Dirichlet's Theorem on Arithmetic Progressions

Bobby Shen, Shend Zhjeqi

June 6, 2021

Theorem: For any two positive relatively prime integers a and d. the arithmetic progression $a, a+d, a+2d, \ldots$ contains infinitely many prime numbers.

For example, let $d = 5$. All primes except 5 are either 1, 2, 3, or 4 mod 5, so Dirichlet's theorem states that each of these four residues occurs infinitely often. Stronger forms of Dirichlet's theorem state that the each of the four residues occurs equally often. This statement takes work to define precisely. For example, perhaps primes up to a bound of $N = 10000$ are 10 percent from being evenly distributed, and as N goes to infinity, they are arbitrarily close to evenly distributed.

We will sketch an outline of an argument for Dirichlet's theorem. The argument here might take a lot of work to make completely rigorous, which is not our focus. We will focus on small values of d but formulate the argument to work for all d with enough work.

An advanced reference for this handout is still this, by Dr. Sutherland. `https://math.mit.edu/classes/18.785/2015fa/LectureNotes17.pdf` .

First, we will start with a famous identity known as the Euler product.

1 Euler product

Here is the simplest case of the Euler product. s is any real number greater than 1. Define functions $\zeta(s)$ and $P(s)$ as follows.

$$\zeta(s) = \sum_{k=1}^{\infty} k^{-s} = 1^{-s} + 2^{-s} + 3^{-s} + \cdots$$

$$P(s) = \prod_{\text{p prime}} \frac{1}{1-p^{-s}} = \left(\frac{1}{1-2^{-s}}\right)\left(\frac{1}{1-3^{-s}}\right)\left(\frac{1}{1-5^{-s}}\right)\left(\frac{1}{1-7^{-s}}\right)\cdots$$

The Euler product "theorem" states that $\zeta(s) = P(s)$. $\zeta(s)$ in fact coincides with the Riemann Zeta function, but we will not use any facts about this function. Note that the sum diverges for $s = 1$, and along similar lines, one can prove that $\zeta(s)$ diverges to $+\infty$ as s approaches 1 from the right, which we will not do. However, for each real number $s > 1$, the sum converges and the product also converges.

Review: What is an infinite product? Wikipedia: Infinite product

Lemma 1. Prove that $\zeta(s) = P(s)$ for $s > 1$

For our approach, here are the major steps. Fix $s > 1$.

- prove that the sum $\zeta(s)$ converges
- Each factor of $P(s)$ is of the form $1/(1-x)$. Expand this as the infinite geometric series $1 + x + x^2 + \cdots$. Thus each factor becomes an infinite sum
- Consider partial products of $P(s)$ given by the smallest n primes. This is the product of a finite number of infinite sums, which is unsurprisingly an infinite sum. The infinite sum looks like "Sum over $k \in \mathbb{Z}+$ whose maximal prime factor is less than the nth prime."

- Expand $\zeta(s)$ minus the nth partial product into an infinite sum, denote this $R(n,s)$
- Prove that $R(n,s)$ converges to 0 as $n \to \infty$ for each fixed s.

There is a terse proof at `https://mathworld.wolfram.com/EulerProduct.html` which emphasizes the intuitive nature by expanding geometric series. In my opinion, this argument from Wolfram is missing some details but it certainly gives the main ideas.

Let us take the natural logarithm of the Euler product.

$$\log \zeta(s) = \log P(s) = \log \prod_{\text{p prime}} \frac{1}{1-p^{-s}} = \sum_{\text{p prime}} (-1)\log(1-p^{-s}).[1]$$

Here, we use the fact that logarithms of partial products equal partial sums of logarithms, and that $\log(1/x) = -\log(x)$. Next, we note the approximation $\log(1-t) \approx -t$. How accurate is this approximation? Well, if throughout this handout $s \geq 1$ and $p > 2$, then $p^{-s} \leq 1/2$. Thus, the value of t would be a positive number at most $1/2$ everywhere.

It turns out that I want to bound the difference $\log(1-t)+t$ by a "global constant" times t^2 which must be valid for all complex numbers t with absolute value $\leq 1/2$.

