Special Step A: Dirichlet's Theorem for $m = 8$

> Dirichlet alone, not I, nor Cauchy, nor Gauss knows what a completely rigorous mathematical proof is. Rather we learn it first from him. When Gauss says that he proved something, it seems to me very probable, when Cauchy says it, you can wager as much pro as con; when Dirichlet says it, it is certain.
>
> Carl Gustav Jacob Jacobi

In the 1830s, Dirichlet proved that there are infinitely many primes $p \equiv a \pmod{m}$ whenever a and m are relatively prime.

Our goal on this set is to show, by Dirichlet's method, that there are infinitely many primes in each of the residue classes 1 mod 8, 3 mod 8, 5 mod 8, and 7 mod 8. This proof of Dirichlet's theorem for $m = 8$ occupies a middle ground between the relatively simple arguments of Step #8 for the cases $m = 3$ and $m = 4$, and the more intricate arguments of the next two Special Steps, where Dirichlet's theorem is proved in general.

Characters of $\mathbb{U}_8$

If G is a finite commutative group, by a "character" of G we mean a homomorphism $\chi\colon G \to \{z \in \mathbb{C} : |z| = 1\}$ (the target set here forming a group under multiplication). We use the symbol χ_0 to denote the "trivial character" mapping all of G to 1. For example, when $G = \mathbb{U}_3$ there is precisely one nontrivial character χ, and the table of characters along with their values is very simple (shown at right).

Table 13.1. Character table of $\mathbb{U}_3$

	χ_0	χ
1 mod 3	1	1
2 mod 3	1	-1

13.126. Show that if χ is a character of $\mathbb{U}_8$, then $\chi(g)^2 = 1$ for all $g \in \mathbb{U}_8$. Use this to show that $\mathbb{U}_8$ has exactly 3 nontrivial characters, with character table as follows:

	χ_0	χ_1	χ_2	χ_3
1 mod 8	1	1	1	1
3 mod 8	1	-1	-1	1
5 mod 8	1	1	-1	-1
7 mod 8	1	-1	1	-1

13.127. Calculate the sum of each row of the table. Conclude that the indicator function $\mathcal{I}_{1 \bmod 8} \colon \mathbb{U}_8 \to \{0, 1\}$ corresponding to the element $1 \bmod 8 \in \mathbb{U}_8$ is given by $\mathcal{I}_{1 \bmod 8} = \frac{1}{4}(\chi_0 + \chi_1 + \chi_2 + \chi_3)$.

13.128. Let a be an odd integer. Using that $n \bmod 8 = a \bmod 8 \iff (n \bmod 8)(a \bmod 8)^{-1} = 1 \bmod 8$, deduce that

$$\mathcal{I}_{a \bmod 8} = \frac{1}{4} \sum_{\chi} \chi(a \bmod 8)^{-1} \chi,$$

where the sum on χ is over all the characters of $\mathbb{U}_8$. Conclude:

$$\mathcal{I}_{1 \bmod 8} = \frac{1}{4}(\chi_0 + \chi_1 + \chi_2 + \chi_3), \quad \mathcal{I}_{3 \bmod 8} = \frac{1}{4}(\chi_0 - \chi_1 - \chi_2 + \chi_3),$$
$$\mathcal{I}_{5 \bmod 8} = \frac{1}{4}(\chi_0 + \chi_1 - \chi_2 - \chi_3), \quad \mathcal{I}_{7 \bmod 8} = \frac{1}{4}(\chi_0 - \chi_1 + \chi_2 - \chi_3).$$

Dirichlet L-functions for $m = 8$

Let m be a positive integer. If χ is a character of $\mathbb{U}_m$, we associate to χ the function on $\mathbb{Z}$ which takes the value $\chi(n \bmod m)$ at integers n coprime to m, and the value 0 at all other integers. We use the same notation for both the original function on $\mathbb{U}_m$ and this "lift" to a function on $\mathbb{Z}$; this will not cause any confusion.

