Chapter 2 Elementary Prime Number Theory for 2018-19

v1 [**5 lectures**]

In keeping with the 'elementary' theme of the title I will attempt to keep away from complex variables. Recall that in Chapter 1 we proved the infinitude of primes by relating $\sum_p 1/p^\sigma$ to $\zeta(\sigma)$ for $\sigma > 1$. From the Euler Product, we formally get (so not worrying about convergence),

$$\log \zeta(\sigma) = \sum_p \log \left(1 - \frac{1}{p^\sigma}\right)^{-1}$$

for $\sigma > 1$. We will equate the derivatives of both sides, using the *logarithmic derivative*

$$\frac{d}{d\sigma} \log f(\sigma) = \frac{f'(\sigma)}{f(\sigma)} = \frac{f'}{f}(\sigma),$$

along with

$$\frac{d}{d\sigma}\frac{1}{p^\sigma} = \frac{d}{d\sigma} e^{-\sigma \log p} = -\frac{\log p}{p^\sigma}.$$

Then, because the *resulting* sum, (1) below, converges uniformly for $\sigma \geq 1 + \delta$, for any $\delta > 0$ (see Background: Complex Analysis II for a discussion of uniform convergence) we can justify differentiating term-by term to get

$$\begin{aligned}
\frac{\zeta'}{\zeta}(\sigma) &= \frac{d}{d\sigma} \log \zeta(\sigma) = -\sum_p \frac{d}{d\sigma} \log\left(1 - \frac{1}{p^\sigma}\right) \\
&= -\sum_p \frac{1}{\left(1 - \frac{1}{p^\sigma}\right)} \frac{d}{d\sigma}\left(1 - \frac{1}{p^\sigma}\right) \\
&= -\sum_p \frac{1}{\left(1 - \frac{1}{p^\sigma}\right)} \frac{\log p}{p^\sigma}. \qquad (1)
\end{aligned}$$

(In the Appendix we show this series converges uniformly for $\sigma \geq 1 + \delta$). Expand $(1 - 1/p^\sigma)^{-1}$ as a geometric series to get

$$-\frac{\zeta'}{\zeta}(\sigma) = \sum_p \frac{\log p}{p^\sigma} \sum_{k \geq 0} \frac{1}{p^{k\sigma}} = \sum_p \sum_{r \geq 1} \frac{\log p}{p^{r\sigma}},$$

on relabelling $k+1$ as r.

The right hand side here is a **double sum**. See the Background: Product of Series notes to see that when the double sum is absolutely convergent, as it is in this case, then it can be rearranged in *any way* and the resulting series will converge to the same value. In particular, we can write out the right hand side starting as

$$\frac{0}{1^s} + \frac{\log 2}{2^s} + \frac{\log 3}{3^s} + \frac{\log 2}{4^s} + \frac{\log 5}{5^s} + \frac{0}{6^s} + \frac{\log 7}{7^s} + \frac{\log 2}{8^s} + \frac{\log 3}{9^s} + \frac{0}{10^s} + \dots$$

This non-rigorous introduction is simply to motivate the following definition.

Definition 2.1 ***von Mangoldt's function*** *is defined by*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^r, \\ 0 & \text{otherwise.} \end{cases}$$

Then the above argument concludes with

$$\frac{\zeta'}{\zeta}(\sigma) = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma},$$

for $\sigma \geq 1+\delta$ for any $\delta > 0$, i.e. $\sigma > 1$.

Note In the next chapter we will show this equality holds with *real* σ replaced by *complex* s for $\operatorname{Re} s > 1$.

Definition 2.2 *A* ***Dirichlet Series*** *is a sum of the form*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

for some sequence $\{a_n\}_{n\geq 1}$ *of complex numbers, where* $s \in \mathbb{C}$.

Aside Given a sequence $\{a_n\}_{n\geq 1}$ the associated Dirichlet Series may not converge for any $s \in \mathbb{C}$. If it does converge for some s then it can be shown that it will converge in some half-plane $\operatorname{Re} s > c$ (which may be the whole of $\mathbb{C}$, i.e. $c = -\infty$). We can also look at absolute convergence; again if it converges absolutely at some point then it will do so in some half-plane $\operatorname{Re} s > c_a$. Since absolute convergence implies convergence we have $c \leq c_a$. It can be shown that $0 \leq c_a - c \leq 1$. **End of Aside**

Example 2.3 *$\zeta(s)$ and $\zeta'(s)/\zeta(s)$ for $\operatorname{Re} s > 1$ are Dirichlet Series.*

Notation For an integer $n > 1$ and prime p, then $p^a \parallel n$ means that a is the largest power of p that divide p.

