18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
Primes in arithmetic progressions

In this unit, we first prove Dirichlet's theorem on primes in arithmetic progressions. We then prove the prime number theorem in arithmetic progressions, modulo some exercises.

1 Dirichlet's theorem

For short, I will say an arithmetic progression is *eligible* if it has the form $m, m+N, m+2N, \dots$ where $\gcd(m, N) = 1$; it is equivalent to ask that any two consecutive terms are relatively prime.

Theorem 1 (Dirichlet)**.** *Any eligible arithmetic progression of positive integers contains infinitely many primes.*

There are a few special cases where one can prove this directly, but otherwise algebraic methods cannot touch this problem. Dirichlet's idea was to prove, in some appropriate quantitative sense, that the primes distribute themselves equally among the eligible arithmetic progressions with a particular difference; this goes back to Euler's proof of the infinitude of primes using the Riemann zeta function.

2 Asymptotic density and Dirichlet density

In order to speak quantitatively about the distribution of certain types of primes, or integers in general, we need some sort of measure theory on the set of primes or the set of integers. Note that Lebesgue-type measure theory is not an option for countable sets: we can only hope to make finitely additive measures.

For $S \subseteq T$ two sets of positive integers, with T infinite, the *upper natural density* and *lower natural density* of S in T are defined as

$$\limsup_{N \to \infty} \frac{\#\{n \in S : n \leq N\}}{\#\{n \in T : n \leq N\}}, \qquad \liminf_{N \to \infty} \frac{\#\{n \in S : n \leq N\}}{\#\{n \in T : n \leq N\}}.$$

Of course the upper density is never less than the lower density. If they coincide, we call the common value the *natural density* (or *asymptotic density*) of S in T.

Many interesting sets fail to have a natural density (e.g., see exercises). We get a less restrictive notion of density by using Dirichlet series.

For $S \subseteq T$ two sets of positive integers, with $\sum_{n \in T} n^{-1}$ divergent, the *upper Dirichlet density* and *lower Dirichlet density* of S in T are defined as

$$\limsup_{s \to 1^+} \frac{\sum_{n \in S} n^{-s}}{\sum_{n \in T} n^{-s}}, \qquad \liminf_{s \to 1^+} \frac{\sum_{n \in S} n^{-s}}{\sum_{n \in T} n^{-s}}.$$

If they coincide, we call the common value the *Dirichlet density* of S in T.

Let us make this explicit in two cases of interest. Recall that $\zeta(s)$ has a simple pole of residue 1 at $s = 1$, so as $s \to 1^+$,

$$(s-1)\sum_{n=1}^{\infty} n^{-s} = 1 + o(1).$$

Hence if $T = \mathbb{N}$, then the Dirichlet density of S is given by

$$\lim_{s \to 1^+} (s-1) \sum_{n \in S} n^{-s}$$

if the limit exists.

Taking logarithms, we see that as $s \to 1^+$,

$$\log \zeta(s) + \log(s-1) = \log(s-1) + \sum_p \sum_{n=1}^{\infty} p^{-ns} = O(1).$$

Moreover, $\sum_p \sum_{n=2}^{\infty} p^{-ns} = O(1)$, so

$$\sum_p p^{-s} = -\log(s-1) + O(1).$$

Hence if T is the set of primes, then the Dirichlet density of S is given by

$$\lim_{s \to 1^+} \frac{\sum_{p \in S} p^{-s}}{-\log(s-1)}$$

if the limit exists.

Here are some easy facts about density. (If I don't specify natural vs. Dirichlet, I mean that the statement holds if you make a choice and use it consistently throughout the statement.)

- Any finite set has density 0 in any infinite set.
- Density is a finitely additive measure: if $S_1, \dots, S_m$ are disjoint subsets of T with densities $\delta_1, \dots, \delta_m$ in T, then their union has density $\delta_1 + \cdots + \delta_m$ in T. Corollary: two subsets of T whose combined density exceeds 1 must have infinite intersection.
- If S has density δ in $\mathbb{N}$, then for any positive integer n, $nS = \{ns : s \in S\}$ has density δ/n.

I can't help mentioning a fun example of the additivity of densities. Let α, β be positive irrational numbers with $1/\alpha + 1/\beta = 1$. Put

$$S_\alpha = \{\lfloor n\alpha \rfloor : n \in \mathbb{N}\}$$
$$S_\beta = \{\lfloor n\beta \rfloor : n \in \mathbb{N}\}.$$

Then S_α, S_β have natural densities $1/\alpha, 1/\beta$. The fact that these add up to 1 is explained by the beautiful result (Beatty's theorem) that S_α, S_β are disjoint and their union is $\mathbb{N}$! (If you've never seen this before, I recommend this as an amusing exercise.)

