Factoring Integers Using Elliptic Curves

Evan P. Dummit

Northeastern University

Northeastern Math Club

September 15th, 2023

Outline of Talk

I will start with a brief discussion of the problem of factoring large arbitrary integers.

I will then introduce elliptic curves and discuss the addition law on elliptic curves.

Next, we will talk a bit about the addition law on elliptic curves modulo a prime p, and more generally modulo an integer n.

Finally, I will discuss how we can use the addition law on elliptic curves to factor integers – and then we will factor some integers.

Factoring Is Hard, I

As most of us learn at some point in elementary school, every positive integer has a prime factorization, and, more interestingly, the prime factorization is unique up to rearranging the terms.

- In fact, the existence of unique factorization is a very interesting subject in its own right (please take Math 3527[1], and then Math 4527[2], if you want to learn all about that!)
- But we're interested in actually computing factorizations.

As it turns out, there are quick ways to show that large integers are composite without actually finding a factorization.

[1] Math 3527 = Number Theory 1, typically runs in Spring and Summer

[2] Math 4527 = Number Theory 2, typically runs whenever I have room in my schedule to teach it

Factoring Is Hard, II

Proposition (Fermat Compositeness Test)

Suppose m is a positive integer. If there exists a positive integer a such that $a^m - a$ is not divisible by m, then m must be composite.

Factoring Is Hard, II

Proposition (Fermat Compositeness Test)

Suppose m is a positive integer. If there exists a positive integer a such that $a^m - a$ is not divisible by m, then m must be composite.

- Proof: We show the contrapositive of this statement: if p is a prime number, then $a^p - a$ is always divisible by p for all positive integers a. For this, induct on a.

Factoring Is Hard, II

Proposition (Fermat Compositeness Test)

Suppose m is a positive integer. If there exists a positive integer a such that $a^m - a$ is not divisible by m, then m must be composite.

- Proof: We show the contrapositive of this statement: if p is a prime number, then $a^p - a$ is always divisible by p for all positive integers a. For this, induct on a.
- The base case $a = 1$ is easy, since $1^p - 1 = 0$ is divisible by p.
- For the inductive step, suppose $a^p - a$ is divisible by p. Then $(a+1)^p - (a+1) =$ $(a^p + pa^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1) - (a+1) = (a^p - a)$ plus a multiple of p, because all of the binomial coefficients are divisible by p.
- So by the inductive hypothesis, we see immediately that $(a+1)^p - (a+1)$ is also a multiple of p, as desired.

Factoring Is Hard, III

For large m we can quickly determine whether $a^m - a$ is divisible by m by reducing modulo m (i.e., taking the remainder upon dividing by m) as we compute the power a^m, which can be done very quickly.

- As an example, with $m = 401,908,261$, my 13-year-old desktop computer (yes, really) reports taking 0.0000 milliseconds to compute the remainder when $2^m - 2$ is divided by m.
- Since this remainder comes out as $72,531,146$, which is not zero, that tells us this number $m = 401,908,261$ is composite.

Factoring Is Hard, IV

Okay... so now, what's the prime factorization of the composite number $m = 401,908,261$?
(I'll wait. No calculators!)

Factoring Is Hard, IV

Okay... so now, what's the prime factorization of the composite number $m = 401,908,261$?
(I'll wait. No calculators!)

- Right, so, even though we know for sure this number is composite, how do we actually find a factorization?
- One way: just test all possible prime factors up to m. One of them has to divide m, and once we find it, we've gotten a factorization.
- In fact we don't even need to go all the way up to m, since the smallest prime factor of m is at most $\sqrt{m}$ when m is composite. (Why?)
- Sadly, however, this is going to take a while, because there are $2,267$ primes less than $\sqrt{m}$.
- I don't want to check all of them... do you?

Factoring Is Hard, V

We would like a better way to find a factor of m.

Factoring Is Hard, V

We would like a better way to find a factor of m.

- There are lots of different factoring algorithms that have been developed over the millennia (!) that mathematicians and others have been investigating number theory.
- Most of the good ones have come onto the scene only in the last 100 years or so, when the advent of effective calculation technology made the necessary computations feasible to perform efficiently.

So now I will tell you one that relies on some properties of elliptic curves.

