3. INFINITELY MANY PRIMES; COMPLEX ANALYSIS

Dirichlet proved that there are infinitely many primes in every arithmetic progression $a \pmod q$ with $(a,q)=1$. Our next objective is to prove Dirichlet's theorem, developing several themes along the way.

3.1. Characteristic functions for arithmetic progressions. We want a way to focus on only the integers in the arithmetic progression $a \pmod q$. Our first method to do this is a modification of the analytic way to identify 0 out of all of the integers: If $a \in \mathbb{Z}$ then[1]

$$\frac{1}{2i\pi}\oint_{|z|=1} z^{a-1}dz = \int_0^1 \exp(2i\pi at)dt = \begin{cases} 1 & \text{if } a=0; \\ 0 & \text{if } a \neq 0. \end{cases} \tag{3.1.1}$$

To determine $0 \pmod q$ we replace powers of all the complex numbers $\exp(2i\pi t)$, $0 \le t < 1$ on the unit circle, with powers of all the qth roots of unity: Complex number α is an qth root of unity if $\alpha^q = 1$. There are q qth roots of unity, namely $\exp(2i\pi j/q)$ for $j = 0,1,2,\dots,q-1$. Note that if q does not divide a then

$$\frac{1}{q}\sum_{\substack{\alpha\in\mathbb{C}\\ \alpha^q=1}} \alpha^a = \frac{1}{q}\sum_{j=0}^{q-1}\exp(2i\pi aj/q) = \frac{1}{q}\cdot\frac{\exp(2i\pi qj/q)-1}{\exp(2i\pi j/q)-1} = 0 \tag{3.1.2}$$

(since we are summing a geometric progression), whereas if q does divide a this same sum evidently equals 1. In other words this complicated sum counts 1 if $a \equiv 0 \pmod q$, and 0 otherwise. It is easy to modify this, by replacing a by $a-b$, so that this counts integer a if and only if $a \equiv b \pmod q$. Therefore the number of primes $\le x$ that are $\equiv a \pmod q$ is given by the formula

$$\begin{aligned}\sum_{\substack{p \text{ prime, } p\le x\\ p\equiv a \pmod q}} 1 &= \sum_{\substack{p \text{ prime}\\ p\le x}} \frac{1}{q}\sum_{j=0}^{q-1}\exp\left(2i\pi\frac{(p-a)j}{q}\right) \\ &= \frac{1}{q}\sum_{j=0}^{q-1}\exp\left(-2i\pi\frac{aj}{q}\right)\sum_{\substack{p \text{ prime}\\ p\le x}}\sum_{j=0}^{q-1}\exp\left(2i\pi\frac{pj}{q}\right).\end{aligned}$$

[1] The notation $\oint f(z)dz$ denotes the integral of the function $f(z)$ over values of z on some closed curve. See section 7.5 for a discussion as to the meaning of this.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

Therefore if we can only accurately estimate the sum of $\exp(2i\pi pj/q)$ over the primes up to x then we can determine the number of primes in each arithmetic progression $\pmod q$. It may seem that we have traded in one rather difficult problem, for another; unless there is some special technique that we can apply to these new sums then what we just did was pointless. Indeed we do not know how to proceed; this approach was given as a prelude to the slightly more difficult, though ultimately successful, approach via Dirichlet characters for focusing on the integers from a particular arithmetic progression.

Exercises

3.1a. In exercise 1.3b we saw that the primitive nth roots of unity may be written as $\exp(2i\pi j/n)$ for each j with $(j, n) = 1$.

a) Determine the value of the sum of the primitive nth roots of unity. (Hint: You may want to use the inclusion-exclusion principle.)

b) Deduce the value of $\sum_{j\leq n:\ (j,n)=1} \exp(2i\pi jb/n)$.

3.2. Dirichlet characters. A *Dirichlet character* is a homomorphism from the integers $\pmod q$ to the complex numbers, though not the function which only takes the value 0. In other words we study the homomorphisms $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, which we extend to $\mathbb{Z}$ simply by defining $\chi(n)$ as $\chi(n \pmod q)$. The simplest Dirichlet character is $\chi(n) = 1$ for all $n \in \mathbb{Z}$, which has period 1. We can extend this to a character $\pmod q$ by taking $\chi_0(n) = 1$ if $(n, q) = 1$ and 0 of $(n, q) > 1$; we call this the *principal* character $\pmod q$. For any character of period > 1 there exists an integer n such that $\chi(n) \neq 1$, so that $\chi(0) = \chi(0 \cdot n) = \chi(0)\chi(n)$, and therefore $\chi(0) = 0$. If $q = p^k$ where p is prime then $\chi(p)^k = \chi(q) = 0$ so that $\chi(p) = 0$, and therefore $\chi(n) = 0$ if $(n, q) > 1$. Now there exists an integer m such that $\chi(m) \neq 0$ and so $\chi(m) = \chi(1 \cdot m) = \chi(1)\chi(m)$ so that $\chi(1) = 1$.

If $p > 2$ then the elements of $(\mathbb{Z}/p^k\mathbb{Z})^*$, that is the residue classes mod p^k that are coprime with p, form a cyclic group of order $\phi(p^k)$. Let g be a generator of that group, so that $\{a \pmod{p^k} : (a, p) = 1\} = \{g^j \pmod{p^k} : 0 \leq j < \phi(p^k)\}$; therefore if $(a, p) = 1$ there exists j for which $a \equiv g^j \pmod{p^k}$ and so $\chi(a) = \chi(g^j) = \chi(g)^j$. That is, χ is completely determined by the value $\chi(g)$. In fact $\chi(g)^{\phi(p^k)} = \chi(g^{\phi(p^k)}) = \chi(1) = 1$, so $\chi(g)$ is a $\phi(p^k)$th root of unity. In fact, for each ℓ, $0 \leq \ell < \phi(p^k)$ there is a character χ_ℓ defined by $\chi_\ell(g) = \exp\left(2i\pi\frac{\ell}{\phi(p^k)}\right)$. Note that $\chi_i\chi_j = \chi_{i+j \pmod{\phi(p^k)}}$, so that the characters $\pmod{p^k}$ form a cyclic group of order $\phi(p^k)$, that is the *character group* is isomorphic to $(\mathbb{Z}/p^k\mathbb{Z})^*$.