Lemma 2. There exists a global constant $C > 0$ such that for all complex numbers t with $abs(t) \leq 1/2$,

$$abs(\log(1-t)+t) < C\,abs(t)^2,$$

and $C = 1$ is a valid constant. Note that as t approaches 0, the error approaches 0 quadratically.

Exercise: Would $C = 1$ work for all $abs(t) \leq 3/4$ instead?

Proof: This needs some facts which are slightly out of scope of this handout. We need that $\log(1-t)$ is pointwise equal to the Taylor series $-t - t^2/2 - t^3/3 - \cdots$ for all t with $|t| < 1$, so certainly for $|t| \leq 1/2$. Then we have the bound.

$$abs\left(\frac{\log(1-t)+t}{t^2}\right) = abs\left(-1/2 - t/3 - t^2/4 - t^3/5\cdots\right) \leq \left(1/2 + t/3 + t^2/4 + t^3/5\right)|_{t=1/2} = 0.7725\ldots < 1.$$

Thus, in the infinite sum labeled [l], we can apply this approximation to each term of the sum, which yields the sum $\sum_{\text{p prime}} p^{-s}$. The absolute difference between these two infinite sums is bounded as follows.

$$\begin{aligned} abs\left(\log P(s) - \sum_{\text{p prime}} p^{-s}\right) &\leq \sum_{\text{p prime}} abs(-\log(1-p^{-s}) - p^{-s}) \\ &< \sum_{\text{p prime}} C\,(p^{-s})^2 \\ &< \sum_{p=2}^{\infty} 1 \cdot p^{-2} \\ &< 1, \end{aligned}$$

where we plugged in $C = 2$, then used $s > 1$ to bound a sum above, then used that the sum of $1/n^2$ equals $\pi^2/6 < 2$. There are some details about infinite sums that are omitted but are straightforward. Note that the final bound, $abs\left(\log P(s) - \sum_{\text{p prime}} p^{-s}\right) < 1$, is true for all $s > 1$.

Since $P(s)$ diverges to $+\infty$ as s approaches 1, so does $\log P(s)$ and so does $\sum_{\text{p prime}} p^{-s}$. Then informally, the sum $\sum_{\text{p prime}} p^{-1}$ must diverge.

2 Euler products with characters

The focus of this section is replacing $P(s)$ with $P(s, \chi)$, where χ is a Dirichlet character. We will use this definition.

Definition 3. χ is a Dirichlet character if χ has a modulus m which is an integer ≥ 2 and the following conditions hold.

- χ is a function from U_m to complex numbers, where U_m is the group of relatively prime residues mod m.
- χ does not map any element to 0
- For any x, y in U_m, $\chi(xy) = \chi(x)\chi(y)$, where xy is multiplication in U_m.

Moreover, stretching notation a little bit, we will also extend χ to a function from positive integers to complex numbers as follows

- If x is in U_m, then $\chi(x)$ remains the same
- If $0 \leq x < m$ amd $\gcd(x, m) > 1$, then $\chi(x)$ is defined to be 0.
- If $x \geq m$, then $\chi(x)$ is defined to be χ(x mod m).

Here is our definition of Euler products with respect to Dirichlet characters.

Definition 4.

$$\zeta(s, \chi) = \sum_{k \in \mathbb{Z}+} \chi(k) k^{-s}.$$

$$P(s, \chi) = \prod_{\text{p prime}} \frac{1}{1 - \chi(p)p^{-s}}.$$

Note: Ideally the exposition should start with trying to informally expand the infinite product $P(s, \chi)$ and trying to figure out what the result of the infinite product is.

Let us discuss these definitions for the following two characters, both of modulus 4, called χ_0 and χ_1. χ_0 is the trivial character, with $\chi_0(1) = \chi_0(3) = 1$. χ_1 is the other character, with $\chi_0(1) = 1.\chi_0(3) = -1$.

χ_0 over the integers is a function that maps odd numbers to 1 and even numbers to 0. Thus $\zeta(s, \chi_0)$ is like $\zeta(s)$ except the former skips terms for all even k. $\chi_0(p)$ equals 1 for all primes except 2. Thus $P(s, \chi_0)$ is like $P(s)$ except the former skips exactly the first factor.

