MATH 539 NOTES—TUESDAY, APRIL 7, 2020

This is the "fun last lecture", with the theme being open problems and conjectures in analytic number theory, and partial progress towards those conjectures. I'll start with material most closely related to what we learned in this course, although I can't resist drifting a little farther afield by the end of these notes.

To be clear, let's make the convention that any statement I label as a "conjecture" in these notes is not yet proved.

I won't be giving you any specific reading for these topics, but most of them are very searchable online (indeed many of the conjectures have their own Wikipedia pages). Searching Terry Tao's blog will reveal several interesting articles on these topics.

Gaps between primes. We are very interested in how far apart consecutive primes can get. To obtain upper bounds on the size of the largest possible prime gaps, many theorems of the form

$$\text{There is always a prime between } x \text{ and } x + f(x)$$

have been proved for various functions $f(x)$:

- Bertrand's postulate is the statement that we can take $f(x) = x$, and Chebyshev's results (Section 2.2) show that we can take $f(x) = \alpha x$ for a constant α rather less than 1 for large x. (We certainly can't take $\alpha < \frac{5}{3}$ for all x, since there are no primes between 3 and 5.)
- The prime number theorem, with the error term we proved in class (Theorem 6.9), implies that we can take $f(x) \ll x \exp(-c\sqrt{\log x})$ for some absolute constant $c > 0$. The derivation of this from the prime number theorem is simple: if not, then $\theta(x + f(x)) - \theta(x) = 0$, but the difference is $f(x) + O(\cdots)$, which cannot be 0 when $f(x)$ is large enough.
- Analytic methods that treat differences like $\theta(x + f(x)) - \theta(x)$ directly, rather than simply $\theta(x)$ itself, can get better upper bounds for $f(x)$. Several authors have successively improved the best upper bounds for $f(x)$; the strongest such result is by Baker/Harman/Pintz in 2001, where they proved that one can take $f(x) \ll x^{0.525}$.
- If we assume the Riemann hypothesis, as in Theorem 13.1, then the simple method of examining $\theta(x + f(x)) - \theta(x)$ shows that we can take $f(x) \ll x^{1/2}(\log x)^2$.
- Legendre conjectured that there is always a prime between consecutive squares n^2 and $(n+1)^2$. If we set $x = n^2$, then $(n+1)^2 = x + (2\sqrt{x} + 1)$; so Legendre's conjecture is morally equivalent to the conjecture that we can take $f(x) \ll \sqrt{x}$. Note that we don't even know how to prove this assuming the Riemann hypothesis!

On the other hand, there are several ways of getting lower bounds for how small we can take $f(x)$, by constructing long intervals free of primes:

- The undergraduate construction $n! + 2, n! + 3, \ldots, n! + n$ produces many consecutive composite numbers; if we take $x = n! + 1$, then Stirling's formula implies that $n \approx \log x / \log\log x$. Therefore any valid function $f(x)$ must be $\gg \log x / \log\log x$.
- The prime number theorem says that the *average* gap between primes up to x is $\log x$, and therefore at least one gap must be that large by the pigeonhole principle. Therefore any valid $f(x)$ must be $\gg \log x$. In 1931, Westzynthius improved this by showing that $f(x)$ must be taken so that $f(x)/\log x \to \infty$.

- Rankin showed in 1938 that any valid $f(x)$ must be
$$\gg \frac{(\log x)(\log\log x)(\log\log\log\log x)}{(\log\log\log x)^2}.$$
Despite the extremely unusual shape of this function, this order of magnitude was the barrier for a very long time. Rankin showed that the implicit constant can be taken to be (almost) e^{C_0}, where C_0 is Euler's constant, and by 1997 this had been improved only to $2e^{C_0}$. Indeed Erdős, who would often assign (usually modest) dollar amounts to important conjectures and barriers in mathematics as prizes, offered a $10,000 prize to anyone who could obtain a better lower order of magnitude for $f(x)$ (equivalently, that the implicit constant above can be taken arbitrarily large); this is the largest prize amount he ever offered.

