Math 3527 (Number Theory 1)

Lecture #17 of 38 $\sim$ February 23rd, 2026

Primality Testing

- The Fermat Test + Lucas Criterion
- The Miller-Rabin Test
- The AKS Primality Test

This material represents §3.4.1–§3.4.3 from the course notes.

Motivation, I

In order to implement the cryptosystems (Rabin, RSA, zero-knowledge protocol) we have discussed, we need a way to generate large prime numbers.

- It might seem that finding large prime numbers would be very difficult, but it is actually relatively simple.
- The Prime Number Theorem says that the approximate number of primes less than X is $X/\ln X$.
- Therefore (roughly) the probability that a randomly-chosen large integer N is prime is about $1/\ln N$.
- So for example, if we choose a random integer with 100 digits (in base 10), it has an approximately $1/\ln(10^{100}) \approx 0.4\%$ chance of being prime.

Motivation, II

A random integer with 100 digits has an approximately $1/\ln(10^{100}) \approx 0.4\%$ chance of being prime.

Motivation, II

A random integer with 100 digits has an approximately $1/\ln(10^{100}) \approx 0.4\%$ chance of being prime.

- We can do better than this, though: half of these integers are even! So if we just pick odd numbers, our probability immediately doubles to 0.8%!
- If we throw away integers divisible by primes less than 20, the probability increases to about 2.5%.
- So, if we take 200 randomly chosen 100-digit integers with no prime factors less than 20 (easy to test for those), the probability that at least one of them is actually prime is about $1 - 0.975^{200} \approx 99.4\%$: quite good!

Even if we want 500-digit primes, we only need to test about 200 or so (skipping numbers with prime factors less than 100) to have a 75% chance of finding at least one prime.

Motivation, III

So, the point is that it's not that difficult to *find* large primes. But how are we going to know which numbers are prime?

- Here's one way: compute its prime factorization. Is this a good approach?

Motivation, III

So, the point is that it's not that difficult to *find* large primes. But how are we going to know which numbers are prime?

- Here's one way: compute its prime factorization. Is this a good approach?
- Answer: no, not really. Because trying to compute prime factorizations seems hard, and also, the whole point is that we don't want composite numbers, we want prime numbers!
- So: is there a way to test whether a given large integer n is prime or composite, without actually needing to find a factorization if n is composite?

Fermat, I

Recall Fermat's Little Theorem, which we proved a few weeks ago:

Theorem (Fermat's Little Theorem)

If p is a prime number, then $a^p \equiv a \pmod{p}$ for every integer a.

Fermat, I

Recall Fermat's Little Theorem, which we proved a few weeks ago:

Theorem (Fermat's Little Theorem)

If p is a prime number, then $a^p \equiv a \pmod{p}$ for every integer a.

Notice that Fermat's Little Theorem is a conditional statement, and remember (from basic logic) that a conditional statement ("if P, then Q") is logically equivalent to its contrapositive ("if not-Q, then not-P"). So what does the contrapositive say?

Fermat, I

Recall Fermat's Little Theorem, which we proved a few weeks ago:

Theorem (Fermat's Little Theorem)

If p is a prime number, then $a^p \equiv a \pmod{p}$ for every integer a.

Notice that Fermat's Little Theorem is a conditional statement, and remember (from basic logic) that a conditional statement ("if P, then Q") is logically equivalent to its contrapositive ("if not-Q, then not-P"). So what does the contrapositive say?

- It says this: "if $a^p \not\equiv a \pmod{p}$ for some integer a, then p is not prime".

Why do we care? Because it gives a condition for when an integer must be composite!

Fermat, II

We have obtained the following result:

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Examples:

Fermat, II

We have obtained the following result:

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Examples:

1. Because $2^{15} \equiv 8 \pmod{15}$, 15 must be composite. (Duh....)

Fermat, II

We have obtained the following result:

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Examples:

1. Because $2^{15} \equiv 8 \pmod{15}$, 15 must be composite. (Duh....)
2. Because $2^{391} \equiv 179 \pmod{391}$, 391 must be composite.

