Most of my handouts will come with exercises attached; see the web site for the due dates. (For example, these are due February 14.)

There are likely to be typos in all of my handouts; it would be helpful if you could report these by email (including ones I point out in class).

Thanks to Ben Brubaker for filling in for me; I will be back February 12.

1 Euler's idea: revisiting the infinitude of primes

To begin our story, we turn to Euler's viewpoint on the fact, originally due to Euclid, that there are infinitely many prime numbers. Euclid's original proof was quite simple, and entirely algebraic: assume there are only finitely many primes, multiply them together, add 1, then factor the result.

Euler realized instead that a basic fact from analysis also leads to the infinitude of primes. This fact is the divergence of the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots,$$

which follows for instance from the fact that

$$\sum_{n=1}^{N} \frac{1}{n} \geq \sum_{n=1}^{N} \frac{1}{2^{\lceil \log_2 n \rceil}} \geq \frac{1}{2} \lfloor \log_2 N \rfloor$$

and the right side tends to ∞ as $N \to \infty$. (We will usually want a more precise estimate; see the exercises.) On the other hand, if there were only finitely many primes, then unique factorization of positive integers into prime powers would imply that

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) = \prod_{p} \left(1 - \frac{1}{p} \right)^{-1},$$

which would give the equality between a divergent series and a finite quantity. Contradiction.

Euler's idea turns out to be quite fruitful: the introduction of analysis into the study of prime numbers allows us to prove distribution statements about primes in a much more flexible fashion than is allowed by algebraic techniques. For instance, we will see in an upcoming unit how Dirichlet adapted this idea to prove that every arithmetic progression whose terms do not all share a common factor contains infinitely many primes.

2 Riemann's zeta function

For the moment, however, let us turn to Riemann's one paper in number theory, in which he fleshes out Euler's idea and fits it into the theory of complex functions of one variable.

He considered the series

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. Note that for $\mathrm{Re}(s) > 1$, the series is absolutely convergent; moreover, it converges uniformly in any region of the form $\mathrm{Re}(s) \geq 1 + \epsilon$ for $\epsilon > 0$. Consequently, it gives rise to an analytic function in the half-plane $\mathrm{Re}(s) > 1$. The boundary $\mathrm{Re}(s) = 1$ is sometimes called the *critical line*.

In the domain of absolute convergence, we can also write

$$\zeta(s) = \prod_{p} \left(1 - p^{-s}\right)^{-1},$$

and this product converges absolutely and uniformly for $\mathrm{Re}(s) \geq 1 + \epsilon$ for $\epsilon > 0$. (Reminder: a product $\prod_i (1 + a_i)$ converges absolutely if and only if $\sum_i a_i$ converges absolutely.) It follows that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$.

For future reference, we note that the product representation is sometimes more useful in the form

$$\log \zeta(s) = \sum_{p} -\log(1 - p^{-s})$$

$$= \sum_{p} \sum_{n=1}^{\infty} \frac{p^{-ns}}{n}.$$

We now show that ζ extends somewhat beyond the domain of absolute convergence of the original series.

Theorem 1. *The function $f(s) = \zeta(s) - \frac{s}{s-1}$ on the domain $\mathrm{Re}(s) > 1$ extends (uniquely) to a holomorphic function on the domain $\mathrm{Re}(s) > 0$. Consequently, $\zeta(s)$ is meromorphic on $\mathrm{Re}(s) > 0$, with a simple pole at $s = 1$ of residue 1 and no other poles.*

Proof. This is an easy application of one of the basic tools in this subject, Abel's method of *partial summation* (or *summation by parts*, as in integration by parts). Namely,

$$\sum_{n=1}^{N} a_n b_n = a_{N+1} B_N - \sum_{n=1}^{N} (a_{n+1} - a_n) B_n, \qquad B_n = \sum_{i=1}^{n} b_i.$$

We apply partial summation to $\zeta(s)$ by taking $a_n = n^{-s}$ and $b_n = 1$, so that $B_n = n$. Rather, we apply partial summation to the truncated sum $\sum_{n=1}^{N} n^{-s}$, and note that the error term $a_{N+1} B_N = (N+1)^{-s} N$ tends to 0 for $\mathrm{Re}(s) > 1$. (Warning: in general, I am not going to be nearly so verbose when applying partial summation. So make sure you understand this example!)

