DIRICHLET'S THEOREM ON PRIMES IN ARITHMETIC PROGRESSIONS

PETE L. CLARK

1. Statement of Dirichlet's theorem

The aim of this section is to give a complete proof of the following result:

Theorem 1. *(Dirichlet, 1837) Let $a, N \in \mathbb{Z}^+$ be such that $\gcd(a, N) = 1$. Then there are infinitely many prime numbers p such that $p \equiv a \pmod{N}$.*

We remark that the proof gives more, that the set of primes $p \equiv a \pmod{N}$ is **substantial** in the sense of [Handout 12].[1]

One of the amazing things about the proof of Dirichlet's theorem is how modern it feels. It is literally amazing to compare the scope of the proof to the arguments we used to prove some of the other theorems in the course, which historically came much later. Dirichlet's theorem comes 60 years before Minkowksi's work on the geometry of numbers and 99 years before the Chevalley-Warning theorem!

Let us be honest that the proof of Dirichlet's theorem is of a difficulty beyond that of anything else we have attempted in this course. On the algebraic side, it requires the theory of characters on the finite abelian groups $U(N) = (\mathbb{Z}/N\mathbb{Z})^\times$. From the perspective of the 21st century mathematics undergraduate with a background in abstract algebra, these are not particularly deep waters. More serious demands come from the analytic side: the main strategy is, as in Euler's proof of the infinitude of primes, to consider the function

$$P_a(s) = \sum_{p \equiv a \pmod{N}} \frac{1}{p^s},$$

which is defined say for real numbers $s > 1$, and to show that $\lim_{s \to 1^+} P_a(s) = +\infty$. Of course this suffices, because a divergent series must have infinitely many terms! The function $P_a(s)$ will in turn be related to a finite linear combination of logarithms of Dirichlet L-series, and the differing behavior of the Dirichlet series for principal and non-principal characters is a key aspect of the proof. Indeed, the fuel for the entire proof is the following surprisingly deep fact:

Theorem 2. *(Dirichlet's Nonvanishing Theorem) For any non-principal Dirichlet character χ of period N, we have $L(\chi, 1) \neq 0$.*

There are many possible routes to Theorem 2. We have chosen (following Serre) to present a proof which exploits the theory of Dirichlet series which we have developed in the previous handout in loving detail. As in our treatment of Dirichlet

[1] In fact, with relatively little additional work, one can show that the primes are, in a certain precise sense, equidistributed among the $\varphi(N)$ possible congruence classes.

series, we do find it convenient to draw upon a small amount of complex function theory. These result are summarized in Appendix C, which may be most useful for a reader who has not yet been exposed to complex analysis but has a good command of the theory of sequences and series of real functions.

I hope that readers who are unable or unwilling to check carefully through all the analytic details of the proof will still gain an appreciation for the sometimes difficult but also quite beautiful ideas which are on display here. It may be appropriate for me to end this introduction with a personal statement. I believe that I first encountered the proof of Dirichlet's theorem during a reading course in (mostly analytic) number theory that I took as an undergraduate with Professor R. Narasimhan, but in truth I have little memory of it. For my entire graduate career I neglected analysis in general and analytic number theory in particular, to the extent that I came to regard the study of conditionally convergent series as a sort of idle amusement. As a postdoc in Montréal I found myself in an environment where analytic and algebraic number theory were regarded with roughly equal importance (and better yet, often practiced simultaneously). Eventually the limitations of my overly algebraic bias became clear to me, and since my arrival at UGA I have made some progress working my way back towards a more balanced perspective.

Dirichlet's theorem points the way towards modern analytic number theory more than any other single result (even more than the Prime Number Theorem, in my opinion, whose analytic proof is harder but less immediately enlightening). Thus I came to the desire to dicsuss the proof of Dirichlet's theorem in the course (which was not done the first time I taught it).

The proof that I am about to present is not substantively different from what can be found in many other texts (and especially, to the proof given in [2]). Nevertheless, in order to both follow every detail of the proof and also to get a sense of what was going on in the proof as a whole took me dozens of hours of work, much more so than any other topic in this course. But to finally be able to present the proof feels wonderful, like coming home again. So although I have done what I can to present this material as transparently as possible, not only will I be sympathetic if you find parts of it confusing the first time around, I will even be a little jealous if you don't! But do try to enjoy the ride.