In the character group the element of order 1 is the principal character. These cyclic groups have even order and so have exactly one element of order 2; this is something you have encountered before – the character $\pmod p$ of order two is the Legendre symbol.

If $p = 2$ and $k \geq 2$ then $(\mathbb{Z}/2^k\mathbb{Z})^*$ is isomorphic to the cyclic group of 2^{k-1} elements. If $p = 2$ and $k \geq 3$ then $(\mathbb{Z}/2^k\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ generated by -1 and 3, respectively. In exercise 3.2a we develop the theory of characters of period 2^k, and observe that the character group is isomorphic to $(\mathbb{Z}/2^k\mathbb{Z})^*$.

Now suppose that $q = p_1^{k_1} \dots p_\ell^{k_\ell}$ where $p_1, \dots, p_k$ are distinct primes. For any given integer $a \pmod q$, define $a_i \pmod q$ so that $a_i \equiv a \pmod{p_i^{k_i}}$ and $a_i \equiv 1 \pmod{q/p_i^{k_i}}$, and a function χ_i by $\chi_i(a) = \chi(a_i)$. One can check that each χ_i is a character $\pmod{p_i^{k_i}}$

and that $\chi(a) = \chi_1(a)\chi_2(a)\dots\chi_\ell(a)$. Therefore the characters $\pmod q$ are a product of the characters $\pmod{p_i^{k_i}}$, $i = 1, 2, \dots, \ell$, so that the character group $\pmod q$ is a direct product of the character groups $\pmod{p_i^{k_i}}$, which implies that the character group $\pmod q$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^*$ for all $q \geq 1$.

If r is a proper divisor of q, with ψ a character $\pmod r$ and χ_0 the principal character $\pmod q$ then $\chi := \psi\chi_0$ is a character $\pmod q$. In fact $\chi(a) = \psi(a)$ if $(a, q) = 1$ and $\chi(a) = 0$ if $(a, q) > 1$, so we say that χ is *induced* by ψ. Any character that is not induced by any character with a smaller modulus is called *primitive*. The modulus for a character is sometimes called the *conductor* of the character. Any *real* character is one that only takes on real values; it must have order one or two. A *complex* character is one that is not real. The *conjugate* $\overline{\chi}$ of χ is simply that character for which $\overline{\chi}(n) = \overline{\chi(n)}$ for all integers n. Notice that $\overline{\chi} = \chi$ if and only if χ has order 1 or 2.

The reason that we have been developing the theory of Dirichlet characters has been to have a different way of identifying the integers in the arithmetic progression $a \pmod q$ with $(a, q) = 1$. We need an identity analogous to (3.1.2). Take the sum of $\chi(n)$ over all of the characters $\chi \pmod q$. If $(n, q) > 1$ then each $\chi(n) = 0$, so we now assume $(n, q) = 1$. If $n \not\equiv 1 \pmod q$ then there exists a character $\chi_1 \pmod q$ for which $\chi_1(n) \neq 1$ (by exercise 3.2c.c). Now since the characters form a group we see that $\{\chi \pmod q\} = \{\chi_1\chi \pmod q\}$ so that $\sum_\chi \chi(n) = \sum_\chi \chi_1(n)\chi(n) = \chi_1(n)\sum_\chi \chi(n)$ and therefore since $\chi_1(n) \neq 1$ we deduce that

$$\frac{1}{\phi(q)} \sum_{\chi \pmod q} \chi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod q \\ 0 & \text{otherwise.} \end{cases} \tag{3.2.1}$$

From this it is easy to deduce that if $(a, q) = 1$ then

$$\frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod q \\ 0 & \text{otherwise.} \end{cases} \tag{3.2.2}$$

Therefore if P is some set of integers n with associated weights $w(n)$ then

$$\begin{aligned} \sum_{\substack{n\in P \\ n\equiv a \pmod q}} w(n) &= \sum_{n\in P} w(n) \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\chi(n) \\ &= \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \left(\sum_{n\in P} \chi(n)w(n) \right). \end{aligned} \tag{3.2.3}$$

Thus we have reduced the problem to a new weighted sum over elements of P we haven't having to concern ourselves with the restriction to an arithmetic progression.

Since the group of characters form a group isomorphic to the original group, we can reverse the roles of the residues mod q, and of the characters mod q, in the argument above. We then deduce that

$$\frac{1}{\phi(q)} \sum_{a \pmod q} \chi(a) = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases} \tag{3.2.4}$$

Exercises

3.2a.a) Let χ be a non-principal, real character of period p, and let g be a primitive root mod p (that is, a generator of the multiplicative group mod p), for odd prime p. Prove that $\chi(g) = -1$.

b) Show that g is not a square mod p (that is, there does not exist $x \pmod p$ for which $x^2 \equiv g \pmod p$); and then that g^a is a square mod p if and only a is even.

c) Deduce that χ is the Legendre symbol $\pmod p$.

3.2b. Prove that if $p = 2$ and $k \geq 3$ then $(\mathbb{Z}/2^k\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ generated by -1 and 3, respectively. Develop the theory of characters of period 2^k.