Lemma 2. *Let $S \subseteq T$ be subsets of $\mathbb{N}$ such that S has natural density δ in T. Then S also has Dirichlet density δ in T.*

Proof. See exercises. (The converse is false; also see exercises.) □

To prove Theorem 1, we will prove the following.

Theorem 3. *For any positive integers m, N with $\gcd(m, N) = 1$, the set of primes congruent to m modulo N has Dirichlet density $1/\phi(N)$ in the set of all primes (hence is infinite).*

3 L-functions and discrete Fourier analysis

For χ a Dirichlet character of level N, we can write

$$\log L(s, \chi) = \sum_p \sum_{n=1}^{\infty} \chi(p^n) p^{-ns}$$

for $\mathrm{Re}(s) > 1$; as $s \to 1^+$, we have

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

For χ nonprincipal, we know that $L(s, \chi)$ is holomorphic and nonvanishing at $s = 1$, so

$$\sum_p \chi(p) p^{-s} = O(1),$$

whereas for χ_0 the principal conductor of level N, we saw above that

$$\sum_p \chi_0(p) p^{-s} = -\log(s-1) + O(1).$$

At this point it may be clear how to proceed: form a certain linear combination of the $\log L(s, \chi)$ to isolate $\sum_{p \equiv m\,(N)} p^{-s}$, and compare the asymptotic contributions of $-\log(s-1)$.

The fact that we can do this amounts to what is sometimes called *discrete Fourier analysis*; if you prefer, it is the representation theory of the finite abelian group $(\mathbb{Z}/N\mathbb{Z})^*$.

Theorem 4 (Discrete abelian Fourier analysis)**.** *Let G be a finite abelian group, and let $\hat{G}$ be the* character group *(or* dual group*) of G, i.e., the group of homomorphisms $G \to \mathbb{C}^*$.*

(a) The order of $\hat{G}$ is equal to the order of G.

(b) (Orthogonality of characters) If $\chi_1, \chi_2 \in \hat{G}$, then

$$\sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \begin{cases} |G| & \chi_1 = \chi_2 \\ 0 & \chi_1 \neq \chi_2. \end{cases}$$

(c) If $g_1, g_2 \in G$, then

$$\sum_{\chi \in \hat{G}} \chi(g_1)\overline{\chi(g_2)} = \begin{cases} |G| & g_1 = g_2 \\ 0 & g_1 \neq g_2. \end{cases}$$

Proof. (a) If $G = G_1 \times G_2$, then clearly $\hat{G} = \hat{G}_1 \times \hat{G}_2$. Since every finite abelian group G is a product of cyclic groups, we may reduce to the case where G is cyclic, and then the result is clear. (For $G = (\mathbb{Z}/N\mathbb{Z})^*$, we can make this more explicit: we can use the Chinese remainder theorem to split N into distinct prime-power factors, then use the fact that $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic unless $p = 2$, in which case it is $\{\pm 1\}$ times a cyclic group.)

(b) We saw this argument once before, but here it goes again: the left side is invariant under multiplication by $\chi_1(h)\overline{\chi_2(h)}$ for any $h \in G$, because there is no difference between summing over g or over gh. If $\chi_1 \neq \chi_2$, then we can make that multiplier different from 1 by choosing suitable h. So the sum vanishes if $\chi_1 \neq \chi_2$. If $\chi_1 = \chi_2$, each summand is equal to 1 because characters of finite groups takes values which are roots of unity.

(c) See exercises.

□

So now it is clear what to do: given a choice of m coprime to N, taking sums of χ over all Dirichlet characters of level N, we obtain

$$\begin{aligned} \frac{1}{\phi(N)} \sum_{\chi} \overline{\chi(m)} \log L(s, \chi) &= \frac{1}{\phi(N)} \sum_{\chi} \sum_{p} \chi(p)\overline{\chi(m)} p^{-s} + O(1) \\ &= \sum_{p \equiv m\,(N)} p^{-s} + O(1) \end{aligned}$$

as $s \to 1^+$. On the other hand,

$$\begin{aligned} \frac{1}{\phi(N)} \sum_{\chi} \overline{\chi(m)} \log L(s, \chi) &= \frac{1}{\phi(N)} \log L(s, \chi_0) + \frac{1}{\phi(N)} \sum_{\chi \neq \chi_0} \overline{\chi(m)} \log L(s, \chi) \\ &= -\frac{1}{\phi(N)} \log(s-1) + O(1). \end{aligned}$$

This yields Theorem 3.

