DIRICHLET PRIME NUMBER THEOREM

JING MIAO

Abstract. In number theory, the prime number theory describes the asymptotic distribution of prime numbers. We all know that there are infinitely many primes,but how are they distributed? Dirichlet's theorem states that for any two positive coprime integers a and d, there are infinitely many primes which are congruent to a modulo d. A stronger form of Dirichlet's theorem states that the sum of the reciprocals of the prime numbers with the same modulo diverges, and different progressions with the same modulus have approximately the same proportions of primes. We will walk through the proofs of Dirichlet's theorem, and introduce some related topics, such as the Riemann-zeta function and quadratic field.

Contents

1. Introduction: the Euclidean method

Many people know that there are infinitely many primes (Euclid's Theorem). The proof is easy. Suppose that there are only finitely many primes, say $p_1, ..., p_r$. Consider $N = p_1...p_r + 1$. Then N is a prime that is not included in $p_1...p_r$. Contradiction. Thus we prove Euclid's Theorem.

What if we want to know how many primes there are that are congruent to a modulo d (a,d are coprime)? In some cases, we can generalize the Euclidean proof to prove there are infinitely many such primes. We will show here for $d = 3$ and 4. Consider primes of the form $n + 2$. Assume $p_1...p_r$ are primes congruent to 2 modulo 3. Take $N = 3p_1...p_r - 1$. It is congruent to 2 modulo 3, so if it is not a prime, it must have a prime factor congruent to 2 modulo 3. Yet all such primes do not divide N. Contradiction. Thus, there are infinitely many primes of the form $3n + 2$. Similar method can be applied to the proof of primes of the form $4n + 3$. Let $N = 4p_1...p_r + 3$ where $p_1...p_r$ are primes of the form $4n + 3$. Then clearly N is congruent to 3 modulo 4. If N is not a prime, it must have a prime factor congruent

Date: October 1, 2013.

to 3 modulo 4. Contradiction. Therefore, there are infinitely many primes of the form $4n+3$. The case of primes of the form $4n+1$ is a little bit tricky, because a non-prime number that is congruent to 1 modulo 4 can have all prime factors not congruent to 1 module 4. In this case, we let $N = 4p_1^2...p_r^2 + 1$, and using the similar idea, we can prove by contradiction (For the proof, see appendix 1).

2. Riemann zeta function

However, not all cases can be shown in the Euclidean way. In this section, we will introduce Euler's proof of the infinitude of primes. First, let's learn the Riemann-zeta function that will be frequently used in our later proofs.

Definition 2.1. The Riemann zeta function $\zeta(s)$, is a function of a complex variable s that analytically continues the sum of the infinite series $\sum_{n=1}^{\infty} \frac{1}{n^s}$.

The summation converges when the real part of s is greater than 1. What happens when s is very close to 1? Note that $\zeta(1)$ is unbounded because we know that $\sum_{n=1}^{\infty} \frac{1}{n}$ does not have an upper bound. Also note that

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{r} 1 + p_i^{-1} + p_i^{-2} + ... = \prod_{i=1}^{r} \frac{1}{1 - p_i^{-1}}.$$

Since $\zeta(1)$ is unbounded, there are infinitely many primes. Otherwise, the right hand side will be finite. We can then simpify the Riemann zeta function into

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=p_1^t...p_r^t \in N} \frac{1}{(p_1^t...p_r^t)^s} \\ &= \prod_p (1 + \frac{1}{p^s} + \frac{1}{p^2 s} + ...) \\ &= \prod_p \frac{1}{1 - \frac{1}{p^s}},\end{aligned}$$

where p is indexed over all prime numbers.

Then we want to see what function $\zeta(s)$ converges to. Since

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

we assume that $\zeta(s) = \frac{1}{s-1} + h(s)$, where the real part of s is greater than 1. The function $h(s)$ is a holomorphic function that is bounded. To prove this,

$$\begin{aligned} h(s) &= \zeta(s) - \frac{1}{s-1} \\ &= \sum_{n\in \mathrm{N}} \frac{1}{n^s} - \int_1^\infty \frac{1}{t^s}\, dt \\ &= \sum_{n\in \mathrm{N}} \int_n^{n+1} (\frac{1}{n^s} - \frac{1}{t^s})\, dt \\ &= \sum_{n\in \mathrm{N}} \int_0^1 (\frac{1}{n^s} - \frac{1}{(n+t)^s})\, dt. \end{aligned}$$