2. The main part of the proof of Dirichlet's theorem

2.1. **Prelude on complex logarithms.**

We begin rather inauspiciously by discussing logarithms. By a complex logarithm, we mean a holomorphic function $L(z)$ such that $e^{L(z)} = z$. As compared to the usual real logarithm, there are two subtleties. First, there are multiple such functions: since $e^{z+2\pi in} = e^z$ for all z, if $L(z)$ is any complex logarithm, so is $L(z)+2\pi in$ for any integer n. More seriously, no complex logarithm can be defined on the entire complex plane. Clearly we cannot have a logarithm defined at 0, since 0 is not in the image of the complex exponential function. In complex analysis one learns that if one removes from the complex line any ray passing through the origin – the real interval $(-\infty, 0]$ being the most standard choice – then one can define a complex logarithm on this restricted domain. In particular, given any open disk in the complex plane which does not contain the origin, there is a complex logarithm

defined on that disk.

For the moment though, let us proceed exactly as in calculus: we define a function $\log(1-z)$ for $|z|<1$ by the following convergent Taylor series expansion:

$$\log(1-z) = -\sum_{n=1}^{\infty} \frac{z^n}{n}. \tag{1}$$

In our analysis, we will come to a point where we have an analytic function, say $f(z)$, and we will want initially want to interpret $\log f(z)$ in a rather formal way, i.e., simply as the series expansion

$$\log(1-(1-f(z))) = \sum_{n=1}^{\infty} \frac{(1-f(z))^n}{n}.$$

It will be clear for our particular $f(z)$ that the series converges to an analytic function, say g, of z. The subtle point is whether g really is a logarithm of f in the above sense, i.e., whether and for which values of z we have $e^{g(z)} = f(z)$. Our expository choice here is to state carefully the claims we are making about logarithms during the course of the proof and then come back to explain them at the end. Readers with less familiarity with complex analysis may skip these final justifications without fear of losing any essential part of the argument.

2.2. **The proof.** To begin the proof proper, we let $X(N)$ denote the group of Dirichlet characters modulo N. Fix a with $\gcd(a,N)=1$ as in the statement of Dirichlet's theorem.

Write $\mathcal{P}_a$ for the set of prime numbers $p \equiv a \pmod N$, so our task is of course to show that $\mathcal{P}_a$ is infinite. For this we consider the function

$$P_a(s) := \sum_{p \in \mathcal{P}_a} \frac{1}{p^s},$$

defined for s with $\Re(s) > 1$. Our goal is to show that $P_a(s)$ approaches infinity as s approaches 1. (It would be enough to show this for real σ – i.e., $\lim_{\sigma \to 1^+} P_a(\sigma) = \infty$ – but nevertheless for the proof it is useful to consider complex s.)

Remark: Notice that this gives more than just the infinitude of $\mathcal{P}_a$: it shows that it is "substantial" in the sense of Handout X.X.

The overarching idea of the proof is to express $P_a(s)$ in terms of some Dirichlet L-series for characters $\chi \in X(N)$, and thus to reduce the unboundedness of $P_a(s)$ as $s \to 1$ from some corresponding analytic properties of L-series near $s=1$.

Why should $P_a(s)$ have anything to do with Dirichlet L-series? First, define $\mathbf{1}_a$ be the characteristic function of the congruence class $a \pmod N$: i.e., $\mathbf{1}_a(n)$ is 1 if $n \equiv a \pmod N$ and is 0 otherwise. Then $P_a(s)$ is reminiscent of the Dirichlet series for the arithmetical function $\mathbf{1}_a$, except it is a sum only over primes. Note that since $\mathbf{1}_a$ is not a multiplicative function, it would be unfruitful to consider its Dirichlet series $D(\mathbf{1}_a, s)$ – it does not have an Euler product expansion. Nevertheless $\mathbf{1}_a$ has some character-like properties: it is N-periodic and it is 0 when $\gcd(n,N) > 1$. Therefore $\mathbf{1}_a$ is entirely determined by the corresponding function

$U(N) \to C$, $n \pmod N \mapsto \mathbf{1}_a(n)$.