For example, if $n = 2^3 5^4 13^2 = 845000$ then

$$2^3 || 845000, \ 5^4 || 845000 \quad \text{and} \quad 13^2 || 845000.$$

Note that

$$\log 845000 = 3 \log 2 + 4 \log 5 + 2 \log 13 = \sum_{p^a || 845000} a \log p,$$

a general form of which will be seen in the next proof.

This notation allows an efficient way of writing an integer n in terms of its prime divisors as

$$n = \prod_{p^a \| n} p^a$$

The basic **and important** property of von Mangoldt's Λ is

Theorem 2.4 *For $n \geq 1$*

$$\sum_{d|n} \Lambda(d) = \log n. \tag{2}$$

Proof If $n = 1$ both sides of (2) are zero.

If $n > 1$ then

$$\sum_{d|n} \Lambda(d) = \sum_{p^r|n} \Lambda(p^r)\,,$$

which simply means that we have excluded the terms with d **not** a prime power, for in such cases $\Lambda(d) = 0$. Yet on prime powers $\Lambda(p^r) = \log p$ so

$$\sum_{p^r|n} \Lambda(p^r) = \sum_{p^r|n} \log p.$$

Observe this is really a *double sum*, over p and r. Write

$$n = \prod_{p^a \| n} p^a,$$

as a product of distinct primes. Then $p^r|n$ if, and only if, $p^a||n$ and $1 \le r \le a$. In which case

$$\begin{aligned} \sum_{p^r|n} \log p &= \sum_{p^a\|n} \left(\sum_{1\le r\le a} 1 \right) \log p = \sum_{p^a\|n} a \log p \\ &= \sum_{p^a\|n} \log p^a = \log \prod_{p^a\|n} p^a = \log n. \end{aligned}$$

Combine all these steps to get the stated result. ■

Notation 2.5 *The summatory function of the von Mangoldt function is denoted by*

$$\psi(x) = \sum_{n\le x} \Lambda(n)\,.$$

Denote the sum over the logarithm of primes by

$$\theta(x) = \sum_{p\le x} \log p,$$

and the unweighted sum by

$$\pi(x) = \sum_{p\le x} 1.$$

Landau's big O-notation If $f(x)$, $g(x)$ and $h(x)$ are functions then we write

$$f(x) = O(h(x))$$

if there exists $C > 0$ such that $|f(x)| < Ch(x)$ for all x. The constant C is referred to as the *implied constant*. The notation is extended so that

$$f(x) = g(x) + O(h(x))$$

means there exists $C > 0$ such that $|f(x) - g(x)| < Ch(x)$ for all x.

It is further extended so that

$$f(x) \le g(x) + O(h(x))$$

means there exists a function $k(x)$ satisfying both $f(x) \le g(x) + k(x)$ and $k(x) = O(h(x))$.

Vinogradov's $\ll$ (read as **"less than less than") notation**. $f(x) \ll g(x)$ means exactly the same as $f(x) = O(g(x))$.

If

$$g(x) \ll f(x) \ll g(x) \text{ we write } f(x) \asymp g(x)\,.$$

Little o-notation We write $f(x) = o\,(g(x))$ iff

$$\lim_{x\to\infty} \frac{f(x)}{g\,(x)} = 0.$$

Asymptotic We write $f(x) \sim g(x)$ iff

$$\lim_{x\to\infty} \frac{f(x)}{g\,(x)} = 1.$$

Example 2.6

$$\sum_{1\leq n\leq x} \frac{1}{n} = \log x + O\,(1)\,. \tag{3}$$

Proof in Chapter 1 it was shown that for integer N

$$\log\,(N+1) \leq \sum_{n\leq N} \frac{1}{n} \leq \log N + 1.$$

Given *real* $x > 1$ apply this with $N = [x]$, the integer part of x. Then $N \leq x < N + 1$ and we deduce

$$\log x \leq \sum_{1\leq n\leq x} \frac{1}{n} \leq \log x + 1. \tag{4}$$

This means, on writing

$$\mathcal{E}(x) = \sum_{1\leq n\leq x} \frac{1}{n} - \log x,$$

that $0 \leq \mathcal{E}(x) \leq 1$. Weaken this to $|\mathcal{E}(x)| \leq 1$, the definition of $\mathcal{E}(x) = O\,(1)$. Hence result. ■

To proceed with our investigation into prime numbers we need a version of this with a smaller error term. This is achieved using the following **important** result.

