The Prime Facts: From Euclid to AKS

1 Introduction

My idea for this talk was to tell you only the *simplest, most basic* things about prime numbers—the things you need to know to call yourself a human being rather than a beast. The trouble is, when I went to prepare the talk, I realized I didn't know all those things myself, or had forgotten them. So thanks for saving me from my own ignorance!

The story will start with Euclid in ancient Greece, and will end with a breakthrough made this August by three guys in India. Along the way we'll talk about quantum computers, the most widely used cryptosystem on Earth, and a few other things. Traditionally, most of the story is told in a language called *abstract algebra*—a language involving such strange objects as fields you can't mow and rings you can't wear. My challenge will be to tell the story without that language.

So what's a prime number? A whole number with exactly two divisors. Is 1 prime? No, it has only one divisor, 1. What about 2? 3? 4? 5? What are the next few primes? 7, 11, 13, 17, 19, 23, 29, 31, 37. What about $827,902,375$? No, 5 goes into it. $14,351$? No, it's 113×127. That was a tough one! On the other hand, if I gave you 113 and 127, you could multiply them pretty easily, couldn't you?

2 Number of Primes

How many primes are there? Infinitely many? How do you know that? As it happens, humans have known for 2300 years that there's no largest prime. The proof goes back to Euclid, and it's by contradiction. He said, suppose there were only three primes, P, Q, and R. Of course, *we* know there are more than three—2, 3, 5, 7 are four already—but the same idea works for any finite number of primes. The idea is, look at $PQR+1$. Does P divide $PQR+1$? No, it leaves a remainder of 1, since P divides PQR. Same thing for Q and R. But then $PQR+1$ is either prime, or else has a prime factor that isn't P, Q, or R. Either way we get a new prime not on the original list.

There's a story that a mathematician (I think Paul Erdös) was trying to explain to a nonmathematician what he did for a living. So, to illustrate what a proof is, he gave the argument that there are infinitely many primes. As he did, the other guy nodded and said "sure, that makes sense . . . P can't go into $PQR+1$ . . . I understand. . . " But at the end he seemed dissatisfied, so Erdös asked what the problem was. "*Why did you lie to me?*" came the reply. "Why did you tell me those are the only primes, when they *aren't*?"

In any case, we now know why there are infinitely many primes. Here's a harder question: if I pick a number at random, what is the chance that it's prime? Of course the question doesn't make sense! But if I pick an N*-digit* number at random, what is the chance that *that's* prime? You may have noticed that the primes 'thin out' as you look at larger and larger numbers—not too surprising, since the bigger the number, the more divisors it could potentially have. The question is, at what *rate* do the primes thin out? Here's the answer, which was discovered 100 years ago by Hadamard and de la Vallée-Poussin:

The chance that an N-digit number is prime is about 1 in 2.3N.

Let's see how good this estimate is:

Up To	Actual # of Primes	Predicted (Closest Integer)
10	4	4
100	25	22
1,000	168	145
10,000	1,229	1,087
100,000	9,592	8,696
1,000,000	78,498	72,464
10,000,000	664,579	621,118
100,000,000	5,761,455	5,434,783
1,000,000,000	50,847,534	48,309,179

As you can see, it's consistently undercounting, though not by much. The accuracy of this estimate is closely related to the *Riemann Hypothesis*, which mathematicians consider the most important unsolved problem today (though I'm not sure exactly why).

3 Unique Factorization

Why are primes important? The usual answer is, because they're the building blocks of the whole numbers. But are they really? Let's put it this way: we know that every whole number can be factored into primes. But is there a number that can be factored into primes in *two different ways*? Saying $15 = 3 \times 5 = 5 \times 3$ doesn't count—I want two *really* different factorizations.