  (By the way, you should definitely go read about Paul Erdős—he was one of the most prolific mathematicians in history and a unique character.)
- Five mathematicians, Ford/Green/Koukoulopoulos/Maynard/Tao, finally overcame this barrier in 2014, and in 2015 they showed that any valid $f(x)$ must be
$$\gg \frac{(\log x)(\log\log x)(\log\log\log\log x)}{\log\log\log x}.$$
In the spirit of Erdős, apparently Tao has offered a new $10,000 prize to anyone who could obtain an even better lower order of magnitude for $f(x)$ (equivalently, that this new implicit constant can be taken arbitrarily large).

The accepted conjecture, based on probabilistic heuristics, is that the right order of magnitude of $f(x)$ is $\asymp (\log x)^2$. In particular, note how far away the upper-bound results are from this conjectured truth, even assuming the Riemann hypothesis.

Note that all of these results are about maximal prime gaps (that is, how large can these gaps occasionally be). The corresponding results for minimal prime gaps (that is, how small can these gaps occasionally be) is related to the twin primes conjecture, which we'll discuss later in these notes.

The least prime in an arithmetic progression. Let $q \geq 2$ and a be integers with $(a, q) = 1$. We saw in class (Corollary 4.10) that there are infinitely many primes congruent to $a \pmod q$ (equivalently, in the arithmetic progression $\{qn + a : n \in \mathbb{N}\}$). There is a prime number theorem for arithmetic progressions, which for any fixed q says that $\pi(x; q, a) \sim \mathrm{li}(x)/\phi(q)$, so that the $\phi(q)$ reduced residue classes (mod q) all contain asymptotically $1/\phi(q)$ of the primes. However, in practice it is usually important to know how uniform this result is in q, or eqivalently how the error term in this asymptotic formula depends on the relationship between x and q. See Corollary 11.21 (Siegel's theorem) for the state of the art at this time.

One tidy way of representing the importance of this relationship between x and q is to ask how long we must wait before we find the first prime in any given arithmetic progression. In other words, if we let $p(q, a)$ denote the smallest prime that is congruent to $a \pmod q$, how large can $p(q, a)$ be? Note that if $0 < a < q$ is itself not prime than $p(q, a) \geq q + a$ at the very least, so we can't expect any upper bound that is less than q itself.

- It follows from Corollary 11.21 (take $A = 1/\varepsilon$) that $p(q, a) \ll_\varepsilon e^{q^\varepsilon}$ for any $\varepsilon > 0$. But note that this upper bound grows faster than any power of q.

- It was therefore a breakthrough when Linnik proved in 1944 that there exists a constant L such that $p(q,a) \ll q^L$. (As above, one can get better results by setting up the analytic arguments to directly detect the first primes in an arithmetic progression rather than derive such bounds from an asymptotic formula for x large.)
- Pan, in 1957, was the first person to work out a specific valid value for L, namely $L = 10{,}000$. Several authors established progressively smaller valid values for L.
- In 1992, Heath–Brown showed that $L = 5.5$ is valid; pushing those techniques further in 2001, Xylouris showed that $L = 5$ is valid, which is the state of the art.
- The generalized Riemann hypothesis, which is the conjecture that all nontrivial zeros of all Dirichlet L-functions lie on the line $\sigma = \frac{1}{2}$, implies that $L = 2 + \varepsilon$ is valid for any $\varepsilon > 0$; indeed, Lamzouri/Li/Soundararajan showed in 2016 that $p(q,a) \le (\phi(q) \log q)^2$ for $q > 3$ if the generalized Riemann hypothesis holds.
- The accepted conjecture, again on probabilistic grounds, is that $L = 1+\varepsilon$ should be valid—that is, that $p(q,a) \ll_\varepsilon q^{1+\varepsilon}$. It has been shown that this upper bound holds for "almost all" arithmetic progressions $a \pmod q$ in a suitable sense.