Now recall from [Handout A2.5, §4.3] that any function $f : U(N) \to \mathbb{C}^\times$ can be uniquely expressed as a $\mathbb{C}$-linear combination of characters; [Ibid, Corollary 18] even gives an explicit formula.

With all this in mind, it is easy to discover the following result (which we may as well prove directly):

Lemma 3. *For all $n \in \mathbb{Z}$, we have*

$$\mathbf{1}_a(n) = \sum_{\chi \in X(N)} \frac{\chi(a)^{-1}}{\varphi(N)} \chi(n).$$

Proof: By the complete multiplicativity of the χ's, the right hand side equals

$$\frac{1}{\varphi(N)} \left(\sum_{\chi \in X(N)} \chi(a^{-1}n) \right),$$

and now by orthogonality the parenthesized sum evaluates to $\varphi(N)$ if $a^{-1}n \equiv 1 \pmod N$ – i.e., if $n \equiv a \pmod N$ – and 0 otherwise. The result follows.

The corresponding identity for $P_a(s)$ is:

$$P_a(s) = \sum_{\chi \in X(N)} \frac{\chi(a)^{-1}}{\varphi(N)} \sum_p \frac{\chi(p)}{p^s}. \tag{2}$$

The terms $\sum_p \frac{\chi(p)}{p^s}$ are clearly reminiscent of Dirichlet L-series. Starting with

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

and "taking logarithms" we get

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

Expanding out this logarithm using the series (1) as advertised above, we get

$$\log(L(\chi, s)) = \sum_p \sum_n (\frac{\chi(p)}{p^s})^n / n. \tag{3}$$

But we regard the above as just being "motivational"; let us now be a little more precise. The right hand side of (3) is absolutely convergent for $\Re(s) > 1$ and uniformly convergent on closed half-planes $\Re(s) \geq 1 + \delta$. So if we simply *define*

$$\ell(\chi, s) := \sum_p \sum_n \left(\frac{\chi(p)}{p^s}\right)^n / n,$$

then, whatever else it may be, $\ell(\chi, s)$ is an analytic function on the half-plane $\Re(s) > 1$. Of course we know what the "whatever else" should be:

First Claim on Logarithms: In the halfplane $\Re(s) > 1$, we have $e^{\ell(\chi,s)} = L(\chi, s)$.

As stated above, we postpone justification of this claim until the next section.

Notice that the $n = 1$ contribution to $\ell(\chi, s)$ alone gives precisely the sums appearing in (2); there are also all the $n \geq 2$ terms, which we don't want. So let's separate out these two parts of the series: defininin

$$\ell_1(\chi, s) = \sum_p \frac{\chi(p)}{p^s}$$

and

$$R(\chi, s) = \sum_{n \geq 2} \sum_p \frac{\chi(p)^n}{np^{ns}},$$

we have

$$\ell(\chi, s) = \ell_1(\chi, s) + R(\chi, s)$$

and also

$$P_a(s) = \sum_{\chi \in X(N)} \frac{\chi(a^{-1})}{\varphi(N)} \ell_1(\chi, s).$$

But recall what we're trying to show: that $P_a(s)$ is unbounded as $s \to 1$. If we're trying to show that something is bounded, any terms which *do* remain bounded as $s \to 1$ can be ignored. But

$$|R(\chi, 1)| \leq \sum_{n \geq 2} \sum_p \frac{1}{np^n} \leq \sum_p \sum_{n \geq 2} \left(\frac{1}{p}\right)^n$$

$$= \sum_p \frac{1}{p^2} \frac{p}{p-1} \leq \sum_p \frac{1}{p^2} \cdot 2 \leq 2 \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty.$$