Elliptic Curves, I

Definition

An elliptic curve E is a curve having an equation of the form

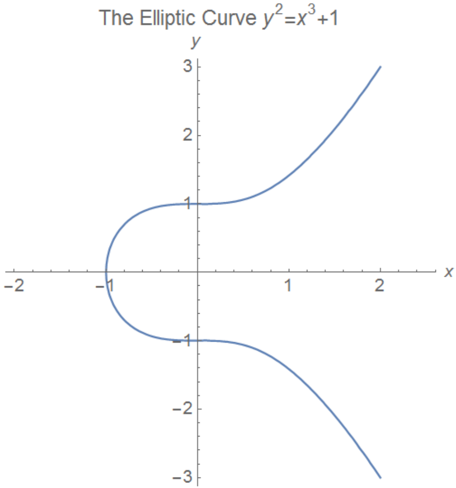
$$y^2 = x^3 + Ax + B$$

for some A and B. This expression is called the reduced Weierstrass form of E.

For us, A and B will be integers. Our interest will be in the set of points (x, y) satisfying the equation $y^2 = x^3 + Ax + B$.

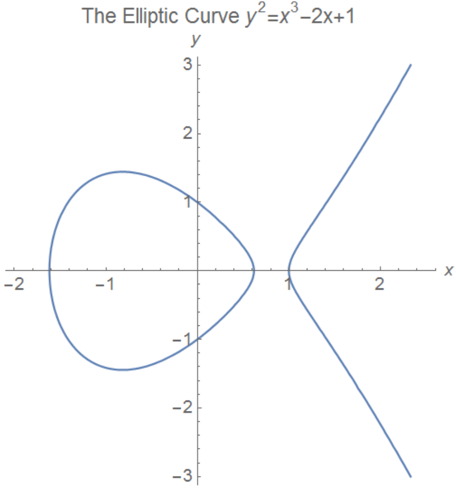
Elliptic Curves, II

We can draw graphs to visualize elliptic curves. Here is the graph of $y^2 = x^3 + 1$:



Elliptic Curves, V

Here is the graph of $y^2 = x^3 - 2x + 1$:



Elliptic Curves, VI

Let's now make a few observations.

Observation

The graph of an elliptic curve $y^2 = x^3 + Ax + B$ will always be symmetric about the x-axis.

- This is easy to see because if (x, y) satisfies the equation then so does $(x, -y)$.

Elliptic Curves, VII

Observation

Elliptic curves are not ellipses.

- The reason for the similar name is that if you want to compute the arclength of an ellipse (an elliptic integral), a few changes of variable will transform the resulting integral into one of the general form $\int \frac{1}{\sqrt{x^3 + Ax + B}}\, dx$.
- Upon setting $y = \sqrt{x^3 + Ax + B}$, we see that this elliptic integral is rather naturally related to the curve $y^2 = x^3 + Ax + B$.
- In fact, studying elliptic integrals was one of the two ways mathematicians discovered that elliptic curves were so interesting! (The other is on the next slide.)

The Addition Law, I

The key property of elliptic curves that makes them so useful is the following algebraic and/or geometric observation:

Observation

If we have two points that lie on an elliptic curve, we can use them to construct a third point on the curve.

The Addition Law, I

The key property of elliptic curves that makes them so useful is the following algebraic and/or geometric observation:

Observation

If we have two points that lie on an elliptic curve, we can use them to construct a third point on the curve.

How do we do this? Simply take the line through the two given points, and find the other intersection point with the elliptic curve.

The Addition Law, I

The key property of elliptic curves that makes them so useful is the following algebraic and/or geometric observation:

Observation

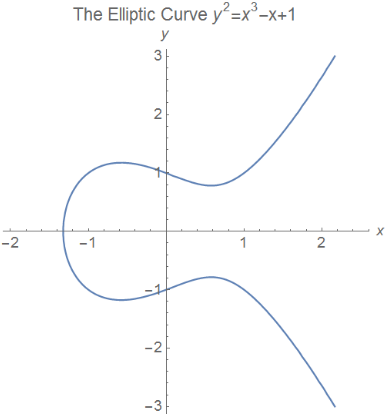
If we have two points that lie on an elliptic curve, we can use them to construct a third point on the curve.

How do we do this? Simply take the line through the two given points, and find the other intersection point with the elliptic curve.

Clearly, this always works[citation needed].

The Addition Law, II

Here is an interactive "proof"[3] by picture (you pick two points and I'll give you a third one):



[3] This proof technique is not valid in mathematics. Your experience in other disciplines (physics, philosophy) may vary.

The Addition Law, III

Here's a proof by example[4]:

Consider the elliptic curve $E : y^2 = x^3 - 7x + 10$ with the two points $P_1 = (-3, 2)$ and $P_2 = (1, -2)$ on E.

[4] This proof technique is also not valid in mathematics. Your experience in other disciplines (computer science, the humanities) may vary.

The Addition Law, III

Here's a proof by example[4]:

Consider the elliptic curve $E : y^2 = x^3 - 7x + 10$ with the two points $P_1 = (-3, 2)$ and $P_2 = (1, -2)$ on E.