Zero-free regions for $\zeta(s)$. We have seen that the locations of the nontrivial zeros of $\zeta(s)$ are intimately connected with the distribution of primes, especially their real parts as those correspond to the powers of x that appear in the infinite sum in the explicit formula, equation (12.1).

- We saw the classical zero-free region for $\zeta(s)$, proved by de la Vallée–Poussin in 1899, which tells us that there exists an absolute constant $c > 0$ such that $\zeta(s) \neq 0$ for $\sigma \ge 1 - c/\log \tau$.
- A wider zero-free region was established by Vinogradov/Korobov in the 1950s: there exists $c > 0$ such that $\zeta(s) \neq 0$ for $\sigma \ge 1 - c/(\log \tau)^{2/3}(\log\log \tau)^{1/3}$. This leads to a somewhat better error term in the prime number theorem, with $x \exp(-c\sqrt{\log x})$ replaced by $x \exp(-c(\log x)^{3/5}/(\log\log x)^{1/5})$. Both of these results are today's state of the art.
- The main conjecture on this topic, of course, is the Riemann hypothesis, that $\zeta(s) \neq 0$ for $\sigma > \frac{1}{2}$. It's worth pointing out that we still can't establish a "zero-free strip" of constant width, that is, we still can't prove that there exists $\Theta < 1$ such that $\zeta(s) \neq 0$ for $\sigma > \Theta$. (As we saw in class, a zero-free strip would lead to a savings of a power of x in the error term of the asymptotic formula for $\pi(x)$ and its relatives.)

Estimates and moments for $\zeta(\frac{1}{2} + it)$. When proving the Hadamard product for $\xi(s)$, we got a glimpse of the importance of knowing how fast $\zeta(s)$ grows as $t \to \infty$, say. It turns out that such bounds are both central and useful in analytic number theory. When $\sigma > 1$ or $\sigma < 0$, we know essentially everything we want to know about upper bounds for $|\zeta(s)|$ as $t \to \infty$; so the main interest is in bounds inside the critical strip $0 \le \sigma \le 1$. It turns out that considering just the critical line $\sigma = \frac{1}{2}$ is already a robust topic.

- In class we showed, or at least used, the fact (Corollary 1.17) that $\zeta(\frac{1}{2} + it) \ll \tau^{1/2}$.
- A clever but simple convexity argument (Lindelöf 1908) shows that $\zeta(\frac{1}{2} + it) \ll \tau^{1/4}$. This type of argument was quickly generalized, and several related results of this type are collectively now called the Phragmén–Lindelöf principle; it essentially says that the maximum modulus principle, that the modulus of an analytic function in the interior of a bounded region inside $\mathbb{C}$ cannot exceed the maximum modulus of the function on the

boundary of the region, can be extended to some unbounded regions as long as the function is known not to grow too ridiculously fast.

- Over the years there have been many improvements to the exponent $\frac{1}{4}$ in the previous upper bound (such improvement are called "subconvexity results"). The state of the art, due to Bourgain in 2017, is that $\zeta(\frac{1}{2}+it) \ll \tau^{0.1548}$.
- The standard conjecture, known as the Lindelöf hypothesis, is that $\zeta(\frac{1}{2}+it) \ll_\varepsilon \tau^\varepsilon$. It is known that this conjecture follows from the Riemann hypothesis, and therefore it is sometimes considered an intermediate conjecture between our current knowledge and RH. If the Lindelöf hypothesis is true, then we could deduce (using the Phragmén–Lindelöf principle) the best-possible estimates for the growth of $\zeta(s)$ on every vertical line, namely the conjecture that
$$|\zeta(s)| \ll_\varepsilon \begin{cases} \tau^\varepsilon, & \text{if } \sigma \geq \frac{1}{2}, \\ \tau^{1/2-\sigma+\varepsilon}, & \text{if } \sigma \leq \frac{1}{2}. \end{cases}$$
- The Lindelöf hypothesis is equivalent to the following upper bounds for even moments of $\zeta(s)$ on the critical line: we conjecture that for every $k \in \mathbb{N}$,
$$\int_0^T |\zeta(\sigma+it)|^{2k}\,dt \ll_{k,\varepsilon} T^{1+\varepsilon}. \tag{1}$$
This was proved for $k=1$ by Littlewood, and for $k=2$ by Ingham in 1926, but it is still open for $k \geq 3$. We'll say more about these moments in the next section of these notes.