Fermat, II

We have obtained the following result:

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Examples:

1. Because $2^{15} \equiv 8 \pmod{15}$, 15 must be composite. (Duh....)
2. Because $2^{391} \equiv 179 \pmod{391}$, 391 must be composite.
3. Because $2^{197583752433463863487} \equiv 43395112453296191228 \pmod{197583752433463863487}$, the number 197,583,752,433,463,863,487 must be composite.

Fermat, III

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Look carefully at the statement of this test. Can we use it to conclude that an integer is prime?

Fermat, III

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Look carefully at the statement of this test. Can we use it to conclude that an integer is prime?

- No, we can't! Because the statement is only a conditional: "if $a^n \not\equiv a \pmod{n}$, then n is composite". It doesn't say anything at all in the situation where $a^n \equiv a \pmod{n}$.
- The Fermat test is not a primality test: it is a compositeness test. (That's why I called it that in the box above!)
- There are only two possible outcomes of the test: either it shows that n is composite, or it yields no result.

Fermat, IV

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Example: Test whether 1387 is composite.

- We try computing 2^{1387} mod 1387. Mathematica says it comes out to 2.
- Can we conclude that 1387 is prime?

Fermat, IV

Proposition (Fermat Compositeness Test)

If a is an integer such that $a^n \not\equiv a \pmod{n}$, then n is composite.

Example: Test whether 1387 is composite.

- We try computing 2^{1387} mod 1387. Mathematica says it comes out to 2.
- Can we conclude that 1387 is prime? No! As just explained on the last slide, that's not a possible conclusion from applying the test. Here, the test is inconclusive.
- Are we stuck? No, we can just try another a: if we try $a = 3$, Mathematica computes $3^{1387} \equiv 1238 \pmod{1387}$.
- This calculation shows 1387 must be composite.

Fermat, V

It would be quite pleasant if the Fermat test were successful for every composite number.

- Unfortunately, it is possible to make a bad choice for a, as we just saw with 1387. ($2^{1387} \equiv 2 \bmod 1387$.)
- If that happens, we can just try a different value of a.

Fermat, V

It would be quite pleasant if the Fermat test were successful for every composite number.

- Unfortunately, it is possible to make a bad choice for a, as we just saw with 1387. ($2^{1387} \equiv 2 \bmod 1387$.)
- If that happens, we can just try a different value of a.
- Example: With 341, trying $a = 2$ fails since $2^{341} \equiv 2 \pmod{341}$. But $a = 3$ will still work: $3^{341} \equiv 168 \pmod{341}$.

Fermat, V

It would be quite pleasant if the Fermat test were successful for every composite number.

- Unfortunately, it is possible to make a bad choice for a, as we just saw with 1387. ($2^{1387} \equiv 2 \bmod 1387$.)
- If that happens, we can just try a different value of a.
- Example: With 341, trying $a = 2$ fails since $2^{341} \equiv 2 \pmod{341}$. But $a = 3$ will still work: $3^{341} \equiv 168 \pmod{341}$.
- Example: With 2701: $2^{2701} \equiv 2 \pmod{2701}$ and $3^{2701} \equiv 3 \pmod{2701}$, but $5^{2701} \equiv 1966 \pmod{2701}$. (We didn't need to check $a = 4$ since 2 failed.)

Will there always be some value of a that succeeds?

Fermat, VI

Claim: For $n = 561 = 3 \cdot 11 \cdot 17$, the Fermat test fails, for *every* value of a, to recognize n as composite.

- We could just try all 561 residue classes ($1^{561} \equiv 1$, $2^{561} \equiv 2$, etc.). Or, better:
- By Fermat, we know $a^3 \equiv a \pmod 3$ for all a.
- Multiplying by a^2 yields $a^5 \equiv a^3$ but since $a^3 \equiv a$ we see $a^5 \equiv a \pmod 3$ as well. By a simple induction, one can iterate this to see $a^{2k+1} \equiv a \pmod 3$ for all k.