The functions on $\mathbb{Z}$ that arise this way are called the "Dirichlet characters" modulo m. By construction, each Dirichlet character χ satisfies

$$\chi(ab) = \chi(a)\chi(b) \qquad \text{for all } a, b \in \mathbb{Z}.$$

For each Dirichlet character χ, we define the "Dirichlet L-function" associated to χ by

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

The unique nontrivial character χ mod 3, along with its associated L-function, appeared already in Problem 8.84 (there $L(s, \chi)$ was denoted $L(s)$).

13.129. Let χ be any Dirichlet character modulo a positive integer m. Show that the series defining $L(s,\chi)$ is absolutely convergent in the complex half-plane $\Re(s) > 1$. Deduce that for $\Re(s) > 1$,

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

This generalizes Problem 8.84(a).

For the rest of the problem set, we retreat from general Dirichlet characters to the safety of $m = 8$.

13.130. Let χ be a Dirichlet character mod 8. Show that for all $s > 1$, the double series $\sum_p \sum_{k\geq 1} \frac{\chi(p^k)}{kp^{ks}}$ converges absolutely (so that the terms may be safely reordered), and

$$\exp\left(\sum_p \sum_{k\geq 1} \frac{\chi(p^k)}{kp^{ks}}\right) = L(s,\chi).$$

Deduce that $L(s,\chi)$ is positive and that $\log L(s,\chi) = \sum_{p \text{ prime}} \sum_{k\geq 1} \frac{\chi(p^k)}{kp^{ks}}$.

13.131. Let χ be a nontrivial Dirichlet character mod 8. You will show in this problem that the nonvanishing of $L(1,\chi)$ implies that $\log L(s,\chi)$ is bounded for s near 1. Set

$$A_\chi(t) = \sum_{n\leq t} \chi(n).$$

(a) Prove that

$$\sum_{n\leq x} \chi(n) n^{-s} = x^{-s} A_\chi(x) + s \int_1^x \frac{A_\chi(t)}{t^{s+1}}\, \mathrm{d}t$$

for all $x \geq 1$.

(b) By examining the column sums of the character table, show that $|A_\chi(t)| \leq 2$ for all $t \geq 0$.

(c) Deduce from (a), (b) that the series defining $L(s,\chi)$ converges for all $s > 0$, to $s\int_1^\infty \frac{A_\chi(t)}{t^{s+1}}\, \mathrm{d}t$.

(d) Use these integral representations to prove that the series defining $L(s,\chi)$ converges *uniformly* for $s \geq \epsilon$, for any fixed $\epsilon > 0$. Since the summands are continuous functions of s, a standard theorem in real analysis guarantees that $L(s,\chi)$ is continuous for $s > 0$.

(e) Deduce: If $L(1,\chi) \neq 0$, then $\log L(s,\chi)$ is defined and continuous for all $s \geq 1$. Conclude that $\log L(s,\chi) = O(1)$ for $1 < s < 2$.

Reduction to the Nonvanishing of $L(1,\chi)$ for $\chi \neq \chi_0$

It follows from Problem 13.128 that for every odd integer a, and all $s > 1$,

$$\sum_{p \equiv a \pmod 8} \frac{1}{p^s} = \sum_{p \text{ odd}} \frac{1}{p^s} \cdot \mathcal{I}_{a \bmod 8}(p \bmod 8)$$
$$= \sum_{p \text{ odd}} \frac{1}{p^s} \left(\frac{1}{4} \sum_{\chi} \chi(a)^{-1} \chi(p) \right) = \frac{1}{4} \sum_{\chi} \chi(a)^{-1} \sum_{p} \frac{\chi(p)}{p^s},$$

where the sums on χ are over all Dirichlet characters χ mod 8.