3.2c.a) Prove that if χ is a non-principal character $\pmod q$ then there exists an integer $n \pmod q$ such that $\chi(n)$ is not equal to either 0 or 1.

b) Deduce that $\chi(n) \neq 1$ for at least half of the residues $n \pmod q$ with $(n, q) = 1$.

c) Show that if $(a, q) = 1$ and $a \not\equiv 1 \pmod q$ then there exists a character $\chi \pmod q$ for which $\chi(a) \neq 1$.

3.2d.a) Show that every non-principal, real character has order two.

b) Show that if q is the product of distinct odd primes then the only primitive, real character mod q, is the Jacobi symbol $(\frac{\cdot}{q})$ (defined for $q = p_1 \dots p_k$ by $(\frac{a}{q}) = (\frac{a}{p_1}) \dots (\frac{a}{p_k})$).

3.2e.a) How many distinct characters are there mod q?

b) How many primitive characters are there mod q?

3.2f. Prove (3.2.4).

3.2g. Use (3.2.4) and the fact that χ has period q, to prove that if χ is a non-principal character mod q then $|\sum_{n \leq N} \chi(n)| \leq q$ for any integer N.

3.3. Infinitely many primes in an arithmetic progression.

If we let P be the set of prime powers, that is numbers of the form p^k with p prime and $k \geq 1$, and take $w(p^k) = 1/k(p^k)^s$ in (3.2.3) where s is a real number > 1, then we obtain

$$\sum_{\substack{p \text{ prime, } k\geq 1 \\ p^k \equiv a \pmod q}} \frac{1}{k(p^k)^s} = \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \left(\sum_{p \text{ prime}} \sum_{k \geq 1} \frac{\chi(p^k)}{k(p^k)^s} \right).$$

Note that the sums on both sides are absolutely convergent by exercise 2.2b. For each χ and each prime p the last sum on the right may be simplified as $-\log(1 - \chi(p)/p^s)$. Therefore

$$\sum_{\substack{p \text{ prime, } k\geq 1 \\ p^k \equiv a \pmod q}} \frac{1}{k(p^k)^s} = \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \log \left(\prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \right).$$

The *Euler product* was obtained by summing the logarithms for the individual primes. If we expand this product, firstly by writing $\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = 1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{(p^2)^s} + \dots$ and then by multiplying the contribution of all of then primes, we deduce as in (2.2.1) from the Fundamental theorem of arithmetic the identity

$$\prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n \geq 1} \frac{\chi(n)}{n^s}. \tag{3.3.1}$$

In fact this proof works so long as $\mathrm{Re}(s) > 1$. The quantity on the right is denoted $L(s,\chi)$, the *Dirichlet L-function for character* χ. We can therefore rewrite the above as

$$\sum_{\substack{p \text{ prime},\ k\geq 1\\ p^k\equiv a \pmod q}} \frac{1}{k(p^k)^s} = \frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \log\left(L(s,\chi)\right). \tag{3.3.2}$$

Notice that the Riemann zeta function is closely related to $L(s,\chi_0)$:

$$\begin{aligned} L(s,\chi_0) &= \prod_{\substack{p \text{ prime}\\ p\nmid q}} \left(1-\frac{1}{p^s}\right)^{-1} = \prod_{\substack{p \text{ prime}\\ p\mid q}} \left(1-\frac{1}{p^s}\right) \prod_{p \text{ prime}} \left(1-\frac{1}{p^s}\right)^{-1} \\ &= \prod_{\substack{p \text{ prime}\\ p\mid q}} \left(1-\frac{1}{p^s}\right) \zeta(s). \end{aligned} \tag{3.3.3}$$

Note that $1 \geq \prod_{p|q}(1-1/p^s) \geq \phi(q)/q$. On the left side of (3.3.2) the terms with $k\geq 2$ contribute $\leq \sum_{n\geq 2,\ k\geq 2} 1/n^k = \sum_{n\geq 2} 1/(n(n-1)) = 1$. Therefore we now obtain

$$\sum_{\substack{p \text{ prime}\\ p\equiv a \pmod q}} \frac{1}{p^s} - \frac{1}{\phi(q)} \sum_{p \text{ prime}} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_{\substack{\chi \pmod q\\ \chi\neq\chi_0}} \overline{\chi}(a)\log\left(L(s,\chi)\right) + O_q(1). \tag{3.3.4}$$

Here we have written $O_q(1)$ to denote a function that is bounded in absolute value by a constant that depends only on q.

We will prove that $\lim_{s\to 1^+} |\log(L(s,\chi))| \ll_q 1$ for each non-principal character $\chi \pmod q$. Therefore taking the limit as $s\to 1^+$ in (3.3.4) we will deduce from (2.2.3) that

$$\sum_{\substack{p \text{ prime}\\ p\equiv a \pmod q}} \frac{1}{p} = \infty,$$

whenever $(a,q)=1$, which implies that there are infinitely many primes $\equiv a \pmod q$.

Now, for $\mathrm{Re}(s)>1$ and χ non-principal, we can write each $n = rq+j$ with $r\geq 0$ and $1\leq j\leq q$ to re-arrange the (absolutely converging) series for $L(s,\chi)$ to obtain

$$\begin{aligned} L(s,\chi) &= \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \sum_{r\geq 0}\sum_{j=1}^{q} \frac{\chi(rq+j)}{(rq+j)^s} = \sum_{r\geq 0}\sum_{j=1}^{q} \frac{\chi(j)}{(rq+j)^s} \\ &= \sum_{r\geq 0} \left\{ \sum_{j=1}^{q} \chi(j) \left(\frac{1}{(rq+j)^s} - \frac{1}{((r+1)q)^s} \right) \right\}, \end{aligned} \tag{3.3.5}$$

since $\sum_{j=1}^{q} \chi(j) = 0$ by (3.2.4). The idea is that by defining $L(s,\chi)$ with this regrouping of terms, that is by taking q of them at a time to effect some cancelation, we will obtain a definition of $L(s,\chi)$ which is valid in a wider region than $\mathrm{Re}(s)>1$. So now suppose that $\mathrm{Re}(s)\le 1$.