Fermat, VI

Claim: For $n = 561 = 3 \cdot 11 \cdot 17$, the Fermat test fails, for *every* value of a, to recognize n as composite.

- We could just try all 561 residue classes ($1^{561} \equiv 1$, $2^{561} \equiv 2$, etc.). Or, better:
- By Fermat, we know $a^3 \equiv a \pmod 3$ for all a.
- Multiplying by a^2 yields $a^5 \equiv a^3$ but since $a^3 \equiv a$ we see $a^5 \equiv a \pmod 3$ as well. By a simple induction, one can iterate this to see $a^{2k+1} \equiv a \pmod 3$ for all k.
- Similarly, $a^{11} \equiv a \pmod{11}$ so by induction one can check $a^{10k+1} \equiv a \pmod{11}$.
- Finally, $a^{17} \equiv a \pmod{17}$ so by another induction one can show $a^{16k+1} \equiv a \pmod{17}$.
- Taking the appropriate values of k one sees $a^{561} \equiv a$ mod 3, mod 11, and mod 17, hence by the Chinese remainder theorem, $a^{561} \equiv a$ mod 561.

Fermat, VII

This kind of counterexample is very upsetting, because it means that there might be more numbers out there for which the Fermat test just fails completely.

Definition

An integer m for which the Fermat test fails modulo m for every a (in other words, where $a^m \equiv a$ for all integers a) is called a Carmichael number, or pseudoprime.

Example: We just proved that 561 is a Carmichael number. (It is in fact the smallest one.)

- The next few Carmichael numbers are 1105, 1729, 2465, 2821, 6601, and 8911.

Fermat, VIII

Here are some general facts about Carmichael numbers:

- There are infinitely many Carmichael numbers, but they are much less common than primes.
- Specifically, the number of Carmichael numbers less than X is between $X^{1/3}$ and $X/(\ln X)^2$ for for large enough X.
- So in "real life", you're unlikely to see a Carmichael number accidentally. (The homework, on the other hand.... 😈)

Fermat, VIII

Here are some general facts about Carmichael numbers:

- There are infinitely many Carmichael numbers, but they are much less common than primes.
- Specifically, the number of Carmichael numbers less than X is between $X^{1/3}$ and $X/(\ln X)^2$ for for large enough X.
- So in "real life", you're unlikely to see a Carmichael number accidentally. (The homework, on the other hand.... 😈)

There is a nice criterion for identifying Carmichael numbers:

Proposition (Korselt's Criterion)

n is a Carmichael number if and only if n is a product of distinct primes, and for each prime p dividing n, $p-1$ divides $n-1$.

Example: For $n = 561$, we see 2, 10, 16 divide $n - 1 = 560$.

Fermat, IX

So as a practical matter, the Fermat test works fairly well if you try it for enough values of a.

- But, because of the existence of Carmichael numbers, it can sometimes fail to identify a number as composite.
- Additionally, the Fermat test can only establish that a particular integer is composite, and cannot be used to establish primality.
- So how can we know for sure an integer is prime?

Lucas, I

Here's one way to prove that a given integer actually is prime:

Proposition (Lucas Primality Criterion)

Suppose that m is a positive integer such that there exists a positive integer a with $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m-1$. Then m is prime.

Lucas, I

Here's one way to prove that a given integer actually is prime:

Proposition (Lucas Primality Criterion)

Suppose that m is a positive integer such that there exists a positive integer a with $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m-1$. Then m is prime.

- This condition should look a little familiar: can you identify what the conditions $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m-1$ actually show?

Lucas, I

Here's one way to prove that a given integer actually is prime:

Proposition (Lucas Primality Criterion)

Suppose that m is a positive integer such that there exists a positive integer a with $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m-1$. Then m is prime.