So $R(\chi, s)$ is absolutely convergent at $s = 1$ hence remains bounded as $s \to 1$, and thus we can safely ignore the terms $R(\chi, s)$. The following notation expresses this:

$$P_a(s) = \sum_{\chi \in X(N)} \frac{\chi(a)^{-1}}{\varphi(N)} \ell(\chi, s) + O(1);$$

here the "$O(1)$" denotes anything which is uniformly bounded as $s \to 1$. Separating the term corresponding to the principal character ξ_N from the other terms, we get

$$P_a(s) = \frac{1}{\varphi(N)} \sum_{p \nmid N} p^{-s} + \sum_{\chi \neq \xi_N} \ell(\chi, s) + O(1).$$

Now $\sum_{p \nmid N} p^{-s}$, is up to a finite number of terms, just the sum $\sum_p p^{-s}$. We know well that $\sum_p p^{-1} = \infty$, and by the Positivity Lemma this implies $\lim_{s \to 1^+} \sum_p p^{-s} = +\infty$. So the first term is unbounded near infinity. Therefore it would suffice to show that for each *nontrivial* character χ, $\ell(\chi, s)$ is bounded as $s \to 1$.

Recall that for every nonprincipal χ we know that the Dirichlet series for $L(\chi, s)$ is convergent on all of $\Re(s) > 0$; in particular, $L(\chi, s)$ is a well-defined analytic function at $s = 1$. Finally, we see the relevance of Theorem 2: if we know that for each nonprincipal $\chi \in X(N)$, $L(\chi, 1) \neq 0$, then

$$L(\chi, 1) = \lim_{s \to 1} L(\chi, s) = \lim_{s \to 1} e^{\ell(\chi, s)}.$$

Second claim on logarithms: Therefore $\ell(\chi, s)$ is bounded as $s \to 1$.

Now, modulo these two claims and the proof of Theorem 2 we're done: since the contribution to $P_a(s)$ from the nonprincipal Dirichlet L-series remains bounded as $s \to 1$ whereas the contribution from the principal Dirichlet L-series does not, it follows that $P_a(s)$ itself is unbounded as s approaches 1: more precisely, as s approaches 1 through real values of $s > 1$, we get

$$\lim_{s \to 1^+} P_a(s) = \sum_{p \equiv a \pmod N} \frac{1}{p^{-s}} = +\infty,$$

hence there must be infinitely many primes $p \equiv a \pmod N$.

2.3. **Tidying up the logarithms.**

Let us now deal with our two claims on logarithms. For the first one, we know from calculus that for a real number s with $|s| < 1$, the Taylor series expansion

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

is valid: in other words, we do have the identity

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

for all such s. By the principle of analytic continuation, the corresponding complex power series gives a well-defined logarithm whenever it is defined, which is at least for complex s with $|s| < 1$. We have

$$\lim_{\Re(s) \to +\infty} L(\chi, s) = 1,$$

so that there exists a σ_0 such that $\Re(s) > \sigma_0$ implies $|1 - L(\chi, s)| < 1$. Thus in this halfplane we do have $e^{\ell(\chi,s)} = L(\chi, s)$. By the principle of analytic continuation, this identity will continue to hold so long as both sides are well-defined analytic functions, which is the case for all $\Re(s) > 1$, justifying the first claim on logarithms.

Similar reasoning establishes the second claim: since $L(\chi, s)$ is analytic and nonzero at $s = 1$, there exists some small open disk about $L(\chi, 1)$ which does not contain the origin, and therefore we can choose a branch of the logarithm such that $\log L(\chi, s)$ is well-defined on the preimage of that disk, so in particular on some small open disk D about $s = 1$. Then $\log L(\chi, 1)$ is a well-defined complex number. It may not be equal to our $\ell(\chi, 1)$, but since any two logarithms of the same analytic function differ by a constant integer multiple of $2\pi i$, by the principle of analytic continuation there exists some $n \in \mathbb{Z}$ such that $\ell(\chi, s) - 2\pi n = \log(\chi, s)$ on the disk D, and no matter what n is, this means that $\ell(\chi, s)$ remains bounded as $s \to 1$.