We have $((r+1)q)^s/(rq+j)^s = (1-(q-j)/rq)^{-s} = \exp(O(|s|/(r+1)))$ since $|q-j|\le q$, using the Taylor series expansion of log. Therefore if $r\ge |s|+1$ then $|(rq+j)^{-s} - ((r+1)q)^{-s}| \ll ((r+1)q)^{-\mathrm{Re}(s)}|s|/(r+1)$, so that, for $k=\lceil |s|+1\rceil$, we have

$$|L(s,\chi)| \ll \sum_{n=1}^{kq} \frac{1}{n^{\mathrm{Re}(s)}} + \sum_{r\ge k} \frac{q}{((r+1)q)^{\mathrm{Re}(s)}} \frac{|s|}{(r+1)}$$

$$\ll \min\left\{ \frac{(kq)^{1-\mathrm{Re}(s)}}{1-\mathrm{Re}(s)}, \log(kq) \right\} + \frac{|s|}{\mathrm{Re}(s)} \frac{q^{1-\mathrm{Re}(s)}}{k^{\mathrm{Re}(s)}} \ll_s q^{1-\mathrm{Re}(s)} + \log q \tag{3.3.6}$$

Therefore the grouping of terms given for the value of $L(s,\chi)$ in (3.3.5) actually converges in the wider region $\mathrm{Re}(s)>0$ and therefore provides an *analytic continuation* of $L(s,\chi)$ to this domain. In particular it gives us a value for $L(1,\chi)$ and that $\lim_{s\to 1^+} L(s,\chi)$ exists and equals $L(1,\chi)$. Hence to prove that $\lim_{s\to 1^+} |\log(L(s,\chi))| \ll_q 1$ we simply need to show that $L(1,\chi)\ne 0$ (as (3.3.6) establishes that $L(1,\chi)\ne\infty$).

We will show that $L(1,\chi)\ne 0$ for complex characters χ in exercise 3.3a. Proving that $L(1,\chi)\ne 0$ for real characters χ is far more difficult than for complex characters, and investigating this question led to Dirichlet to one of the greatest results of number theory, the *Dirichlet class number formula* which we will discuss a little later. There are now many proofs of the fact that $L(1,\chi)\ne 0$. We will give the quickest, due to Gel'fond, in the next section, and then follow Dirichlet by giving a proof that highlights the interplay between the $\exp(2i\pi\frac{j}{q})$ and the characters $\chi \pmod q$, preceeding this with a discussion of the properties of *Gauss sums*.

Exercises

3.3a. Above we saw that if χ is a non-principal character then $L(s,\chi)$ is an analytic function in $\mathrm{Re}(s)>0$, so that it has a Taylor series at $s=1$.

a) Deduce that $|L(s,\chi)-L(1,\chi)|\le C_\chi|s-1|$ when $|s-1|<1/2$ for some constant $C_\chi>0$.

b) Suppose that $\chi_1,\chi_2 \pmod q$ are distinct non-principal characters for which $L(1,\chi_1)=L(1,\chi_2)=0$. Using part a, exercise 2.2b, and (3.3.6) show that $|\prod_{\chi \pmod q} L(s,\chi)| \ll_q s-1$ for $1<s\le 3/2$.

c) Use (3.3.2) with $a=1$ to show that $\prod_{\chi \pmod q} L(s,\chi)$ is a real number ≥ 1, for each real $s>1$.

d) Use parts b and c to show that there can be no more than one character $\chi \pmod q$ for which $L(1,\chi)=0$.

e) Prove that $L(1,\overline{\chi})=\overline{L(1,\chi)}$. Deduce from this and part d that if $L(1,\chi)=0$ then χ is real.

f) Show that there is no more than one primitive character χ for which $L(1,\chi)=0$. (Hint: If there are two, then consider the characters they induce for some common modulus.) The idea that there can be no more than one "exceptional" character will appear again later.

3.3b. Use (3.3.6) to deduce that $L(1,\chi)=\sum_{n\ge 1}\frac{\chi(n)}{n}$ for all non-principal characters $\chi \pmod q$. (When we take an infinite sum we mean $\sum_{n\ge 1} = \lim_{N\to\infty}\sum_{n=1}^N$, so we are asking whether this latter limit exists and, if so, whether the limit gives the correct value.) We remark that one can show that the Euler product representation (3.3.1) cannot hold in such a wide region – more on that in section *.*.

3.3c. By taking $s=1+1/\log x$ in (3.3.4) so that $\frac{1}{p^s}=\frac{1}{p}+O(\frac{1}{\log x}\cdot\frac{\log p}{p})$ for $p<x^N$, and using our estimates for $L(s,\chi)$, prove that

$$\sum_{\substack{p \text{ prime},\ p\le x\\ p\equiv a \pmod q}} \frac{1}{p} = \frac{\log\log x}{\phi(q)} + O_q(1). \tag{3.3.7}$$

3.4. Gel'fond's and Selberg's proofs that $L(1,\chi)\neq 0$ for real characters χ.

Gel'fond's proof. Let $t\in(0,1)$ and define $a_n(t)=\frac{1}{n(1-t)}-\frac{t^n}{1-t^n}$. We will use the identity

$$\sum_{n\geq 1} a_n(t)\chi(n)=\frac{L(1,\chi)}{1-t}-\sum_{n\geq 1}\chi(n)\frac{t^n}{1-t^n}. \tag{3.4.1}$$

