DIRICHLET'S THEOREM ON PRIMES IN PROGRESSIONS, I

K. Soundararajan

Over the next several lectures we shall develop a proof of Dirichlet's famous theorem on primes in arithmetic progressions.

Dirichlet's theorem. *If $(a,q)=1$ then there are infinitely many primes p with $p\equiv a \pmod q$.*

We now describe Dirichlet's proof in the case that $q=4$. Although in this case we may find elementary proofs, along the lines of Euclid's argument, the proof we now describe is the one that generalizes to other moduli. Dirichlet's proof builds on the ideas behind Euler's proof of the infinitude of primes (which in fact shows that $\sum_p 1/p$ diverges). Let us now recall Euler's proof.

For a real number $s>1$ we considered there the Riemann zeta-function

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\Big(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots\Big)=\prod_p\Big(1-\frac{1}{p^s}\Big)^{-1}. \tag{1}$$

Note that in the domain $s>1$ the sum and the product converge. It may be helpful for you to recall that the convergence of a product

$$\prod_n (1+a_n)$$

is equivalent to the convergence of $\sum_n a_n$; to see this note that $\log(1+a_n)$ is approximately a_n if a_n is small. Euler's proof is then to note that if there are only finitely many primes then the RHS of (1) must be bounded as $s\to 1^+$. On the other hand we may see that the LHS of (1) must be unbounded as $s\to 1^+$ by appealing to the divergence of the harmonic series. Let's make this last observation a little more precise.

Lemma 1. *For real numbers $s>1$ we have*

$$\frac{1}{s-1}<\zeta(s)<\frac{1}{s-1}+1.$$

Proof. If f is a monotone decreasing function on $\mathbb{R}^+$ then note that

$$\int_n^{n+1} f(t)dt\le f(n)\le\int_{n-1}^{n} f(t)dt.$$

Typeset by $\mathcal{AMS}$-TeX

Therefore

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \ge \sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{t^s} dt = \int_1^{\infty} \frac{dt}{t^s} = \frac{1}{s-1},$$

and also

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \sum_{n=2}^{\infty} \frac{1}{n^s} \le 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dt}{t^s} = 1 + \int_1^{\infty} \frac{dt}{t^s} = 1 + \frac{1}{s-1}.$$

This proves our Lemma.

For future use, we introduce now the O (Big Oh) notation. We say that a function $f(x)$ is $O(g(x))$ as $x \to a$ if there is a constant C such that as $x \to a$ (that is in some small neighborhood of a) we have $|f(x)| \le Cg(x)$. Sometimes the condition $x \to a$ will be clear from the context, in which case we'll omit it and simply say $f(x) = O(g(x))$. Examples: as $x \to \infty$ we have $\sin x = O(1)$, $x^{100} = O(2^x)$ (why?), $\log x = O(x^{0.01})$ etc. As another example, we could rewrite Lemma 1 as

$$\zeta(s) = \frac{1}{s-1} + O(1),$$

as $s \to 1^+$; the above statement means that there is some constant C such that as $s \to 1^+$ we have $|\zeta(s) - 1/(s-1)| \le C$, and Lemma 1 tells us that in fact we could choose $C = 1$. Here's a final important example on using O-notation. I claim that for small values of x (e.g. $|x| \le 1/2$) we have

$$\log(1+x) = x + O(x^2).$$

To see this we may use the Taylor series for $\log(1+x)$ getting

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots ,$$

so that for $|x| \le 1/2$

$$|\log(1+x) - x| \le \frac{x^2}{2} + \frac{|x|^3}{3} + \dots \le \frac{x^2}{2}\Big(1 + |x| + |x|^2 + \dots\Big) \le x^2$$

which justifies our claim.

Returning to primes, we see from (1) that

$$\log \zeta(s) = \sum_p \log\Big(1 - \frac{1}{p^s}\Big)^{-1},$$

and using our approximation $\log(1+x) = x + O(x^2)$ (so that $-\log(1-x) = x + O(x^2)$ also), we have

$$\log \zeta(s) = \sum_p \Big(\frac{1}{p^s} + O\Big(\frac{1}{p^{2s}}\Big)\Big). \tag{2}$$

Now for $s > 1$ we have that

$$\sum_p \frac{1}{p^{2s}} \leq \sum_p \frac{1}{p^2} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} = O(1),$$

and so (2) gives that for $s > 1$

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + O(1). \tag{3}$$

Now we use Lemma 1 and see that the LHS of (3) is

$$\log \zeta(s) = \log\Big(\frac{1}{s-1} + O(1)\Big) = \Big(\log \frac{1}{s-1}\Big) + O(1),$$

as $s \to 1^+$; make sure you understand the last step, it's simple but will help you getting familiar with the O-notation. We conclude as follows:

Corollary 2. *As $s \to 1^+$ we have*

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

In particular, $\sum_p 1/p$ diverges and there are infinitely many primes.