Denote $f_n(t) = \frac{1}{n^s} - \frac{1}{(n+t)^s}$, $f_n(0) = 0$, $f_n'(t) = \frac{s}{(n+t)^{s+1}}$. When $0 < t < 1$,

$$|f_n(t)| \leq \sup |f_n'(t)| \times 1 \leq |\frac{s}{n^{s+1}}|.$$

Thus, $h(s) \leq \sum_{n\in N} |\frac{s}{n^{s+1}}|$, which converges when the real part of s is greater than 0. Thus, $\log \zeta(s) \approx \log \frac{1}{s-1}$. On the other hand, we have

$$\begin{aligned} \log \zeta(s) &= \log \prod_p \frac{1}{1-p^{-s}} \\ &= -\sum_p \log(1-p^{-s}) \\ &= \sum_p (p^{-s} + 1/2p^{-2s} + 1/3p^{-3s} + ...). \end{aligned}$$

Note that when real part of s is greater than $1/2$,

$$|1/2p^{-2s} + 1/3p^{-3s} + ...| \leq |p^{-2s}||\frac{1}{1-p^{-s}}| \leq 2|p^{-2s}|.$$

Thus, $\sum_p (1/2p^{-2s} + 1/3p^{-3s} + ...)$ converges. Therefore, $\sum_p p^{-s} \approx \log \frac{1}{s-1}$.

3. Dirichlet characters

We showed in the previous section that $\sum_{p\text{prime}} \frac{1}{p^s} \approx ln\frac{1}{s-1}$. Now we want to show that for any $(a,b) = 1$, $\sum_{p\equiv a \mathrm{mod} b} \frac{1}{p^s} \approx \frac{1}{\phi(b)} ln\frac{1}{s-1}$ as s goes to 1, where $\phi(b)$ is the number of $a < b$, such that $(a,b) = 1$. The infinitude of primes of the form $a + bn$ follows from this. Thus, we want a nice way to write the characteristic function, such that

$$1(x) = \begin{cases} 1 & : n \equiv a \bmod b \\ 0 & : n \not\equiv a \bmod b. \end{cases}$$

Then $\sum_{p\equiv a \bmod b} \frac{1}{p^s} = \sum_p \frac{1(p)}{p^s}$. Such characteristic functions are called Dirichlet characters χ. There are two basic properties of Dirichlet characters: $\chi(1) = 1$; if $a \equiv b \bmod N$, then $\chi(a) = \chi(b)$.

Theorem 3.1. *If $(a, N) = 1$, then $a^{\phi(N)} \equiv 1$ mod N. This is called Euler's Thoerem.*

Thus, $\chi(a)$ is a $\phi(N)$-th root of unity.

Definition 3.2. A congruent class g mod N is called a primitive root mod N if for any $a \in Z$ and $(a, N) = 1$, $a \equiv g^k(\text{ mod } N)$ for some k.

The result is that there exists a unique k in the interval $0 \leq k \leq \phi(N) - 1$, such that $a \equiv g^k(\text{mod } N)$. We label such k: $k = \text{ind}_g a$ and call it the index of a to base $g \text{mod} N$. So $a \equiv g^{ind_g a}$.

Proposition 3.3. *Let g be a primitive root modulo N, and $(a, N) = (b, N) = 1$. Then*

$ind_g(ab) = ind_g a + ind_g b \ mod\ \phi(N)$,

$ind_g(a^k) = k ind_g a \ mod\ \phi(N)$,

If g' is another primitive root, then $ind_g a = ind_g g' \times ind_{g'} a \ mod\ \phi(N)$.

So for general natural number$N$, do primitive roots exist? The answer is that they do not always exist.

Theorem 3.4. *For only $N = 1, 2, 4, p^\alpha, 2p^\alpha$, where p is an odd prime and $\alpha \geq 1 \in N$,there exists a primitive root.*

Proof. It is easy to check that 1,2,4 have primitive roots. Then we shall prove that all odd primes have primitive roots. Let n be the least universal exponent for p, i.e. n is the smallest positive integer such that $x^n \equiv 1 \text{ mod } p$, for all non-zero $x \in 0, 1...p - 1$. Notice that there is some element $g \in 1, 2...p - 1$, such that $g^n \equiv 1$ but $g^m \not\equiv 1 \text{ mod } p$ for any $m < n$, i.e. the multiplicative order of g is precisely n. Also, notice that by Euler's theorem, $n \leq p - 1$.Now, notice that the polynomial $f(x) = x^n - 1$ has at most n roots over the field $\mathbb{Z}_p$.(The proof is in the appendix.) $f(x) \equiv 0 \text{ mod } p$ for all non-zero x mod p. Thus, $n \geq p - 1$. Hence, $n = p - 1$ and g is of exact order $p - 1$. Therefore, g is a primitive root. □