2

With that said, we have

$$\zeta(s) = \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s})$$

$$= s \sum_{n=1}^{\infty} n \int_{n}^{n+1} x^{-s-1} \, dx$$

$$= s \int_{1}^{\infty} \lfloor x \rfloor x^{-s-1} \, dx.$$

We can thus write

$$f(s) = -s \int_{i=1}^{\infty} \{x\} x^{-s-1} \, dx,$$

for $\{x\}$ the fractional part of x; the integral converges absolutely for $\mathrm{Re}(s) > 0$, and uniformly for $\mathrm{Re}(s) \geq \epsilon$ for any $\epsilon > 0$. This proves the claim. $\square$

We already know that $\zeta(s)$ cannot vanish for $\mathrm{Re}(s) > 1$; to prove the prime number theorem, we need to also exclude zeroes on the boundary of that half-plane.

Theorem 2 (Hadamard, de la Vallée-Poussin). *The function $\zeta(s)$ has no zero on the line $\mathrm{Re}(s) = 1$.*

Proof (Mertens). See exercises. $\square$

We will return to Riemann's memoir, establishing more detailed properties of ζ, in a subsequent unit.

3 Towards the prime number theorem

Using the aforementioned properties of the zeta function, Hadamard and de la Vallée-Poussin independently established the prime number theorem in 1897. We'll follow here an argument due to D.J. Newman; our presentation is liberally plagiarized from D. Zagier, Newman's short proof of the Prime Number Theorem, *American Mathematical Monthly* **104** (1997), 705–708.

For $x \in \mathbb{R}$, write

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

$$\vartheta(x) = \sum_{p \leq x} \log p.$$

The prime number theorem then asserts that

$$\pi(x) \sim \frac{x}{\log x}.$$

This is equivalent to

$$\vartheta(x) \sim x,$$

because for any $\epsilon > 0$,

$$\vartheta(x) \leq \sum_{p \leq x} \log x = \pi(x) \log x$$

$$\vartheta(x) \geq \sum_{x^{1-\epsilon} \leq p \leq x} \log x^{1-\epsilon} = (1 - \epsilon)(\pi(x) + O(x^{1-\epsilon})) \log x.$$

What we will prove is that the improper integral

$$\int_1^\infty \frac{\vartheta(x) - x}{x^2} \, dx \tag{1}$$

converges; remember that this means that for every $\epsilon > 0$, there exists N such that for $y, z \geq N$,

$$\left| \int_y^z \frac{\vartheta(x) - x}{x^2} \, dx \right| < \epsilon.$$

(It is much easier to prove that these integrals are bounded; see exercises.) To then deduce $\vartheta(x) \sim x$, suppose that there exists $\lambda > 1$ such that $\vartheta(x) \geq \lambda x$ for arbitrarily large x. Since ϑ is nondecreasing, it then follows that for any such x,

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2} \, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2} \, dt = \int_1^\lambda \frac{\lambda - t}{t^2} \, dt > 0,$$

contradiction. Likewise, if there exists $\lambda < 1$ such that $\vartheta(x) \leq \lambda x$ for arbitrarily large x, then such x satisfy

$$\int_{\lambda x}^x \frac{\vartheta(t) - t}{t^2} \, dt \leq \int_{\lambda x}^x \frac{\lambda x - t}{t^2} \, dt = \int_\lambda^1 \frac{\lambda - t}{t^2} \, dt < 0,$$

contradiction.

4 The Tauberian argument

We have thus reduced the prime number theorem to the convergence of the integral (1); we turn to this next. Consider the function $\Phi(s) = -\zeta'(s)/\zeta(s)$; from the log-product representation for ζ, using partial summation as in Theorem 1, and substituting $x = e^t$, we find

$$\Phi(s) = \sum_p (\log p) p^{-s} + \sum_p \sum_{n=2}^\infty (\log p) p^{-ns}$$

$$= s \int_1^\infty \vartheta(x) x^{-s-1} \, dx + s \int_1^\infty \vartheta(x) \left(\sum_{n=2}^\infty n x^{-ns-1} \right) dx$$

$$= s \int_0^\infty e^{-st} \vartheta(e^t) \, dt + s \int_0^\infty \frac{2e^{-2st} - e^{-3st}}{(1 - e^{-st})^2} \vartheta(e^t) \, dt$$

4

Define the functions

$$f(t) = \vartheta(e^t)e^{-t} - 1$$

$$g(z) = \frac{\Phi(z+1)}{z+1} - \frac{1}{z};$$

by the above,

$$g(z) = \int_0^\infty f(t)e^{-zt}\,dt + \int_0^\infty \frac{2e^{-2(z+1)t} - e^{-3(z+1)t}}{(1 - e^{-(z+1)t})^2}\vartheta(e^t)\,dt.$$

Right now, we know that the integral defining $g(z)$ makes sense for $\mathrm{Re}(z) > 0$, but we will deduce (1) (after substituting $x = e^t$) and hence the prime number theorem if we can obtain convergence of $g(z)$ in the case $z = 0$. (Note that the second term converges absolutely for $z = 0$, so we only have to worry about the first term.)