You need to understand that the answer to this question isn't obvious. In math class, a lot of the rules you learn probably seem pointless, because you never see any situation where they're *false*. I mean, *of course* every number has a unique factorization! How could it not? Well, I'll give an example of a number system where numbers can be factored more than one way. Take numbers of the form $A + B\sqrt{5}$, where A and B are integers (positive, negative, or zero). That's a perfectly valid number system. Now, what are the prime factors of 4? 2×2 works; it turns out 2 is still prime in this system. But there's another factorization:

$$4 = \left(1 + \sqrt{5}\right)\left(-1 + \sqrt{5}\right).$$

So for ordinary whole numbers, the fact that primes are 'building blocks'—that every number has one and only one prime factorization—isn't obvious. But it was proved, again by Euclid.

The key step is this: *If P is prime and P divides AB, then either P divides A or P divides B.* Why? Suppose P doesn't divide B. Let $R > 0$ be the remainder when P goes into B; then $B = CP + R$ for some whole number C. Now suppose P divides AB; then P divides $A(CP + R) = ACP + AR$. So P divides AR, and $PK = AR$ for some whole number K. Thus $P/A = R/K$. But R is less than P, since it's a remainder from dividing by P. So P/A can't be in lowest terms; something greater than 1 divides both P and A. But nothing divides P except 1 and itself, so P divides A.

Once we know that, it's easy to see why every whole number has a unique factorization. Let P be a prime factor of N; then $N = PK$ for some whole number K. Let Q be another prime factor of N. Then Q has to divide K, unless $Q = P$. So we can split up K, and keep going until all that's left is primes.

4 Patterns

Look again at the first few primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 \ldots$$

Question: Is there a pattern here, or are the primes sprinkled pretty much randomly throughout the whole numbers, apart from the statistical law I mentioned before?

That's the kind of question you can never answer until you get clear about what it means! On the one hand, there are thousands of *little* patterns. For instance, let's ask which primes can be written as a sum of two squares.

2	Yes: $1^2 + 1^2$
3	No
5	Yes: $2^2 + 1^2$
7	No
11	No
13	Yes: $3^2 + 2^2$
⋮	

Do you see a pattern? Amazingly enough, the rule is this: *A prime can be written as a sum of two squares if (and only if) it leaves a remainder of 1 or 2 when divided by 4.* I won't prove that here, but it's one example of a pattern.

Another example: which even numbers can be written as a sum of two primes?

2	No
4	Yes: $2 + 2$
6	Yes: $3 + 3$
8	Yes: $5 + 3$
10	Yes: $7 + 3$, $5 + 5$
12	Yes: $7 + 5$
⋮	

The famous *Goldbach conjecture* says that *every* even number greater than 2 can be written as a sum of two primes. Since 1742, no one has been able to prove it—but we know it's true for all even numbers up to 400 trillion. We also know that every *odd* number *greater* than about $10^{43,000}$ can be written as a sum of *three* primes (that's called Vinogradov's Theorem).

5 Pascal's Triangle

I'm going to draw a triangle that you might or might not have seen before.

```
0                  1
1                1   1
2              1   2   1
3            1   3   3   1
4          1   4   6   4   1
5        1   5  10  10   5   1
6      1   6  15  20  15   6   1
7    1   7  21  35  35  21   7   1
8  1   8  28  56  70  56  28   8   1
9 1  9  36  84  126  126  84  36  9  1
```

Suppose we number each row, starting from 0. Do you see a difference between the prime-numbered and the composite-numbered rows?

Found it yet? If N is prime, then the N^{th} row contains only multiples of N, ignoring the 1's on the left and right. But if N is composite, then the N^{th} row has numbers other than 1 that are *not* multiples of N—for instance, 15 and 20 in the 6^{th} row.

Let's try to see why that is. In the N^{th} row of Pascal's Triangle, the K^{th} number from the left (starting at 0) is

$$\binom{N}{K} = \frac{N!}{K!\,(N-K)!} = \frac{N\,(N-1)\cdots(N-K+1)}{K\,(K-1)\cdots 2\cdot 1}.$$

First suppose N is prime. Does anyone see why N has to divide $\binom{N}{K}$? Well, there's an N in the numerator there, and all the numbers in the denominator are smaller than N, so none of them cancel it.