But first a **Subtle Point.** If f is differentiable on an interval containing $[a, b]$ it may appear obvious that

$$f(b) - f(a) = \int_a^b f'(t)\, dt, \tag{5}$$

but it may **not,** in fact, be true**.** You need to invoke the Fundamental Theorem of Calculus that says that if f' is continuous on $[a, b]$ (alternatively that f has *continuous derivative*) then (5) holds.

Theorem 2.7 ***Abel or Partial Summation (Continuous Version)*** *Let $g : \mathbb{N} \to \mathbb{C}$ and set $G(x) = \sum_{n \le x} g(n)$. Let $f : \mathbb{R}_{>0} \to \mathbb{C}$ have a continuous derivative on $x > 0$. Then*

$$\sum_{1 \le n \le x} g(n)\, f(n) = f(x)\, G(x) - \int_1^x G(t)\, f'(t)\, dt.$$

Note We sometimes write this as

$$\sum_{1 \le n \le x} g(n)\, f(n) = f(x)\, G(x) - \int_1^x G(t)\, df(t)\,.$$

Proof The proof is an exercise in the interchange of a *finite* sum and a *finite* integral. Start with the simple observation that, since f has a continuous derivative,

$$f(n) = f(x) - \big(f(x) - f(n)\big) = f(x) - \int_n^x f'(t)\, dt.$$

Then, multiplying by $g(n)$ and summing over $n \le x$ gives

$$\begin{aligned} \sum_{1 \le n \le x} g(n)\, f(n) &= \sum_{1 \le n \le x} g(n) \left(f(x) - \int_n^x f'(t)\, dt \right) \\ &= f(x)\, G(x) - \sum_{1 \le n \le x} g(n) \int_n^x f'(t)\, dt. \end{aligned}$$

The second term here can be written as

$$\sum_{\substack{1 \le n \le x \\ t \ge n}} \int_1^x g(n)\, f'(t)\, dt.$$

Finite integrals and sums can be interchanged, with the restriction on the *integral* of $t \geq n$ **reinterpreted** as a condition on the *sum* of $n \leq t$. This gives

$$\underbrace{\sum_{1\leq n\leq x} \int_1^x}_{t\geq n} g(n)\, f'(t)\, dt = \underbrace{\int_1^x \sum_{1\leq n\leq x}}_{n\leq t} g(n)\, f'(t)\, dt \quad = \quad \int_1^x f'(t) \sum_{1\leq n\leq t} g(n)\, dt$$

$$= \int_1^x G(t)\, f'(t)\, dt,$$

as required. ■

An important **Special Case** is when $g(n) = 1$ for all $n \geq 1$.

Notation For $x \in \mathbb{R}$ define $[x]$, the **integer part** of x, to be the largest integer $\leq x$. Define $\{x\} = x - [x]$, the **fractional part** of x. This satisfies $0 \leq \{x\} < 1$ for all real x.

Thus, in the notation of the previous Theorem, $G(x) = \sum_{n\leq x} 1 = [x]$.

We can now state a fundamental result on approximating sums by integrals.

Proposition 2.8 ***Euler Summation*** *Let f have a* ***continuous derivative*** *on $x > 0$. Then*

$$\sum_{1\leq n\leq x} f(n) = \int_1^x f(t)\, dt + f(1) - \{x\}\, f(x) + \int_1^x \{t\}\, f'(t)\, dt$$

for all real $x \geq 1$.

Notes i) If $x = N$ is an integer then the $\{N\}\, f(N)$ term is zero. So we can use the proposition to prove results valid for all real x and *improved* results for *integral* x.

ii) We have $f(1)$ on both sides of this result, so it could have been written as

$$\sum_{2\leq n\leq x} f(n) = \int_1^x f(t)\, dt - \{x\}\, f(x) + \int_1^x \{t\}\, f'(t)\, dt,$$

but there is a danger that if this was done, you would not have noticed that the left hand side was a sum only over $2 \leq n \leq x$, not $1 \leq n \leq x$.