13.132. Estimating $\sum_p \chi(p) p^{-s}$

(a) For each Dirichlet character χ mod 8:

$$\sum_{p} \frac{\chi(p)}{p^s} = \log L(s,\chi) + O(1) \quad \text{for } 1 < s < 2.$$

(b) $L(s,\chi_0) = (1 - 2^{-s})\zeta(s)$ when $s > 1$. Hence:

$$\sum_{p} \frac{\chi_0(p)}{p^s} = \log \frac{1}{s-1} + O(1) \quad \text{for } 1 < s < 2.$$

(c) Suppose $\chi \neq \chi_0$ and $L(1,\chi) \neq 0$. Then

$$\sum_{p} \frac{\chi(p)}{p^s} = O(1) \quad \text{for } 1 < s < 2.$$

13.133. Assume $L(1,\chi) \neq 0$ for all $\chi \neq \chi_0$. Then for every odd a, and all s with $1 < s < 2$,

$$\sum_{p \equiv a \pmod 8} \frac{1}{p^s} = \frac{1}{4} \log \frac{1}{s-1} + O(1).$$

Consequently, there are infinitely many primes $p \equiv a \pmod 8$.

Nonvanishing of $L(1,\chi)$ for $\chi \neq \chi_0$

13.134. Write out the series for $L(1,\chi)$, for each nontrivial character χ mod 8. Use familiar facts about alternating series to prove that each such series converges to a positive real number.

Techniques of Generalization

13.135. Use the ideas of this problem set to prove Dirichlet's theorem when $m = 12$.

Special Step B: Dirichlet's Theorem for $m = \ell$ (odd prime)

In this sequence of problems you will carry out a proof of Dirichlet's theorem when $m = \ell$, an odd prime. The general outline of the proof is the same as for $m = 8$. Since the characters of $\mathbb{U}_\ell$ are no longer necessarily real-valued, we will appeal to results in complex analysis rather than real analysis. Having to use complex analysis as opposed to real is more a technical inconvenience than a significant obstacle. We encounter a more serious difficulty when it comes to proving the required nonvanishing of $L(1, \chi)$ for nontrivial χ. For this we follow a clever argument suggested by Sarvadaman Chowla and Louis Mordell.

	χ_0	χ_1	χ_2	χ_3
1 mod 5	1	1	1	1
2 mod 5	1	i	-1	$-$i
3 mod 5	1	$-$i	-1	i
4 mod 5	1	-1	1	-1

Table 14.2. Character table of $\mathbb{U}_5$

Characters of $\mathbb{U}_\ell$

14.136. Every character of $\mathbb{U}_\ell$ maps $\mathbb{U}_\ell$ into the group of $(\ell - 1)$th complex roots of unity.

14.137. Recall that $\mathbb{U}_\ell$ is cyclic, and fix a generator g. For every complex $(\ell - 1)$th root of unity ω, there is a unique character χ of $\mathbb{U}_\ell$ with $\chi(g) = \omega$. Thus, there are $\ell - 1$ distinct characters of $\mathbb{U}_\ell$.

14.138. Show that every row of the character table of $\mathbb{U}_\ell$ sums to 0, except the row headed by 1 mod ℓ, which sums to $\ell - 1$. Deduce that for every $a \in \mathbb{Z}$ not divisible by ℓ, the indicator function of $a \bmod \ell \in \mathbb{U}_\ell$ is given by

$$\mathcal{I}_{a \bmod \ell} = \frac{1}{\ell - 1} \sum_{\chi} \chi(a \bmod \ell)^{-1} \chi.$$

The L-functions $L(s, \chi)$

14.139. Let χ be a Dirichlet character modulo ℓ. The same argument you supplied on the last problem set shows that, for all complex s with real part larger than 1, the double series $\sum_p \sum_{k\geq 1} \frac{\chi(p^k)}{kp^{ks}}$ converges absolutely and

$$\exp\left(\sum_p \sum_{k\geq 1} \frac{\chi(p^k)}{kp^{ks}}\right) = L(s, \chi).$$

(The key fact is that, even in the complex world, $\exp(\sum_{k\geq 1} \frac{z^k}{k}) = \frac{1}{1-z}$ whenever $|z| \leq 1$, $z \neq 1$.) We now *define* (!) "$\operatorname{Log} L(s, \chi)$" by the equation

$$\operatorname{Log} L(s, \chi) = \sum_{\substack{p \text{ prime} \\ k\geq 1}} \frac{\chi(p^k)}{kp^{ks}}.$$

Verify that the right-hand series in this definition converges uniformly on compact subsets of $\Re(s) > 1$, under any ordering of the terms. Since each summand is analytic, a well-known theorem in complex variables guarantees that $\operatorname{Log} L(s, \chi)$ is analytic for $\Re(s) > 1$.