Now suppose N is composite. Can anyone tell me an entry other than 1 in the N^{th} row of Pascal's Triangle that N *doesn't* divide? This is trickier! Well, let me just show you the simplest case, which is that $N = PQ$, where P and Q are distinct prime numbers. We have

$$\begin{aligned}\binom{N}{P} &= \frac{N\,(N-1)\cdots(N-P+1)}{P\,(P-1)\cdots 2\cdot 1}\\ &= \frac{PQ\,(PQ-1)\cdots(PQ-P+1)}{P\,(P-1)\cdots 2\cdot 1}\\ &= \frac{Q\,(PQ-1)\cdots(PQ-P+1)}{(P-1)\cdots 2\cdot 1}.\end{aligned}$$

After we cancel the P's out, I claim that P doesn't divide the numerator any longer. Why not? Because P doesn't divide Q by assumption, and since it *does* divide PQ and $PQ-P$, it can't divide any of $PQ-1,\ldots,PQ-P+1$. So P doesn't divide $\binom{N}{P}$, and therefore neither does N. (If you want a challenge, try to prove that if N is an *arbitrary* composite number, there's an entry other than 1 in the N^{th} row of Pascal's Triangle that N doesn't divide.)

Stop to think about this. What it means is, if you have a number N, and you want to know whether it's prime or composite, you can *test* that by looking at the N^{th} row of Pascal's Triangle. Is this a good test for primality? Why not?

The trouble is, the N^{th} row of Pascal's Triangle has $N+1$ numbers. And as long as you're looking at $N+1$ numbers, you might as well just try all possible divisors of N! So this is not an *efficient* test. In spite of that, I want to convince you that this Pascal's Triangle fact is somehow the *central* fact about prime numbers. It's the starting point for almost everything else I'll talk about today.

6 Fermat's Little Theorem

If you've heard of Fermat's *Last* Theorem, this is different, and much, much easier to prove. It says:

If P is prime, then P divides $X^P - X$.

Let's do an example. Pick a prime P, say 3. And an X, say 4. Then $X^P - X$ is $4^3 - 4$, or $64 - 4 = 60$. Sure enough, 3 goes into 60. Another example:

$$\begin{aligned}P &= 7\\ X &= 2\\ X^P - X &= 2^7 - 2\\ &= 126\end{aligned}$$

which is indeed divisible by 7.

But why is this always true? Let's prove it by induction on X. When $X = 0$ it says that P divides 0, which is clearly true. Suppose it holds for X; then the remainder when P goes into X^P is X. What is the remainder when P goes into $(X+1)^P$? Let's expand:

$$(X+1)^P = X^P + \binom{P}{P-1} X^{P-1} + \binom{P}{P-2} X^{P-2} + \cdots + \binom{P}{1} X + 1.$$

From our Pascal's Triangle fact, we know that the $\binom{P}{K} X^K$ terms can't matter, since P divides $\binom{P}{K}$. So the remainder is the same as when P goes into $X^P + 1$, and therefore it's $X + 1$.

One more observation: $X^P - X$ is just $X(X^{P-1} - 1)$. So if X is not a multiple of P, then P must divide $X^{P-1} - 1$. This is another way to state Fermat's Little Theorem.

7 Primes and the Mob

Let's switch gears for a while and talk about something *completely* unrelated to prime numbers.

You're in the mob—but you're a double-crosser. So you write a book that reveals all the mob's secrets: who murdered whom, where the hideouts are, etc. Your first idea is to publish the book with your name on the cover, so you'll be hailed as a hero who brought down the mob. But after thinking it through, you realize that's not the best idea—you don't want your feet in cement. So you'll publish it anonymously. But then you'll never get credit for what you did! Later on, after the mob leaders have been arrested (thanks to your efforts) and it's safe, you could tell people you wrote the book, but there'd be no reason for them to believe you. *Question:* Is there a way to publish the book so that (1) it's anonymous now, but (2) later on you can prove that no one but you could have written it?

