18.1.2 Dirichlet's Theorem

Theorem 18.1.3 (Primes in Arithmetic Progressions). *Let a and b be relatively prime integers. Then there are infinitely many primes in the progression $an + b$. Further, for a fixed a, to first order all relatively prime b give progressions having the same number of primes.*

Notice that the condition $(a, b) = 1$ is necessary. If $\gcd(a, b) > 1$, $an + b$ can be prime at most once. Dirichlet's remarkable result is that this condition is also sufficient.

Exercise 18.1.4. *Dirichlet's theorem is not easy to prove, but try to prove it in the particular case $a = 4, b = -1$, i.e. for the arithmetic progression $4n - 1$, using an argument similar to Euclid's. Proving there are infinitely many primes of the form $4n + 1$ is a lot harder.*

18.1.3 Prime Number Theorem

Theorem 18.1.5. *(Prime Number Theorem or PNT) As $X \to \infty$,*

$$\pi(X) \sim \frac{X}{\log X} \tag{18.3}$$

The Prime Number Theorem was proved in 1896 by Jacques Hadamard and Charles Jean Gustave Nicolas Baron de la Vallée Poussin. Of course, we need to quantify what $\pi(X) \sim \frac{X}{\log X}$ means. Basically, there is an error function $E(X)$ such that $|\pi(X) - \frac{X}{\log X}| \leq E(X)$, and $E(X)$ grows slower than $\frac{X}{\log X}$.

A weaker version was proved by Pafnuty Chebyshev (around 1850).

Theorem 18.1.6 (Chebyshev). *There exist explicit positive constants A and B such that, for $X > 30$:*

$$\frac{AX}{\log X} \leq \frac{\pi(X)}{X} \leq \frac{BX}{\log X}. \tag{18.4}$$

Chebyshev showed one can take $A = \log\left(\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}4^{\frac{1}{4}}}{30^{\frac{1}{30}}}\right) \approx .921$ and $B = \frac{6A}{5} \approx 1.105$, which are indeed very close to 1. To highlight the method, we will use cruder arguments and prove the theorem for a smaller A and a larger B.

Chebyshev's argument uses an identity using von Mangoldt's Lambda function $\Lambda(n)$, where $\Lambda(n) = \log p$ if $m = p^k$ for some prime p, and 0 otherwise.

Define the function

$$T(X) = \sum_{1 \leq n \leq X} \Lambda(n) \left[\frac{X}{n} \right] = \sum_{n \geq 1} \Lambda(n) \left[\frac{X}{n} \right]. \tag{18.5}$$

Exercise 18.1.7. *Show that $T(X) = \sum_{n \leq X} \log n$.*

Now, it is easy to see (compare upper and lower sums) that

$$\sum_{n \leq X} \log n = \int_1^X \log \text{t dt} + O(\log X) = X \log X - X + O(\log X), \tag{18.6}$$

giving a good approximation to the function $T(X)$. The trick is to look at

$$T(X) - 2T\left(\frac{X}{2}\right) = \sum_n \Lambda(n) \left(\left[\frac{X}{n} \right] - 2 \left[\frac{X}{2n} \right] \right) \tag{18.7}$$

By the previous remarks, the LHS $= X \log 2 + O(\log X)$. Also,

$$\text{RHS} \leq \sum_{p \leq X} (\log p) \frac{\log X}{\log p} = \pi(X) \log X. \tag{18.8}$$

Hence we immediately obtain the lower bound:

$$\pi(X) \geq \frac{X \log 2}{\log X} + O(\log X) \tag{18.9}$$

Exercise 18.1.8. *Prove the bound in Equation 18.8.*

To obtain an upper bound for $\pi(X)$, we notice that, since $[2\alpha] \geq 2[\alpha]$, the sum in equation (18.7) has only positive terms. By dropping terms we get a lower bound.

$$
\begin{aligned}
T(X) - 2T\Big(\frac{X}{2}\Big) &\geq \sum_{X/2<n\leq X} \Lambda(n)\left(\left[\frac{X}{n}\right] - 2\left[\frac{X}{2n}\right]\right) \\
&\geq \sum_{X/2<p\leq X} \log p \\
&\geq \log\Big(\frac{X}{2}\Big) \sum_{X/2<p\leq X} 1 \\
&= \log\Big(\frac{X}{2}\Big)\left(\pi(X) - \pi\Big(\frac{X}{2}\Big)\right) \qquad (18.10)
\end{aligned}
$$

Hence we obtain an upper bound for the number of primes between $\frac{X}{2}$ and X:

$$
\pi(X) - \pi(X/2) \leq \frac{X\log 2}{\log(\frac{X}{2})} + O(1) \qquad (18.11)
$$