The idea is to do this by leveraging complex function-theoretic information about Φ; this sort of operation is known as a *Tauberian argument*. To be precise, by what we know about ζ, $\Phi(s)$ is meromorphic on $\mathrm{Re}(s) > 0$, with a simple pole at $s = 1$ of residue 1 and no other poles in $\mathrm{Re}(s) \geq 1$. It follows that f and g satisfy the conditions of the following theorem.

Theorem 3 (Newman). *Let $f : [0, +\infty) \to \mathbb{R}$ be a bounded, locally integrable function, and define $g(z) = \int_0^\infty f(t)e^{-zt}\,dt$; note that this integral converges absolutely uniformly for $\mathrm{Re}(z) \geq \epsilon$ for any $\epsilon > 0$. Suppose that $g(z)$ extends to a holomorphic function on a neighborhood of $\mathrm{Re}(z) \geq 0$. Then $\int_0^\infty f(t)\,dt$ exists and equals $g(0)$.*

Proof (Zagier, after Newman). For $T > 0$, put $g_T(z) = \int_0^T f(t)e^{-zt}\,dt$; each function g_T is entire, and we want $\lim_{T\to\infty} g_T(0) = g(0)$.

For R large (but fixed until further notice), let C be the boundary of the region

$$\{z \in \mathbb{C} : |z| \leq R, \quad \mathrm{Re}(z) \geq -\delta\}$$

for some $\delta = \delta(R) > 0$ chosen small enough that C lies inside the domain on which g is holomorphic. By the Cauchy integral theorem,

$$g(0) - g_T(0) = \frac{1}{2\pi i}\int_C (g(z) - g_T(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}; \tag{2}$$

namely, the only pole of the integrand is a simple pole at $z = 0$, so we simply pop out the residue there.

To bound the right side of (2), we separate the contour of integration C into

$$C_+ = C \cap \{z \in \mathbb{C} : \mathrm{Re}(z) \geq 0\}$$
$$C_- = C \cap \{z \in \mathbb{C} : \mathrm{Re}(z) \leq 0\}.$$

Remember that we assumed f is bounded; choose $B > 0$ so that $|f(t)| \leq B$ for all t. For $\text{Re}(z) > 0$ with $|z| = R$, we have

$$
\begin{aligned}
|g(z) - g_T(z)| &= \left| \int_T^\infty f(t)e^{-zt}\, dt \right| \\
&\leq B \int_T^\infty |e^{-zt}|\, dt \\
&= \frac{Be^{-\text{Re}(z)T}}{\text{Re}(z)}
\end{aligned}
$$

and

$$
\left| e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z} \right| = e^{\text{Re}(z)T} \frac{2\,\text{Re}(z)}{R^2}.
$$

Since the length of the contour is at most $2\pi R$, the contribution over C_+ to (2) is bounded in absolute value by

$$
\frac{1}{2\pi}(2\pi R) \frac{Be^{-\text{Re}(z)T}}{\text{Re}(z)} e^{\text{Re}(z)T} \frac{2\,\text{Re}(z)}{R^2} = \frac{2B}{R}.
$$

Over C_-, we separate the integral into integrals involving g and g_T. Since g_T is entire, its integral over C_- can instead be calculated over the semicircle $C'_- = \{z \in \mathbb{C} : |z| = R, \text{Re}(z) \leq 0\}$. Since for $\text{Re}(z) < 0$ we have

$$
\begin{aligned}
|g_T(z)| &= \left| \int_0^T f(t)e^{-zt}\, dt \right| \\
&\leq B \int_{-\infty}^T |e^{-zt}|\, dt \\
&= \frac{Be^{-\text{Re}(z)T}}{|\text{Re}(z)|},
\end{aligned}
$$

as above we bound this contribution to (2) by $2B/R$.

Finally, we consider the contribution to (2) from g over C_-; we are going to show that this contribution tends to 0 as $T \to \infty$. By parametrizing the contour, we can write

$$
\frac{1}{2\pi i} \int_{C_-} g(z)e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} = \int_0^1 a(u)e^{b(u)T}\, du,
$$

where $a(u)$ and $b(u)$ are continuous, and $\text{Re}(b(u)) < 0$ for $0 < u < 1$; the key point is that a does not depend on T, so as $T \to \infty$ the integrand tends to 0 pointwise except at the endpoints. Since the integrands are all bounded, Lebesgue's dominated convergence theorem implies that the integral tends to 0 as $T \to \infty$. (Again, I'm being more explicit with the analysis than I will be in general.)