As you might have guessed, I was lying when I said this is unrelated to prime numbers. Here's what you can do: pick two enormous primes at random. We'll talk later about how to do that, but for now suppose the primes are $47,287$ and $48,869$. (In reality you'd want them much bigger, say 300 digits.) Then multiply the primes to get a composite, in this case $2,310,868,403$. Finally, print that composite in an appendix to the book. Later, when it's safe, you can prove you're the author by revealing the primes you multiplied. It's easy to check that those are the right primes (just multiply them), but for anyone who didn't know them, they'd be pretty hard to find!

The key here, which seems incredible the first time you hear it, is the following:

> *There are quick ways to test whether a number N is prime or composite.*
>
> *But if N is composite, then actually finding its factors takes a huge amount of time by any current method.*

8 Public-Key Cryptography

I'll say more about this, but first, here's a slightly more legitimate scenario. How many of you have ordered stuff from Amazon.com (or any web site)? Did you have to enter your credit card number? If so, did you worry about the number being stolen? After all, a message sent over the Internet is no more secret than a postcard. Anyone can read it who has access to a server relaying the message. So what's the solution?

Well, it turns out modern web browsers have something called Secure Sockets Layer (SSL), which encrypts messages—that is, translates them into a secret code. But how is *that* possible? Did you ever meet an Amazon employee in a dark alley to agree on a code? How can you send someone a secret message if you've never even *met* them before to agree on a code? I mean, you don't exactly want to send a message on the Internet announcing, "The password is ROSEBUD. From now on, all messages from me will be encrypted using ROSEBUD as the key."

You have to realize that cryptography has played a major role in world history for several thousand years. For instance, you can't understand World War II without knowing about a place called Bletchley Park, where a group of mathematicians (including Alan Turing) broke the code that the Nazis used to communicate with U-boats. So people have been making and breaking codes for thousands of years, and yet this problem I mentioned—that you can't send a secret message to someone without agreeing on a code beforehand—had never been solved. And then, in 1978, the problem was solved. It was solved by three guys named Rivest, Shamir, and Adleman (RSA), by using properties of prime numbers.

Here's how a variant of the RSA system works.

(1) Amazon (*not* you) chooses two huge prime numbers, say P and Q. (A technical requirement is that neither $P-1$ nor $Q-1$ is a multiple of 3.)

(2) Amazon sends you the *product* of P and Q, call it N—but the primes themselves it keeps secret.

(3) Whatever message you want to send (i.e. your credit card information), you encode as a whole number X. We'll assume X is less than N and relatively prime to it. (If X is greater than N, you can break your message up into several smaller ones and send them independently.)

(4) You send Amazon the following:

$$Y = X^3 \bmod N.$$

Here "$X^3 \bmod N$" just means the remainder when N goes into X^3. (That's good notation to get used to.)

(5) Given Y, Amazon has to figure out what X was.

Step (5) seems hard! But recall, Amazon knows not only N, but the prime factors P and Q of N. Remember when we proved Fermat's Little Theorem? It said that if P is prime and X is not a multiple of P, then P divides $X^{P-1}-1$. It turns out that this can be generalized to composite numbers as follows:

If $N = PQ$ where P and Q are primes, and X is relatively prime to N, then N divides $X^{(P-1)(Q-1)}-1$.

It follows that N divides $X^{1+(P-1)(Q-1)}-X$, or in other words, $X^{1+(P-1)(Q-1)} \bmod N$ equals X. Now think about this sequence:

$$\begin{gathered} X \bmod N \\ X^2 \bmod N \\ X^3 \bmod N \\ \vdots \end{gathered}$$

For a fixed N, each value in the sequence depends only on the last one. Therefore, since there are only N possible values (0 to $N-1$), the sequence has to repeat eventually. What's more, by the above, the *period* of the sequence (the number of values until it starts repeating itself) has to divide $(P-1)(Q-1)$. For observe that it makes no difference whether we take the remainder mod N at every step, or whether we wait until the end to do so. (In fact, we could imagine an 'alternate universe' of arithmetic, where *everything* is a remainder mod N! Hmm...)