14.140.

(a) Show that every column in the character table for $\mathbb{U}_\ell$ sums to 0, except the one headed by χ_0.
(b) Deduce that if χ is a Dirichlet character mod ℓ with $\chi \neq \chi_0$, then $|\sum_{n\leq t} \chi(n)| < \ell$ for all t.
(c) Show that $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges uniformly on compact subsets of $\Re(s) > 0$. Hence, $L(s, \chi)$ is analytic for $\Re(s) > 0$.

14.141. Let χ be a nontrivial Dirichlet character mod ℓ, and suppose that $L(1, \chi) \neq 0$. Since $L(s, \chi)$ is analytic and nonzero in a neighborhood of $s = 1$, a standard theorem in complex variables implies that there is some analytic logarithm of $L(s, \chi)$ in a neighborhood of $s = 1$.

Deduce that our particular logarithm function, $\operatorname{Log} L(s, \chi)$ (which is initially defined only when $\Re(s) > 1$), analytically continues to a neighborhood of $s = 1$.

Conclude (assuming $L(1, \chi) \neq 0$): $\operatorname{Log} L(s, \chi) = O_\chi(1)$ for $1 < s < 2$.

Reduction to the Nonvanishing of $L(1, \chi)$ for $\chi \neq \chi_0$

It follows from Problem 14.138 that for every integer a not divisible by ℓ, and all $s > 1$,

$$\sum_{p\equiv a \pmod{\ell}} \frac{1}{p^s} = \frac{1}{\ell-1}\sum_{\chi}\chi(a)^{-1}\sum_{p}\frac{\chi(p)}{p^s},$$

where the sums on χ are over all Dirichlet characters χ mod ℓ.

14.142. For $1 < s < 2$: $\displaystyle\sum_{p}\frac{\chi_0(p)}{p^s} = \sum_{p}\frac{1}{p^s} - \sum_{p\mid\ell}\frac{1}{p^s} = \log\frac{1}{s-1} + O_\ell(1).$

14.143. Estimating $\sum_p \chi(p)p^{-s}$

(a) For each Dirichlet character χ mod ℓ:

$$\sum_{p}\frac{\chi(p)}{p^s} = \operatorname{Log} L(s,\chi) + O_\chi(1) \quad \text{for } 1 < s < 2.$$

(b) Suppose $\chi \neq \chi_0$ and $L(1,\chi) \neq 0$. Then

$$\sum_{p}\frac{\chi(p)}{p^s} = O_\chi(1) \quad \text{for } 1 < s < 2.$$

14.144. Assume $L(1,\chi) \neq 0$ for all $\chi \neq \chi_0$. Then for every integer a not divisible by ℓ, and all s with $1 < s < 2$,

$$\sum_{p\equiv a \pmod{\ell}} \frac{1}{p^s} = \frac{1}{\ell-1}\log\frac{1}{s-1} + O_\ell(1).$$

Consequently, there are infinitely many primes $p \equiv a \pmod{\ell}$.

Nonvanishing of $L(1,\chi)$ for $\chi \neq \chi_0$

14.145. Suppose that $L(1,\chi)$ vanishes for two distinct nontrivial Dirichlet characters mod ℓ, say χ_1 and χ_2.

(a) The quotients $\dfrac{L(s,\chi_1)}{s-1}$ and $\dfrac{L(s,\chi_2)}{s-1}$ remain bounded as $s \downarrow 1$, as does $(s-1)L(s,\chi_0)$. Deduce: $\dfrac{1}{s-1}\displaystyle\prod_{\chi} L(s,\chi)$ remains bounded as $s \downarrow 1$.

