JUNE 21ST/22ND MATH PROBLEM SET

It will be another million years, at least, before we understand the primes. – Paul Erdös.

We will discuss a test which is good at finding numbers that are "probably" prime. It is really a test for checking if a number is composite but each time you try it on a prime, you become more "sure" that your number is prime.

First however, some motivation. Here's a reasonable way to check if a number n is prime. Choose a number $1 \leq a \leq n-1$. Compute $a^{n-1} (\text{mod } n)$. There are two outcomes.

(1) $a^{n-1} \equiv_n 1$.
(2) $a^{n-1} \not\equiv_n 1$.

If you ever end up in outcome #2, you have just proven that n is not prime. If n is prime, then condition (1) will always be satisfied and should be viewed as *evidence* that n is prime.

Try a bunch of different random a, and if they all satisfy (1), you might expect that n really is prime (even if it is too big to factor). There is one problem with this strategy though. There are numbers that look prime in that most numbers satisfy (1) even though they aren't really prime. These are called *Carmichael numbers*.[1]

1. Consider $n = 561$. Have everyone in your group choose three different a which are relatively prime to n. Verify that they satisfy condition (1) above.

There is a better test though which uses a similar idea. It relies on the fact that if n is prime, then $a^{\frac{n-1}{2}} \equiv_n \pm 1$.

2. Verify that if n is prime and odd, then $a^{\frac{n-1}{2}} \equiv_n \pm 1$. If you can't figure it out, try it in several examples and then move on (or get me or a nearby TA to explain it).

[1] This is not exactly the definition of Carmichael numbers, but it is close.

Now we come to the Miller-Rabin algorithm. It can prove n is composite (depending on the a you choose). Write $n-1 = 2^k \cdot q$ where q is odd. Next choose a random $1 \leq a \leq n-1$.

Theorem. *If*

(i) $a^q \not\equiv_n 1$, *and*
(ii.0) $a^q \not\equiv_n -1$, *and*
(ii.1) $a^{2q} \not\equiv_n -1$, *and*
(ii.2) $a^{2^2 q} \not\equiv_n -1$, *and*
...
(ii.k-1) $a^{2^{k-1} q} \not\equiv_n -1$,

then n is composite. (note $2^{k-1}q = \frac{n-1}{2}$).

3. Use the Theorem above to verify that the following numbers are composite. Choose your own a.

(a) 899
(b) 3599

It turns out that for a given composite[2] number n, at least three quarters (75%) of the numbers $2 \leq a \leq n-1$ satisfy the theorem. So it is a very fast way to show that a number is composite.

4. Find all the $2 \leq a \leq 20$ that satisfy the theorem for $n = 21$. Is it true that 75% of them really fail the theorem?

5. Mull over why the theorem is structured the way it is. In particular if $a^{2^{k-1}q} = a^{\frac{n-1}{2}} \not\equiv_n 1$, must one of the earlier conditions hold? Might this make a good algorithm?

[2]Non-prime