Let's do an example. Take $N = 15$ and any X relatively prime to N, say $X = 2$. The prime factors of 15 are $P = 5$ and $Q = 3$. So $(P-1)(Q-1) = 8$, and we predict that the period of the sequence should divide 8. Does it?

$$\begin{aligned}
2 \bmod 15 &= 2\\
4 \bmod 15 &= 4\\
8 \bmod 15 &= 8\\
16 \bmod 15 &= 1\\
32 \bmod 15 &= 2\\
64 \bmod 15 &= 4\\
128 \bmod 15 &= 8\\
256 \bmod 15 &= 1\\
&\vdots
\end{aligned}$$

Indeed! The period is 4, which divides 8.

So the general law is:

$$\text{For any whole number } K,\ X^{1+K(P-1)(Q-1)} \bmod N = X.$$

Remember, Amazon's goal is to find X, given $Y = X^3 \bmod N$. Recall that $(P-1)(Q-1)$ is not divisible by 3, since neither $P-1$ nor $Q-1$ is. It's easy to check, then, that either $1+(P-1)(Q-1)$ or $2+(P-1)(Q-1)$ *must* be divisible by 3. Suppose $1+(P-1)(Q-1)$ is, and let

$$C = \frac{1+(P-1)(Q-1)}{3}.$$

Then

$$\begin{aligned}
Y^C \bmod N &= \left(X^3\right)^C \bmod N\\
&= X^{3C} \bmod N\\
&= X^{1+(P-1)(Q-1)} \bmod N\\
&= X \bmod N.
\end{aligned}$$

Bingo! All Amazon needs to do is raise Y to the C power and take the remainder mod N, and it gets back the original message X. Only one question remains: how does Amazon raise Y to the C power? One way would be just to multiply Y by itself C times. But if C is large, then this method takes way too long. A better method uses what's called *repeated squaring.* Starting from Y, it's easy to produce Y raised to any power of 2:

$$\begin{aligned}
\left(Y^2\right)^2 &= Y^4\\
\left(Y^4\right)^2 &= Y^8\\
\left(Y^8\right)^2 &= Y^{16}\\
\left(Y^{16}\right)^2 &= Y^{32}\\
&\vdots
\end{aligned}$$

Since we take the remainder mod N after each squaring step, the numbers never get too big to handle. Now, we can write any whole number C as a sum of powers of 2—for example, if $C = 25$, then $C = 16 + 8 + 1$. Then (in this example) $Y^C = Y^{16+8+1} = Y^{16} \times Y^8 \times Y^1$. So we can write Y^C as a *product* of terms, each of which we can compute using repeated squaring.

Remember, this (or something close to it) is what *actually* happens when you order books from Amazon! The security of the system rests on the assumption that an eavesdropper, who knows Y and N but not the prime factors P and Q of N, would have an extremely hard time figuring out X. So it goes without saying that, if there's a fast method for *factoring* N into $P \times Q$, then the whole RSA scheme is broken.

9 Finding Factors

So if you discovered a fast method for factoring whole numbers, you could certainly make a lot of money, and possibly topple governments! Needless to say, a lot of smart people have thought about the problem for a long time, but they haven't solved it. There *are* advanced methods that are *somewhat* faster than the naïve method of just trying all possible divisors, but those methods still aren't fast enough to factor, say, a 1000-digit number in less than the current age of the Universe. Some people speculate that the National Security Agency (NSA) knows a fast factoring method, but aren't telling anyone! But there are reasons for doubting that—for example, if they're so omniscient, why didn't they know about 9-11?