Next we shall show that numbers of the form of p^α have primitive roots. First, we shall show if a is a primitive root of p, then a is a primitive root of p^2. Let $n \equiv a \text{mod} p$. Then $n \equiv (a + kp) \text{mod} p$ for some $k < p$. By Euler's theorem, we know $(a + kp)^{p(p-1)} \equiv 1 \text{mod} p^2$. By contradiction, if a is not a primitive root, there exists some $f|p - 1$ such that $(a + kp)^{p(p-1)/f} \equiv 1 \text{mod} p^2$. Since $f|p - 1$, $p = tf + 1$ for some integer t.Then

$$\begin{aligned}(a + kp)^{p(p-1)/f} &= (a + kp)^{p-1)(t+1/f)} \\ &\equiv (i + kp)^{t+1/f} \\ &= (1 + kp)^t (1 + kp)^{1/f} \\ &\equiv (1 + mp) \cdot (b) \\ &\not\equiv 1 \text{ mod } p^2,\end{aligned}$$

where b is any number but not 1 that is congruent to p. This is a contradiction. Thus, a is a primitive root of p^2. Then we will prove if a is a primitive root of p^2, a is also a primitive root of p^α. Using similar method, we can prove that a is also a primitive root for p^α.

Next we will prove that if p^α has primitive root, then $2p^\alpha$ also has primitive root. If the primitive root a is an odd number, since p^α and $2p^\alpha$ have the same order, a

must also be a primitive root for $2p^\alpha$. If a is even, take $a' = a + p^\alpha$, a' is odd and $(a', 2p^\alpha) = 1$. Consider $(a + p^\alpha)^{\phi(2p^\alpha)/f}$, it is not congruent to 1 mod $2P^\alpha$.Thus, $2p^\alpha$ has primitive roots.

We also have to show that $2^n (n > 2)$ and any other composite numbers except the power of prime numbers do not have primitive. First, consider 2^n. For any odd number $2k+1$, $(2k+1)^{2^{n-2}} \equiv 1 \bmod 2^n$. So 2^n does not have primitive root. Then, consider composite number $N = p_1^{t_1}...p_r^{t_r}$. The order of N is the multiplication of the orders of $p_j^{t_j}$, which are all even number. So there is no primitive roots. Thus, we finish the proof of this theorem.

Now let's learn how to construct the Dirichlet characters. Let g be a primitive root of of p^α where p is odd. For any $(n, p) = 1$, we write $b(n) = \text{ind}_g n$. So $g \equiv g^{b(n)} \bmod p^\alpha$. For $h = 0, ..., \phi(p^\alpha) - 1$, define

$$\chi_h(n) = \begin{cases} e^{2\pi i h b(n)/\phi(p^\alpha)} & : (n, p^\alpha) = 1 \\ 0 & : (n, p^\alpha) \neq 1. \end{cases}$$

Examples 3.5. Take $p = 5, \alpha = 1, g = 3$. Thus, $b(1) = 4, b(2) = 3, b(3) = 1, b(4) = 2$.

Notice that if $(nm, p^\alpha) = 1$,

$$\chi_h(nm) = e^{\frac{2\pi i h b(nm)}{\phi(p^\alpha)}} = e^{\frac{2\pi i h (b(n)+b(m))}{\phi(p^\alpha}} = \chi_h(m)\chi_h(n).$$

As there are $\phi(p^\alpha)$ h's, there exist $\phi(p^\alpha)$ distinct Dirichlet characters. This construction also works for 2,4. However, there is no primitive root for modulo 2^n when $n \geq 3$. Similarly, for $N = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, there is no primitive root. If χ_i is a Dirichlet character modulo $p_i^{\alpha_i}$, then $\chi = \chi_1 \chi_2 ... \chi_r$. Since $\phi(p_i^{\alpha_i} p_j^{\alpha_j}) = \phi(p_i^{\alpha_i})\phi(p_j^{\alpha_j})$, we know that $\phi(N) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_r^{\alpha_r})$.

It is easy to check that if χ, ψ are Dirichelet characters, then $\phi \cdot \psi$ is also a Dirichlet character. This property is very useful. Now consider $\sum_{\chi \bmod N} \chi(x)$. If we multiply it with $\psi(x)$ for some $\psi(x) \neq 1$, we get

$$\psi(x) \sum_{\chi \bmod N} \chi(x) = \sum_{\chi \bmod N} \psi(x)\chi(x) = \sum_{\chi \bmod N} (\psi \cdot \chi)(x) = \sum_{\chi \bmod N} \chi(x),$$

$$(\psi(x) - 1) \sum_{\chi \bmod N} \chi(x) = 0,$$

$$\sum_{\chi \bmod N} \chi(x) = 0 \text{ if } x \not\equiv 1 \bmod N.$$

If $x \equiv 1 \bmod N$, then $\sum_{\chi \bmod N} \chi(x) = \phi(N)$. Thus,we have

$$\frac{1}{\phi(N)} \sum_{\chi} (x) = \begin{cases} 1 & : \chi \equiv 1 \bmod N \\ 0 & : \chi \not\equiv 1 \bmod N. \end{cases}$$