- This condition should look a little familiar: can you identify what the conditions $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m-1$ actually show?
- They are proving that a has order $m-1$ modulo m.
- The idea is that this is only possible when m is a prime. Why? Because to have order $m-1$, there must be $m-1$ units modulo m. Since 0 isn't a unit, this means all of 1, 2, ... , $m-1$ must be units, so they're relatively prime to m. That can only happen if m is prime.

Lucas, II

Proposition (Lucas Primality Criterion)

Suppose $a^{m-1} \equiv 1$ (mod m) but $a^{(m-1)/p} \not\equiv 1$ (mod m) for any prime p dividing $m-1$. Then m is prime.

Proof:

- By our properties of order, if $a^{m-1} \equiv 1 \pmod{m}$ but $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ for any prime p dividing $m-1$, then a has order $m-1$ modulo m.
- Since a has order $m-1$, the $m-1$ elements $a^0, a^1, \ldots a^{m-2}$ must all be distinct units modulo m.
- Since 0 is not a unit, this means each of 1, 2, ... , $m-1$ are units. Equivalently, they are all relatively prime to m, but this happens if and only if m is prime.

Lucas, III

Example: Show that the integer 2029 is prime.

Lucas, III

Example: Show that the integer 2029 is prime.

- With $m = 2029$ we have $m - 1 = 2028 = 2^2 \cdot 3 \cdot 13^2$. Now we test small values of a to see if they will work.
- Using successive squaring we can compute $2^{2028} \equiv 1$, $2^{2028/2} \equiv -1$, $2^{2028/3} \equiv 975$, and $2^{2028/13} \equiv 302 \pmod{2029}$.
- Therefore, 2 must have order 2028 modulo 2029, so by Lucas's primality criterion, we conclude that 2029 is prime.

Lucas, IV

So, how well does the Lucas criterion work?

- In order to apply the criterion, we need to find an a that has order $p-1$ modulo p, which is to say, a primitive root mod p.
- As we discussed previously (and will prove in about a month), there always exist primitive roots mod any prime, and in fact there will be $\varphi(\varphi(p)) = \varphi(p-1)$ of them, so there will certainly exist values of a that work.
- But...

Lucas, IV

So, how well does the Lucas criterion work?

- In order to apply the criterion, we need to find an a that has order $p-1$ modulo p, which is to say, a primitive root mod p.
- As we discussed previously (and will prove in about a month), there always exist primitive roots mod any prime, and in fact there will be $\varphi(\varphi(p)) = \varphi(p-1)$ of them, so there will certainly exist values of a that work.
- But... there is no known recipe for constructing a primitive root modulo a prime.
- Worse, we need a factorization of the integer $p-1$, which is needed in order to verify that the claimed element actually has order $p-1$ and not something smaller. If p is a large prime, it may be infeasible to factor $p-1$.

Improving Fermat, I

We would like to improve on the Fermat test.

- To begin, suppose p is prime and consider the solutions to $x^2 \equiv 1 \pmod{p}$. As we have seen several times, the solutions are $x \equiv \pm 1 \pmod{p}$.

Improving Fermat, I

We would like to improve on the Fermat test.

- To begin, suppose p is prime and consider the solutions to $x^2 \equiv 1 \pmod{p}$. As we have seen several times, the solutions are $x \equiv \pm 1 \pmod{p}$.
- So, if m is an odd prime, and a is any nonzero residue class, Fermat (or Euler) implies that for $x = a^{(m-1)/2}$, we have $x^2 = a^{m-1} \equiv 1 \pmod{m}$.
- Putting these together, we see $a^{(m-1)/2} \equiv \pm 1 \pmod{m}$.

So: if m is prime, then $a^{(m-1)/2} \equiv \pm 1 \pmod{m}$.

Improving Fermat, I

We would like to improve on the Fermat test.

