MATH 539 NOTES—THURSDAY, MARCH 19, 2020

Asymptotic formula for $N(T)$. On Tuesday we learned that $N(T)$, the counting function for the nontrivial zeros of $\zeta(s)$ of height between 0 and T, has an exact formula given by *Theorem 14.1*:

$$N(T) = \frac{1}{\pi} \arg \Gamma\left(\frac{1}{4} + \frac{iT}{2}\right) - \frac{T}{2\pi} \log \pi + S(T) + 1,$$

where

$$S(T) = \frac{1}{\pi} \arg \zeta\left(\frac{1}{2} + iT\right). \tag{1}$$

The Gamma function is so regularly behaved, as it turns out, that this formula can be converted into an asymptotic formula with an extremely good error term, given by *Corollary 14.2*:

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi e} + \frac{7}{8} + S(T) + O\left(\frac{1}{T}\right). \tag{2}$$

(I've intentionally written the main terms in a slightly different form from the book, so that you see both forms. Note that the left-hand side has jump discontinuities of integer size; convince yourself that the right-hand side does as well.) And indeed, one can get a decent upper bound for $S(T)$, and so this asymptotic formula can be simplified (*Corollary 14.3*) if we don't need such a strong error.

As a preliminary step, read Lemma 12.3 and its proof. Between the statement and proof, there is a remark on complex logarithms similar to the one from the notes from Tuesday.

You are now ready to derive Corollary 14.2 from Theorem 14.1. Note that equation (14.3) (Stirling's formula) is relevant because $\arg \Gamma(z)$ is the imaginary part of $\log \Gamma(z)$. The details of this (short) derivation are worth going through carefully. *It will then be immediate to derive Corollary 14.3 from previous results.*

Strategy for verifying RH to finite heights. We have heard statements like "The Riemann hypothesis has been verified up to height H" (for some impressive numbers H, but for this discussion we can even think of $H = 100$ for example). As we mentioned in class, it's not immediately clear how we could verify such a statement: not only are zeros of complex-valued functions nontrivial to find at all, but we would have to be convinced that we've found them all.

Nevertheless, the zeta function is so well-understood in many ways that we can actually accomplish this task. Here is the general strategy (of course, actual computational implementations are much more complicated in an effort to gain as much speed as possible): we

- Make a function that can evaluate the completed zeta function $\xi(s)$ to however much precision you need. Not trivial (especially for fast calculation), but definitely doable.
- Note that the combination of the functional equation and Schwarz reflection gives us the identity $\xi(1 - \bar{s}) = \overline{\xi(s)}$. In particular, $\xi(s)$ is *real-valued* on the critical line $\sigma = \frac{1}{2}$.
- That means we can sample $\xi(s)$ at many values on the critical line and look for sign changes; every time we have a sign change between two sampled values, it is guaranteed that $\xi(s)$ (and hence $\zeta(s)$) has at least one zero on the critical line between the two sample points, by the usual intermediate value theorem.

- In this way, for example, we can show that $\zeta(s)$ has *at least* 29 zeros up to height $H = 100$. (There might be multiple zeros in those sampled intervals or zeros off of the critical line; but we can be sure that there are at least 29 zeros.)

Then, independently: we

- Make a function that can evaluate the argument of the zeta function, and hence equation (1), to a reasonable precision. Again, not trivial but definitely doable.
- Derive a version of equation (2) with an explicit constant, that is, with an error term that is at most C/T in absolute value for some explicit $C > 0$. (Try doing it yourself, if only to convince yourself how helpful our O-notation is. . . .)
- Then, simply calculate the right-hand side of (that explicit version of) equation (2). Note the answer must be an integer, so we don't even need our calculations to be all that precise!
- In this way, for example, we calculate $N(100)$ and the answer "just happens" to be 29. Therefore we know that there are no zeros other than the ones we found on the critical line (and, for that matter, that all those zeros are simple; it is indeed also conjectured that all zeros of $\zeta(s)$ are simple zeros). We just verified the Riemann hypothesis up to height 100—fantastic!

Now, we make a big jump in topics to something with a more algebraic feel. Our ultimate goal is to examine arithmetic progressions (that is, residue classes modulo q for various integers q) and see how primes are distributed within them. To do so, we need to understand "group characters"—fortunately, in the simplest possible situation, namely finite abelian groups.

As a preliminary, look through the beginning of Section 4.1, up through equation (4.4) and the following sentence. We won't directly use this material, but it has parallels to the material we are about to learn, and also this material is mathematically fundamental enough that it's good for you to have familiarity with it. (If you're really interested, you can read the rest of Section 4.1, as it uses only techniques that you learned earlier in the course; in particular, Theorem 4.1 is a generalization of problem 3 from Homework #1.)