We will bound the left side of this equation: By the arithmetic-geometric mean inequality we have $\frac{1-t^n}{n(1-t)}=\frac{1}{n}\sum_{j=0}^{n-1}t^j\geq\left(\prod_{j=0}^{n-1}t^j\right)^{1/n}=t^{(n-1)/2}>t^n$. Dividing through by $1-t^n$ we deduce that $a_n>0$. Moreover $\frac{1-t^n}{n(1-t)}\cdot\frac{1-t^{n+1}}{(n+1)(1-t)}\geq t^{(n-1)/2}\cdot t^{n/2}>t^n$, and dividing through by $(1-t^n)(1-t^{n+1})/(1-t)$ we obtain $a_n>a_{n+1}$. Now

$$\begin{aligned}\sum_{n\geq 1}a_n(t)\chi(n)&=\sum_{n\geq 1}a_n(t)\left(\sum_{m\leq n}\chi(m)-\sum_{m\leq n-1}\chi(m)\right)\\ &=\sum_{N\geq 1}(a_N(t)-a_{N+1}(t))\sum_{m\leq N}\chi(m).\end{aligned}$$

Therefore, by exercise 3.2g and the fact that the a_i are decreasing, we deduce that

$$\left|\sum_{n\geq 1}a_n(t)\chi(n)\right|\leq\sum_{N\geq 1}|a_N(t)-a_{N+1}(t)|q=qa_1(t)=q.$$

For the sum on the right side of (3.4.1) we have

$$\sum_{n\geq 1}\chi(n)\frac{t^n}{1-t^n}=\sum_{n\geq 1}\chi(n)\sum_{\substack{m\geq 1\\ n|m}}t^m=\sum_{m\geq 1}\left(\sum_{\substack{n\geq 1\\ n|m}}\chi(n)\right)t^m. \tag{3.4.2}$$

Now $\sum_{n|m}\chi(n)\geq 0$ for all $m\geq 1$, and is ≥ 1 is m is a square. Therefore, if $L(1,\chi)=0$ we can combine the above information in (3.4.1) to obtain

$$q\geq\sum_{n\geq 1}\chi(n)\frac{t^n}{1-t^n}\geq\sum_{r\geq 1}t^{r^2}.$$

Since there are infinitely many squares we obtain a contradiction by taking t close enough to 1. Therefore $L(1,\chi)\neq 0$.

This completes our first proof that $L(1,\chi)\neq 0$ if χ is non-principal, and therefore that there are infinitely many primes in any arithmetic progression $a \pmod q$ with $(a,q)=1$. In fact we can deduce slightly more, that the right side of (3.3.4) is bounded by some function of q alone for all real $s\geq 1$. Now, take $s=1+\epsilon/\log x$, for some small $\epsilon>0$, in

(3.3.4). Note that if $p \leq x$ then $\frac{1}{p^s} = \frac{1}{p}(1 + O(\epsilon))$. On the other hand if $X = x^{2^j}$ then $\sum_{X<p<X^2} 1/p^s \leq X^{-\epsilon/\log x} \sum_{X<p<X^2} 1/p \ll \exp(-\epsilon 2^j)$, by (2.*.*). Summing this over $j \geq 0$ we see that $\sum_{p>x} 1/p^s \ll 1/\sqrt{\epsilon}$. Therefore taking (3.3.4) and our estimates here, together with (2.*.*), and letting $\epsilon \to 0$, we obtain

$$\sum_{\substack{p \text{ prime} \\ p \leq x \\ p \equiv a \pmod q}} \frac{1}{p} \sim \frac{1}{\phi(q)} \sum_{\substack{p \text{ prime} \\ p \leq x}} \frac{1}{p} \sim \frac{1}{\phi(q)} \log\log x. \tag{3.4.3}$$

Selberg's proof. Given integer D define

$$P(N) := \sum_{\substack{(x,y) \in \mathbb{Z}^2 \setminus (0,0) \\ x^2 + |D| y^2 \leq N}} \log |x^2 - Dy^2|.$$

We will proceed much as we did with (2.4.1), first evaluating our sum by looking at the size of each term, and then by studying the contribution to the sum of each prime power. If $|x^2 - Dy^2| < T (< N)$ then either $x^2 + |D|y^2 \ll T$, for which there are $\ll T/\sqrt{|D|}$ such terms, or else $\sqrt{T/|D|} \ll |y| \leq \sqrt{N/|D|}$ and x lies in an interval of length $\ll T/(\sqrt{|D|}y)$, yielding a total of $\ll (T/\sqrt{|D|}) \log(2N/T)$ such terms. Therefore

$$\log N \sum_{\substack{(x,y) \in \mathbb{Z}^2 \setminus (0,0) \\ x^2 + |D| y^2 \leq N}} 1 - P(N) \leq \sum_{i=1}^{\lceil \log N \rceil} \sum_{\substack{(x,y) \in \mathbb{Z}^2 \setminus (0,0) \\ x^2 + |D| y^2 \leq N \\ N/e^i < |x^2 - Dy^2| \leq N/e^{i-1}}} i \ll \frac{N}{\sqrt{|D|}} \sum_{i \geq 1} \frac{i^2}{e^i} \ll \frac{N}{\sqrt{|D|}}.$$

To count the number of lattice points in $x^2 + |D|y^2 \leq N$ we can proceed in several different ways, for instance by taking the area of this ellipse, $\pi N/\sqrt{|D|}$, with an error bounded by a multiple of the perimeter, $O(\sqrt{N})$ (see also exercise 3.4c). Combining this with the equation above yields

$$P(N) = \pi \frac{N}{\sqrt{|D|}} \log N + O\left(\frac{N}{\sqrt{|D|}}\right)$$

for $N \geq |D|$.