- To begin, suppose p is prime and consider the solutions to $x^2 \equiv 1 \pmod{p}$. As we have seen several times, the solutions are $x \equiv \pm 1 \pmod{p}$.
- So, if m is an odd prime, and a is any nonzero residue class, Fermat (or Euler) implies that for $x = a^{(m-1)/2}$, we have $x^2 = a^{m-1} \equiv 1 \pmod{m}$.
- Putting these together, we see $a^{(m-1)/2} \equiv \pm 1 \pmod{m}$.

So: if m is prime, then $a^{(m-1)/2} \equiv \pm 1 \pmod{m}$.

- Taking the contrapositive (like with Fermat) we see that if $a^{(m-1)/2} \not\equiv \pm 1 \pmod{m}$ then m must be composite.

Example: As $3^{(561-1)/2} \equiv 441 \pmod{561}$, 561 is composite.

Improving Fermat, II

Already, this idea of testing whether $a^{(m-1)/2} \pmod{m}$ is $\pm 1 \pmod{m}$ gives us more than the Fermat test. But it can still fail to show an integer is composite.

Improving Fermat, II

Already, this idea of testing whether $a^{(m-1)/2} \pmod m$ is $\pm 1 \pmod m$ gives us more than the Fermat test. But it can still fail to show an integer is composite.

- You might have noticed I used $a = 3$ in the 561 example earlier: that's because $a = 2$ fails.
- Specifically, $2^{(561-1)/2} = 2^{280}$ comes out congruent to 1 modulo 561, which doesn't tell us anything.
- But here's a sneaky observation: the exponent 280 is even, so we have $(2^{140})^2 \equiv 2^{280} \equiv 1 \pmod{561}$. We can now just compute $2^{140} \equiv 67 \pmod{561}$.
- This means 561 must be composite! (Why? Because $67^2 \equiv 1 \pmod{561}$, but the only solutions to $x^2 \equiv 1$ modulo a prime are ± 1.)

Improving Fermat, III

So we can improve this idea: if we compute $a^{(m-1)/2} \pmod{m}$ and get $1 \pmod{m}$, then if $(m-1)/4$ is an integer we can try computing $a^{(m-1)/4} \pmod{m}$ to see if it is something other than $\pm 1 \pmod{m}$: if so, m must be composite.

Improving Fermat, III

So we can improve this idea: if we compute $a^{(m-1)/2} \pmod{m}$ and get $1 \pmod{m}$, then if $(m-1)/4$ is an integer we can try computing $a^{(m-1)/4} \pmod{m}$ to see if it is something other than $\pm 1 \pmod{m}$: if so, m must be composite.

- But why stop there? If we can pull out more factors of 2 from the exponent, we could keep going by taking out factors of 2 until there aren't any left.
- For instance, with $m = 561$ we could have tried a^{70} if a^{140} had ended up being 1 modulo m. And if a^{70} had been 1 mod m too, we could have tried a^{35}.
- If at any point we find a value x where $x^2 \equiv 1 \pmod{m}$ but $x \not\equiv \pm 1 \pmod{m}$, then m must be composite.

This is the idea behind the Miller-Rabin test.

Miller-Rabin, I

Here is the formalized statement:

Theorem (Miller-Rabin Test)

Let m be an odd integer and write $m-1=2^k d$ for d odd. For a residue class a modulo m, calculate each of the values a^d, a^{2d}, a^{4d}, ... , $a^{2^k d}$ modulo m. If the last entry is $\not\equiv 1 \pmod{m}$ then m is composite. Furthermore, if any entry in the list is $\equiv 1 \pmod{m}$ and the previous entry is not $\equiv \pm 1 \pmod{m}$, then m is composite.

Proof:

- Since $2^k d = m-1$, the last entry is just a^{m-1} so the first statement is simply applying the Fermat test.
- The second statement is an application of the contrapositive of the statement "$r^2 \equiv 1 \pmod{p}$ implies $r \equiv \pm 1 \pmod{p}$" established before.

Miller-Rabin, II

Example: Use the Miller-Rabin test to determine whether $m = 561$ is prime.