Thus, we have for $(a, b) = 1$,

$$\begin{aligned}\sum_{p\equiv a \bmod b} \frac{1}{p^s} &= \sum_{pa'\equiv 1 \bmod b} \frac{1}{p^s} \text{ where } aa' \equiv 1 \bmod b \\ &= \sum_p \frac{1}{p^s}(\frac{1}{\phi(b)} \sum_{\chi \bmod b} \chi(pa')) \\ &= \frac{1}{\phi(b)} \sum_{\chi \bmod b} (\chi(a') \sum_p \frac{\chi(p)}{p^s}).\end{aligned}$$

4. Dirichlet L function

In this section, we introduce the Dirichlet L function. We want to show that $L(s, \chi)$ is finite near $s = 1$, and also $L(1, \chi) \neq 0$.

Definition 4.1. A Dirichlet L-series is a function of the form $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, where χ is a Dirichlet character and s a complex variable with real part greater than 1.

Since we proved in the previous section that

$$\frac{1}{\phi(N)} \sum_{\chi}(x) = \begin{cases} 1 & : \chi \equiv 1 \bmod N \\ 0 & : \chi \not\equiv 1 \bmod N, \end{cases}$$

we can write $I(x) = \frac{1}{\phi(N)} \sum_{\chi} \chi(a')\chi(x)$, where $I(x)$ is the identity function, and $a' \in \mathbb{Z}_p$, such that $xa' \equiv 1 \bmod N$. Then let $x = ay$. If $a = 1$, then $a' = 1$. Thus $I_a(y) = \frac{1}{\phi(N)} \sum_{\chi} \chi(y)$, when $y \equiv 1 \bmod N$. Now,

$$\begin{aligned}\sum_{p\equiv a \bmod N} \frac{1}{p^s} &= \sum_p \frac{I_a(p)}{p^s} \\ &= \frac{1}{\phi(N)} \sum_{\chi} \chi(a') \sum_p \frac{\chi(p)}{p^s} \\ &= \frac{1}{\phi(N)} \sum_{p\nmid N} \frac{1}{p^s} + \frac{1}{\phi(N)} \sum_{\chi \text{ nontrivial}} \chi(a') \sum_p \frac{\chi(p)}{p^s}.\end{aligned}$$

The first term is the summation of the trivial character ($\chi(p) = 1$). This is the case when $h = 0$. And the second is the summation of non-trivial characters. We will show later that the contribution of the second term is finite, thus, implying that different progressions with the same modulo diverge, and different progressions with the same modulus have approximately the same proportions of primes. We will show that for each χ, $\sum_p \chi(p)/p^s$ is bounded as s goes to 1.

Since as s goes to 1, $\frac{1}{p^s}$ is unbounded, while $\frac{1}{p^2 s}$, $\frac{1}{p^3 s}$... are all bounded, we have

$$\begin{aligned}\sum_p \frac{\chi(p)}{p^s} &\approx \sum_p \frac{\chi(p)}{p^s} + \frac{1}{2}\sum_p \frac{\chi(p)}{p^{2s}} + \frac{1}{3}\sum_p \frac{\chi(p)}{p^{3s}} + ... \\ &= \sum_p -\log(1-\frac{\chi(p)}{p^s}) \\ &= \log\prod_p \frac{1}{1-\frac{\chi(p)}{p^s}} \\ &= \log\prod_p (1+\frac{\chi(p)}{p^s}+\frac{\chi(p^2)}{p^{2d}}+...) \\ &= \log\sum_n \frac{\chi(n)}{n^s} \text{ since } \chi(n)\cdot\chi(m)=\chi(nm).\end{aligned}$$

Notice that what is inside the ln is $L(s,\chi)$. We will show that $L(s,\chi)$ is finite and non-zero for $s>0$ when χ is non-trivial. Notice that
$\sum_{x\in\mathbb{Z}_N}\chi(x)=0$ when χ is non-trivial; $\sum_{x\in\mathbb{Z}_N}\chi(x)=\phi(N)$ when χ is trivial.
$\sum_\chi \chi(x)=0$ when $x\not\equiv 1$ mod N; $\sum_\chi\chi(x)=\phi(N)$ when $x\equiv 1 \bmod N$.
We will first prove the finitude of the Dirichlet L-function when χ is non-trivial.

