it converges only for $\Re s > 0$, the Gamma function may be considered to by analogous, for any complex s, to the Gauss sum $\tau(\chi)$.

Consider (30) with a non-principal character χ replaced by $\overline{\chi}$. Since $\tau(\overline{\chi}) \ne 0$ we can divide by this quantity to find that

$$\chi(a) = \frac{1}{\tau(\overline{\chi})}\sum_{n=1}^{p}\overline{\chi(n)}e(an/p) \tag{33}$$

for all a. Here we have expressed the multiplicative character $\chi(a)$ as a linear combination of the additive characters $e(an/p)$. The above has many important applications. As an example, we show that it is now a routine matter to evaluate the sum

$$S(h) = \sum_{a=1}^{p}\Big(\frac{a}{p}\Big)\Big(\frac{a+h}{p}\Big).$$

By two applications of (33) we see that the above is

$$\sum_{a=1}^{p}\frac{1}{\tau_p^2}\sum_{m=1}^{p}\Big(\frac{m}{p}\Big)e\Big(\frac{am}{p}\Big)\sum_{n=1}^{p}\Big(\frac{n}{p}\Big)e\Big(\frac{n(a+h)}{p}\Big).$$

By (32) we see that $\tau_p^2 = p\big(\frac{-1}{p}\big)$. Thus the above is

$$\frac{\big(\frac{-1}{p}\big)}{p}\sum_{m=1}^{p}\Big(\frac{m}{p}\Big)\sum_{n=1}^{p}\Big(\frac{n}{p}\Big)\sum_{a=1}^{p}e\Big(\frac{(m+n)a+hn}{p}\Big).$$

Here the innermost sum vanishes unless $n \equiv -m \pmod p$, in which case it has the value $pe(hn/p)$. Thus the above is

$$\begin{aligned}\Big(\frac{-1}{p}\Big)\sum_{m=1}^{p}\Big(\frac{-m^2}{p}\Big)e\Big(\frac{-mh}{p}\Big) &= \sum_{m=1}^{p-1}e\Big(\frac{-mh}{p}\Big)\\ &= \begin{cases}-1 & \text{if } h \not\equiv 0 \pmod p,\\ p-1 & \text{if } h \equiv 0 \pmod p.\end{cases}\end{aligned}$$

4. Exercises

1. (a) Show that if $p > 2$ and $p \nmid b$, then

$$\sum_{n=1}^{p} \left(\frac{n}{p}\right)\left(\frac{n+b}{p}\right) = -1.$$

(b) Suppose that $p > 2$ and that $p \nmid d$. Explain why

$$\sum_{x=1}^{p} \left(\frac{x^2-d}{p}\right) = \sum_{n=1}^{p} \left(1 + \left(\frac{n}{p}\right)\right)\left(\frac{n-d}{p}\right),$$

and deduce that this sum is -1.
(c) Put $d = b^2 - 4ac$, and suppose that $p > 2$, $p \nmid d$. Show that

$$\sum_{x=1}^{p} \left(\frac{ax^2+bx+c}{p}\right) = \left(\frac{a}{p}\right).$$

2. Let p be a prime, $p \equiv 1 \pmod 4$, and let $\mathcal{N}$ be a set of Z residue classes modulo p.
(a) Explain why

$$\sum_{m\in\mathcal{N}}\sum_{n\in\mathcal{N}} \left(\frac{m-n}{p}\right) = \frac{1}{\sqrt{p}}\sum_{a=1}^{p}\left(\frac{a}{p}\right)\Big|\sum_{n\in\mathcal{N}} e(an/p)\Big|^2.$$

(b) Suppose that $\left(\frac{m-n}{p}\right) = 1$ whenever $m \in \mathcal{N}$, $n \in \mathcal{N}$, and $m \neq n$. Show that $Z \le \sqrt{p}$.

