MATHEMATICS 6180, SPRING 2023
SOME MOTIVATIONAL PROBLEMS IN NUMBER THEORY

KATHERINE E. STANGE

Number theory may be loosely defined as the study of the integers: in particular, the interaction between their additive and multiplicative structures. However, modern number theory is often described as the study of such objects as algebraic number fields and elliptic curves, which we have invented in order to answer elementary questions about the integers. Therefore, an argument can be made that the best way to define number theory is to exhibit some of these motivational problems.

0.1. **Are there infinitely many primes?** Yes, and you are invited to invent your own proofs of this fact (there are many). Here are two:

Due to Furstenberg. The idea is to define a topology on $\mathbb{Z}$. First, we call $a + m\mathbb{Z}$, $m > 0$ an *arithmetic progression*. We say $S \subset \mathbb{Z}$ is open if $S = \emptyset$ or it is a union of arithmetic progressions (check this is a topology). First, an arithmetic progression A is both open and closed (as the complement of finitely many arithmetic progressions). Suppose for a contradiction that there are only finitely many primes. Then

$$X = \bigcup_p p\mathbb{Z}$$

is closed, so $\mathbb{Z} \setminus X$ is open. But this latter set is the set of integers without prime factors, which is $\{-1, 1\}$. This is *not* open, a contradiction. □

The proof above doesn't require the language of topology; the key is actually hidden in checking that the given topology is a topology. Roughly, the core idea is that X, as a finite union of periodic sets, must be periodic, but then its complement would be periodic.

Due to Chaitin. Define the notion of Kolmogorov complexity $C(n)$ of an integer n to be the length of the shortest computer program that outputs n (you can fix a programming language).

Now suppose there are only finitely many primes $p_1, \ldots, p_k$. Then every integer n can be expressed by specifying the k exponents e_i of its factorization $n = \pm p_1^{e_1} \ldots p_k^{e_k}$, together with a sign. This representation is rather short: each exponent $e_i \leq \log n$ and can therefore be represented in $\log \log n$ bits. As k is a constant, we have $C(n)$ is bounded above by a constant multiple of $\log \log n$.

However, by a counting argument, there exist n having $C(n) \geq \log n$ (these are called 'random' because they do not have enough 'pattern' to admit a shorter description than their own decimal/binary expansion). This is a contradiction. □

A closer examination of this proof can actually give a surprisingly good lower bound on the counting function of the primes.

Date: Last revised: January 20, 2023.

Due to Euler. By manipulation of geometric series,

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \left(\sum_{k=1}^{\infty} \frac{1}{p^k}\right) = \sum_{n=1}^{\infty} \frac{1}{n}.$$

The sum on the right diverges; this is impossible if the product on the left is finite. Note that this depends on the fundamental theorem of arithmetic (unique prime factorization). □

The nice thing about this proof is that it introduces the function

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

at least for $s = 1$. This function is related to the primes because it is a product over primes:

$$\prod_{p \text{ prime}} \left(\sum_{k=1}^{\infty} \frac{1}{p^{sk}}\right) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

By introducing the variable s, we have built a sort of *generating function* for the prime numbers, called the *Riemann zeta function*. In other words, a function whose algebraic structure encodes information about what we want to study (the primes). If we let s be a *complex* variable, then we can consider this a complex function and we can ask all sorts of interesting questions about it. Among these is the question of *where are its zeroes?*[1]. It turns out to have some so-called 'trivial zeroes' on the real line, but it has others. The famous unsolved problem called the *Riemann Hypothesis* (one of the seven *Millenium Problems*) states that the non-trivial zeroes all have real part 1/2. Amazingly, the position of the zeros of the Riemann zeta function mirrors the positions of the prime numbers amongst the integers. I mean this very literally: there's a formula for the positions of the primes in terms of the positions of the zeroes!

The Riemann Hypothesis is considered one of the premier unsolved problems in modern mathematics, and most mathematicians both firmly believe the hypothesis and yet don't believe it will be proven in our lifetimes. It has so many powerful consequences in number theory, that the result must lie very deep. There are a great many research papers which prove results conditional on various forms of the Riemann Hypothesis; hundreds (thousands?) of results will suddenly be unconditionally true when a proof is eventually found.

The paradigm is that information about the zeta function translates to information about the primes:

(1) Euler's proof says that since the zeta function diverges at $s = 1$, there are infinitely many primes.
(2) If we can restrict the zeroes of zeta enough, then we obtain a growth rate on the primes (the Prime Number Theorem, below).
(3) If we know the Riemann Hypothesis, that the zeroes lie on the *critical line* of real part 1/2, then we know the growth rate of the primes to fantastic accuracy.