Miller-Rabin, II

Example: Use the Miller-Rabin test to determine whether $m = 561$ is prime.

- Observe $m - 1 = 2^4 \cdot 35$, so $k = 4$ and $d = 35$.
- We need to compute a^{35}, a^{70}, a^{140}, a^{280}, a^{560} modulo 561.
- We can do this rapidly by successive squaring (just find a^{35} then keep squaring it).
- With $a = 2$, this yields the list 263, 166, 67, 1, 1.
- Since the fourth term is 1 and the previous term is not $\equiv \pm 1 \pmod{561}$, we conclude that 561 is composite.

Miller-Rabin, III

Example: Use the Miller-Rabin test to determine whether $m = 2047$ is prime.

Miller-Rabin, III

Example: Use the Miller-Rabin test to determine whether $m = 2047$ is prime.

- Observe $m - 1 = 2 \cdot 1023$, so $k = 1$ and $d = 1023$.
- We need to compute a^{1023}, a^{2046} modulo 2047.
- With $a = 2$ this yields the list 1, 1. Since there are no terms preceding the initial 1, the test is inconclusive for $a = 2$.
- Next we try $a = 3$: this yields the list 1565, 1013. The last entry is not $\equiv 1$, so m is composite.

Miller-Rabin, III

Example: Use the Miller-Rabin test to determine whether $m = 1373653$ is prime.

Miller-Rabin, III

Example: Use the Miller-Rabin test to determine whether $m = 1373653$ is prime.

- Observe $m - 1 = 2^2 \cdot 343413$, so $k = 2$ and $d = 343413$.
- We need to compute a^d, a^{2d}, a^{4d} modulo m.
- With $a = 2$ the list is 890592, -1, 1. Since the -1 precedes the 1, the test is inconclusive.
- With $a = 3$ the list is 1, 1, 1. Since there are no terms preceding the initial 1, the test is inconclusive.
- With $a = 5$ the list is 1199564, 73782, 1370338. The last entry is not 1, so we see m is composite.

Miller-Rabin, IV

The Miller-Rabin test is much stronger than the Fermat test.

- This can be seen from 561: it is a Carmichael number, meaning that the Fermat test will never show it is composite.
- On the other hand, the Miller-Rabin test succeeds in showing 561 is composite using only the residue $a = 2$.

Miller-Rabin, IV

The Miller-Rabin test is much stronger than the Fermat test.

- This can be seen from 561: it is a Carmichael number, meaning that the Fermat test will never show it is composite.
- On the other hand, the Miller-Rabin test succeeds in showing 561 is composite using only the residue $a = 2$.

Definition

If m is odd and composite, and the Miller-Rabin test fails for a modulo m, we say that m is a strong pseudoprime to the base a.

It turns out that strong pseudoprimes are fairly uncommon.

- For example, one can prove that for any odd composite m, the Miller-Rabin test succeeds for at least 75% of the residue classes modulo m.
- In particular, there are no "Carmichael numbers" for the Miller-Rabin test, where the test fails for every residue class.

Miller-Rabin, V

If an integer m passes the Miller-Rabin test for more than $m/4$ residue classes modulo m, then m is prime.

- This is not a computationally effective way to show that an integer is prime, since it requires $m/4$ calculations (far more than trial division).
- However, if we assume the Generalized Riemann Hypothesis (typically believed to be true), it has been proven that testing the first $2(\log m)^2$ residues modulo m is sufficient.

Miller-Rabin, V

If an integer m passes the Miller-Rabin test for more than $m/4$ residue classes modulo m, then m is prime.

- This is not a computationally effective way to show that an integer is prime, since it requires $m/4$ calculations (far more than trial division).
- However, if we assume the Generalized Riemann Hypothesis (typically believed to be true), it has been proven that testing the first $2(\log m)^2$ residues modulo m is sufficient.

In practice, the Miller-Rabin test is used "probabilistically": we apply the test many times to the integer m, and if it passes sufficiently many times, we say m is probably prime.