3. Put $f_{\boldsymbol{a}}(r) = r^2 + a_1 r + a_0$ where $\boldsymbol{a} = (a_0, a_1)$. Show that if r_1, r_2, r_3 are distinct modulo p, then

$$\sum_{a_0=1}^{p}\sum_{a_1=1}^{p} \left(\frac{f_{\boldsymbol{a}}(r_1)}{p}\right)\left(\frac{f_{\boldsymbol{a}}(r_2)}{p}\right)\left(\frac{f_{\boldsymbol{a}}(r_3)}{p}\right) = p.$$

4. Let

$$G_k(a) = \sum_{n=1}^{p} e\Big(\frac{an^k}{p}\Big).$$

(a) Let $N_k(h)$ denote the number of solutions of the congruence $x^k \equiv h \pmod p$. Explain why

$$G_k(a) = \sum_{h=1}^{p} N_k(h) e\Big(\frac{ah}{p}\Big).$$

(b) Let $l = (k, p-1)$. Show that if k is a positive integer, then $N_k(h) = N_l(h)$ for all h, and hence that $G_k(a) = G_l(a)$.
(c) Suppose that $k \mid (p-1)$. Explain why

$$\sum_{a=1}^{p} |G_k(a)|^2 = p \sum_{h=1}^{p} N_k(h)^2.$$

(d) Suppose that $k \mid (p-1)$. Show that there are $(p-1)/k$ residues $h \pmod p$ for which $N_k(h) = k$, that $N_k(0) = 1$, and that $N_k(h) = 0$ for all other residue classes $(\mathrm{mod}\ p)$. Hence show that the right hand side above is $p(1 + (p-1)k)$.
(e) Let k be a divisor of $p-1$. Suppose that $p \nmid a$, $p \nmid c$, and that $b \equiv ac^k \pmod p$. Show that $G_k(a) = G_k(b)$.
(f) Suppose that $k \mid (p-1)$. Show that if $p \nmid a$, then $|G_k(a)| < k\sqrt{p}$.

5. Suppose that $k \mid (p-1)$, that $N_k(h)$ is as in Exercise 4(a), and let χ be a character of order k, say $\chi(n) = e((\operatorname{ind} n)/k)$.
(a) Show that for all h,

$$N_k(h) = 1 + \sum_{j=1}^{k-1} \chi^j(h).$$

(b) Show that if $p \nmid a$ then

$$G_k(a) = \sum_{j=1}^{k-1} \overline{\chi}^j(a)\tau(\chi).$$

(c) Show that if $p \nmid a$, then $|G_k(a)| \le (k-1)\sqrt{p}$.

6. Let $N(q)$ denote the number of pairs x, y of residue classes $(\mathrm{mod}\ q)$ such that $y^2 \equiv x^3 + 7 \pmod q$.
(a) Show that $N(q)$ is a multiplicative function of q, that $N(2) = 2$, $N(3) = 3$, $N(7) = 7$, and that $N(p) = p$ when $p \equiv 2 \pmod 3$.
(b) Suppose that $p \equiv 1 \pmod 3$. Let $\chi_1(n)$ be a cubic character modulo p, and let $\chi_2(n) = \left(\frac{n}{p}\right)$ be the quadratic character modulo p. Show that

$$\begin{aligned} N(p) &= \frac{1}{p} \sum_{a=1}^{p} e(7a/p) \Big(\sum_{h=1}^{p} \big(1 + \chi_1(h) + \chi_1^2(h)\big) e(ah/p) \Big) \Big(\sum_{k=1}^{p} \big(1 + \chi_2(k)\big) e(-ak/p) \Big) \\ &= p + \frac{2}{p} \Re\big(\tau(\chi_1)\tau(\chi_2)\tau(\chi_1^2\chi_2)\chi_1\chi_2(-7)\big), \end{aligned}$$

and deduce that $|N(p) - p| \le 2\sqrt{p}$.
(c) Deduce that $N(p) > 0$ for all p.
(d) Show that $N(2^k) = 2^{k-1}$ for $k \ge 2$, that $N(3^k) = 2{\cdot}3^{k-1}$ for $k \ge 2$, that $N(7^k) = 6{\cdot}7^{k-1}$

for $k \ge 2$, and that $N(p^k) = N(p)p^{k-1}$ for all other primes.
(e) Conclude that the congruence $y^2 \equiv x^3 + 7 \pmod q$ has solutions for every positive integer q.
(f) Suppose that x and y are integers such that $y^2 = x^3 + 7$. Show that $2 \mid y$, $x \equiv 1 \pmod 4$, and that $x > 0$. Note that $y^2 + 1 = (x+2)(x^2 - 2x + 4)$, so that $y^2 + 1$ is composed of primes $\equiv 1 \pmod 4$, and yet $x + 2 \equiv 3 \pmod 4$. Deduce that this equation has no solution in integers.