Ordinates of zeros of $\zeta(s)$. I want to mention a few more problems connected more to the imaginary parts of the zeros of $\zeta(s)$.

- As we learned in class, we do have very strong information concerning $N(T)$, the number of zeros of $\zeta(s)$ satisfying $0 < \gamma < T$. (Note that this information is indifferent to the real parts of these zeros.) These zeros grow slowly denser, so that the number of zeros near height T has order of magnitude $\log T$.
- In 1973, Montgomery made a "pair correlation conjecture" regarding the joint spacing of pairs of nontrivial zeros of $\zeta(s)$, essentially giving a conjectured asymptotic formula for the number of pairs of zeros up to height T that are within $\lambda/\log T$ of each other, as a function of λ. Upon hearing this, Dyson remarked that the proposed asymptotic formula was actually the same as the formula established for the pair correlation of eigenvalues of random Hermitian matrices.
- The moments of $\zeta(\frac{1}{2}+it)$ on the left-hand side of equation (1) should have asymptotic formulas, but even the leading constants of those formulas were hard to pin down. However, using the connection to random matrices first noted by Dyson, in 2000 Keating/Snaith proposed very specific conjectures for these asymptotic formulas, of the form
$$\int_0^T |\zeta(\sigma+it)|^{2k}\,dt \sim T P_k(\log T) + O(T^{1-\varepsilon})$$
where P_k is an explicit polynomial of degree k^2 that arises in large part from random matrix theory.
- We alluded briefly in our course to how convenient it would be if the imaginary parts of the nontrivial zeros of $\zeta(s)$ were linearly independent over the rational numbers; this is a conjecture, albeit one more based on general principles than on concrete partial evidence.

For example, as (our own) Silberman pointed out, we can't yet even disprove the (extremely unlikely) assertion that *all* of the zeros of $\zeta(s)$ have rational imaginary part.

Irrationality and transcendence. Several quantities associated with $\zeta(s)$ have connections with Diophantine equations, in particular with irrationality and transcendence. (Recall that a complex number is *algebraic* if it is the root of a nonconstant polynomial with integer coefficients, and *transcendental* otherwise. Clearly every transcendental number is irrational, since any rational number $\frac{a}{b}$ is the root of $bx - a$.)

- The existence of irrational numbers is usually attributed to Hippasus in the 5th century BC.
- In the 1730s, Euler proved that $\zeta(2k)$ is a rational multple of π^{2k} for all $k \in \mathbb{N}$. (I couldn't figure out whether Euler knew the exact rational numbers involved yet.)
- Euler proved that e is irrational (as well as e^2) in 1737. Lambert proved that π is irrational in 1761.
- Liouville gave a criterion/construction in 1844 showing that transcendental numbers exist.
- It wasn't until 1874 that Cantor's seminal set theory paper revealed that "most" numbers are transcendental.
- Hermite proved in 1873 that e is transcendental. Using similar methods, Lindemann established the transcendence of π in 1882. In particular, the transcendence of π implies that π^{2k} is transcendental, and hence that $\zeta(2k)$ is transcendental for every $k \in \mathbb{N}$.

In contrast to this result aboutvalues of $\zeta(s)$ at positive even integers, we suspect that there is no nice relationship between values $\zeta(s)$ at positive odd integers and any other quantities we know. In particular, it is definitely conjectured that both $\zeta(2k+1)$ and $\zeta(2k+1)/\pi^{2k+1}$ are irrational for all $k \geq 1$ (and I suspect most people would agree with the conjecture that these quantities are in fact transcendental).

