MATH 25 CLASS 8 NOTES, OCT 7 2011

Contents

1. Prime number races

We proved that there were infinitely many primes of the form $4k+3$, and we said that there were infinitely many primes of the form $4k+1$, and that we would give a proof of this fact later in this class. Recall that $\pi(x)$ is the number of primes less than or equal to x; let $\pi(x;q,a)$ be the number of primes less than or equal to x of the form $qk+a$. Based on what we talked about last class, this function is only interesting when $\gcd(a,q)=1$.

Dirichlet's Theorem can be rephrased as saying that $\lim_{x\to\infty}\pi(x;q,a)=\infty$ when $\gcd(q,a)=1$. On the other hand, the prime number theorem says that $\pi(x)\sim x/\log x$. A slight modification of the proof of the PNT can yield an analogous asymptotic result for primes in arithmetic progression: if $\gcd(q,a)=1$, then

$$\pi(x;q,a)\sim\frac{1}{\phi(q)}\frac{x}{\log x},$$

where $\phi(q)$ is the Euler-totient function, a function we will carefully study in a few weeks. $\phi(q)$ is equal to the number of integers a with $1\leq a\leq q$ which are relatively prime to q; for instance, $\phi(4)=2,\phi(6)=2,\phi(8)=4$. The previous theorem says that, at least asymptotically speaking, each particular arithmetic progression $qk+a$ gets its 'fair share' of the primes.

Or does they? After all, the above result only says something about asymptotic density, which is a first-order approximation to the size of functions. If one were to actually look at a plot of the number of primes of the form $4k+1$ vs $4k+3$, the first feature that would jump out is that $\pi(x;4,3)>\pi(x;4,1)$ for the entire time, at least if x is not too large. The fact that $\pi(x;4,3)>\pi(x;4,1)$ for most values of x is called *Chebyshev's bias*, after the Russian mathematician who first observed this phenomenon.

However, $\pi(x;4,3)$ is not ahead the entire time. As a matter of fact, in the early 20th century, J.E. Littlewood proved that $\pi(x;4,1)$ beats $\pi(x;4,3)$ for an infinite number of x, despite the data for small x suggesting otherwise. However, perhaps $\pi(x;4,3)$ beats $\pi(x;4,1)$ for 'most' x?

It was initially conjectured that the fraction of such numbers x has density 1. However, this was later proven to be false. One can then ask, does this fraction have a limit as $x\to\infty$? Well, it was also proven, under a conjecture known as the

Generalized Riemann Hypothesis, that there is no such limit; ie, the proportion of the time $\pi(x;4,3) > \pi(x;4,1)$ has no limit as $x \to \infty$!

At least, this is true if we weight each number x by the same amount in the count. However, if we use what is known as a *logarithmic density*, then we have the following result of Rubinstein and Sarnak:

Theorem 1. *Assuming two unproven conjectures (the GRH and another conjecture known as* Linear Independence*), the following is true:*

$$\frac{1}{\log x} \sum_{\substack{x \leq X, \\ \pi(x;4,3) > \pi(x;4,1)}} \frac{1}{x} \to .9959\ldots.$$

This result opened up a small speciality in number theory dedicated to understanding such phenomenon in general. Needless to say, the techniques for the proofs of theorems like these require rather advanced techniques.

2. Special kinds of prime numbers: Fermat and Mersenne numbers

Let's consider some special prime numbers. First, we'll look at numbers of the form $2^n - 1$, which are called *Mersenne numbers*. Notice that when $n = 2, 3, 5, 7$, $2^n - 1 = 3, 5, 31, 127$, and these are all prime numbers. One might be led to think that $2^p - 1$ is prime when p is prime from these examples, but actually $2^{11} - 1 = 2047 = 23 \cdot 89$ is not a prime number. Nevertheless, it is true that if $2^p - 1$ is prime, then p is a prime:

Proposition 1. *Suppose $2^n - 1$ is prime. Then n is prime.*

Proof. We prove the contrapositive. Suppose n is composite; say $n = ab$, for $1 < a, b < n$. Then we can factor $2^n - 1 = 2^{ab} - 1$ as follows:

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 1).$$

Checking that this equation is true is routine algebra. In any case, if $1 < a, b$, then $2^a - 1 > 1$, and $2^{a(b-1)} + \ldots + 1 > 1$ as well. So this factorization shows that $2^n - 1$ is divisible by some number between $1, 2^n - 1$ if n is composite. □

Part of the reason why Mersenne primes are interesting is because there exists a very rapid test, called the Lucas-Lehmer test, to determine whether a Mersenne number is actually prime. The Internet project "GIMPS", which is short for the *Great Internet Mersenne Prime Search*, is one of the first distributed computing projects which appeared on the Internet in the 1990s. All the largest known prime numbers (by far) are Mersenne primes. Let $M_n = 2^n - 1$. Then as of late 2010 the largest known Mersenne prime (and the largest known prime) is $M_{43112609}$, which has almost 13 million digits. This is the 47th known Mersenne prime, although currently it is unknown whether this is the 47th smallest Mersenne prime, since GIMPS has yet to rule out the existence of Mersenne primes under $M_{43112609}$. Incidentally, the Lucas-Lehmer primality test does not actually tell you any of the factors of M_p when it tells you that M_p is composite. This might seem to be a drawback, but this is

an illustration of the general empirical principle that (based on current knowledge) primality testing is much faster than factorization.

If you are interested in learning more about and possibly participating in GIMPS, head to their website at `www.mersenne.org`. In general, it takes about a month to run a primality test on a single candidate. GIMPS statistics There has been a discovery of a new prime about once every two years or so, with the most recent coming in 2009. There are also small cash prizes available for discovering new Mersenne primes, and a $\$150,000$ prize for the first discoverer of a prime with more than 100 million digits. However, there is very little hope for discovering such a large prime in any reasonable time with current computer hardware. Maybe in another ten or twenty years!

The GIMPS webpage statistics indicate that GIMPS is running at about 50 teraflops (50 trillion floating point operations per second, a measure of the computational power of all the computers running GIMPS right now). By way of comparison, the project SETI@Home (which searches for intelligent extraterrestrial life by scanning stars for unusual electromagnetic signals) has about 750 teraflops of capacity, while the largest distributed computing project, Folding@Home, has about 6 petaflops (6,000 teraflops) of computing power. The current top supercomputer in the world, the K Computer in Japan, has peak capacity of about 8 petaflops, while IBM is designing a new supercomputer called Sequoia, which apparently will run at 20 petaflops when finished. So if we unleashed the power of these supercomputers (or if GIMPS just became more popular), then Mersenne primes would probably be discovered more quickly. However, it's probably true that testing Mersenne numbers for primality is not the best use of such expensive computing hardware!

By the way, it is unknown whether there actually are infinitely many Mersenne primes. Proving this theoretical fact (as opposed to experimental computations) would be a great breakthrough.

3. Fermat numbers

We very briefly looked at numbers of the form $2^n - 1$ and considered the problem of when they were prime. We found that if $2^n - 1$ is prime, then n is prime, but for many primes $2^p - 1$ can be composite. As a matter of fact only 47 such primes have been discovered so far, with p getting as large as 43 million or so. Whether there are infinitely many such primes is still an open question, but distributed computing projects exist to try to find larger and larger such primes. There is a specialized primality test, the Lucas-Lehmer test, for numbers of this form, and we may come back to this near the end of the class.

Let us now consider numbers of the form $2^n + 1$, and in particular consider the question of when these numbers are prime. If you calculate the first few instances of this number, you get $2^1 + 1 = 3, 2^2 + 1 = 5, 2^3 + 1 = 9, 2^4 + 1 = 17, 2^5 + 1 = 33, 2^6 + 1 = 65, 2^7 + 1 = 129, \ldots$. The pattern is not obvious, but perhaps one thing which jumps out at us is that $2^n + 1$ seems to be composite if n is odd. As a matter of fact, we can prove something slightly better:

Proposition 2 (Proposition 2.11 of the text)**.** *Let n be an integer with $n \geq 2$. Then 2^n+1 is composite if n is not a power of 2. (Evidently this condition on n is equivalent to saying that no odd prime divides n.)*

Proof. Suppose that n is not a power of 2. Then we may write $n = 2^k m$, for some integer $k \geq 0$, m an odd number greater than 1. Let $a = 2^{2^k}$. Then we may factor $2^n + 1$ as follows:

$$2^{2^k m} + 1 = a^m + 1 = (a+1)(a^{m-1} - a^{m-2} + a^{m-3} - \ldots - a + 1).$$

Notice that we use the fact that m is odd to ensure that the final term in the expression on the right really is a $+1$ as opposed to a -1.