Proof By the result above

$$\begin{aligned}\sum_{1\le n\le x} f(n) &= f(x)\,[x] - \int_1^x [t]\,f'(t)\,dt \\ &= f(x)\,[x] - \int_1^x (t-\{t\})\,f'(t)\,dt \\ &= f(x)\,[x] - \int_1^x tf'(t)\,dt + \int_1^x \{t\}\,f'(t)\,dt.\end{aligned}$$

We integrate the second integral by parts to get

$$\begin{aligned}\int_1^x tf'(t)\,dt &= [tf(t)]_1^x - \int_1^x f(t)\,dt \\ &= f(x)\,x - f(1) - \int_1^x f(t)\,dt.\end{aligned}$$

Substituting back in we get

$$\begin{aligned}\sum_{1\le n\le x} f(n) &= f(x)\,[x] - f(x)\,x + f(1) + \int_1^x f(t)\,dt + \int_1^x \{t\}\,f'(t)\,dt \\ &= \int_1^x f(t)\,dt + f(1) - \{x\}\,f(x) + \int_1^x \{t\}\,f'(t)\,dt.\end{aligned}$$

■

To see the strength of Proposition 2.8 we improve (3),

Theorem 2.9 *There exists a constant* γ *such that*

$$\sum_{n\le x}\frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right),$$

for real $x > 1$.

Note how the estimate on the error here is *best possible* (i.e. you could **not** replace it by a faster diminishing function of x). This is because as x varies by a minuscule amount from just below an integer n to just above it, the left hand changes by $1/n$, yet the main terms $\log x + \gamma$ change imperceptibly (being continuous in x); it is the error term $O\left(1/x\right)$ which exactly matches the change in the left hand side.

Proof From above with $f(x) = 1/x$ we have

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

The second integral converges absolutely since

$$\int_1^\infty |\{t\}| \frac{dt}{t^2} \le \int_1^\infty \frac{dt}{t^2} = 1.$$

Thus we can *complete the integral up to* ∞, the error in doing so is

$$\le \int_x^\infty |\{t\}| \frac{dt}{t^2} \le \int_x^\infty \frac{dt}{t^2} = \frac{1}{x}.$$

Combining,

$$\sum_{n \le x} \frac{1}{n} = \log x + 1 + O\left(\frac{1}{x}\right) - \int_1^\infty \{t\} \frac{dt}{t^2}.$$

Hence the result follows with

$$\gamma = 1 - \int_1^\infty \{t\} \frac{dt}{t^2}.$$

■

Fundamental Idea. This method of completing a *convergent* integral up to infinity and then bounding the tail end is often used and **should be remembered**.

The constant γ is the called **Euler's constant** or sometimes the **Euler-Mascheroni constant**. Reinterpreted, Theorem 2.9 says

$$\gamma = \lim_{x \to \infty} \left(\sum_{n \le x} \frac{1}{n} - \log x \right).$$

This can be used to calculate γ though the speed of convergence is **very** slow. Numerically

$$\gamma \approx 0.57721566490153286060...$$

It is not known if γ is irrational!

If we assume more about the function f we can state a very useful version of Euler's summation. Useful in that it easily allows a sum to be replaced by an integral.

Corollary 2.10 *If f has a continuous derivative on $x > 0$, is **non-negative and monotonic** then*

$$\sum_{1 \le n \le x} f(n) = \int_1^x f(t)\, dt + O(\max(f(1), f(x))), \tag{6}$$

for all real $x \ge 1$.

Proof Since f is monotonic its derivative $f'(x)$ is of *constant sign*. Thus

$$\begin{aligned}
\left| \int_1^x \{t\} f'(t)\, dt \right| &\le \int_1^x |\{t\} f'(t)|\, dt \\
&\le \int_1^x |f'(t)|\, dt \quad \text{since } |\{t\}| \le 1 \\
&= \left| \int_1^x f'(t)\, dt \right| \quad \text{since } f'(t) \text{ is of constant sign} \\
&= |f(x) - f(1)|.
\end{aligned}$$

Hence, by the triangle inequality applied twice

$$\begin{aligned}
\left| f(1) - \{x\} f(x) + \int_1^x \{t\} f'(t)\, dt \right| &\le |f(1)| + |\{x\} f(x)| + \left| \int_1^x \{t\} f'(t)\, dt \right| \\
&\le f(1) + f(x) + |f(x) - f(1)| \\
&\le f(1) + f(x) + f(x) + f(1) \\
&\le 4 \max(f(1), f(x)).
\end{aligned}$$

■

In the last lines of this proof we have used $a + b \le 2\max(a, b)$ for $a, b > 0$. Make sure you believe this.

An immediate application of Corollary 2.10 is

Example 2.11 *Choose* $f(x) = \log x$ *to deduce*

$$\sum_{1 \le n \le x} \log n = x \log x - x + O(\log x)$$

for real $x > 1$.

Again we have the best possible error term for *real* x. We can though do better when $x = N$ an integer and in a number of Problem Sheet questions we look at improving and generalising this result on the sum of logarithms. The interest comes from the fact that $\sum_{n \le N} \log n = \log N!$ and we thus get bound on $N!$.