- It wasn't until 1978 that the irrationality of $\zeta(3)$ was proved by Apéry.
- Rivoal showed in 2000 that infinitely many of the numbers $\zeta(3), \zeta(5), \zeta(7), \ldots$ are irrational. Soon thereafter, in 2001, those ideas were refined by Zudilin to show, for example, that one of the four numbers $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ is irrational.
- Euler's constant C_0 is conjectured to be irrational. (This can morally be considered the "$\zeta(1)$" case, since $\zeta(s) - 1/(s-1) \to C_0$ as $s \to 1$.)

I can't resist sharing some other conjectures about irrationality and transcendence, even though they have little to do with the material in this course.

- There are many theorems that imply results of the shape "in this list of numbers (all of which we suspect are transcendental), at least one of them must be transcendental". Some of these theorems are extremely deep, but here is a simple proof that at least one of $\pi + e$ and πe is transcendental: if both $\pi + e$ and πe were algebraic, then the polynomial $P(x) = x^2 - (\pi + e)x + (\pi e) = (x - \pi)(x - e)$ would have algebraic coefficients, hence its roots would be algebraic, a contradiction.
- Our knowledge about combinations of π and e is very meager. It is conjectured that all of the constants $\pi + e$, $\pi - e$, πe, π/e, π^π, e^e, π^e, 2^e, $\ldots$ are irrational. (Indeed they are conjectured to be transcendental.)

- We actually know that the specific combination e^π is transcendental, from a result called the Gelfond–Schneider theorem (1934), which says that if α and β are both algebraic then α^β must be transcendental, "except for obvious cases". In this case, $(e^\pi)^i = -1$ shows that e^π cannot be algebraic.

The twin primes and Goldbach conjectures and generalizations. Earlier we discussed the maximal gaps between primes; here we discuss minimal gaps between primes. The twin primes conjecture is the conjecture that there are infinitely many primes p such that $p+2$ is also prime; if true, this would of course settle the question of minimal prime gaps (since a gap of 1 occurs only once; our phrase "minimal gap" refers to gap sizes that occur infinitely often). However, for the majority of my life, we couldn't even disprove the possibility that the sequence of prime gaps tended to infinity!

- As before, the prime number theorem implies that the average gap among primes up to x is $\log x$, and therefore the minimal gap is at most $\log x$. In other words, there are infinitely many intervals of the form $(x, x + \log x)$ that contain primes.
- For about a century, the best we could do was to improve the constant in front of that order of magnitude $\log x$; the best result of this type was by Maier in 1988, showing that the minimal gap is at most $0.2485 \log x$.
- Finally in 2005, Goldston/Pintz/Yildirim showed that the constant in front of $\log x$ could be taken arbitrarily small. (There is actually a great human story here: Goldston/Yildirim had a paper claiming this result a few years earlier; the manuscript earned them a lot of positive attention until a flaw was found in that earlier paper, which had to be retracted. Fortunately, they managed to work their way back to the excellent result. Goldston, who is a fantastic storyteller in any circumstance, has certainly talked about this roller-coaster experience; it would be worth reading about or listetning to if you can find anything online.) In 2007 they improved the result on minimal prime gaps to $C\sqrt{\log x}(\log\log x)^2$ for some constant $C > 0$.
- It was completely unexpected when in 2013, Zhang and then independently Maynard and Tao announced proofs that the minimal prime gap was *bounded*. Zhang showed that there were infinitely many pairs of primes whose difference was at most $70{,}000{,}000$. Subsequently Maynard, Tao, and a Polymath project (also worth looking up) lowered this upper bound on the minimal gap to 246.

Despite not being able to prove conjectures like the twin primes conjecture, we have a very good idea of what should be true, coming once again from thoughtful probabilistic heuristics.