Use the notation $\pi(x)$ for the number of primes up to x. The Prime Number Theorem (Hadamard and De La Vallée Poussin, 1896) famously states that $\pi(x) \sim x/\log x$, or actually the slightly better approximation $\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. The $\sim$ notation indicates that the

[1]Strictly speaking, we need to use analytic continuation first, to define it on the entire plane of complex numbers

ratio of the two functions tends to 1 in the limit. This growth rate, as a conjecture, goes back to Dirichlet and Gauss around 1800. Proofs of the prime number theorem all depended on complex analysis until a proof of Selberg and Erdös in 1949.

The Riemann Hypothesis, in one form, states that

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log x).$$

This is "big O" notation, and it means that $|\pi(x) - \mathrm{Li}(x)|$ is eventually bounded above by a constant multiple of $x^{1/2}\log x$.

0.2. **Is there a closed formula for the n-th prime?** Believe it or not, there are some contenders, but they are not simple. Willans gives the formula

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{n} \left(\sum_{x=1}^{m} \left\lfloor \cos^2 \pi \frac{(x-1)! + 1}{x} \right\rfloor \right)^{-1/n} \right\rfloor,$$

which is certainly a closed formula in some sense. In fact, it is just a sort of obfuscation of the relationship between p_n and $\pi(x)$, using Wilson's theorem as a primality test:

Theorem 0.1 (Wilson's Theorem)**.** *p is prime or 1 if and only if $(p-1)! \equiv -1 \pmod{p}$.*

Neither is it particularly useful for computation, so I would say it is not a very satisfactory answer.

0.3. **Is there a (possibly multivariate) non-constant polynomial that gives only primes when evaluated on all integer inputs?** No, for fairly simple reasons: Suppose f is a non-constant polynomial. If a prime p divides $f(0, 0, \ldots, 0)$, then it also divides $f(kp, kp, \ldots, kp)$ for all integers k; however this is a non-constant polynomial in k which must eventually tend to infinity in size, and one eventually obtains composite multiples of p.

However, there are multivariate polynomials whose *positive* values are exactly all the primes, as the variables range over *natural* numbers. Such a polynomial in 26 variables, due to Jones, Sato, Wada and Wiens, is

$$\begin{aligned}
(k+2)(1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2 - \\
[16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 - [2n + p + q + z - e]^2 - \\
[e^3(e+2)(a+1)^2 + 1 - o^2]^2 - [(a^2-1)y^2 + 1 - x^2]^2 - \\
[16r^2y^4(a^2-1) + 1 - u^2]^2 - [n + l + v - y]^2 - \\
[(a^2-1)l^2 + 1 - m^2]^2 - [ai + k + 1 - l - i]^2 - \\
[((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 - \\
[p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 - \\
[q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 - \\
[z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2)
\end{aligned}$$

If you prefer fewer variables, you can get down to 10 variables if you let the degree go up to 15905. The proof is based on the logical notion of a Diophantine set.

0.4. **Are there infinitely many primes of the form $4n+1$?** Yes. More generally, there are infinitely many primes of the form $an+b$ for any coprime a and b. This is Dirichlet's celebrated theorem on arithmetic progressions (1837). We won't cover the proof; it's more typically done in your analytic number theory course. However, there is a sense in which this question lies very much in the realm of algebraic number theory, and we will touch on related topics. In general, we expect about half of all primes to be congruent to 1 modulo 4 and the other half to be congruent to 3 mod 4. However, there are more in the former category, in the sense that, counting up to N, the former category is usually larger. This is called Chebyshev's Bias. See 'Prime Number Races' by Granville and Martin (American Mathematical Monthly).

0.5. **If you know the nth prime ends in a particular digit, is the final digit for the $(n+1)$-st prime equally likely to be any of the four possibilities $1, 3, 7, 9$?** Something we only noticed this millenium: conjecturally/datawise NO. Primes don't seem to like to repeat final digits, so if p_n ends in 1, then p_{n+1} is less likely to end in 1. What? See *Unexpected Biases in the Distribution of Consecutive Primes* by Oliver and Soundararajan. Some pictures follow:

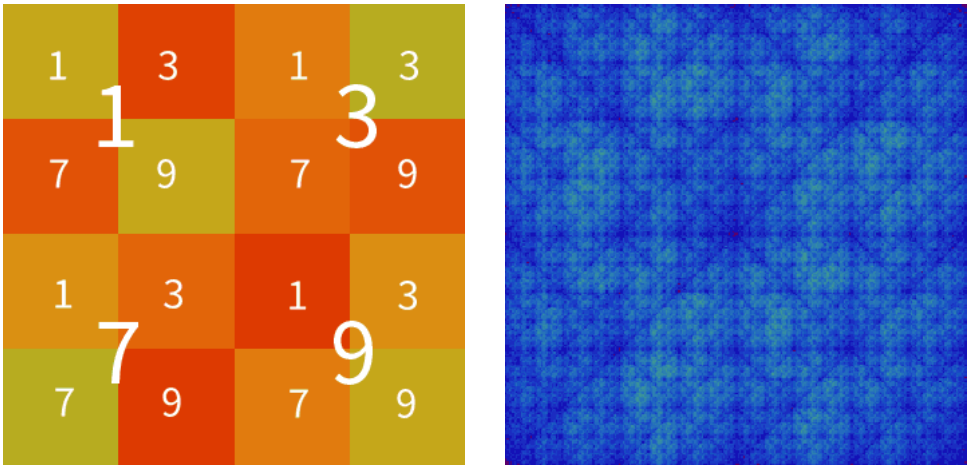
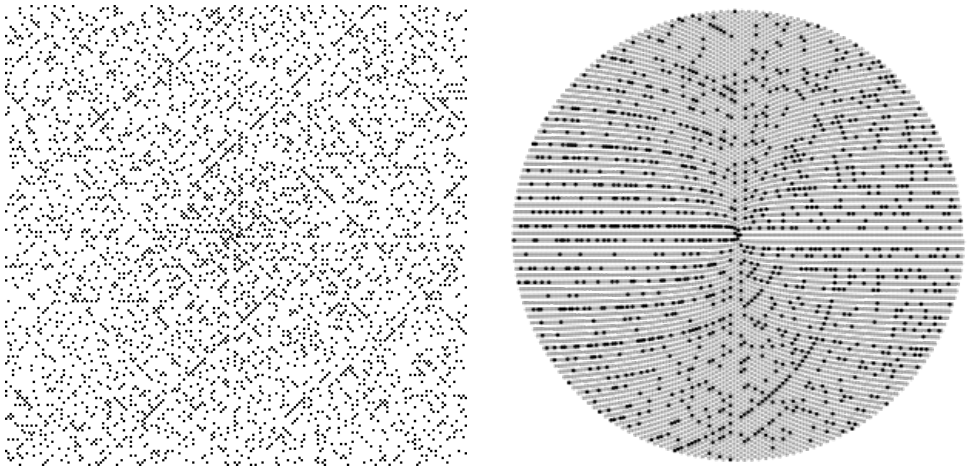


Image due to matthen.com.

0.6. **Are there infinitely many primes of the form n^2+1?** The more general question is a variation on the polynomial that produces only primes – but we now require only that it produce infinitely many primes. It is unknown for any quadratic polynomial. Iwaniec has shown that there are infinitely many n for which n^2+1 is the product of at most two primes.

Ulam noticed that if you draw the primes in a spiral around the origin on a square grid, it looks far from random. The integers which are values of certain quadratic polynomials eventually head out along diagonal lines. The most visible diagonal on his spiral is n^2-n+41, which is prime for $0 \leq n < 40$ (but not for $n = 40$). There's a conjecture of Hardy and Littlewood about the density along these diagonals as it depends on the coefficients of the quadratic. Below is the Ulam spiral at left and the Sacks, a variation in which the diagonals become curved lines, at right.



0.7. **Are there infinitely many primes p for which $p+2$ is prime?** This is the famous twin primes conjecture (in the affirmative). It is still unsolved. More generally, one can ask how often $f_1(x)$ and $f_2(x)$ are simultaneously prime for some polynomials f_1 and f_2. Of course, there are infinitely many pairs of integers a, d such that a and $a+d$ are prime; we just don't know if we can take $d = 2$ infinitely often. In fact, van der Corput showed there are infinitely many 3-term arithmetic progressions in 1929. In 2004, Green and Tao showed there are infinitely many length k arithmetic progressions for all k.

Why do we think the answer is yes? This is an example of a pervasive heuristic argument in number theory. Using the Prime Number Theorem, we can guess that the 'probability' of a number x between 1 and N being prime is about $1/\log N$. Therefore, we expect the chance that both x and $x+2$ are prime is about $1/\log^2 N$: there will be about $N/\log^2 N$ twin prime pairs below N.