Next, $\zeta(s, \chi_1)$ looks like $\zeta(s, \chi_0)$ except in the former sum, terms for k with $k \equiv 3 \pmod 4$ have coefficient -1. Terms with $k \equiv 1 \pmod 4$ still have coefficient $+1$. Terms with even k are still omitted (or have coefficient 0). $P(s, \chi_1)$ is trickier. It is like $P(s, \chi_0)$ except the former modifies all terms $1/(1 - p^{-s})$ to $1/(1 + p^{-s})$ for exactly the primes which are $3 \pmod 4$.

You may except that $\zeta(s, \chi) = P(s, \chi)$ for either character! Why is this? Here is an argument that lacks some details but is the general idea.

- Partial products of $P(s, \chi)$ have the form $\sum_{k \in \mathbb{Z}+} k^{-s} a(k)$, where $a(k)$ is some coefficient function.
- As we build up partial products by including more and more primes (in increasing order), $a(k)$ jumps to a single value, after which it remains. For example, $a(11 * 9 * 7 * 5 * 3 * 1)$ would start out as zero then jump to a certain value as soon as we include the partial product for $p = 11$, then it would remain
- By notions of absolute convergence, we can prove that the infinite product equals $\sum_{k \in \mathbb{Z}+} k^{-s} A(k)$ where $A(k)$ is the final stable value for each k. $A(k)$ is a simpler function!
- $A(k)$ is determined by the prime factors of k. Precisely speaking (although I recommend finding an intuitive explanation for yourself), let k be the product of prime powers in the set S. $A(k)$ equals the product of A over the set S. By the nature of expanding the geometric series $1/(1 - \chi(p)p^{-s})$, the coefficient of p^r equals $\chi(p)^r$, which equals $\chi(p^r)$ by the character axioms. Thus $A(x)$ equals the product of χ over the set S, which equals $\chi(x)$ again by the character axioms.

- Based on the very regular structure of χ, $A(k)$ in fact equals $\chi(k)$

Having argued that $\zeta(s,\chi) = P(s,\chi)$, let us again take the natural logarithm

$$\log P(s,\chi) = \log \prod_{\text{p prime}} \frac{1}{1-\chi(p)p^{-s}} = \sum_{\text{p prime}} (-1)\log(1-\chi(p)p^{-s}).$$

Since $\chi(p)$ has absolute value exactly 1 or 0, and $s > 1$, we have $abs(\chi(p)p^{-s}) \leq 1/2$, and we can apply the bounding lemma to get the following.

$$\begin{aligned} abs\left(\log P(s,\chi) - \sum_{\text{p prime}} \chi(p)p^{-s}\right) &\leq \sum_{\text{p prime}} abs(-\log(1-\chi(p)p^{-s}) - \chi(p)p^{-s}) \\ &< \sum_{\text{p prime}} C\,(\chi(p)p^{-s})^2 \\ &< \sum_{p=2}^{\infty} 1 \cdot p^{-2} \\ &< 1. \end{aligned}$$

$$abs\left(\log P(s,\chi) - \sum_{\text{p prime}} \chi(p)p^{-s}\right) < 1.$$

3 Final algebraic steps

We are close to Dirichlet's Theorem! We need to have a few clever ideas to isolate primes which are, say, $j \pmod m$ where j is relatively prime to m. Fix j and m. The "divine idea" is to consider the function

$$f(s) := \sum_{\text{p prime}} I(p \equiv j \pmod m)p^{-s},$$

as s ranges over real numbers > 1 and I is the indicator function which is 1 if true else 0.

Using fundamental results about Dirichlet characters, the function $I(p \equiv j \pmod m)$, interpreted as a function over U_m, is a linear combination of all the unique Dirichlet characters on U_m, of which there are $\varphi(m)$ of them, and in this linear combination, all coefficients are nonzero. Let $M = \varphi(m)$ and enumerate these characters $\chi_0, \chi_1, \ldots, \chi_{M-1}$, where χ_0 is the trivial character. Then

$$I(* \equiv j \pmod m) = \sum_{k=0}^{M-1} z_k \chi_k(*)$$

as functions over U_m, where z_k are some nonzero complex coefficients.