$$\begin{aligned}L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}&=\sum_{m=0}^{\infty}\sum_{i=1}^{N}\frac{\chi(i)}{(i+mN)^s} \\ =\sum_{m=0}^{N}(\sum_{i=1}^{N}\frac{\chi(i)}{(i+mN)^s}&-(\sum_{i=1}^{N}\chi(i))\cdot\frac{1}{(mN)^s}) \\ &=\sum_{m=0}^{\infty}\sum_{i=1}^{N}\chi(i)(\frac{1}{(i+mN)^s}-\frac{1}{(mN)^s}).\end{aligned}$$

The second step is true because $\sum_1^N\chi(i)=0$. Note that $|\frac{1}{(i+mN)^s}-\frac{1}{(mN)^s}|=|\frac{1-(1+\frac{i}{mN})^s}{(i+mN)^s}|$. Let $x=\frac{1}{m}$. $\frac{i}{mN}\le\frac{N}{mN}=\frac{1}{m}$. Since $s>0$, $(i+mN)^s\ge m^s=\frac{1}{x^s}$. Thus, we have

$$|\frac{1}{(i+mN)^s}-\frac{1}{(mN)^s}|=|\frac{1-(1+\frac{i}{mN})^s}{(i+mN)^s}|\le|\frac{1-(1+x)^s}{x^{-s}}|\approx|1-(1+sx)||x^s|=s\cdot x^{s+1},$$

$$\sum_{m=0}^{\infty}|\sum_{i=1}^{N}\frac{\chi(i)}{(i+mN)^s}-(\sum_{i=1}^{N}\chi(i))\cdot\frac{1}{(mN)^s}|\le\sum_{m=0}^{\infty}\frac{c}{m^{s+1}},$$

where c is some finite number. The right hand side of the above equation converges absolutely when $Re(s)>0$. Thus, $L(s,\chi)$ has the least upper bound.

Next, we want to show $L(1,\chi)\neq 0$. First, suppose that χ is not quadratic, i.e. χ is not real-valued. Then $\overline{\sum_{n\ge1}\frac{\chi(n)}{n^s}}=\sum_{n\ge1}\frac{\overline{\chi(n)}}{n^s}$ when s is real. Thus, $\overline{L(s,\chi)}=L(s,\overline{\chi})$. In particular, if we assume $L(1,\chi)=0$, then $L(1,\overline{\chi})=0$. Then we have at least two specific characters ,χ, $\overline{\chi}$, such that $L(1,\chi)=L(1,\overline{\chi})=0$. By the equation

$$\sum_{p\equiv a \bmod N}\frac{1}{p^s}=\frac{1}{\phi(N)}\sum_{p\nmid N}\frac{1}{p^s}+\frac{1}{\phi(N)}\sum_{\chi\text{nontrivial}}\chi(a')\sum_p\frac{\chi(p)}{p^s},$$

we have

$$\phi(N)\sum_{p\equiv 1 \bmod N}\frac{1}{p^s}=\sum\frac{1}{p^s}+\log L(s,\chi)+\log L(s,\overline{\chi})+\text{other characters.}$$

We have proved that $\sum\frac{1}{p^s}\approx\log\frac{1}{s-1}$. Since the following two L functions have pole at $s=1$, $\log L(s,\chi)=\log L(s,\overline{\chi})\approx\log(s-1)$ when s approaches to 1. Thus, the first two terms on the right hand side cancel, leaving the third term and the remaining other L functions from other characters. When s is very close to 1, say 1.0001, the $LHS>0$ while the $RHS<0$. There is a contradiction. Thus, when χ is not real-valued, the Dirichlet L-function can never be 0.

5. Nonvanishing of $L(\chi,1)$ when χ is real-valued

In order to prove the nonvanishing of $L(\chi,1)$,we introduce the Dedekind zeta function: $\zeta_N(s)=\prod_\chi L(\chi,s)$ near $s=1$. We know that for each nontrivial χ, $L(\chi,s)$ is holomorphic at $s=1$, whereas for trivial 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 it 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 $g(p)=\frac{\phi(N)}{f(P)}$, which is a positive integer.

Proposition 5.1. *a) We have* $\zeta_N(s)=\prod_{p\nmid N}\frac{1}{(1-\frac{1}{p^{f(p)s}})^{g(p)}}$.

b) Therefore, $\zeta_N(s)$ is a Dirichlet series with non-negative integral coefficients, converging absolutely when the real part of s is greater than 1.