But wait, this also predicts that there are infinitely many primes p such that $p+1$ is prime! Refine the model: odd numbers between 1 and N have a $2/\log N$ chance of being prime, while even ones have a 0 chance. Refine it for multiples of 3, of 5, etc. and eventually we obtain a count of twin primes that is

$$2 \prod_{p \text{ odd prime}} \left(1 - \frac{1}{(p-1)^2}\right) \frac{N}{\log^2 N}.$$

(This is the *Hardy Littlewood* conjecture.) Not seeing any obvious reasons this is wrong, we conjecture this as the growth rate of twin primes. This relies on the oft-used heuristic that, having identified the 'obvious' ways in which primes are not random (congruence conditions, like most even numbers are not prime), they are otherwise *entirely random*! This is, of course, absurd.

Chen has shown in the 70's that there are infinitely many primes p such that $p+2$ is a product of at most two primes. This uses 'sieve methods'. In 2013, Yitang Zhang proved that there is some integer $N < 7 \times 10^7$ such that there are infinitely many prime pairs $(p, p+N)$. The bound on N was reduced to 246 in 2014 by a Polymath Project led by Tao.

0.8. **Up to N, are there always more natural numbers with an odd number of prime factors than with an even number of prime factors (counted with multiplicity)?** This is known as the Pólya Conjecture, and it seems heuristically reasonable that 'most' integers have an odd number of prime factors. It has important consequences

in number theory and was widely believed between 1919 (when the conjecture was made) and 1958, when Haselgrove showed that it is false for infinitely many N. It is true until $N = 906,150,257$, when it fails. Never trust numerical evidence.

0.9. **Does $x^2 - 1141y^2 = 1$ have any solutions? (Note: if you ask the computer to check up to 25 digits, it will find none.)** Another case of misleading numerical evidence. The first solution to $x^2 - 1141y^2 = 1$ has y of 26 digits; there are infinitely many solutions. This is an example of a Pell equation (another topic we could see in this course). For more examples of 'The Strong Law of Small Numbers' (don't trust them), see Richard Guy's article by the same name.

0.10. **Does $x^3 - y^2 = 1$ have any integer solutions besides $(1, 0)$? (Note: if you ask the computer to check up to 25 digits, it will find none.)** No. This is an example of an elliptic curve, and all elliptic curves have finitely many integral solutions. This is consequence, in some sense, of the topology of the curve: curves which (as complex surfaces) have genus 0 can have infinitely many integer solutions (e.g. $x^2 - 1141y^2 = 1$ above), while higher genus have finitely many. Even knowing it is finite, it is hard to figure out how many. We'll tackle this example as our first motivational problem for the development of algebraic number theory.

0.11. **Does $x^n + y^n = z^n$ have any integer solutions for integers $n > 2$? (Note: if you ask the computer to check up to 25 digits, it will find none.)** No. We know it should be finite by the general theory (these are higher genus), but it is much harder to show there are no solutions at all. This is Fermat's famous Last Theorem, and Fermat's famous non-marginal solution is often presumed to have been a misapplication of the methods of algebraic number theory which we'll use on the previous question. We'll show how far those methods get and where they break down. Fermat's Last Theorem may have been one of the drivers behind the development of algebraic number theory, as well as the theory of elliptic curves and modular forms, which finally solved it. The objects of study in number theory are hidden deeply behind the simple problems which motivate the area.

0.12. **Is there an algorithm to determine if a given polynomial equation in any number of variables has an integer solution?** This is Hilbert's 10th Problem. Actually, he asked the audience to devise such a process, as it came as quite a surprise that the answer would be NO. This is a celebrated result of Davis, Matiyasevich, Putnam and Robinson. The existence of a polynomial whose positive values on natural numbers are all the primes is a corollary. The proof lies in the realm of logic, and uses facts about the Fibonacci numbers in an essential way. For a wonderful read, see the book "Hilbert's Tenth Problem," by Matiyasevich.

The same question for rationals, in place of integers, is an open problem.

0.13. **Are there any quadratic forms with integer coefficients which represent all positive integers?** This is a bit of a trick question unless you include the stipulation that the forms be *positive definite*, i.e. do not take zero or negative values. Otherwise xy is such a form.

For positive definite forms, the answer is no, for binary and ternary forms (i.e. 2 and 3 variables). You will see in any algebraic number theory course (including this one) a classification of which integers are the sum of two squares; this fundamental result goes back to Fermat in 1640, but an elementary proof is not very easy.