Now we will determine $P(x)$ by counting how often each prime power $\leq 2N^2$ divides the terms of the product: If $(D/p) = -1$ then p^{2k} divides $x^2 - Dy^2$ if and only if p^k divides (x, y). Writing $x = p^k u, y = p^k v$ this happens whenever $u^2 + |D|v^2 \leq N/p^{2k}$; and by the previous paragraph for $\pi N/(p^{2k}\sqrt{|D|}) + O(\sqrt{N}/p^k)$ such pairs. Thus the total contribution of such prime powers to $\log P(N)$ is $\ll \sum_{p \leq N} (N/\sqrt{|D|})(\log p/p^2) + \sqrt{N}(\log p/p) \ll N/\sqrt{|D|}$ for $N \geq |D| \log^2 |D|$.

If $(D/p) = 1$ then there exists $b \pmod p$ for which $b^2 \equiv D \pmod p$. Moreover p divides $x^2 - Dy^2$ if and only if $x \equiv \pm by \pmod p$. Now the set of pairs of integers (x, y) satisfying $x \equiv by \pmod p$ form a two-dimensional proper sublattice of $\mathbb{Z}^2$, which contains the parallelogram $\{(0,0),(p,0),(b,1),(p+b,1)\}$ of volume p. Note that this must be a fundamental cell of the lattice since a smaller cell would have to have volume which is a proper divisor of p, but then would be volume 1, contradicting the fact that this is a sublattice.

There exists a solution (x_1,y_1) of $x_1 \equiv by_1 \pmod p$ with $x_1^2+|D|y_1^2 \leq 2\sqrt{|D|}p$: To see this, note that there are more than p elements $i+jb$ with $0 \leq i \leq p^{1/2}|D|^{1/4}$ and $0 \leq j \leq p^{1/2}/|D|^{1/4}$, so that two are congruent mod p, say $i+jb \equiv I+Jb$, and we take $x_1 = i-I, y_1 = j-J$ and divide out any common factor. Select (x_2,y_2) to be the smallest vector in the lattice that is not a multiple of (x_1,y_1), so that $|x_1y_2-y_1x_2| = p$. Then $(x_1,y_1),(x_2,y_2)$ form a basis for our lattice and we are counting the number of pairs of integers u,v for which $x = ux_1+vx_2, y = uy_1+vy_2$ satisfying $x^2+|D|y^2 \leq N$. Substituting in, we need $au^2+buv+cv^2 \leq N$ where $a = x_1^2+|D|y_1^2,\ b = x_1x_2+|D|y_1y_2,\ c = x_2^2+|D|y_2^2$, so that $d = b^2-4ac = -4|D|(x_1y_2-y_1x_2)^2 = -4|D|p^2$. By exercise 3.4c the number of solutions is therefore $\pi N/(p\sqrt{|D|})$ plus an error term which is $\ll \sqrt{aN/(|D|p^2)}+\sqrt{N/a} \ll \sqrt{N/p}$, since $2\sqrt{|D|}p \geq |a| \geq |x_1^2-Dy_1^2| \geq p$.

This estimate also holds for the solutions with $x \equiv -by \pmod p$. We have double counted the solutions with $x \equiv y \equiv 0 \pmod p$, but we have already bounded the number of these above. A similar argument gives a good estimate for how often p^k divides x^2-Dy^2, though if $p=2$ and $k \geq 3$, there may be as many as four square-roots of $D \pmod{2^k}$. If $p|D$ then p divides x^2-Dy^2 if and only if p divides x, so that there are $\pi N/(p\sqrt{|D|}) + O(\sqrt{N/|D|}+\sqrt{N}/p)$ solutions.

Combining all of these estimates yields that

$$\begin{aligned} P(N) &= \sum_{\substack{p \text{ prime}, k\geq 1 \\ p^k \leq N \\ (D/p)=1}} \left\{ \frac{2\pi N}{p^k\sqrt{|D|}} \log p + O\left(\sqrt{\frac{N}{p^k}}\log p\right)\right\} \quad + O(N) \\ &= \frac{2\pi N}{\sqrt{|D|}} \sum_{\substack{p \text{ prime}, p\leq N \\ (D/p)=1}} \frac{\log p}{p} + O(N). \end{aligned}$$

Comparing the two evaluations of $P(N)$ implies that

$$\sum_{\substack{p \text{ prime}, p\leq N \\ (D/p)=1}} \frac{\log p}{p} = \frac{1}{2}\log N + O(1). \tag{3.4.4}$$

Subtracting this from (2.7.1), gives the same estimate though with the condition "$(D/p)=1$" in the sum replaced by "$(D/p)=-1$". Imitating the deduction of (2.7.3) from (2.7.1), we deduce that there exist constants c_D^+, c_D^- such that

$$\sum_{\substack{p \text{ prime}, p\leq N \\ (D/p)=\pm 1}} \frac{1}{p} = \frac{1}{2}\log\log N + c_D^{\pm} + O\left(\frac{1}{\log N}\right); \tag{3.4.5}$$

and therefore

$$\log L(1,(D/.)) = \lim_{N\to\infty} \sum_{p \text{ prime}, p\le N} \frac{(D/p)}{p} + \sum_{k\ge 2} \frac{(D/p^k)}{kp^k}$$

exists and equals some constant. Therefore $L(1,(D/.)) \neq 0$.

Exercises

3.4a. If $m = \prod_p p^{k_p}$ then determine the value of $\sum_{n|m} \chi(n)$ as a function of the $\chi(p)$ and $k_p \pmod 2$.