Proof. Let $\mu_{f(p)}$ be the group of $f(p)$-th roots of unity as roots (with multiplicity one). 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 when $T=0$. Now by the Character Extension Lemma, 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). □

Since we know that $\zeta_N(s)$ has 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 singularity at σ. Clearly $\sigma\geq 1$, so, 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 where the real part of s is greater than $1-\epsilon$, but it extends until it meets a singularity on the real line. But we have already seen that each Dirichlet L-function is holomorphic when the real part of s is greater than 0 and less than 1, so Landau's theorem tells us that $\sigma\leq 0$. However, in our cases, it is unlikely that

a Dirichlet series with non-negative integral coefficients has absissca of convergence $\sigma \leq 0$. To see it more explicitly,

$$\begin{aligned}\frac{1}{(1-\frac{1}{p^{f(p)s}})^{g(p)}} &= (1+\frac{1}{p^{f(p)s}}+\frac{1}{p^{2f(p)s}}+...)^{g(p)} \\ &\geq 1+\frac{1}{p^{f(p)s}}+\frac{1}{p^{2f(p)s}}+....\end{aligned}$$

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

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

Multiplying this over all p, it follows that

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

When we evaluate at $s = \frac{1}{\phi(N)}$, 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 $\sum_{k=1}^{\infty} \frac{1}{Nk+1} = \infty$. Thus, the $\zeta_N(s)$ has a singularity at $s = 1$. Therefore, $L(\chi, 1) \neq 0$ for all nontrivial χ.

In conclusion, if we define the density of the primes of the form $p \equiv a \mod b$ to be $\rho(a \mod b) = \frac{\sum_{p\equiv a \mod b} \frac{1}{p}}{\sum_p \frac{1}{p}}$, then we get the result of Dirichlet's Theorem: different progressions (different a) with the same modulus have the same density. This is true because

$$\sum_{p\equiv a \mathrm{mod} N} \frac{1}{p^s} = \frac{1}{\phi(N)} \sum_{p\nmid N} \frac{1}{p^s} + \frac{1}{\phi(N)} \sum_{\chi \mathrm{nontrivial}} \chi(a') \sum_p \frac{\chi(p)}{p^s},$$

and the second term on the right hand side is finite. Thus, we complete the proof of Dirichlet's Theorem on the density of primes.

Acknowledgements

I would like to thank my mentor, Henry Chan, for providing me with knowledge about number theory and advice on this paper.

Appendix A. Proofs of Theorems and Lemma

Theorem A.1. *In number theory, Euler's theorem states that if n and a are coprime positive integers, then*

$$a^{\phi(n)} \equiv 1 \mod n$$

where $\phi(n)$ is the number of all integers less than n that are coprimes to n.

Proof. This theorem can be proven using concepts from the theory of groups: The residue classes (mod n) that are coprime to n form a group under multiplication. The order of any subgroup of a finite group divides the order of the entire group, in this case $\phi(n)$. If a is any number coprime to n, then a is in one of these residue

classes, and its powers $a, a^2, ..., a^k \equiv 1 \mod n$ are a subgroup. Then k must divide $\phi(n)$, i.e. there is an integer M such that $kM = \phi(n)$. Then

$$a^{\phi(n)} = a^{kM} = (a^k)^M \equiv 1^M = 1 \mod n$$

. □

Theorem A.2. *Let* $\boldsymbol{F}$ *be a field and let* $\boldsymbol{p(x)}$ *be a non-zero polynoial in* $\boldsymbol{F[x]}$ *of degree* $n \geq 0$. *Then* $\boldsymbol{p(x)}$ *has at most* n *roots in* $\boldsymbol{F}$ *(counted with multiplicity).*

Proof. We proceed by induction. The case $n = 0$ is trivial since $\mathbf{p(x)}$ is a non-zero constant, thus $\mathbf{p(x)}$ cannot have any roots.

Suppose that any polynomial in $\mathbf{F[x]}$ of degree n has at most n roots and let $\mathbf{p(x)} \in \mathbf{F[x]}$ be a polynomial of degree $n+1$. If $\mathbf{p(x)}$ has no roots then the result is trivial, so let us assume that $\mathbf{p(x)}$ has at least one root $a \in F$. Then,there exists a polynomial $\mathbf{q(x)}$ such that $\mathbf{p(x)} = (x-a) \cdot \mathbf{q(x)}$. Hence,$\mathbf{q(x)} \in \mathbf{F[x]}$ is a polynomial of degree n. By the induction hypothesis, the polynomial $\mathbf{q(x)}$ has at most n roots. It is clear that any root of $\mathbf{q(x)}$ is a root of $\mathbf{p(x)}$ and if $b \neq a$ is a root of $\mathbf{p(x)}$ then b is also a root of $\mathbf{q(x)}$. Thus, $\mathbf{p(x)}$ has at most $n+1$ roots, which concludes the proof of the theorem. □

Lemma A.3. *(Character Extension Lemma) Let* H *be a subgroup of a finite commutative group* G. *For any character* $\psi : H \to \mathbb{C}$, *there are* $[G : H]$ *characters* $\psi : G \to \mathbb{C}$ *such that* $\psi|_H = \psi$.