- We conjecture that the number of twin prime pairs up to x is $\sim 2C_2 x/(\log x)^2$, where
$$C_2 = \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right)$$
is the "twin primes constant". Numerical data shows excellent agreement with this conjecture, even with a roughly $\sqrt{x}$ error term (analogous to what the Riemann hypothesis would give for $\pi(x)$ itself). Similar conjectures exist for the number of primes $p \leq x$ for which $p + k$ is prime, for any even $k \in \mathbb{N}$, with a different explicit constant C_k.
- Goldbach wrote in 1742 (essentially) that every odd number $n \geq 7$ can be written as the sum of three primes. This was proved for sufficiently large n by Vinogradov in 1937;

assuming the generalized Riemann hypothesis for Dirichlet L-functions, it was proved for all odd $n \geq 7$ by Deshouillers/Effinger/te Riele/Zinoviev in 1997; and Helfgott (using computations of Platt) has announced an unconditional proof for all odd $n \geq 7$ (although it has not yet appeared in a peer-reviewed journal).

- Goldbach also conjectured that every even number $n \geq 4$ can be written as the sum of two primes. This conjecture is still open. We conjecture that the number of ways an even $n \geq 4$ can be written as the sum of two primes is

$$\sim 2C_2 \Bigg(\prod_{\substack{p|n \\ p \text{ odd}}} \frac{p-1}{p-2} \Bigg) \frac{x}{(\log x)^2},$$

where C_2 is the twin primes constant defined above.

- Hardy/Littlewood made many conjectures in 1923, one of which was the prime k-tuples conjecture: if there are no obvious congruence obstacles among $a_1, a_2, \ldots, a_k$, there should be infinitely many positive integers n such that $n+a_1, n+a_2, \ldots, n+a_k$ are simultaneously prime. (Obvious congruence obstacles include situations like $\{a_1, a_2\} = \{0, 1\}$, since consecutive integers always include an even number, and $\{a_1, a_2, a_3\} = \{0, 8, 46\}$, since one of $n, n+8, n+46$ is always a multiple of 3.)
- Schinzel generalized this conjecture in 1958 from linear polynomials to general polynomials (often known as "Schinzel's Hypothesis H"), and Bateman/Horn wrote down the quantitative conjecture in 1962: if $q_1(x), \ldots, q_k(x) \in \mathbb{Z}[x]$ are distinct irreducible polynomials with degrees $d_1, \ldots, d_k \geq 1$, then the number of $n \leq x$ for which $q_1(n), \ldots, q_k(n)$ are simultaneously prime is

$$\sim \frac{1}{d_1 \ldots d_k} \frac{x}{(\log x)^k} \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\sigma(q_1 q_2 \cdots q_k; p)}{p}\right),$$

where $\sigma(q; p)$ is the number of solutions of $q(a) \equiv 0 \pmod{p}$. This conjecture generalizes all of the above quantitative conjectures, and it incorporates the "obvious congruence obstacles" described above as they would correspond to some $\sigma(q_1 q_2 \cdots q_k; p)$ equaling p.

One last questionable conjecture.

- Hardy/Littlewood also conjectured in 1923 that the largest number of primes one can find in an interval of length y should be found in the first y integers; more specifically, they conjectured that $\pi(x+y) - \pi(x) \leq \pi(y)$ for all $x, y \geq 2$.
- In 1973, Hensley/Richards showed that this conjecture is actually incompatible with the prime k-tuples conjecture: at most one of those two conjectures can be true. (The consensus now seems to be that the prime k-tuples conjecture is true, and that the largest number of primes in an interval of length y should actually be found in the interval $[-\frac{y}{2}, \frac{y}{2}]$, counting negatives of primes as primes—in other words, that $\pi(x+y) - \pi(x) \leq 2\pi(\frac{y}{2})$.)
- It's entertaining to note that these two incompatible conjectures were actually made by Hardy/Littlewood in the same paper!