Dirichlet's theorem on primes in arithmetic progressions

December 20, 2013

The next thing we were going to do was to analyze the Dedekind zeta function $\zeta_F(s)$ as $s \to 1^+$. But that's kind of a long story, and I don't think it makes sense to start it in a small lecture right before the break. So instead let's do something fun, and use the Dirichlet L-series we've been studying to prove Dirichlet's theorem (1837):

Theorem 0.1. *Let $m \in \mathbb{N}$, and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then there are infinitely many primes p such that p is congruent to a (mod m).*

The argument is based on Euler's analytic argument for the infinitude of primes, so let me start by recalling that. The rough idea is that there is an implication:

$$\sum_{n \leq N} \frac{1}{n} \sim log(N) \Rightarrow \sum_{p \leq N} \frac{1}{p} \sim log(log(N)),$$

as a consequence of the Euler product expansion of $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$, or in other words as a consequence of unique prime factorization. Here n runs over natural numbers, but p runs over primes. And of course, if $\sum_{p \leq N} \frac{1}{p}$ grows like $log(log(N))$, then the set of primes is certainly infinite (even though $log(log(N))$ grows *reeeallly* slowly, it does tend to ∞!).

Now let's give the argument. We won't exactly establish that $\sum_{p \leq N} \frac{1}{p} \sim log(log(N))$, though that could be done if we were to take a little more care. Instead we'll just show that, as $s \to 1^+$, the sum

$$\sum_p \frac{1}{p^s}$$

tends to ∞. This also clearly implies that there are infinitely many primes.

Here is the argument. Start with the Euler product expansion

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

for real $s > 1$. Now take log. This gives

$$log(\zeta(s)) = \sum_p (p^{-s} + \frac{1}{2}p^{-2s} + \frac{1}{3}p^{-3s} + \ldots).$$

Now consider what happens when $s \to 1^+$. On the left, since $\zeta(s) = \sum_n 1/n^s$, we get something comparable to log of the harmonic series $\sum_{n=1}^{\infty} 1/n$. This diverges, so we get that the left-hand side tends to ∞. (To make a rigorous argument, compare $\zeta(s)$ with the integral $\int_1^\infty x^{-s} dx$.)

On the right, we exactly want to see that just the sum of the first terms p^{-s} tends to ∞ as $s \to 1^+$. Given that we know this for the left-hand side, it suffices to see that the remaining terms stay bounded as $s \to 1^+$, i.e. that

$$\sum_p (\frac{1}{2}p^{-2s} + \frac{1}{3}p^{-3s} + \ldots)$$

is bounded as $s \to 1^+$. But in fact I claim it's bounded by $2\zeta(2)$. Indeed, we can certainly remove the $\frac{1}{2}$, $\frac{1}{3}$, etc., coefficients for the purposes of bounding the sum. Then consider the even terms. These give

$$\sum_p (p^{-2s} + p^{-4s} + \ldots).$$

But in totality all these terms are just a subset of the terms defining the sum of $\zeta(2)$: they are the subset corresponding to the prime powers among all natural numbers. So this sum is bounded by $\zeta(2)$. On the other hand, the odd terms are clearly less than the even terms. So in total we do get the claimed bound, and that finishes Euler's proof.

Now let's give Dirichlet's proof. Similarly, we will show that

$$\sum_{p \equiv a(m)} \frac{1}{p^s}$$

tends to ∞ as $s \to 1^+$. To prove this, let's make a similar study of $log(L(s,\chi))$ as $s \to 1^+$, where $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ is an arbitrary character (i.e. homomorphism). Again from the Euler expansion, we see

$$log(L(s,\chi)) = \sum_p (\chi(p)p^{-s} + \frac{1}{2}\chi(p^2)p^{-2s} + \ldots + \frac{1}{3}\chi(p^3)p^{-3s} + \ldots).$$

Now let us use the symbol "$\simeq$" to mean that the difference between the quantities is bounded in absolute value as $s \to 1^+$. Then just as above, we can neglect the degree ≥ 2 terms on the right hand side, and we find

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

This is the basic estimate, which will let us use knowledge of the L-series to conclude information about primes.

To go further with it, we note that the characters χ provide a basis for the set of functions $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$, just as in the previous lecture the p^{th} roots of unity (= characters of $\mathbb{Z}/p\mathbb{Z}$) formed a basis of the set of functions $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$. Thus, if $f : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$ is any function, we can write

$$f(k) = \sum_\chi f_\chi \cdot \chi(k)$$

for some complex numbers f_χ. Thus we deduce

$$\sum_{p \nmid m} \frac{f(p)}{p^s} \simeq \sum_\chi f_\chi \cdot log(L(s,\chi)).$$

Now let's look at the right-hand side, and input our knowledge of $L(s,\chi)$. When $\chi = 1$, then $L(s,\chi)$ is just $\zeta(s)$ again, except that it's missing the (finitely many) Euler factors at primes dividing m. It follows that $log(L(s,1)) \simeq log(\zeta(s))$. On the other hand, when $\chi \neq 1$, we know that $L(s,\chi)$ converges to a continuous function in a neighborhood of $s = 1$, and we've asserted that

$$L(1,\chi) \neq 0.$$

Thus $log(L(s,\chi))$ is bounded as $s \to 1^+$, i.e. $log(L(s,\chi)) \simeq 0$. Putting this back in to the above formula, we deduce that only the trivial character contributes, and so

$$\sum_{p \nmid m} \frac{f(p)}{p^s} \simeq f_1 \cdot log(\zeta(s)).$$

We've already analyzed $log(\zeta(s))$ as $s \to 1^+$: it goes to ∞. So we deduce the following: if the coefficient f_1 is nonzero, then $\sum_{p \nmid m} \frac{f(p)}{p^s}$ tends to ∞ as $s \to 1^+$; but if $f_1 = 0$ then instead the sum is bounded as $s \to 1^+$.