We conclude that

$$
\limsup_{T \to \infty} |g(0) - g_T(0)| \leq \frac{4B}{R};
$$

since R can be chosen arbitrarily large, this yields the desired result. $\qquad\square$

You might be thinking at this point that if one knew g extended to a holomorphic function on a region a bit larger than $\mathrm{Re}(s) \geq 0$, then maybe one could prove something about the rate of convergence of the integral $\int_0^\infty f(t)\,dt$. In particular, if one can exclude zeroes of ζ in some region beyond the line $\mathrm{Re}(s) = 1$, one should correspondingly get a prime number theorem with an improved error term. We will see that this is correct in a subsequent unit, at least if we replace the approximation $\pi(x) \sim x/(\log x)$ with Gauss's approximation $\pi(x) \sim \mathrm{li}(x)$ (see exercises).

Historical aside: the Erdős-Selberg method

About 40 years after the original proof, Erdős and Selberg gave so-called elementary proofs of the prime number theorem, which do not use any complex analysis. The key step in Selberg's proof is to give an elementary proof of the bound

$$|R(x)| \leq \frac{1}{\log x} \int_1^x |R(x/t)|\,dt + O\left(x\frac{\log\log x}{\log x}\right), \tag{3}$$

where $R(x) = \vartheta(x) - x$; I will probably say something about this result in the section on sieving.

Using (3) and the fact that

$$\int_1^x \frac{R(t)}{t^2}\,dt = O(1) \tag{4}$$

(much easier than the convergence of the integral; see exercises), one then produces $0 < c < 1$ such that if there exists $\alpha > 0$ such that $|R(x)| < \alpha x$ for x large, then also $|R(x)| < \alpha c x$ for x large. I find this step somewhat unenlightening; if you must know the details, see A. Selberg, An elementary proof of the prime number theorem, *Annals of Math.* **50** (1949), 305–313. Or see Chapter XXII of Hardy-Wright, or Nathanson's *Elementary Methods in Number Theory*.

Exercises

1. Prove that there exists a positive constant γ such that

$$\sum_{i=1}^n \frac{1}{i} - \log n = \gamma + O(n^{-1}),$$

by comparing the sum to a Riemann sum for $\int_1^n \frac{1}{x}\,dx$. The number γ is called *Euler's constant*, and it is one of the most basic constants in analytic number theory. However, since it is defined purely analytically, we remain astonishingly ignorant about it; for instance, γ is most likely irrational (even transcendental) but no proof is known.

2. Let $d(n)$ denote the number of divisors of $n \in \mathbb{N}$. Prove that
$$\sum_{i=1}^{n} d(i) = n \log n + (2\gamma - 1)n + O(n^{1/2}),$$
by estimating the number of lattice points in the first quadrant under the curve $xy = n$.

3. (Mertens) Fix $t \in \mathbb{R}$ nonzero. Prove that the function
$$Z(s) = \zeta(s)^3 \zeta(s + it)^4 \zeta(s + 2it)$$
extends to a meromorphic function on $\mathrm{Re}(s) > 0$. Then show that if $s \in \mathbb{R}$ and $s > 1$, then $\log|Z(s)| = \mathrm{Re}(\log Z(s))$ can be written as a series of nonnegative terms, so $|Z(s)| \geq 1$.

4. Use the previous exercise to prove that $\zeta(s)$ has no zeroes on the line $\mathrm{Re}(s) = 1$.

5. (Chebyshev) Prove that
$$\prod_{n < p \leq 2n} p \leq 2^{2n}$$
by considering the central binomial coefficient $\binom{2n}{n}$. Then deduce that $\vartheta(x) = O(x)$.

6. Let k be a positive integer. Prove that for any $c > 0$, if we write C_R for the straight contour from $c - iR$ to $c + iR$, then
$$\lim_{R \to \infty} \frac{1}{2\pi i} \int_{C_R} \frac{x^s \, ds}{s(s+1)\cdots(s+k)} = \begin{cases} \frac{1}{k!}\left(1 - \frac{1}{x}\right)^k & x \geq 1 \\ 0 & 0 \leq x \leq 1. \end{cases}$$
(Hint: use a contour-shifting argument.)

7. (Gauss) Define the *logarithmic integral function*
$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}.$$
(Warning: there is some disagreement in the literature about what lower limit of integration to use.) Prove that $\mathrm{li}(x) \sim x/(\log x)$, so that the prime number theorem is equivalent to $\pi(x) \sim \mathrm{li}(x)$. In fact, Gauss noticed empirically, and we will prove later, that $\mathrm{li}(x)$ gives a somewhat better approximation to $\pi(x)$ than $x/(\log x)$.

8. Using the identity
$$\sum_{n \leq x} \log n = \sum_{i=1}^{\infty} \sum_{p : p^i \leq x} \left\lfloor \frac{x}{p^i} \right\rfloor \log p,$$
prove that
$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1),$$
then deduce (4) by partial summation.