With this in the background, let us proceed to Dirichlet's theorem in the case $q = 4$. Here we construct a cousin of the Riemann zeta-function namely

$$L(s, \chi_{-4}) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \ldots = \sum_{n=1}^{\infty} \frac{\chi_{-4}(n)}{n^s},$$

where

$$\chi_{-4}(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ 0 & \text{if } n \equiv 0, 2 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Note that this series converges (absolutely) in $s > 1$, and by the alternating series test, it converges (conditionally) in $s > 0$. Moreover, just like ζ it can be written as a product over primes (such products are called *Euler products*)

$$L(s, \chi_{-4}) = \prod_p \Big(1 + \frac{\chi_{-4}(p)}{p^s} + \frac{\chi_{-4}(p^2)}{p^{2s}} + \ldots\Big) = \prod_p \Big(1 - \frac{\chi_{-4}(p)}{p^s}\Big)^{-1}.$$

Notice that the key property responsible for the Euler product is that the χ_{-4} is *multiplicative*: $\chi_{-4}(mn) = \chi_{-4}(m)\chi_{-4}(n)$ for all m, and n, which reduces the determination of χ_{-4} to its behavior on primes. Taking logarithms we find that for $s > 1$

$$\begin{aligned} \log L(s, \chi_{-4}) &= \sum_p -\log\Big(1 - \frac{\chi_{-4}(p)}{p^s}\Big) = \sum_p \Big(\frac{\chi_{-4}(p)}{p^s} + O\Big(\frac{1}{p^{2s}}\Big)\Big) \\ &= \sum_p \frac{\chi_{-4}(p)}{p^s} + O(1), \end{aligned} \tag{4}$$

arguing exactly as in (2) and (3).

What does all this have to do with primes $\pmod 4$? Note that $\chi_{-4}(p) = 1$ if $p \equiv 1 \pmod 4$, and $\chi_{-4}(p) = -1$ if $p \equiv 3 \pmod 4$. Therefore, adding the equations (3) and (4) we find that

$$\log \zeta(s) + \log L(s, \chi_{-4}) = 2 \sum_{\substack{p \\ p\equiv 1 \pmod 4}} \frac{1}{p^s} + O(1), \tag{5,}$$

and subtracting (4) from (3) we have

$$\log \zeta(s) - \log L(s, \chi_{-4}) = 2 \sum_{\substack{p \\ p\equiv 3 \pmod 4}} \frac{1}{p^s} + O(1). \tag{6}$$

Now consider (5) as $s \to 1^+$. We already know that $\log \zeta(s) = \log(1/(s-1)) + O(1) \to \infty$. If we knew that $\log L(s, \chi_{-4})$ does not go to $-\infty$ as $s \to 1^+$ we would be able to conclude that there are infinitely many primes that are $1 \pmod 4$, and indeed that the sum of their reciprocals diverges. Similarly if we consider (6) as $s \to 1^+$ then we find that so long as $\log L(s, \chi_{-4})$ does not go to $+\infty$ we would be able to conclude that there are infinitely many primes $\equiv 3 \pmod{}$.

Thus we have boiled our problem down to determining the limiting behavior of $L(s, \chi_{-4})$ as $s \to 1^+$. But as $s \to 1^+$ we see that

$$L(s, \chi_{-4}) \to 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = L(1, \chi_{-4})$$

We already noted that by the alternating series test the series above converges, and so $L(s, \chi_{-4})$ certainly stays bounded as $s \to 1^+$. This shows that there are infinitely many primes $\equiv 3 \pmod 4$. It remains lastly to explain why $L(s, \chi_{-4})$ doesn't go to zero as $s \to 1^+$ (and so $\log L(s, \chi_{-4})$ doesn't go to $-\infty$). There are two ways in which we can see this: First

$$L(1, \chi_{-4}) = \Big(1 - \frac{1}{3}) + \Big(\frac{1}{5} - \frac{1}{7}\Big) + \ldots$$

is evidently positive. Second we may note that $L(1, \chi_{-4}) = \pi/4$ (known to Gregory and Leibniz) which follows from

$$L(1, \chi_{-4}) = \int_0^1 (1 - t^2 + t^4 - t^6 + \ldots)dt = \int_0^1 \frac{dt}{1+t^2} = \tan^{-1}(t)\Big|_0^1 = \frac{\pi}{4}.$$

We have established Dirichlet's theorem in the case $q = 4$!

Corollary 3. *There are infinitely many primes $p \equiv 1 \pmod 4$, and infinitely many primes $p \equiv 3 \pmod 4$. Moreover, as $s \to 1^+$,*

$$\sum_{\substack{p \\ p\equiv 1 \pmod 4}} \frac{1}{p^s} = \frac{1}{2} \log \frac{1}{s-1} + O(1),$$

and

$$\sum_{\substack{p \\ p\equiv 3 \pmod 4}} \frac{1}{p^s} = \frac{1}{2} \log \frac{1}{s-1} + O(1).$$