Now, if we write inequality (18.11) for $X, \frac{X}{2}, \frac{X}{2^2}, \ldots$ we get

$$
\begin{aligned}
\pi(X) - \pi(X/2) &\leq 2\frac{X/2}{\log(X/2)} \\
\pi(X/2) - \pi(X/2^2) &\leq 2\frac{X/2^2}{\log(X/2^2)} \\
&\vdots \\
\pi(X/2^{k-1}) - \pi(X/2^k) &\leq 2\frac{X/2^k}{\log(X/2^k)} \qquad (18.12)
\end{aligned}
$$

as long as $\frac{X}{2^k} \geq 1$, i.e. $k \leq [\log_2 X] = k_0$. Summing the above inequalities we get on the left hand side a telescoping sum. All the terms cancel, except for the leading term $\pi(X)$ and $\pi(X/2^{k_0}) = 0$.

Thus

$$
\pi(X) \leq 2\sum_{k=1}^{k_0} \frac{X/2^k}{\log(X/2^k)} \qquad (18.13)
$$

To evaluate the sum in the above inequality we split it into two parts, k small and k large. More precisely, let $n_0 = \log_2(X^{1/10})$ so that $2^{n_0} = X^{1/10}$ and note that:

$$2\sum_{k>n_0}\frac{X/2^k}{\log(X/2^k)} \le 2\sum_{k>n_0}\frac{X}{2^k} \le \frac{2X}{2^{n_0}} = \frac{2X}{X^{1/10}} = 2X^{9/10}. \tag{18.14}$$

Hence the contribution from k large is very small compared to what we expect (i.e. order of magnitude $\frac{X}{\log X}$), or we can say that the main term comes from the sum over k small.

We now evaluate the contribution from small k.

$$2\sum_{k=1}^{n_0}\frac{X}{2^k}\frac{1}{\log(X/2^k)} \le \frac{2X}{\log(X/2^{n_0})}\sum_{k=1}^{n_0}\frac{1}{2^{n_0}} \le \frac{2X}{\log(X^{9/10})} = \frac{20}{9}\frac{X}{\log X} \tag{18.15}$$

Hence the right hand side of the equation (18.13) is made up of two parts, a main term of size $\frac{BX}{\log X}$ coming from equation (18.15), and a lower order term coming from equation (18.14).

For X sufficiently large,

$$\pi(X) \le \frac{BX}{\log X} \tag{18.16}$$

where B can be any constant strictly bigger than $\frac{20}{9}$.

To obtain Chebyshev's better constant we would have to work a little harder along these lines, but it is the same method.

Gathering equations (18.9) and (18.16) we see we have proven

$$\frac{AX}{\log X} \le \pi(X) \le \frac{BX}{\log X}. \tag{18.17}$$

While this is not an asymptotic for $\pi(X)$, it does give the right order of magnitude for $\pi(X)$, namely $\frac{X}{\log X}$.

Exercise 18.1.9. *Using Chebyshev's Theorem, prove Bertrand's Postulate: for any integer $n \ge 1$, there is always a prime number between n and $2n$.*

18.2 Partial Summation

Lemma 18.2.1 (Partial Summation: Discrete Version). *Let $A_N = \sum_{n=1}^{N} a_n$. then*

$$\sum_{n=M}^{N} a_n b_n = A_N b_N - A_{M-1} b_M + \sum_{n=M}^{N-1} A_n (b_n - b_{n+1}) \tag{18.18}$$

Proof. Since $A_n - A_{n_1} = a_n$,

$$\begin{aligned}
\sum_{n=M}^{N} a_n b_n &= \sum_{n=M}^{N} (A_n - A_{n-1}) b_n \\
&= (A_N - A_{N-1}) b_N + (A_{N-1} - A_{N-2}) b_{N-1} + \cdots + (A_M - A_{M-1}) b_M \\
&= A_N b_N + (-A_{N-1} b_N + A_{N-1} b_{N-1}) + \cdots + (-A_M b_{M+1} + A_M b_M) - a_{M-1} b_M \\
&= A_N b_N - a_{M_1} b_M + \sum_{n=M}^{N-1} A_n (b_n - b_{n+1}). \qquad (18.19)
\end{aligned}$$

□

Lemma 18.2.2 (Abel's Summation Formula - Integral Version). *Let $h(x)$ be a continuously differentiable function. Let $A(x) = \sum_{n \leq x} a_n$. Then*

$$\sum_{n \leq x} a_n h(n) = A(x) h(x) - \int_1^x A(u) h'(u) du \tag{18.20}$$

See, for example, [Rud], page 70.

Partial Summation allows us to take knowledge of one quantity and convert that to knowledge of another.

For example, suppose we know that

$$\sum_{p \leq x} \log p \ = \ x + O(x^{\frac{1}{2}+\epsilon}). \tag{18.21}$$

We use this to glean information about $\sum_{p \leq x} 1$.