Lagrange showed in 1770 that every positive integer is the sum of four squares. For quaternary and higher, it has been proven by Bhargava and Hanke (the '290 theorem' in 2005), that to determine if a form is 'universal' in this manner, it suffices to determine if it represents $1, 2, \ldots, 290$. (This came after the '15 theorem' of Conway and Schneeberger which applies to so called 'matrix-integral' forms; i.e. forms whose non-diagonal coefficients are even.)

0.14. **Does there exist a deterministic polynomial-time algorithm (in the number of digits) to determine if n is prime?** A first method would be to check all divisors up to $\sqrt{n}$; this takes $O(\sqrt{n})$ time. At first glance, Fermat's Little Theorem seems a promising criterion.

Theorem 0.2 (Fermat's Little Theorem)**.** *For any prime p and a coprime to p,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

However, many composite n also satisfy this equation for some a. If a composite n satisfies this equation for all coprime a, then it is called a *Carmichael number*, about which there are many questions (there are infinitely many such numbers).

In 1975, a deterministic polynomial time-algorithm was given by Miller, but this is only assuming the *Extended Riemann Hypothesis*[2]. Around the same time some randomized polynomial-time algorithms were discovered (meaning it can return NO when it should return YES, but with random probability $< 1/2$), and many more have appeared since. Finally, in 2002, Agrawal, Kayal and Saxena found the desired algorithm, running in $O(\log^{15/2} n)$ time.

0.15. **Can we factor numbers in deterministic polynomial time?** A good reference on this extensive subject is the book "Prime Numbers: A Computational Perspective," by Crandall and Pomerance. The quick answer is that there are sub-exponential algorithms known since the 70's, but no polynomial time algorithms, even under various generalised Riemann Hypotheses. However, there does not seem to be any evidence indicating that it is not possible, besides the fact that we have tried and failed, especially since the 70's. However, there are a great many very interesting algorithms, some of which we will meet in this class. With current methods, we can factor integers up to about 232 decimal digits (it took two years / 2000 computing years in 2009).

What complexity class is it? $\mathcal{P}$ refers to problems for which there are deterministic polynomial time algorithms[3]. $\mathcal{NP}$ refers to problems for which a correct answer can be verified in polynomial time. Because of the AKS primality testing algorithm of 2005 (see above), factoring is in $\mathcal{NP}$. Famously, we do not know if $\mathcal{P} = \mathcal{NP}$.

0.16. **For any irrational number α, are there infinitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^2$?** True for all irrational α; this is an application of the pigeonhole principle due to Dirichlet. It is Fields Medal work that for any algebraic α, there are only finitely many p/q such that $|\alpha - p/q| < 1/q^{2+\epsilon}$ (Roth's Theorem, 1955). This is the fundamental question of the area called *Diophantine approximation*.

[2]A note on the Extended Riemann Hypothesis. The terminology on the various extensions of the Riemann Hypothesis is confusing; see the book "The Riemann hypothesis: a resource for the afficionado and virtuoso alike," by Peter Borwein, Stephen Choi, Brendan Rooney and Andrea Weirathmueller. The version used here is the usual critical-strip statement, applied to some particular Dirichlet L-functions (but not all).

[3]$\mathcal{P}$ actually refers to decision problems, but you can accomplish factoring via a yes/no problem something like "does n have a divisor with k-th digit j?" etc.

0.17. **Given n, if it is even, divide by 2 and if it is odd, return $3n+1$; if we iterate this rule, must we eventually reach the loop $1 \to 4 \to 2 \to 1$?** This is known as the Collatz Conjecture, and it is famous for driving mathematicians crazy in every mathematical discipline. It is an open question, and it is not clear which methods will resolve it.

0.18. **Given a real number $\alpha > 0$, if it is > 1, then subtract 1 and if it is < 1, then invert it; if we iterate this rule, must we eventually reach a loop?** The process above expresses any α as a *continued fraction*:

$$\alpha = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}$$

Every real number has a continued fraction expansion. The a_i are eventually periodic (corresponding to a loop in the dynamical system of the question), if and only if α is rational or quadratic. A few famous continued fraction expansions are:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cdots}}}}}}}}$$

which has the pattern $2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots$, and

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cdots}}}}}}}}$$

which has no discernable pattern. Chopping off the fraction at any finite point, we obtain good rational approximations to α; in fact, these are the best rational approximations of Dirichlet's theorem above!