Proof. The result is clear if $H = G$, so we may assume that there exists $g \in G \backslash H$. Let $G_g =< g, H >$ be the subgroup generated by H and g. Now we may or may not have $G_g = G$, but suppose that we can establish the result for the group G_g and its subgroup H. Then the general case follows by induction, since for any $H \in G$, choose $g_1, ..., g_n$ such that $G =< H, g_1, ..., g_n >$. Then we can define $G_0 = H$ and for $1 \leq i \leq n$, $G_i =< G_{i-1}, g_i >$. Applying the Lemma in turn to G_{i-1} as a subgroup of G_i gives that in all the number of ways to extend the character ψ of $H = G_0$ is

$$[G_1 : H][G_2 : G_1]...[G_n : G_{n-1}] = [G : G_0] = [G : H].$$

□

So let us now prove that the number of ways to extend ψ from H to $G_g =< H, g >$ is $[G_g : H]$. For this, let d be the order of g in G, and consider $\bar{G} := H \times < g >$. The number of ways to extend a character ψ of H to a character of $\bar{G}$ is equal to $\# < g >= d$: such a homomorphism is uniquely specified by the image of $(1, g)$ in $\mu_d \in \mathbb{C}$, and all d such choices give rise to homomorphisms.

Moreover, there is a surjective homomorphism $\psi : H \times < g >$ to G_g: we just take $(h, g^i) \mapsto hg^{-i}$. The kernel of ψ is the set of all pairs (h, g^i) such that $g^i = h$. In other words, it is precisely the intersection $H \cap < g >$, which has cardinality, say e, some divisor of d. It follows that

$$\#H_g = \frac{\#H \times < g >}{\#H \cap < g >} = \frac{d}{e} \cdot \#H,$$

so

$$[H_g : H] = \frac{d}{e}.$$

But a homomorphism $f : H \times < g > \to \mathbb{C}$ descends to a homomorphism on the quotient H_g iff it is trivial on the kernel of the quotient map, i.e., is trivial on

$H\cap < g >$. In other words, the extensions of ψ to a character of H_g correspond precisely to the number of ways to map the order d element g into $\mathbb{C}$ such that $g^{\frac{d}{e}}$ gets mapped to 1. Thus we must map g to a $\frac{d}{e}$th root of unity, and conversely all such mappings induce extensions of ψ. Thus the number of extensions is $\frac{d}{e} = [H_g : H]$.

Theorem A.4. *Let $\sigma_k(x)$ be the number of integers $n \leq x$ which are the product of just k prime factors so that $n = p_1p_2...p_k$, and let $\pi_k(x)$ be the number of such n for which all the p_i are different. The behavior of $\pi_k(x)$ and $\sigma_k(x)$ as $x \to \infty$ is given by*

$$\pi_k(x) \sim \sigma_k(x) \sim \frac{x(loglogx)^{k-1}}{(k-1)!logx}.$$

Proof. A.Selberg found an elementary proof of $\sum_{p\leq x} logp\ x$, which is equivalent to the Prime Number Theorem. We use an elementary deduction of the Landau's Theorem for $k \geq 2$ from the above finding and the well-known elementary result $\sum_{p\leq x} \frac{1}{p} \sim loglogx$.

We wrtie c_n for the number of ways of expressing n in the form of $n = p_1p_2...p_k$, order being relevant. Clearly $c_n = 0$, unless n is a product of just k prime factors; in this case, $c_n = k!$ or $1 \leq c_n < k!$ according as the k primes are or are not, all different. We write

$$\prod_k(x) = \sum_{n\leq x} c_n = \sum_{p_1p_2...p_k\leq x} 1,$$

and so have

$$k!\pi_k(x) \leq \prod_k(x) \leq k!\sigma_k(x). \tag{A.5}$$

Again, there are just $\sigma_k(x)-\pi_k(x)$ values of $n \leq x$, each of which is representable in the form $n = p_1p_2...p_k$ with two at least of the p_i eqaul. We may take $p_{k-1} = p_k$ and so

$$\sigma_k(x) - \pi_k(x) \leq \sum_{p_1p_2...p_{k-2}p_{k-1}^2} 1 \leq \sum_{p_1...p_{k-1}} 1 = \prod_{k-1}(x) \tag{A.6}$$