(b) For $s > 1$: $\displaystyle\sum_{\chi}\operatorname{Log} L(s,\chi) = (\ell-1)\sum_{p^k\equiv 1 \pmod{\ell}}\frac{1}{kp^{ks}} \geq 0.$

Hence, $\displaystyle\prod_{\chi} L(s,\chi) \geq 1$, contrary to the conclusion of (a). Thus, there can be at most one Dirichlet character $\chi \neq \chi_0$ for which $L(1,\chi) = 0$.

14.146. Now consider more closely the situation where there is some (necessarily unique!) nontrivial Dirichlet character χ mod ℓ with $L(1,\chi) = 0$. Show that in this case:

(a) χ assumes only real values,

(b) χ coincides with the Legendre symbol mod ℓ: $\chi(a) = \left(\frac{a}{\ell}\right)$ for all a.

Let G be the Gauss sum associated to ℓ (as on Problem 5.43), and let

$$L = L(1, \left(\frac{\cdot}{\ell}\right)) = \sum_{n=1}^{\infty} \left(\frac{n}{\ell}\right)\frac{1}{n}.$$

We show in the remaining three exercises that $L \neq 0$, completing the proof of Dirichlet's theorem when $m = \ell$.

14.147. Set

$$A = \prod_{0<a<\ell} \left(1 - \mathrm{e}^{2\pi \mathrm{i} a/\ell}\right)^{-\left(\frac{a}{\ell}\right)}.$$

Prove: $A = \exp(G \cdot L)$.

14.148. (Chowla–Mordell) Fix a positive integer n with $\left(\frac{n}{\ell}\right) = -1$. Let

$$P(T) = \prod_{0<r<\ell,\ \left(\frac{r}{\ell}\right)=1} \frac{1-T^{nr}}{1-T^r} \ (\in \mathbb{Z}[T]).$$

Assuming $L = 0$, prove:

(a) $\omega := \mathrm{e}^{2\pi \mathrm{i}/\ell}$ is a root of $P(T) - 1$.
(b) $P(T) = 1 + (1 + T + T^2 + \cdots + T^{\ell-1})Q(T)$ for some $Q(T) \in \mathbb{Z}[T]$.

Finally, show that plugging $T = 1$ into the purported identity of (b) leads to a contradiction when considering both sides mod ℓ.

Ingenuity

14.149. Let $\Phi(n)$ denote the number of "Farey fractions" of order n (reduced fractions in $[0,1]$ with denominator $\leq n$). Then $\{\Phi(n)\}_{n=1}^{\infty}$ begins

$$2, 3, 5, 7, 11, 13, 19, 23, 29, \ldots.$$

Show that despite this promising start, $\Phi(n)$ is infinitely often composite — in fact, infinitely often a multiple of 3.

Note. We do not know if $\Phi(n)$ is prime infinitely often.

Special Step C: Dirichlet's Theorem in the General Case

A careful reading of Special Step B reveals that the primality of $m = \ell$ was used in an essential way only to prove the following.

"Magic" properties of the character table: Each row in the character table for $\mathbb{U}_m$ sums to 0, except for the row headed by $1 \bmod m$, which sums to $\phi(m)$. Each column in the character table for $\mathbb{U}_m$ sums to 0, except for the column headed by χ_0, which sums to $\phi(m)$.

Nonvanishing of $L(1, \chi)$: For all Dirichlet characters $\chi \bmod m$, with $\chi \neq \chi_0$, we have $L(1, \chi) \neq 0$.

On this final problem set, you will prove that the above assertions hold for arbitrary positive integers m. The remaining arguments of Special Step B then apply to show that for every integer a coprime to m,

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \frac{1}{\phi(m)} \log \frac{1}{s-1} + O_m(1).$$

It follows that $\sum_{p \equiv a \pmod{m}} \frac{1}{p}$ diverges (in fact, diverges like $\frac{1}{\phi(m)} \log \log x$ — compare with Problem 8.84), and so there are infinitely many primes $p \equiv a \pmod{m}$.