Define

$$h(n) = \frac{1}{\log n} \quad \text{and} \quad a_n = \begin{cases} \log n & \text{if } n \text{ is prime} \\ 0 & \text{otherwise.} \end{cases} \tag{18.22}$$

Applying partial summation to $\sum_{p \leq x} a_n h(n)$ will give us knowledge about $\sum_{p \leq x} 1$. Note as long as $h(n) = \frac{1}{\log n}$ for n prime, it doesn't matter how we define

$h(n)$ elsewhere; however, to use the integral version of Partial Summation, we need h to be a differentiable function.

Thus

$$\begin{aligned} \sum_{p \le x} 1 &= \sum_{p \le x} a_n h(n) \\ &= \Big(x + O(x^{\frac{1}{2}+\epsilon})\Big) \frac{1}{\log x} - \int_2^x \Big(u + O(u^{\frac{1}{2}+\epsilon})\Big) h'(u) du. \end{aligned} \tag{18.23}$$

The main term ($A(x)h(x)$) equals $\frac{x}{\log x}$ plus a significantly smaller error.

We now calculate the integral, noting $h'(u) = -\frac{1}{u \log^2 u}$. The error piece in the integral gives a constant multiple of

$$\int_2^x \frac{u^{\frac{1}{2}+\epsilon}}{u \log^2 u} du. \tag{18.24}$$

As $\frac{1}{\log^2 u} \le \frac{1}{\log^2 2}$ for $2 \le u \le x$, the integral is bounded by

$$\frac{1}{\log^2 2} \int_2^x u^{-\frac{1}{2}+\epsilon} < \frac{1}{\log^2 2} \frac{1}{\frac{1}{2}+\epsilon} x^{\frac{1}{2}+\epsilon}, \tag{18.25}$$

which is significantly less than $A(x)h(x) = \frac{x}{\log x}$.

We now need to handle the other integral:

$$\int_2^x \frac{u}{u \log^2 u} du = \int_2^x \frac{1}{\log^2 u} du. \tag{18.26}$$

The obvious approximation to try is $\frac{1}{\log^2 u} \le \frac{1}{\log^2 2}$. Unfortunately, plugging this in bounds the integral by $\frac{x}{\log^2 2}$. This is larger than the expected main term, $A(x)h(x)$!

As a rule of thumb, whenever you are trying to bound something, try the simplest, most trivial bounds first. Only if they fail should you try to be clever.

Here, we need to be clever, as we are bounding the integral by something larger than the observed terms.

We split the integral into two pieces:

$$\int_2^x = \int_2^{\sqrt{x}} + \int_{\sqrt{x}}^x \tag{18.27}$$

For the first piece, we use the trivial bound for $\frac{1}{\log^2 u}$. Note the interval has length $\sqrt{x} - 2 < \sqrt{x}$. Thus, the first piece contributes at most $\frac{x^{\frac{1}{2}}}{\log^2 2}$, significantly less than $A(x)h(x)$.

The reason trivial bounds failed for the entire integral is the length was too large (of size x); there wasn't enough decay in the function.

The advantage of splitting the integral in two is that in the second piece, even though most of the length of the original interval is here (it is of length $x - \sqrt{x} \approx x$), the function $\frac{1}{\log^2 u}$ is small here. Instead of bounding it by a constant, we now bound it by substituting in the smallest value of u on this interval, $\sqrt{x}$. Thus, the contribution from this integral is at most $\frac{x-\sqrt{x}}{\log^2 \sqrt{x}} < \frac{4x}{\log^2 x}$. Note that this is significantly less than the main term $A(x)h(x) = \frac{x}{\log x}$.

18.3 Introduction to L-Functions

NOTE – THIS SECTION IS IN VERY ROUGH FORM – MORE DETAIL WILL BE ADDED, WE'RE NOT SURE YET HOW MUCH WE WANT TO SAY. WE NEED ENOUGH TO TALK ABOUT ZEROS OF L-FUNCTIONS, AS WE WANT TO RELATE THIS TO RANDOM MATRIX THEORY

18.3.1 $\zeta(s)$

Many exciting problems in modern number theory involve L-functions. Below we briefly review some background information.

An L-function is of the form $L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$. The simplest is the Riemann Zeta Function, $\zeta(s)$, which for $Re(s) > 1$ is given by

$$\zeta(s) \ = \ \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{18.28}$$

Using Unique Factorization, one has the Euler Product Expansion

$$\zeta(s) \ = \prod_{p \in Primes} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{18.29}$$

The above formula allows us to translate knowledge of $\zeta(s)$ to knowledge about properties of primes. Using Analytic Continuation, $\zeta(s)$ can be extended to a meromorphic function on $\mathbb{C}$ with only a simple pole at $s = 1$.