7. Explain why the number N of solutions of the congruence $c_1 x_1^{k_1} + \cdots + c_m x_m^{k_m} \equiv c \pmod p$ is

$$N = \frac{1}{p} \sum_{a=1}^{p} e(-ac/p) \prod_{j=1}^{m} G_{k_j}(ac_j)$$

where G_k is defined as in Exercise 4.
(b) Suppose that $c = 0$ but that p does not divide any of the numbers c_j. Show that $|N - p^{m-1}| \le C p^{m/2}$ where $C = \prod_{j=1}^{m}((k_j, p-1) - 1)$.
(c) Suppose that $c \not\equiv 0 \pmod p$ and that for all j, $c_j \not\equiv 0 \pmod p$. Show that $|N - p^{m-1}| \le C p^{(m-1)/2}$ where C is defined as above.

8. Let χ_1 and χ_2 be nonprincipal characters $\pmod p$.
(a) Show that if $(a, p) = 1$, then

$$\sum_{n=1}^{p} \chi_1(n)\chi_2(a-n) = \chi_1\chi_2(a) p \frac{\tau(\overline{\chi}_1\overline{\chi}_2)}{\tau(\overline{\chi}_1)\tau(\overline{\chi}_2)}.$$

(b) Show that if $\chi_1\chi_2$ is nonprincipal, then

$$\sum_{n=1}^{p} \chi_1(n)\chi_2(a-n) = \chi_1\chi_2(a) \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)} \tag{34}$$

for all a.

When $a = 1$, the sum (34) is known as the *Jacobi sum* $J(\chi_1, \chi_2)$. In the same way that the Gauss sum is analogous to the gamma function, the Jacobi sum (and it's evaluation in terms of Gauss sums) is analogous to the Beta function

$$B(\alpha, \beta) = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\, dx = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}.$$

9. Let C be the smallest field that contains the field $\mathbf{Q}$ of rational numbers and is closed under square roots. Thus C is the set of complex numbers that are constructible by ruler-and-compass. We show that if p is of the form $p = 2^k + 1$ then $\zeta = e(1/p) \in C$, which is

to say that a regular p-gon can be constructed.
(a) Let p be any prime, and χ any nonprincipal character modulo p. Explain why

$$\tau(\chi)^2 \sum_{n=1}^{p} \overline{\chi}(n)\overline{\chi}(1-n) = p\tau(\chi^2).$$

(b) From now on assume that p is of the form $p = 2^k + 1$. Explain why $\chi^{2^k} = \chi_0$ for any character modulo p, and deduce that $\chi(n) \in C$ for all χ and all integers n.
(c) Deduce that if $\tau(\chi^2) \in C$, then $\tau(\chi) \in C$.
(d) Suppose that χ has order 2^r. Show successively that the numbers

$$-1 = \tau(\chi^{2^r}),\ \tau(\chi^{2^{r-1}}),\ \dots,\ \tau(\chi^2),\ \tau(\chi)$$

lie in C.
(e) Explain why $\sum_\chi \tau(\chi) = (p-1)\zeta$.
(f) (Gauss) If $p = 2^k + 1$, then $\zeta \in C$.

12. Let χ be a character modulo p and put $J(\chi) = \sum_{n=1}^{p} \chi(n)\chi(1-n)$.
(a) Show that if $\chi^2 \neq \chi_0$, then $|J(\chi)| = \sqrt{p}$.
(b) Show that if $p \equiv 1 \pmod 4$, then there is a quartic character χ modulo p.
(c) Show that if χ is a quartic character, then $J(\chi)$ is a Gaussian integer. That is, $J(\chi) = a + ib$ where a and b are rational integers.
(d) Deduce that $a^2 + b^2 = p$