3. Nonvanishing of $L(\chi, 1)$

We claim that $L(\chi, 1) \neq 0$ for all nonprincipal characters $\chi \in X(N)$. Our argument is as follows: consider the behavior of the Dedekind zeta function

$$\zeta_N(s) = \prod_{\chi \in X(N)} L(\chi, s).$$

near $s = 1$. We know that for each nonprincipal χ, $L(\chi, s)$ is holomorphic at $s = 1$, whereas for principal χ we get essentially the Riemann zeta function, which we have seen has a simple pole at $s = 1$: we have seen that

$$(s-1)\zeta(s) \to 1$$

as $s \to 1$. It follows from basic function theory that $\zeta_N(s)$ has at most a simple pole at $s = 1$, and indeed has a pole iff $L(\chi, 1) \neq 0$ for all nontrivial χ. Thus our goal is to show that the Dedekind zeta function $\zeta_N(s)$ has a singularity at $s = 1$.

The key is that the Dirichlet series $\zeta_N(s)$ has a very particular form. To see this, we need just a little notation: for a prime p not dividing N, let $f(p)$ denote the order of p in the unit group $U(N)$, and put $g(p) = \frac{\varphi(N)}{f(p)}$, which is by Lagrange's theorem a positive integer. Now:

Proposition 4. *a) We have*

$$\zeta_N(s) = \prod_{p \nmid N} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}}.$$

b) Therefore $\zeta_N(s)$ is a Dirichlet series with non-negative integral coefficients, converging absolutely in the half-plane $\Re(s) > 1$.

Proof: Let $\mu_{f(p)}$ be the group of $f(p)$th roots of unity. Then for all $p \nmid N$ we have the polynomial identity

$$\prod_{w \in \mu_{f(p)}} (1 - wT) = 1 - T^{f(p)}.$$

Indeed, both sides have the $f(p)$th roots of unity as roots (with multiplicity one), so they differ at most by a multiplicative constant; but both sides evaluate to 1 at $T = 0$. Now by the Character Extension Lemma [Lemma 13, Handout A2.5], for all $w \in \mu_{f(p)}$ there are precisely $g(p)$ elements $\chi \in X(N)$ such that $\chi(p) = w$. This establishes part a), and part b) follows from the explicit formula of part a).

Now for a *deus ex machina*. We are given that $\zeta_N(s)$ is a Dirichlet series with non-negative real coefficients. Therefore we can apply Landau's Theorem: if σ is the abscissca of convergence of the Dirichlet series, then the function $\zeta_N(s)$ has a singulariety at σ. Clearly $\sigma \geq 1$, so, contrapositively, if $\zeta_N(s)$ does not have a singularity at $s = 1$, then not only does $\zeta_N(s)$ extend analytically to some larger halfplane $\Re(s) > 1-\epsilon$, but it extends until it meets a singularity on the real line. But we have already seen that each Dirichlet L-series is holomorphic for $0 < \Re(s) < 1$, so Landau's theorem tells us that $\sigma \leq 0$.

If you think about it for a minute, it is exceedingly unlikely that a Dirichlet series with non-negative integral coefficients has absissca of convergence $\sigma \leq 0$, and in our case it is quite straightforward to see that this is not the case: take s to be in the real interval $(0, 1)$. Expanding out the pth Euler factor we get

$$\frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}} = \left(1 + \frac{1}{p^{f(p)s}} + \frac{1}{p^{2f(p)s}} + \dots\right).$$

Ignoring all the crossterms gives a crude upper bound: this quantity is at least

$$1 + \frac{1}{p^{\varphi(N)s}} + \frac{1}{p^{2\varphi(N)s}} + \ldots.$$

Multiplying this over all p, it follows that

$$\zeta_N(s) \geq \sum_{n \mid (n,N)=1} \frac{1}{n^{\varphi(N)s}}.$$

When we evaluate at $s = \frac{1}{\varphi(N)}$ we get

$$\sum_{(n,N)=1} \frac{1}{n}.$$

Since the set of integers prime to N has positive density, it is substantial. More concretely, since every n of the form $Nk+1$ is coprime to N, this last sum is at least as large as

$$\sum_{k=1}^{\infty} \frac{1}{Nk+1} = \infty.$$

QED!

References

[1] Apostol, Tom M. Introduction to analytic number theory. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Serre, J.-P. A course in arithmetic. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.