However, all of that applies only to *classical* computers. In the 1980's, people such as David Deutsch and Richard Feynman asked what would happen if you could build a computer out of individual electrons or atomic nuclei. They realized that such a computer would be governed by *quantum mechanics*, in which a particle can be in a 'superposition' of many locations at once. In principle, such a computer might be *fundamentally* more powerful than a classical one—not in the sense that, say, a Pentium is 10 times faster than a 486, but in the sense that entirely new problems could be solved, which were hopelessly intractable for *any* classical computer. However, they couldn't come up with a specific example of such a problem.

That changed in 1994, when Peter Shor showed that a quantum computer could factor whole numbers extremely quickly—and could therefore break the RSA system! Shor's breakthrough launched the field of *quantum computing*, which is quite active today, and which is what I study. Tiny quantum computers have even been built in the lab, which are able, for example, to factor 15 into 3×5. As for building larger, more useful quantum computers, there are huge engineering obstacles, but there's a chance it will happen within your lifetime. If it happens, then Amazon and everyone else will have to switch from RSA to a different cryptosystem! (For despite their power, quantum computers are not a panacea. They're great for factoring whole numbers, but for many other tasks, they're just as slow as classical computers so far as anyone knows.)

10 Testing Primality

Anyhow, factoring enormous numbers remains hard given the computers we have today. But what if you just want to know whether a number is prime or composite, and not what the factors are? Even in 1801, Gauss seemed to realize that factoring and primality testing are two different problems, as is shown in an oft-repeated passage:

> *The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.*

Indeed, as I mentioned before, testing primality is much easier than actually finding factors. That's good, because otherwise the RSA system wouldn't work! Recall that the first step was for Amazon to choose two huge prime numbers P and Q. Recall also that, among N-digit numbers, about one in $2.3N$ is prime—a pretty big fraction. So if there's a quick way of distinguishing primes from composites, then Amazon's problem is solved: they can just keep picking N-digit numbers at random, and stop as soon as they find a prime.

But given a whole number, say $241,099$, how would you test if it's prime or composite? The most obvious way is just to try all possible divisors: Does 2 go into it? No. Does 3? No. 4? It can't, since 2 doesn't. And so on. Incidentally, how many possible divisors do you need to try? Everything from 2 up to $241,099$? Clearly not: for if $241,099$ has a divisor greater than $\sqrt{241,099}$ (or about 491), then it also has a divisor less than $\sqrt{241,099}$. Even with that improvement, though, this method is slow. To test whether a 300-digit number is prime, we'd need to try about 10^{150} divisors!

Is there a better way? We hinted at one when we proved Fermat's Little Theorem, which says that if N is prime, then N divides $X^N - X$. An implication is that if N *doesn't* divide $X^N - X$ for some X, then N can't be prime. For instance, taking $X = 3$ and $N = 4$,

$$\begin{aligned} X^N - X &= 3^4 - 3 \\ &= 78 \end{aligned}$$

which is not divisible by 4. This proves that 4 must be composite, even though it doesn't tell us what the divisors are! The reason the Fermat test is faster than trial division is that we can do all the arithmetic 'mod N,' so the numbers never get too big for us to handle.

The trouble with the Fermat test is that it doesn't always work. For some composite N and some X, N *does* divide $X^N - X$, just as if N were prime. For instance, $2^{341} - 2$ is divisible by 341, even though $341 = 11 \times 31$ is a composite number. Actually the situation is worse: there are composite numbers N that 'think they're prime,' i.e., that pass the Fermat test for *every* X relatively prime to N. These are called the *Carmichael numbers*; the smallest is $561 = 3 \times 11 \times 17$. It was proved in 1992, by Alford, Granville, and Pomerance, that there are infinitely many Carmichael numbers.