3.4b. Verify that our proof yields the lower bound $L(1,\chi) \ge (1-t)(\sum_{r\ge 1} t^{r^2} - q)$ for $0<t<1$. By a cunning choice of t, deduce that there exists a constant $C>0$ such that $L(1,\chi) > C/q^2$.

3.4c. Suppose that integers $a>0, b, c$ are given with $d = b^2-4ac<0$. We wish to count $\mathcal{N}$, the number of pairs of integers (u,v) for which $au^2+buv+cv^2 \le N$.

a) By completing the square show that $v^2 \le 4aN/|d|$ and that u lies in an interval of length $\sqrt{4aN+dv^2}/2a$.

b) Justify that $\mathcal{N}$ can be estimated by the volume of the region $au^2+buv+cv^2\le N$ with an error term $\ll \sqrt{4aN/|d|} + \sqrt{N/a}$.

c) Show that the volume is $2\pi N/\sqrt{|d|}$.

3.5. Gauss sums. For a character $\chi \pmod q$, let the *Gauss sum* $g(\chi)$ be defined as

$$g(\chi) := \sum_{a \pmod q} \chi(a) \exp\left(2i\pi \frac{a}{q}\right).$$

For fixed m with $(m,q)=1$ we change the variable a to mb, as b varies through the residues mod q, coprime to q, so that

$$\overline{\chi}(m) g(\chi) = g(\chi, m), \text{ where } g(\chi,m) := \sum_{a \pmod q} \chi(a) \exp\left(2i\pi \frac{am}{q}\right). \tag{3.5.1}$$

As in section 3.2 let us suppose that $q = p_1^{k_1}\dots p_\ell^{k_\ell}$ where $p_1,\dots,p_k$ are distinct primes, so there exist characters $\chi_i \pmod{p_i^{k_i}}$ such that $\chi = \chi_1\chi_2\cdots\chi_\ell$. If $a_i \equiv a \pmod{p_i^{k_i}}$ with $(a_i, q/p_i^{k_i}) = 1$ then, by the Chinese Remainder Theorem, there exist integers b_j such that $a \equiv \sum_{j=1}^k a_j b_j (q/p_j^{k_j}) \pmod q$. In particular this implies that $a/q \equiv \sum_{j=1}^{\ell} a_j b_j / p_j^{k_j}$ (mod 1) so that

$$\begin{aligned} g(\chi) &= \sum_{\substack{a_1 \pmod{p_1^{k_1}},\dots \\ \dots, a_\ell \pmod{p_1^{k_\ell}}}} \chi_1(a_1)\chi_2(a_2)\dots\chi_\ell(a_\ell) \prod_{j=1}^{\ell} \exp\left(2i\pi \frac{a_j b_j}{p_j^{k_j}}\right) \\ &= \prod_{j=1}^{\ell} \sum_{a_j \pmod{p_j^{k_j}}} \chi_j(a_j) \exp\left(2i\pi \frac{a_j b_j}{p_j^{k_j}}\right) = \prod_{j=1}^{\ell} \overline{\chi}_j(b_j) g(\chi_j). \end{aligned}$$

Hence if we can understand Gauss sums for prime power moduli then this formula allows us to lift our understanding to Gauss sums mod q, for any q. We will do so for $q = p$ and leave the case of $q = p^k, k \geq 2$ for exercise 3.5c. Now $g(\chi, 0) = 0$ by (3.2.4). Therefore, by (3.5.1), we have for $q = p$ prime,

$$\begin{aligned}
|g(\chi)|^2 &= \frac{1}{\phi(p)} \sum_{(m,p)=1} |g(\chi, m)|^2 = \frac{1}{\phi(p)} \sum_{m=0}^{p-1} |g(\chi, m)|^2 \\
&= \frac{1}{\phi(p)} \sum_{m=0}^{p-1} \sum_{a \pmod p} \chi(a) \exp\left(2i\pi \frac{am}{p}\right) \sum_{b \pmod p} \overline{\chi}(b) \exp\left(-2i\pi \frac{bm}{p}\right) \\
&= \sum_{a \pmod p} \sum_{b \pmod p} \chi(a)\overline{\chi}(b) \frac{1}{\phi(p)} \sum_{m=0}^{p-1} \exp\left(2i\pi \frac{(a-b)m}{p}\right) \\
&= \sum_{\substack{a,b \pmod p \\ a \equiv b \pmod p}} \chi(a)\overline{\chi}(b) \frac{p}{\phi(p)} = p
\end{aligned} \tag{3.5.2}$$

by (3.1.2).

Therefore $|g(\chi)| = \sqrt{p}$. Now, by changing variables $b = q - a$,

$$\overline{g(\chi)} = \sum_{a \pmod q} \chi(a) \exp\left(-2i\pi \frac{a}{q}\right) = \sum_{b \pmod q} \overline{\chi}(q-b) \exp\left(2i\pi \frac{b}{q}\right) = \chi(-1) g(\overline{\chi}). \tag{3.5.3}$$

Therefore if χ is a real character with $\chi(-1) = 1$ then $g(\chi) \in \mathbb{R}$, so that $g(\chi) = \sqrt{p}$ or $-\sqrt{p}$; and if χ is a real character with $\chi(-1) = -1$ then $g(\chi) \in i\mathbb{R}$, so that $g(\chi) = i\sqrt{p}$ or $-i\sqrt{p}$. (This can be written more neatly as $g(\chi) = \pm\sqrt{\chi(-1)p}$.) Deciding which of these two choices gives the value of $g(\chi)$ is a substantially more difficult question, which we will address in section 7.3.

Exercises:

3.5a. Prove that $\frac{1}{\phi(q)} \sum_{\chi \pmod q} \overline{\chi}(n) g(\chi) = \exp\left(2i\pi \frac{n}{q}\right)$.