This does show that $2^n + 1$ is composite, because $a + 1 > 1$ (as a matter of fact, $a + 1 \geq 3$), and $a + 1 < a^m + 1$ because $m \geq 3$. □

This proposition tells us that if we want to find primes of the form 2^n+1, we should be looking for numbers of the form $2^{2^n}+1$. These numbers are called *Fermat numbers*, after Pierre de Fermat, a French lawyer in the 17th century who also happened to be one of the most important mathematicians of the time, who was perhaps the first person to systematically study these numbers.

Let's write $F_n = 2^{2^n} + 1$. The first few Fermat numbers are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Evidently F_5 is quite large; it is equal to 4294967297. Fermat looked at the beginning of this sequence and it is not too time-consuming to check that $3, 5, 17, 257, 65537$ are all prime numbers. On the basis of this evidence, Fermat conjectured that all Fermat numbers are prime.

This provides a historical lesson in perhaps not making general conjectures on a small amount of numerical evidence. About a hundred years later, Euler showed that F_5 is composite by exhibiting a factorization of F_5, and every Fermat number past F_5 which has been checked for primality/compositeness has been shown to be composite! As a matter of fact, it is still an open question whether there are either infinitely many prime Fermat numbers or infinitely many composite Fermat numbers. One of these must be true, but we still don't know which one! The general belief is that there are infinitely many composite Fermat numbers, and probably only finitely many prime Fermat numbers, but no one seems to have any real idea how to tackle these problems.

Fermat numbers have some interest outside of number theory. As a young man, Gauss proved that a regular n-gon is constructible by straightedge and compass (a type of problem very important in classical Euclidean geometry) if $n = 2^k p_1 \ldots p_r$, where $k \geq 0$ and the p_i are distinct Fermat primes. This condition was later proved to also be necessary; Gauss claimed this but did not give a proof himself (although it is possible he found one but never published it). As a matter of fact, the story is that Gauss discovered the constructibility of a regular 17-gon in his late teens, and it was this discovery which convinced him to become a professional mathematician.

We can use Fermat numbers to give a clever proof of the fact that there are infinitely many prime numbers. First we start with the following proposition, still in the flavor of the last two propositions we have proved:

Proposition 3 (Lemma 2.12 of the text)**.** *Let $n \geq 0, m > 0$. Then F_n, F_{n+m} have distinct prime factors; equivalently,* $\gcd(F_n, F_{n+m}) = 1$.

Proof. We claim that $F_n | (F_{n+m} - 2)$. Let $a = 2^{2^n}$. Then $F_n = a + 1$. Notice that $F_{n+m} = 2^{2^{n+m}} + 1 = (2^{2^n})^{2^m} + 1 = a^{2^m} + 1$. Then $F_{n+m} - 2 = a^{2^m} - 1$. But then we may factor $a^{2^m} - 1$ as follows:

$$a^{2^m} - 1 = (a+1)(a^{2^m-1} - a^{2^m-2} + \ldots + a - 1).$$

This time, we are critically using the fact that 2^m is even for this factorization to make sense. In any case, this shows that $(a+1)|(a^{2^m} - 1)$. But then this means that $\gcd(F_n, F_{n+m}) = \gcd(a+1, (a^{2^m} - 1) + 2) = \gcd(a+1, 2)$. Because $a + 1$ is odd, this gcd is equal to 1, as desired. □

This shows that there are infinitely many primes, because each Fermat number has prime factors which are distinct from the prime factors of any of the other Fermat numbers, and there are infinitely many Fermat numbers.