So, is there a *fast* primality test that *always* works? By "fast," we mean that the number of steps needed to decide whether N is prime should be at most the *number of digits* of N raised to some fixed power. Is the trial division method fast? Clearly not, since it may need to try $\sqrt{N}$ possible divisors—and $\sqrt{N}$ grows *exponentially* in the number of digits of N. We want the amount of time to grow *polynomially* in the number of digits.

In 1976, Miller gave a fast primality test that always works, *assuming* an extended version of the Riemann Hypothesis (which we mentioned when we talked about the number of primes). What if we remove that assumption? Well, soon afterward, Solovay and Strassen and (separately) Rabin gave fast primality tests that always work under no assumptions, but are *randomized.* Here's what that means: suppose you want to know whether a number N is prime or composite. Then you run the test with N *and* another number X, which you choose at random. So far that's the same as for the Fermat test. But unlike the Fermat test, the new tests have the following nice guarantee:

(1) If N is prime, then for *any* choice of X, the output is 'prime.'

(2) If N is composite, then for *most* choices of X, the output is 'composite.'

This means that if the test outputs 'composite,' N is definitely composite. On the other hand, if the test outputs 'prime,' N is *probably* prime, but there's a small chance that it isn't. If you want to be more confident that N is prime, you can keep repeating the test with different choices of X. If you try, say, 500 values of X, and every time the output is 'prime,' then you can be sure N is prime *for all practical purposes.*

For it's much more likely that a cosmic ray hit your computer and made it malfunction, than that the test failed because of bad choices of X!

But what if that's not good enough? What if you want to be *certain* a number is prime? In 1992, Adleman and Huang proposed a test that lets you achieve this. Their test has the following guarantee, which is the "opposite" of the previous one:

(1) If N is prime, then for *most* choices of X, the output is 'prime.'

(2) If N is composite, then for *any* choice of X, the output is 'composite.'

So if this test outputs 'prime,' N is definitely prime; if it outputs 'composite,' N is probably composite.

Notice that by combining these two tests, you can get a primality test that *never* makes a mistake. Just run the Solovay-Strassen and the Adleman-Huang tests *alternately*, until either the first one outputs 'composite,' or the second one outputs 'prime'! The only trouble is that, after a fixed number of runs, there's a small chance that *neither* of these things will have happened. In that case you have to give up; you don't know whether N is prime. Again, the chance of this can be made so small that it never matters in practice, but annoyingly, it's still there!

11 The AKS Breakthrough

That's where things stood until this August. Then "AKS"—Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, from the Indian Institute of Technology at Kanpur—announced a fast primality test that *always* works under *no* assumptions and is *not* randomized. Since the problem had been unsolved for so long, this result won the admiration of everyone in the field, and was even covered in the *New York Times.* Notably, although Agrawal was already a well-known computer scientist, Kayal and Saxena were *undergrads* at the time they did most of the work.

Not only does the new test never fail, but it's considerably simpler than older tests (particularly Adleman-Huang). On the other hand, the AKS test is also slower than older tests. Originally the number of steps in AKS grew like the number of digits of N raised to the 12^{th} power. A few months ago Lenstra improved this; now it's the number of digits raised to roughly the 6^{th} power. For older tests, by comparison, the growth rate is like the number of digits cubed.

So how does the AKS test work? The key is the Pascal's Triangle fact I showed you a while ago, which I claimed was somehow the 'central' fact about prime numbers. Recall: if N is prime, then every number in the N^{th} row of Pascal's Triangle (besides 1) is a multiple of N. If N is composite, this is no longer true; there are numbers besides 1 in the N^{th} row that are not multiples of N. A corollary of this fact (and of Fermat's Little Theorem) is that, for any A that's relatively prime to N,

$$(X+A)^N \bmod N = \left(X^N + A\right) \bmod N$$

for all values of X, *if and only if* N is prime.