We then turn this into an identity on $f(s)$.

$$
\begin{aligned}
f(s) &= \sum_{\text{p prime}} I(p \equiv j \pmod m) p^{-s} \\
&= \sum_{\text{p prime}} \left(\sum_{k=0}^{M-1} z_k \chi_k(p) p^{-s} \right) \\
&= \sum_{k=0}^{M-1} z_k \left(\sum_{\text{p prime}} \chi_k(p) p^{-s} \right) \\
&= \sum_{k=0}^{M-1} z_k \left(\log P(s, \chi_k) + (\text{error\_k, abs} < 1) \right) \\
&= \sum_{k=0}^{M-1} z_k \left(\log \zeta(s, \chi_k) + (\text{error\_k, abs} < 1) \right).
\end{aligned}
$$

In one step, we changed the order of summation of a tricky double sum, one of which was an infinite summation. Next, we make some statements about $\log \zeta(s, \chi_k)$ as $s \to 1^+$.

Lemma 5. Let $\chi_0, \ldots, \chi_{M-1}$ be all unique characters over U_m. Then $\zeta(s, \chi_0)$ diverges to $+\infty$ as $s \to 1^+$. For $k \neq 0$, $\zeta(s, \chi_k)$ has a finite limit as $s \to 1^+$.

This lemma can be proven with standard methods about real sequences. Informally, the idea is that the harmonic series diverges, but the alternating harmonic series converges. The previous lemma mostly follows from the next lemma and additional facts about Dirichlet characters which was that $\sum_{x \in U_m} \chi_k(x) = \varphi(m) I(k = 0)$, e.g. the sum of function values of a Dirichlet character is nonzero for χ_0 and exactly 0 for $\chi_k (k \neq 0)$. Some details are omitted.

Lemma 6. Let $m > 1$ be an integer and $a : \mathbb{Z}_+ \to \mathbb{C}$ be a function with period m. Define $S(a) := a(1) + \cdots + a(m)$. Define the function $g(s)$ for reals $s \geq 1$ as

$$
g(s) = \sum_{k \in \mathbb{Z}+} a(k) k^{-s}.
$$

- The sum for $g(s = 1)$ would diverge if $S(a) \neq 0$ and converge if $S(a) = 0$.
- The sum always converges if $s > 1$.
- For a fixed function a with $S(a) = 0$, we have the limit $\lim_{s \to 1^+} g(s) = g(1)$.
- For a fixed function a with $S(a) \neq 0$, the limit $\lim_{s \to 1^+} g(s)$ diverges.

Going back to our expansion of $f(s)$,

$$
\begin{aligned}
f(s) &= \sum_{k=0}^{M-1} z_k \left(\log \zeta(s, \chi_k) + (\text{error\_k, abs} < 1) \right) \\
&= z_0 \left(\log \zeta(s, \chi_0) + (\text{error\_0, abs} < 1) \right) + \sum_{k=1}^{M-1} z_k \left(\log \zeta(s, \chi_k) + (\text{error\_k, abs} < 1) \right) \\
&= z_0 \left(\log \zeta(s, \chi_0) + (\text{error\_0, abs} < 1) \right) + (\text{bounded near s=1}).
\end{aligned}
$$

The sum $f(1)$ (if we had defined it), would be $\sum_{\text{p prime, j mod m}} p^{-1}$. This is a sum of positive numbers so it must either converge or diverge to $+\infty$. If it converged, then $f(s)$ would be a decreasing function of s (increasing as

$s \to 1+$) which is bounded. This would imply that $\log \zeta(s, \chi_0)$ is bounded, and therefore that $\zeta(s, \chi_0)$ is bounded. This contradicts what we know, that $\zeta(s, \chi_0)$ diverges to $+\infty$. Therefore, the sum for $f(1)$ diverges to $+\infty$. It follows that there are infinitely many primes $j \pmod k$, or else $f(1)$ would be a finite sum.

Moreover, in some precise way which I did not make fully precise, $f(1)$ $\sum_{\text{p prime, j mod m}} p^{-1}$. diverges at a very similar rate to the similar sum for all other relatively prime residues mod k, e.g. $f_j(s)$ over the $\phi(m)$ relatively prime residues have bounded difference and diverge to $+\infty$ as $s \to 1^+$.