Character Table Magic

Let G be a finite abelian group.

15.150. (Magic column sums) For each character χ of G, let S_χ be the sum of the character table entries in the column headed by χ. Then $S_{\chi_0} = |G|$. Moreover, for each character χ and each $g \in G$: $\chi(g) S_\chi = S_\chi$. Consequently: $S_\chi = 0$ if $\chi \neq \chi_0$.

15.151. Suppose that H is a proper subgroup of G, and take $g \in G \setminus H$. Let n be the smallest positive integer with $g^n \in H$.

(a) $H' := H \cup gH \cup g^2H \cup \cdots \cup g^{n-1}H$ is a subgroup of G with $|H'| = n|H|$.
(b) Every character of H extends in precisely n distinct ways to a character of H'.

15.152. There are exactly $|G|$ characters of G.

15.153. If g is any non-identity element of G, then there is a character χ of G with $\chi(g) \neq 1$.

15.154. (Magic row sums) Let $g \in G$. If S_g is the sum of the entries in the row headed by g, then $S_g = 0$ unless g is the identity, in which case $S_g = |G|$.

Nonvanishing of $L(1, \chi)$ for $\chi \neq \chi_0$

Let $m \in \mathbb{Z}^+$. The same argument employed in Special Step B will show that $L(1, \chi)$ can vanish for at most one nontrivial Dirichlet character χ mod m, which must assume only real values.

Henceforth, χ denotes a real-valued Dirichlet character mod m. Note that since ± 1 are the only real numbers of absolute value 1,

$$\chi(\mathbb{Z}) \subseteq \{-1, 0, 1\}.$$

15.155. For $x \geq 1$: $\displaystyle L(1, \chi) = \sum_{n \leq x} \frac{\chi(n)}{n} + O_m(1/x)$.

15.156. For $x \geq 1$: $\displaystyle \sum_{n \leq x} \frac{\chi(n)}{n} = \int_1^x \left(\sum_{n \leq t} \chi(n) \right) t^{-2} \, \mathrm{d}t + O_m(1/x)$.

By Problems 15.155 and 15.156,

$$L(1, \chi) = \int_1^x \left(\sum_{n \leq t} \chi(n) \right) t^{-2} \, \mathrm{d}t + O_m(1/x).$$

We now define

$$R(x) = \int_1^x \left(\sum_{n \leq t} \chi(n) \right) \left(\sum_{m \leq x/t} 1 \right) \frac{\mathrm{d}t}{t}.$$

15.157. For $x \geq 1$: $R(x) = x \cdot L(1, \chi) + O_m(\log(\mathrm{e}x))$.

15.158. $R(x)$ is a weighted sum of the numbers $r(n)$ with $n \le x$, where

$$r(n) := \sum_{d|n} \chi(d).$$

Precisely:

$$R(x) = \sum_{nm \le x} \chi(n) \int_n^{x/m} \frac{\mathrm{d}t}{t} = \sum_{k \le x} r(k) \log \frac{x}{k}.$$

15.159. The arithmetic function $r(n)$ from Problem 15.158 is multiplicative. Also: $r(n) \ge 0$ for all $n \in \mathbb{Z}^+$, and $r(n) \ge 1$ if n is a square.

15.160. $R(x) > x^{1/2}$ for all large x.

15.161. $L(1, \chi) \ne 0$.

This proof that $L(1, \chi) \ne 0$ is a modern variant, due to Naoki Yanagisawa, of a classical argument of Franz Mertens.

Ingenuity

15.162. (Powell, Israel) Let $m, n \in \mathbb{Z}^+$, with $m > 1$. Assume that $(m, n) \ne (2, 1)$. Then $m^p - n$ is composite for infinitely many primes p.

Note. It is an open problem to prove the same assertion when $m = 2$ and $n = 1$.

15.163. Show that the difference

$$\#\{p \le x : p \equiv 1 \pmod 4\} - \#\{p \le x : p \equiv 3 \pmod 4\}$$

is not a bounded function of x.