Characters of finite abelian groups. A (multiplicative group) *character* is a group homomorphism with $\mathbb{C}^*$ as the codomain. For example, the group homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{C}^*$ that sends a generator of $\mathbb{Z}/4\mathbb{Z}$ to i is a character, as is the map that sends all elements to 1; indeed, it is easy to write down all characters on cyclic groups. Moreover, the set of characters, $\widehat{G}$, on any given group G itself forms a group under pointwise multiplication; and one can show that the character group $\widehat{G_1 \times G_2}$ of $G_1 \times G_2$ is simply $\widehat{G}_1 \times \widehat{G}_2$. Consequently, we can give a complete description of the character group of any finite abelian group (remembering that any such group can be written as the direct product of cyclic groups, via either its primary decomposition or its invariant factor decomposition).

At this point, read from Lemma 4.2 to the remark following the proof of Theorem 4.4.

Dirichlet characters. We now focus attention on groups of the form $M_n = (\mathbb{Z}/q/Z)^*$ (the multipicative group modulo q, which is a finite abelian group of order $\phi(q)$) and their character groups. In particular, for any such character $\chi \in \widehat{M_q}$, there is a closely related function $\chi\colon \mathbb{Z} \to \mathbb{C}$ (we abuse notation by writing χ for both functions), called a *Dirichlet character* (mod q), whose value

on a equals $\chi(a+q\mathbb{Z})$ if $(a,q)=1$ and equals 0 otherwise. Equivalently (as you should verify), a Dirichlet character (mod q) is a totally multiplicative function on the integers with period q that is supported on the integers coprime to q. For example, the function χ given by

$$\{\dots,\chi(-1),\chi(0),\chi(1),\chi(2),\chi(3),\chi(4),\chi(5),\chi(6),\chi(7),\chi(8),\chi(9),\chi(10),\dots\}$$
$$=\{\dots,-1,0,1,i,-i,-1,0,1,i,-i,-1,0,\dots\}$$

is a Dirichlet character (mod 5), while

$$\{\dots,\chi(-1),\chi(0),\chi(1),\chi(2),\chi(3),\chi(4),\chi(5),\chi(6),\chi(7),\chi(8),\chi(9),\chi(10),\chi(11),\chi(12),\dots\}$$
$$=\{\dots,-1,0,1,0,0,0,-1,0,1,0,0,0,-1,0,\dots\}$$

is a Dirichlet character (mod 6). For any $q\in\mathbb{N}$, the function

$$\chi_0(a)=\begin{cases}1, & \text{if } (a,q)=1,\\ 0, & \text{if } (a,q)>1\end{cases}$$

is a Dirichlet character, called the *principal character* (mod q) (it is the identity in the group $\widehat{M_n}$).

Read the first long paragraph in Section 4.2 to reinforce this discussion.

Miscellaneous remarks:

- By Euler's theorem, all the nonzero values of a Dirichlet character (mod q) are $\phi(q)$th roots of unity, since for $(a,q)=1$ we have $\chi(a)^{\phi(q)}=\chi(a^{\phi(q)})$ (by total multiplicativity) and $\chi(a^{\phi(q)})=\chi(1)$ (by periodicity) and $\chi(1)=1$ (by properties of group homomorphisms).
- A similar argument shows that $\chi(q-1)=\chi(-1)=\pm1$ for any Dirichlet character (mod q).
- As it turns out, the Legendre symbol $\chi(n)=(\frac{n}{p})$ is a Dirichlet character (mod p), and its extensions (the Jacobi symbol and the Kronecker symbol) are also Dirichlet characters. Moreover, by quadratic reciprocity, the Kronecker symbol $\chi(n)=(\frac{a}{n})$ is also a Dirichlet character (mod $4a$), and it turns out that every real-valued character can be written in essentially this way.

Orthogonality relations. For many mathematical objects, the properties that they satisfy are much more important than their actual definition. (The Möbius function is an excellent example: the fact that $\sum_{d|n}\mu(d)$ detects when $n=1$ is far more important than the definition of $\mu(n)$ in terms of the factorization of n. For that matter, the properties that the set of real numbers satisfies is incredibly more important than the definitions of that set in terms of Dedekind cuts or Cauchy sequences!) While we can construct Dirichlet characters by listing all their values, it's much more useful to have some global relations that Dirichlet characters satisfy.

The most important relations satisfied by Dirichlet characters are the *orthogonality relations*, which are equations (4.14) and (4.15) in the textbook.

Read Corollary 4.5 and commit it to memory! You can also skim the remainder of Section 4.2 enough to understand that there is a known procedure for writing down all Dirichlet characters (mod q) *for any* $q\in\mathbb{N}$.