Let's do two examples. Take $N = 3$ and $A = 2$. Then

$$\begin{aligned}(X+A)^N \bmod N &= (X+2)^3 \bmod 3 \\ &= \left(X^3 + 6X^2 + 12X + 8\right) \bmod 3 \\ &= X^3 + 2\end{aligned}$$

which is $X^N + A$. So the identity holds, and we conclude that 3 is prime. Now take $N = 4$ and $A = 3$. Then

$$\begin{aligned}(X + A)^N \bmod N &= (X + 3)^4 \bmod 4\\ &= \left(X^4 + 12X^3 + 54X^2 + 108X + 81\right) \bmod 4\\ &= X^4 + 2X^2 + 3.\end{aligned}$$

Because of the extra $2X^2$ term, this is *not* equal to $X^N + A = X^4 + 3$ for all values of X. So we conclude that 4 is composite, even though we haven't learned what its prime factors are.

This means that, if only we could examine the whole binomial expansion of $(X + A)^N$, we'd have an infallible test for whether N is prime! If all the "middle" terms have coefficients divisible by N, then N is prime; otherwise N is composite.

What's the trouble with this binomial test? Same as with the original Pascal's Triangle test: for huge N, there are too many terms in the binomial expansion to check them all! *The idea of AKS was to speed up the binomial test, while still being able to prove that it gives the right answer whenever N is composite.* The way they speed things up is to work, not only mod N, but also mod a polynomial $X^R - 1$ (where R is a reasonably small prime). That is, instead of computing $(X + A)^N$, they compute the *remainder* when $(X + A)^N$ is divided by $X^R - 1$. That's done using the same method you learn in algebra class for dividing one polynomial by another. What's nice about the remainder is that it has only $R + 1$ terms, as opposed to $N + 1$ for the expansion of $(X + A)^N$. So if R is small enough, you can actually compute the remainder—using the same repeated squaring trick we talked about before, except with polynomials instead of whole numbers.

Now, since the original identity was always true when N is prime, it's obvious that the new identity

$$(X + A)^N \bmod \left(N, X^R - 1\right) = \left(X^N + A\right) \bmod \left(N, X^R - 1\right)$$

is also always true when N is prime. If two things are equal, then the remainder when you divide $X^R - 1$ into the first thing equals the remainder when you divide $X^R - 1$ into the second! What *isn't* obvious is that the new identity is always *false* when N is composite. For even though

$$(X + A)^N \bmod N \neq \left(X^N + A\right) \bmod N,$$

it's possible that two different polynomials could leave the same remainder when we divide $X^R - 1$ into both of them. What AKS showed was this: *if N is composite, and if you choose the "right" value of R, then you need to try only a small number of A's until you find one such that*

$$(X + A)^N \bmod \left(N, X^R - 1\right) \neq \left(X^N + A\right) \bmod \left(N, X^R - 1\right).$$

Once you find such an A, you've proved that N is composite. What's more, you don't have to pick the A's at random; there's a deterministic way to do it.

Throughout their proof of this claim, AKS use "heavy-duty" math in only one place: they appeal to a theorem of Fouvry to show that the "right" value of R can be found efficiently. Aside from that, the proof rests entirely on facts that any undergrad math major would know. I'll end on that note. Thank you.

12 Further Reading

An excellent source of prime number facts, which I used in preparing this talk, is *The Book of Numbers* by John Conway and Richard Guy (Copernicus Books, 1997). There are many books and websites about public-key cryptography, but one place to start is Martin Gardner's "Mathematical Games" column, reprinted in *Penrose Tiles to Trapdoor Ciphers* (MAA Press, 1997), which first introduced the subject to the world. For a popularization of quantum computing, try Julian Brown's *Minds, Machines, and the Multiverse* (Simon & Schuster, 2000), or my own little essay, "Quantum Computing for High School Students" (http://www.cs.berkeley.edu/~aaronson/highschool.html). Finally, you can read more about the AKS algorithm at http://fatphil.org/maths/AKS/.

13 Acknowledgment

Thanks to Vaidy Sivaraman and Luis Rodriguez for pointing out errors in earlier versions of this talk.