- This is similar to the argument for zero-knowledge proofs: the probability of accidentally passing the test 30 times is less than $(1/4)^{30} \approx 10^{-18}$, which is small enough to ignore.

Other Primality Tests, I

It would be nice to have a provably fast algorithm that determines whether a given integer m is prime. In fact, there is one, based on the following observation:

Observation

If a is relatively prime to m and x is a variable, then $(x+a)^m \equiv x^m + a$ (modulo m) holds, as a polynomial congruence in x with coefficients modulo m, if and only if m is prime.

Examples:

- For $a = 2$ and $m = 5$, the result says $(x+2)^5 = x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32$ is equivalent (modulo 5) to the polynomial $x^5 + 2$, which it is.

Other Primality Tests, I

It would be nice to have a provably fast algorithm that determines whether a given integer m is prime. In fact, there is one, based on the following observation:

Observation

If a is relatively prime to m and x is a variable, then $(x+a)^m \equiv x^m + a$ (modulo m) holds, as a polynomial congruence in x with coefficients modulo m, if and only if m is prime.

Examples:

- For $a = 2$ and $m = 5$, the result says $(x+2)^5 = x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32$ is equivalent (modulo 5) to the polynomial $x^5 + 2$, which it is.
- For $a = 1$ and $m = 4$, the result says $(x+1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1$ should not be equivalent (modulo 4) to the polynomial $x^4 + 1$, which it is not.

Other Primality Tests, II

Although this result is a primality test, it is not especially useful, since computing the necessary binomial coefficients is slow.

- One way to speed it up is to take both sides modulo the polynomial $x^r - 1$ for some small r: in other words, to check whether the relation $(x + a)^m \equiv x^m + a \pmod{x^r - 1}$ holds, where coefficients are also considered modulo m.
- The difficulty is that we may lose information by doing this.
- But it turns out that if we choose r carefully, and verify the congruence for enough different values of a, we can prove that it necessarily holds in general (essentially, via the Chinese Remainder Theorem).

Other Primality Tests, III

Here is the resulting primality test:

Theorem (Agrawal-Kayal-Saxena Test)

Let $m > 1$ be an odd integer not of the form a^b for any $b > 1$. Let r be the smallest value[a] such that the order of r modulo m is greater than $(\log m)^2$: if $m > 10^7$ then there will always be such an r satisfying $r \leq 1 + (\log m)^5$.

- *For each a with $1 \leq a \leq \sqrt{\varphi(r)} \log m$, check whether $(x + a)^m \equiv x^m + a \ (mod\ x^r - 1, m)$.*
  - *If any of these congruences fails, m is composite.*
  - *Otherwise, m is prime.*

---

[a] The value r can be computed simply by finding the orders of 2, 3, ... , until one of them has an order exceeding this bound; if any of these integers divide m clearly m is composite, and if no such r exists then m is prime.

Other Primality Tests, IV

We will not prove the correctness of the AKS algorithm here.

- However, we will note that the algorithm gives an affirmative declaration of whether m is prime or composite (unlike the previous tests we have discussed).
- Furthermore, the runtime of this algorithm is a polynomial in $\log m$: it is much more efficient than (say) trial division, which has a runtime of roughly $\sqrt{m}$.
- The version described here runs in time roughly equal to $(\log m)^{12}$, and there have been subsequent modifications that lowered the time to approximately $(\log m)^6$.
- However, this is much slower than the "probabilistic" tests like the Miller-Rabin test, which is believed to run in time approximately $(\log m)^4$.

Summary

We discussed the Fermat compositeness test and showed how it can prove large numbers are composite.

We discussed the Lucas primality criterion and showed how it can prove a large number is prime.

We discussed the Miller-Rabin test and how it is used probabilistically for primality testing.

We outlined the AKS primality test, a deterministic polynomial-time algorithm for primality testing.

Next lecture: Algorithms for prime factorization.