Friday, February 8

Last time, we ended with:
Q: What is the largest prime?
We voted that there isn't one, so the primes go on forever.
(There is a largest prime we know of, and finding more and more large primes is important to cryptography. This also relies on it being hard to factor numbers, which isn't known, but we'll get to cryptography later.)
Before we tackle primes, let's look at something slightly different:
Q: What is the largest integer?
Theorem: There is no largest integer.
Proof: Let n be an integer. Then there exists a larger integer $n+1$. Q.E.D.
Now let's go back to primes!
Want: Given prime p, find a larger prime.
Is $p+1$ prime? Usually not. (It is if $p=2$.)
Is $p+2$ prime? Sometimes. (It works for $p=3, 5$, and 11, but not $p=7$ or 13)
(This second question is related to the twin primes conjecture, which asks if there are an infinite number of p values such that p and $p+2$ are both prime. Nobody knows!)
It turns out that we don't have a method to take an prime and generate a larger prime! Oh no! This leads us to Pólya, who wrote "How to solve it" ("it" being a math problem). This work gives us the following wisdom:
If you can't solve a problem, find an easier version of that problem that you <u>can</u> solve.
Thus, we need something solvable. What's a simpler version of our desire? This leads us to:
Given a prime p, find a different prime.

Let's go back to $p+1$. $p+1$ definitely has a prime factor. Let's call it p'. Can $p'=p$? No. Why? $\frac{p+1}{p}=1+\frac{1}{p}$, which is not an integer. (This is another reason why it's helpful that 1 is not classified as a prime.) However, since p' is a factor of $p+1$, $\frac{p+1}{p'}$ is an integer, so $p \neq p'$.

Now we have a new prime! How can we use p and p' to make a new prime? $p+p'$ was proposed, and it could work (note that $\frac{p+p'}{p}=1+\frac{p'}{p}$ and $\frac{p+p'}{p'}=1+\frac{p}{p'}$, and since p and p' are prime and $p \neq p'$, neither of these are integers). However, this could be hard to generalize, so we'll go in a different direction. After some deliberation, we reached $pp'+1$. This has a prime factor. Let's call it p''. Note that $\frac{pp'+1}{p}=p'+\frac{1}{p}$, which is not an integer, but $\frac{pp'+1}{p''}$ has to be an integer, so $p \neq p''$. By the same reasoning, $p' \neq p''$. Now we have three primes, and we can repeat the process! This leads us to:

Algorithm: Given a bunch of primes, multiply them together, add 1, and pick the smallest prime factor of this. This is a new prime.

Now we can prove the claim!

Strategy: Given any finite collection of primes, show that it's incomplete.

Wait a second! Our strategy relies on every number (greater than or equal to 2) having a prime factor, which we haven't proved yet. Let's take it on faith for now and write it as a lemma:

Lemma: Any integer $n \geq 2$ has a prime factor. (We'll come back to it!)

Theorem: There are infinitely many primes.

Proof: Given any finite collection $p_1, p_2, \ldots, p_k$ of primes, consider $p_1, p_2, \ldots, p_k + 1$.

By the lemma, this number has a prime factor. Let's call it q.
We claim $q \neq p_j$ for any j. This is because:

$$\frac{p_1p_2\cdots p_k+1}{p_j} = \frac{p_1p_2\cdots p_k}{p_j} + \frac{1}{p_j}. \quad \frac{p_1p_2\cdots p_k}{p_j} \text{ is an integer,}$$

$$\text{but } \frac{1}{p_j} \text{ isn't, so } \frac{p_1p_2\cdots p_k}{p_j} + \frac{1}{p_j} \text{ isn't an integer.}$$

However, $\frac{p_1p_2\cdots p_k+1}{q}$ is an integer, so $q \neq p_j$ for all valid values of j.
Thus, q is a new prime. Q.E.D.

Now let's prove the lemma!

Proof of lemma: Given $n \geq 2$:

If n is prime, we're done!

~~If n is composite~~ Otherwise, n is composite, so $n = a_1b_1$ where $1 < a_1 < n$.

If a_1 is prime, we're done!

Otherwise, a_1 is composite, so $a_1 = a_2b_2$ where $1 < a_2 < a_1$.

If a_2 is prime, we're done!

Otherwise... (We continue.)

If we keep doing this, we get a sequence of integers

$$n > a_1 > a_2 > \cdots > 1.$$

This can only continue for at most n steps, i.e. the process terminates after a finite number of steps, i.e. one of the a_i is prime.

Q.E.D.

Thus, the lemma is proved, so the previous theorem is completely proved!