Friday, April 26

Q: Is 133 prime?

How can we check this?

We could answer this by trial-and-error: testing a bunch of potential factors of 133. (We'd only have to check up to $\sqrt{133}$ (between 11 and 12), and we only have to check primes - if no primes less than $\sqrt{133}$ divide 133, then only primes greater than $\sqrt{133}$ divide 133. If q is the smallest prime greater than $\sqrt{133}$ such that $q \mid 133$, the minimum value of a product of primes greater than $\sqrt{133}$ that divide 133 would be $q^2 > \sqrt{133}^2 = 133$, so the minimum product of prime factors is greater than 133, which we can't have.)

Also, note that $7 \mid 133 \Leftrightarrow 7 \mid (13 - 2 \cdot 3) \Leftrightarrow 7 \mid 7$. $7 \mid 7$, so $7 \mid 133$.

We got lucky, though! Today, we'll show how to test whether 133 is prime without factoring it! We'll use Fermat's Little Theorem:

Given p a prime, $a^{p-1} \equiv 1 \pmod{p}$

$\forall a \not\equiv 0 \pmod{p}$.

If we can find some a such that $a^{132} \not\equiv 1 \pmod{133}$, then 133 can't be prime.

For example, what is $2^{132} \pmod{133}$?

One approach is to plug this into WolframAlpha. We could also compute 2^{132}, then reduce (mod 133).

2^{132} is MASSIVE! There has to be a better way!

There is! We can multiply sequentially by 2 and reduce as we go!

e.g. $2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16, 2^5 \equiv 32, 2^6 \equiv 64, 2^7 \equiv 128, 2^8 \equiv -10, 2^9 \equiv -20, \ldots$

Reaching 2^{132} will take FOREVER! There has to be a better way!

There is! Let's square powers of 2 along the way! $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv -10$ (we found that earlier), $2^{16} \equiv 100$, $2^{32} \equiv 10000$. (Note that $400 \equiv 1 \pmod{133}$, so $10000 \equiv 25 \pmod{133}$.) $2^{32} \equiv 10000 \equiv 25$. $2^{64} \equiv 25^2 \equiv 5^4 \equiv 125 \cdot 5 \equiv (-8) \cdot 5 \equiv -40$. $2^{128} \equiv 1600 \equiv 4$.

Then $2^{132} \equiv 2^{128} \cdot 2^4 \equiv 4 \cdot 16 \equiv 64 \not\equiv 1 \pmod{133}$.

Therefore, 133 isn't prime! Hooray!

Wait a second... did we get lucky again? What are the odds 132 could be written as a sum of powers of 2?

They're quite good, actually – we've proved that every positive integer can be written as a sum of powers of 2 because binary works!

Caveat: Just because $a^{n-1} \equiv 1 \pmod{n}$ for some a doesn't mean n must be prime. ($561 = 3 \cdot 11 \cdot 17$, but for every valid value of a, $a^{560} \equiv 1 \pmod{560}$.)

Example: $4^{14} \equiv (2^2)^{14} \equiv (2^4)^7 \equiv 16^7 \equiv 1^7 \equiv 1 \pmod{15}$, but 15 isn't prime.

We're moving on! CRYPTOGRAPHY!

Alice and Bob want to communicate securely over email, but Eve is spying on the exchange. How can Alice create a message, encrypt it, and send it to Bob so Bob is able to decrypt it but Eve isn't?

They need a secret key. How do they do this without Eve seeing the key?

This was resolved by Diffie and Hellman in 1976. Let's see the method!

Diffie-Hellman Key Exchange Protocol

Step 1: Alice and Bob publicly agree on a huge prime p and some $g \in \{1, 2, \ldots, p-1\}$.
Privately, Alice picks $a \in \{2, \ldots, p-2\}$ and $b \in \{2, \ldots, p-2\}$.

Step 2: Alice sends Bob $X := g^a \pmod p$.
Bob sends Alice $y := g^b \pmod p$.

Step 3: Alice evaluates $y^a \equiv (g^b)^a \equiv g^{ab} \pmod p$.
Bob evaluates $x^b \equiv (g^a)^b \equiv g^{ab} \pmod p$.
$g^{ab} \pmod p$ is the shared secret key.

Q: Why can't Eve figure this out?
Well, here's what Eve knows: g, p, $g^a \pmod p$, $g^b \pmod p$.
Eve doesn't know a or b.
Can Eve deduce $g^{ab} \pmod p$?
This boils down to:

Discrete Log Problem:
Given $g^a \pmod p$, g, and p, find a.
We can solve this by trial-and-error, but nobody knows how to solve it in a more efficient way!