Finding Prime Numbers

- There are some pretty slow and pretty fast methods for producing prime numbers. (We want a fast one!)
- The classic method is called the "sieve of Eratosthenes." (Yes, another Greek!)
- You can think of it like "panning for primes." Start with a big linear array of integers starting

$$(2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \ldots, n)$$

  where n is some big number.
- Erase all multiples of 2 bigger than 2:

$$(2, 3, \ , 5, , 7, \ , 9, \ , 11, \ , 13, \ , 15, \ldots, ?n)$$

- Erase all (remaining) multiples of 3 bigger than 3:

$$(2, 3, \ , 5, , 7, \ , \ , \ , 11, \ , 13, \ , \ , \ldots, ?n)$$

- In general choose the lowest remaining number not having had its multiples erased, and erase all of its multiples which happen to be left.
- This method will find all primes $\leq n$, but you might have to go up to $\sqrt{n}$ to find out. (E.G., when n = 49, you have to try 7.)
- If n is a 200-digit number, you might go through, say, 10^{50} passes.

Testing a number for being prime

- The sieve method might take a long time. Maybe there is a quick and easy formula.
- The Chinese mathematicians thought that

$$n \text{ is prime } \iff 2^{n-1} \equiv 1 \pmod{n}.$$

- Try this with $n = 2$ through 50 — it always works. But it is NOT true for all n. The integer $n = 341$ is the first counterexample. That is,

$$2^{340} \equiv 1 \pmod{341},$$

  but $341 = 11 \cdot 31$.
- It's actually true that

$$n \text{ is prime} \rightarrow 2^{n-1} \equiv 1 \pmod{n}.$$

- Counterexamples to the converse statement occur very rarely.

Pseudoprimes and Probabilistic Primality Tests

- The text defines a *pseudoprime* as a number n that satisfies $2^{n-1} \equiv 1 \pmod{n}$, but isn't prime.
- We mentioned that pseudoprimes are pretty rare.
- We'd like a more restrictive notion, a number that satisfies a lot of tests like $a^{n-1} \equiv 1 \pmod{n}$, for various carefully chosen a's.
- If a number passes a whole bunch of such tests, then it's almost certain to be prime. You can make the probability of n being one of these pseudoprimes "exponentially small" by doing a few more tests.
- Of course, we still have to know that any true prime number will pass the tests. That's the content of the next theorem.

Fermat's Little Theorem

- **Theorem** *Let p be a prime number and a be a positive integer such that p does not divide a. Then $a^{p-1} \equiv 1 \bmod p$.*

- *Proof:* Let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ be the set of remainders mod p. Consider the function $h : \mathbb{Z}_p \to \mathbb{Z}_p$ given by

$$h(x) = ax \bmod p.$$

For example, when $a = 2$ and $p = 5$, $h(3) = (2 \cdot 3) \bmod 5 = 1$. We claim that h is a bijective function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. To do that, we'll show that h is a surjective (onto) function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. By the lemma of the last lecture, this will show that h is also one-to one.

Let $y \in \mathbb{Z}_p$. We have to find an $x \in \mathbb{Z}_p$ such that $h(x) = y$; that is, $ax \bmod p = y$. This amounts to solving this congruence for x, which we can do because $\gcd(a, p) = 1$. In more detail, there is a unique $s \in \mathbb{Z}_p$ such that $as \equiv 1 \pmod p$. So if $y \in \mathbb{Z}_p$, $h(sy) = asy \bmod p = 1 \cdot y \bmod p$. Since $y \in \mathbb{Z}_p$, $y \bmod p = y$. Thus

$$h(sy \bmod p) = a(sy \bmod p) \bmod p = asy \bmod p = y,$$

and so we can take $x = sy \bmod p$. Therefore, h is onto, and by our lemma, h is also one-to one.

Now since $h(0) = 0$, we have that h is also a bijective fumction from $\{1, \ldots, p-1\}$ to itself. For example, when $a = 2$ and $p = 5$, we have $h(1) = 2$, $h(2) = 4$, $h(3) = 1$, and $h(4) = 3$.

Consider the product

$$h(p-1) \cdot h(p-2) \cdot \ldots \cdot h(1).$$

(In our example, this is $3 \cdot 1 \cdot 4 \cdot 2$.) This product is just $(p-1)!$, because h is bijective. Writing out the product, we get

$$(a(p-1) \bmod p) \cdot (a(p-2) \bmod p) \cdot \cdots \cdot (a \cdot 1 \bmod p) \equiv (a^{p-1} \cdot (p-1)!) \pmod{p}.$$

Therefore,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

or

$$(a^{p-1} - 1)(p-1)! \equiv 0 \pmod{p}.$$

This means that $p \mid (a^{p-1} - 1)(p-1)!$.

But p is a prime number, so if it divides a product of numbers, then it must divide one of the factors of the product. Since p does not divide $(p-1)!$, it must divide $a^{p-1} - 1$; and this is just the conclusion of the theorem. $\square$

OK, so what's Fermat's BIG theorem?

and who was Fermat anyway?

- Fermat was a very good French mathematician who lived in the 17th century. He was very prolific, and proved a whole lot of theorems.
- He also had the habit of claiming theorems, without giving proofs. (Sometimes he would give hints.) In all but one case, other mathematicians were able to prove his claims.
- The one exception was therefore called Fermat's LAST theorem, and it remained unproved until 1995, despite the best efforts of the world's greatest mathematicians.
- Fermat claimed the following statement: if x, y, z are positive integers, and n is a positive integer ≥ 3, then
$$x^n + y^n \neq z^n.$$
(For n = 2, this does not hold, as $3^2 + 4^2 = 5^2$.)
- Do not try this proof at home. For professionals only. Induction on n does not work, at least directly.
- The result was proved by a Princeton mathematician named Andrew Wiles, with some help from a colleague, Richard Taylor. It took Wiles seven years holed up in his attic. Even when he announced the result in 1993, the proof was not correct, but with Taylor's help, Wiles fixed it up.