4 The prime number theorem in arithmetic progressions

The proof of Dirichlet's theorem only uses information about the behavior of the $L(s, \chi)$ near $s = 1$. Using the fact that $L(s, \chi) \neq 0$ on the entire line $\mathrm{Re}(s) = 1$, we can prove a much stronger result.

Theorem 5 (Prime number theorem in arithmetic progressions)**.** *For m, N positive integers with* $\gcd(m, N)$*, the set of primes congruent to m modulo N has* natural *density* $1/\phi(N)$*. In other words, the number of primes $p \leq x$ with $p \equiv m \pmod{N}$ is asymptotic to $\frac{1}{\phi(N)} \frac{x}{\log x}$ as $x \to \infty$.*

Proof. Given what we now know, this is a straightforward adaptation of our proof of the prime number theorem. For χ a Dirichlet character of level N, define

$$\vartheta_\chi(x) = \sum_{p \leq x} \chi(p) \log p.$$

Given a choice of m coprime to N, put

$$\begin{aligned} \vartheta_m(x) &= \frac{1}{\phi(N)} \sum_\chi \overline{\chi(m)} \vartheta_\chi(x) \\ &= \sum_{p \leq x : p \equiv m \, (N)} \log p. \end{aligned}$$

As in the proof of the prime number theorem, if we prove that the improper integral

$$\int_1^\infty \frac{\phi(N)\vartheta_m(x) - x}{x^2}\, dx$$

converges, we may then deduce that $\vartheta_m(x) \sim \frac{1}{\phi(N)} x$ as desired.

It suffices in turn to check that for χ principal,

$$\int_1^\infty \frac{\vartheta_\chi(x) - x}{x^2}\, dx$$

converges, and for χ nonprincipal,

$$\int_1^\infty \frac{\vartheta_\chi(x)}{x^2}\, dx$$

converges. The former is an immediate consequence of the corresponding fact for ϑ (which we proved in the unit on the prime number theorem), since ϑ and ϑ_χ differ in only finitely many terms. For the latter, see exercises. □

As with the proof of the prime number theorem, we get very little information about the error term, i.e., the difference between the actual number of primes $p \leq x$ with $p \equiv m \pmod{N}$ and the asympotic count $\frac{1}{\phi(N)} \frac{x}{\log x}$. That becomes a problem if, for instance, we want to know how long it takes to find *one* prime in an arithmetic progression. To address this, we must first get better results on zero-free regions for the $L(s, \chi)$, then make a better analytic argument to take advantage of the improved analytic information. We turn to this in the next few lectures.

Exercises

1. Prove Lemma 2. (Hint: use partial summation.)

2. Let S be the set of positive integers which have first digit 1 when written in base 10.

   (a) Compute the upper and lower natural density of S, and verify that S does not have a natural density.

   (b) Prove that S has a natural Dirichlet density, and compute it.

   Optional (not to be turned in): generalize to an arbitrary base $b \geq 3$. Even more optional: prove the analogous result for the set of primes with first digit 1 in base b.

3. Prove that there exists a constant c such that

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + c + o(1).$$

   (Hint: you established asymptotics for $\sum_{p \leq x} \frac{\log p}{p}$ on a previous homework. Apply partial summation.)

4. (a result of Mertens; tricky, optional) In the previous exercise, prove that

$$c = \gamma + \sum_{p} \left(\log(1 - p^{-1}) + p^{-1} \right),$$

   where γ is Euler's constant. Then deduce that

$$\prod_{p \leq x} (1 - p^{-1}) \sim \frac{e^{-\gamma}}{\log x}.$$

5. Deduce point (c) of Theorem 4 from points (a) and (b). (Hint: form the matrix A with rows indexed by $g \in G$, columns indexed by $\chi \in \hat{G}$, and entries $\chi(g)$. Then compare AA^* with A^*A, where $*$ denotes conjugate transpose. Or if you prefer, prove that the dual of $\hat{G}$ is canonically isomorphic to G.)

6. Prove that $\int_1^\infty \frac{\vartheta_\chi(t)}{t^2}\, dt$ converges for χ nonprincipal, by applying the Tauberian theorem from the unit on the prime number theorem. (Hint: use the fact that $L(s, \chi) \neq 0$ for $\mathrm{Re}(s) \geq 1$ to argue that $-L'(s, \chi)/L(s, \chi)$ is holomorphic in a neighborhood of $\mathrm{Re}(s) \geq 1$. There will be an extra term to deal with, just as there was a term I neglected in the original notes from the prime number theorem unit; see the corrected notes online.)