Thus, to prove Dirichlet's theorem, it suffices to see that when we write the "indicator function" for a (i.e. the function $k \mapsto c_a(k)$ which outputs 1 when $k \equiv a \pmod m$ and 0 otherwise) as a linear combination of the characters $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$, then the coefficient of the trivial character is nontrivial. But there's the explicit formula

$$c_a(k) = \frac{1}{\varphi(m)} \sum_\chi \overline{\chi(a)} \cdot \chi(k),$$

which again follows from the fact that the sum of the f^{th} roots of unity is 0 when $f > 1$. So the coefficient of the trivial character is $\frac{\overline{\chi_{triv}(1)}}{\varphi(m)} = \frac{1}{\varphi(m)}$, and the proof is complete.

We remark that more analytic input (a "Tauberian theorem", plus the fact that $L(s,\chi) \neq 0$ even for $Re(s) = 1$) can be used to show the stronger claim that the "natural density" of the set of primes $\equiv a \pmod m$ is this coefficient $\frac{1}{\varphi(m)}$. In other words, in the limit, the primes are equally distributed among all the possible residue classes (mod m). By "natural density" we mean the limit, as $N \to \infty$, of the ratio of the number of primes $\equiv a \pmod m$ which are $\leq N$ to the total number of all primes $\leq N$.

Now, a crucial input to the above proof was the fact that $L(1,\chi) \neq 0$ for $\chi \neq 1$. This was how we knew that $log(L(s,\chi))$ stays bounded as $s \to 1^+$. If it had gone to infinity, then by a fluke of signs it could have canceled the infinity coming from $log(\zeta(s))$, and we might not know anything about the sum we cared about.

In the last lecture I mentioned that this fact $L(1,\chi) \neq 0$ can be deduced from our product formula

$$\zeta_{\mathbb{Q}(\zeta_p)} = \zeta(s) \cdot \prod_{\chi \neq 1} L(s,\chi).$$

(Provided we generalize from primes p to arbitrary natural numbers m; but this requires no new ideas, only more complicated notation. So we'll stick with the prime case.) Namely, it follows from the fact

(which we'll prove later) that $\zeta_F(s)$ for any number field F has a meromorphic continuation to a neighborhood of $s = 1$, with its only pole being a simple pole at $s = 1$. Recall the argument: if any of the $L(1, \chi)$ were equal to 0, then that zero would cancel the pole of $\zeta(s) = \zeta_{\mathbb{Q}}(s)$, leaving no pole for $\zeta_{\mathbb{Q}(\zeta_p)}(s)$, which is a contradiction.

But I learned from Serre's book *A Course in Arithmetic* that one can actually show that $L(1, \chi) \neq 0$ without such a detailed study of $\zeta_F(s)$, if one is willing to input the following analytic theorem:

Theorem 0.2. *Let*

$$F(s) = \sum_{n=1}^{\infty} a_n \cdot n^{-s}$$

be a Dirichlet series with nonnegative real coefficients $a_n \geq 0$. Suppose that $F(s)$ converges in some right half-plane $Re(s) > \alpha$. Let $\alpha' < \alpha$. Then if $F(s)$ extends to a holomorphic function in $Re(s) > \alpha'$, the defining series must also converge for $Re(s) > \alpha'$.

In other words, convergence of the series "further to the left" can only be obstructed by a singularity of the function (and actually, there's also a further statement to the effect that such a singularity must be present on the real axis). This is similar to the usual story of convergence of power series in complex analysis. But here we need the requirement $a_n \geq 0$.

We can apply this to $F(s) = \zeta_{\mathbb{Q}(\zeta_p)}(s)$. We know this has non-negative coefficients, since the coefficients just count the number of ideals of $\mathbb{Z}[\zeta_p]$ of a given norm. We also know it converges for $Re(s) > 1$, since it's a product of Dirichlet series which we know converge for $Re(s) > 1$.

Now, I claim that $\zeta(s) - \frac{1}{s-1}$ extends to a holomorphic function in $Re(s) > 0$. You can prove this by comparing the sum defining $\zeta(s)$ with the integral $\int x^{-s}$. We also know that the $L(s, \chi)$ extend to homolorphic functions in $Re(s) > 0$. Thus, if any $L(1, \chi)$ were to be zero, we'd cancel the $\frac{1}{s-1}$, and so the product, i.e. $\zeta_{\mathbb{Q}(\zeta_p)}(s)$, would be holomorphic in $Re(s) > 0$. Thus, by the above theorem, the series defining $\zeta_{\mathbb{Q}(\zeta_p)}(s)$ would converge for $Re(s) > 0$.

But it's pretty easy to see that this can't be the case. The series defining $\zeta_F(s)$, for a general number field F, is

$$\sum_{I \neq 0} \frac{1}{N(I)^s}.$$

But just look at the principal ideals. Heck, even just look at the principal ideals (n), where n is a natural number. These have norm n^d, where $d = [F : \mathbb{Q}]$ (since $\mathcal{O}_F \simeq \mathbb{Z}^d$.) Thus this sum is bigger than

$$\sum_{n \geq 1} \frac{1}{n^{ds}} = \zeta(ds).$$

But we know this sum doesn't converge when $ds \leq 1$, by comparison with the integral. Thus we have a contradiction when $0 < s \leq 1/d$.