3.5b. Determine $|g(\chi)|$ when χ has modulus p^k for some $k \geq 2$. (You may want to use exercise 3.1a.b.)

3.6. Finite expressions for the value of $L(1, \chi)$. In (3.5.2) we saw that $g(\chi) \neq 0$, and therefore (3.5.1) yields that $\chi(n) = g(\overline{\chi}, n)/g(\overline{\chi})$. Substituting this into the value obtained for $L(1, \chi)$ in exercise 3.3b, we obtain

$$\begin{aligned}
L(1, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n} &= \frac{1}{g(\overline{\chi})} \sum_{n \geq 1} \frac{1}{n} \sum_{a \pmod q} \overline{\chi}(a) \exp\left(2i\pi \frac{an}{q}\right) \\
&= \frac{1}{g(\overline{\chi})} \sum_{a \pmod q} \overline{\chi}(a) \sum_{n \geq 1} \frac{\exp\left(2i\pi \frac{an}{q}\right)}{n}.
\end{aligned}$$

The sum $\sum_{n\geq 1} z^n/n$ is the Taylor series for $-\log(1-z)$ for $|z|\leq 1,\ z\neq 1$, where the logarithm takes its principal value;[2] now $\text{Re}(1-z)>0$ in this domain and so if $z=e^{2i\pi\theta}$ with $0<\theta<1$ then $1-z=1-e^{2i\pi\theta}=-e^{i\pi\theta}(e^{i\pi\theta}-e^{-i\pi\theta})=-2ie^{i\pi\theta}\sin(\pi\theta)=e^{i\pi(\theta-\frac{1}{2})}\cdot 2\sin(\pi\theta)$. Therefore

$$\begin{aligned} g(\overline{\chi})L(1,\chi) &= -\sum_{a \pmod q} \overline{\chi}(a)\ \log\left(1-\exp\left(2i\pi\frac{a}{q}\right)\right) \\ &= -\sum_{a \pmod q} \overline{\chi}(a)\ \left(i\pi\left(\frac{a}{q}-\frac{1}{2}\right)+\log\left(2\sin\left(\pi\frac{a}{q}\right)\right)\right). \end{aligned}$$

Now if $\chi(-1)=1$ then $\overline{\chi}(q-a)\left(\frac{q-a}{q}-\frac{1}{2}\right)=-\overline{\chi}(a)\left(\frac{a}{q}-\frac{1}{2}\right)$ so that

$$g(\overline{\chi})L(1,\chi)=-\sum_{a \pmod q}\overline{\chi}(a)\log\left(2\sin\left(\pi\frac{a}{q}\right)\right); \tag{3.6.1}$$

and, similarly, if $\chi(-1)=-1$ then

$$g(\overline{\chi})L(1,\chi)=-i\pi\sum_{a \pmod q}\overline{\chi}(a)\left(\frac{a}{q}-\frac{1}{2}\right)=-\frac{i\pi}{q}\sum_{a \pmod q}\overline{\chi}(a)a, \tag{3.6.2}$$

by (3.2.4). In exercise 3.6b we then deduce that

$$g(\overline{\chi})L(1,\chi)=\frac{i\pi}{2-\chi(2)}\cdot\sum_{1\leq a<q/2}\overline{\chi}(a). \tag{3.6.3}$$

If q is prime and χ is real with $\chi(-1)=-1$ then $\sum_{1\leq a<q/2}\overline{\chi}(a)\equiv\frac{q-1}{2}\equiv 1 \pmod 2$, as each $\overline{\chi}(a)=1$ or -1 when $(a,q)=1$. We deduce that $\sum_{1\leq a<q/2}\overline{\chi}(a)\neq 0$ and therefore $L(1,\chi)\neq 0$.

It is more difficult to prove that $L(1,\chi)\neq 0$ when $\chi(-1)=1$. In the case that q is prime this follows from exercise 3.6c below.

Exercises:

3.6a. Justify (3.6.2) properly (i.e. in place of the word "similarly" given there).

3.6b. Suppose that $\chi(-1)=-1$ and let $S:=\sum_{a \pmod q}\chi(a)a$, $S_1:=\sum_{1\leq a<q/2}\chi(a)a$ and $S_2:=\sum_{1\leq a<q/2}\chi(a)$.

a) Replacing a by $q-a$ in S_1, and then adding that to S_1 show that $S=2S_1-qS_2$.

b) Now replace $2a$ by $q-2a$ in $S_3:=\sum_{1\leq a<q/2}\chi(2a)2a$ and obtain $S=4\chi(2)S_1-q\chi(2)S_2$.

c) Deduce (3.6.3).

3.6c. Let $\alpha=\exp(\frac{2i\pi}{q})$ and suppose that χ is a primitive real character $\pmod q$ with $\chi(-1)=1$. Define $f(x)=\prod_{a:\chi(a)=1}(x-\alpha^a)$ and $g(x)=\prod_{a:\chi(a)=-1}(x-\alpha^a)$; so that $f(x)g(x)=\phi_q(x)$.

a) Show that f and g are fixed by the automorphism $\alpha\to\alpha^b$ where $\chi(b)=1$.

b) Deduce that if χ is a primitive character mod q then $f(x),g(x)\in\mathbb{Z}[\sqrt{\chi(-1)q}][x]$.

c) Prove that if $q=p$ is prime then $\phi_p(1)=p$, deduce that $f(1)/g(1)\neq 1$, and then that $L(1,\chi)\neq 0$ using (3.6.1).

[2] Note that $re^{i\theta}=re^{i\theta+2i\pi k}$ for any integer k, so the value of the logarithm function is only well-defined up to an integer multiple of 2π; hence we must specify a suitable range of values.