We write $\Omega_0(x) = 1$ and ,for $k \geq 1$,

$$\Omega_k(x) = \sum_{n\leq x} \frac{c_n}{n} = \sum_{p_1...p_k\leq x} \frac{1}{p_1...p_k},$$

so that

$$k\vartheta_{k+1}(x) = \sum_{p_1...p_{k+1}\leq x} log(p_2p_3...p_{k+1}) + log(p_1p_3...p_{k+1}) + ... + log(p_1p_2...p_k)$$

$$= (k+1)\sum_{p\leq x} \vartheta(\frac{x}{p}).$$

Hence, if

$$\phi_k(x) = \vartheta_k(x) - kx\Omega_{k-1}x),$$

we have

$$k\phi_{k+1}(x) = (k+1)\sum_{p\leq x} \phi_k(\frac{x}{p}), (k \geq 1).$$

If, for some fixed $k \geq 1$,

$$\phi_k(x) = o(loglogx)^{k-1}, \tag{A.7}$$

it follows that

$$|\phi_{k+1}(x)| \leq x(loglogx)^{k-1} \sum_{p \leq x} \frac{1}{p} f(\frac{x}{p}),$$

where, for any $\epsilon > 0$,

$$0 < f(x) \leq A(x \geq 1), f(x) < \epsilon(x \geq x_0 = x_0(\epsilon)).$$

Hence

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} f(\frac{x}{p}) &\leq \epsilon \sum_{p \leq x/x_0} \frac{1}{p} + A \sum_{x/x_0 \leq pleqx} \frac{1}{p} \\ &\leq \epsilon loglog(\frac{x}{x_0}) + Alog(\frac{logx}{logx - logx_0}) + O(1) \\ &\leq 2\epsilon loglogx \end{aligned}$$

. for $x \geq x_1 \geq x_0$, and so

$$\phi_{k+1}(x) = o[x(loglogx)^k],$$

which is (A.7) with $k+1$ for k. But, for $k = 1$, (A.7) is equivalent to $\sum_{p \leq x} logp \sim x$. Hence (A.7) is true for all $k \geq 1$.

Next we have

$$(\sum_p \frac{1}{p})^k \leq \Omega_k(x) \leq (\sum_{p \leq x} \frac{1}{p})^k$$

and so, by $\sum_{p \leq x} \frac{1}{p} \sim loglogx$,

$$\Omega_k(x) \sim (loglogx)^k.$$

Hence, by (A.7),

$$\vartheta_k(x) \sim kx(loglogx)^{k-1}.$$

Trivially,

$$\vartheta_k(x) = \sum_{n \leq x} c_n logn \leq \prod_k (x) logx \tag{A.8}$$

and, if $X = \frac{x}{logx}$,

$$\vartheta(x) \geq \sum_{X < n \leq x} c_n logn \geq \Pi_k(x) - \Pi_k(X) logX.$$

But $logX \sim logx$ and ,for $k \geq 2$,

$$\Pi_k(X) = O(X) = O(\frac{x}{logx}) = o(\frac{\vartheta_k(x)}{logx}) = o(\Pi_K(x))$$

by (A.8). Hence

$$\Pi_k(x) \sim \frac{\vartheta_k(x)}{logx} \sim \frac{kx(loglogx)^{k-1}}{logx}.$$

and so, by (A.5) and (A.6),

$$\pi_k(x) \sim \sigma_k(x) \sim \frac{x(loglogx)^{k-1}}{(k-1)!logx}, (k \geq 2).$$

This completes our proof. □

Lemma A.9. *There are infinitely many primes of the form* $4n + 1$.

Proof. For every k, all prime divisors of $k^2 + 1$ are $\equiv 1 \mathrm{mod} 4$. This is because any $p|n^2 + 1$ fulfills $n^2 \equiv -1 \mathrm{mod} p$ and therefore $(\frac{-1}{p}) = 1$, which is, since p must be odd, equivalent to $p \equiv 1 \mathrm{mod} 4$. Assume that there are only t primes $p_1, ..., p_t$ of the form $4m + 1$, where m is a prime. Then we can derive a contradiction from considering the prime factors of $(2p_1...p_t)^2 + 1$. □

References

[1] E. Landau, *Ueber Eine Verallgemeinerung Des Picardschen Satzes*. Sitzungsber. Preuss. Akad. Wiss., 1904.

[2] S. Stoilov, *The theory of functions of a complex variable*. Transl. Math. Monogr., 1962.

[3] L. Xiao, *Course Notes on Number Theory*. 2012.

[4] Tom M. Apostol *Introduction to Analytic Number Theory*. Springer, 2002.

[5] Serge Lang, *Complex Analysis*. Springer, New York, 4th Edition, 1999.