- The equation of the line joining these points is $y = -x - 1$.

[4] This proof technique is also not valid in mathematics. Your experience in other disciplines (computer science, the humanities) may vary.

The Addition Law, III

Here's a proof by example[4]:

Consider the elliptic curve $E : y^2 = x^3 - 7x + 10$ with the two points $P_1 = (-3, 2)$ and $P_2 = (1, -2)$ on E.

- The equation of the line joining these points is $y = -x - 1$.
- Plugging this into the equation for E yields $(-x - 1)^2 = x^3 - 7x + 10$, or $x^3 - x^2 - 9x + 9 = 0$.

[4] This proof technique is also not valid in mathematics. Your experience in other disciplines (computer science, the humanities) may vary.

The Addition Law, III

Here's a proof by example[4]:

Consider the elliptic curve $E : y^2 = x^3 - 7x + 10$ with the two points $P_1 = (-3, 2)$ and $P_2 = (1, -2)$ on E.

- The equation of the line joining these points is $y = -x - 1$.
- Plugging this into the equation for E yields $(-x - 1)^2 = x^3 - 7x + 10$, or $x^3 - x^2 - 9x + 9 = 0$.
- We know this cubic has roots $x = -3, 1$ so we can quickly get the factorization $(x + 3)(x - 1)(x - 3) = 0$. Thus the third root is $x = 3$, yielding $y = -4$.
- This means the other intersection point is $(3, -4)$.

[4] This proof technique is also not valid in mathematics. Your experience in other disciplines (computer science, the humanities) may vary.

The Addition Law, IV

It's not so hard to show that the argument from the example will work in general. If you want the details, here they are:

- Suppose $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ are two distinct points on the elliptic curve E: $y^2 = x^3 + Ax + B$.
- Let L be the line through P_1 and P_2 with equation $y = mx + b$: we claim it intersects E in a third point Q.
- The intersection points of L with E are the solutions to the system $y = mx + b$ and $y^2 = x^3 + Ax + B$.
- Equivalently, we must solve $(mx + b)^2 = x^3 + Ax + B$, or $x^3 + (-m^2)x^2 + (A - 2mb)x + (B - b^2) = 0$.
- However, this cubic already has the two roots $x = x_1$ and $x = x_2$, so it must have a third root (in fact, the root is $m^2 - x_1 - x_2$): this gives us the third point Q we wanted.

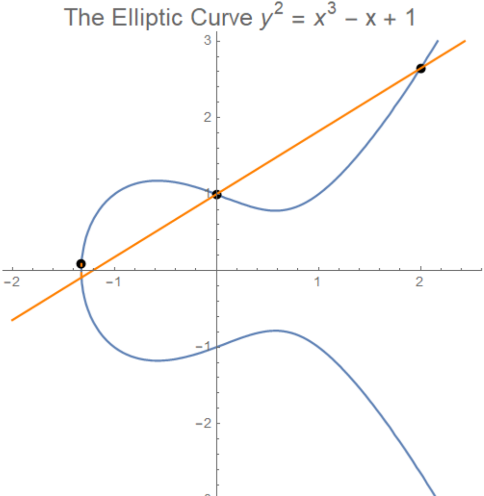
The Addition Law, V

Once we construct a third point on an elliptic curve this way, we might try to find more points.

- If we try this procedure directly using our points P_1, P_2, and Q, however, we will not get anywhere: the line through any of these two points intersects the elliptic curve at the other point.
- However, we can also exploit the vertical symmetry of the curve to make new points: if $P = (x, y)$ lies on the curve, then the point $-P = (x, -y)$ also lies on the curve.
- We can then take lines through one of our starting points and this point $-P$ to find even more points on the curve.

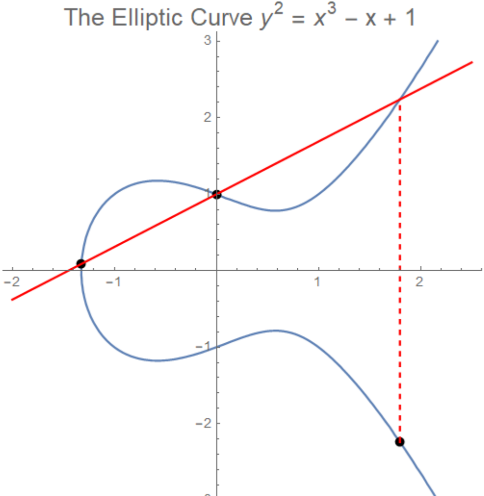
The Addition Law, VI

Here's a picture of what happens if we repeatedly apply this starting with $P_1 = (0, 1)$ on $y^2 = x^3 - x + 1$:



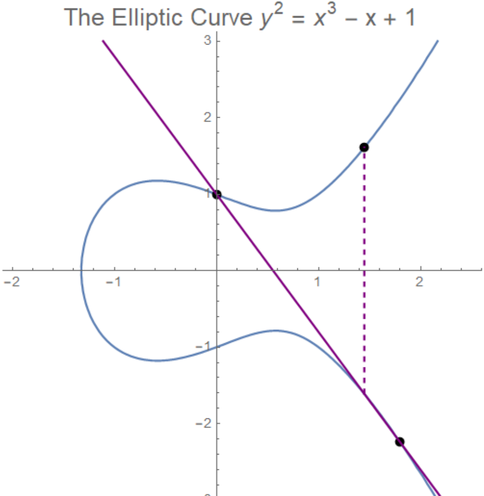
The Addition Law, VI

Here's a picture of what happens if we repeatedly apply this starting with $P_1 = (0, 1)$ on $y^2 = x^3 - x + 1$:



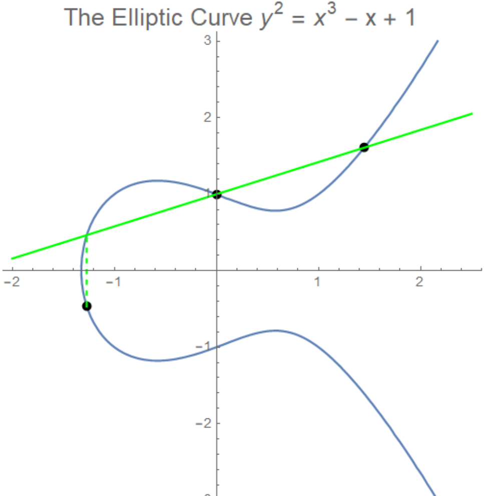
The Addition Law, VI

Here's a picture of what happens if we repeatedly apply this starting with $P_1 = (0, 1)$ on $y^2 = x^3 - x + 1$:



The Addition Law, VI

Here's a picture of what happens if we repeatedly apply this starting with $P_1 = (0, 1)$ on $y^2 = x^3 - x + 1$:



The Addition Law, VII

If we combine these two procedures (taking the third point on the line through two given points and then reflecting this point vertically), we can often generate many points on the curve starting from just two.

Definition (Addition Law I)

If P_1 and P_2 are two distinct points on the elliptic curve $E : y^2 = x^3 + Ax + B$, let $Q = (x', y')$ be the third intersection point of E with the line L joining P_1 and P_2. We define the sum $P_1 + P_2$ to be the point $-Q = (x', -y')$.

- We saw this in the examples already, but just to emphasize, the sum $P_1 + P_2$ is not the pointwise coordinate sum of P_1 and P_2!

The Addition Law, VIII

There is an important issue that I completely glossed over, that definitely none of you noticed.

- Specifically, if we attempt to add two points which are vertical reflections of one another on the graph of $y^2 = x^3 + Ax + B$, the resulting line will not intersect the curve again.
- One option would simply be to declare that this operation is invalid.

The Addition Law, VIII

There is an important issue that I completely glossed over, that definitely none of you noticed.

- Specifically, if we attempt to add two points which are vertical reflections of one another on the graph of $y^2 = x^3 + Ax + B$, the resulting line will not intersect the curve again.
- One option would simply be to declare that this operation is invalid. However, there is a much better approach: we will simply declare that E also includes a point at ∞ (which we denote simply as ∞) lying on every vertical line.
- So, the line through P and ∞ is the vertical line through P.
- With this convention, this point ∞ actually behaves as an identity in our addition law, and the point $-P$ is an additive inverse of P: in other words, $P + \infty = P$ for any P, and $P + (-P) = \infty$ for any P as well.

The Addition Law, IX: The Rise of Skywalker

Actually, there's another issue that I also glossed over, but luckily nobody noticed it either.

- Specifically, our approach of taking the line through two points P and Q does not work correctly when $P = Q$: what exactly is the line through P and then P again?

The Addition Law, IX: The Rise of Skywalker

Actually, there's another issue that I also glossed over, but luckily nobody noticed it either.

- Specifically, our approach of taking the line through two points P and Q does not work correctly when $P = Q$: what exactly is the line through P and then P again?
- Let's take a cue from calculus and think about what the line looks like as we slide Q closer to P: it turns out to be the tangent line.
- So we can define $P + P$ by letting L be the tangent line to E at P, and then take $P + P$ to be the vertical reflection of the third intersection point of the tangent line with E.

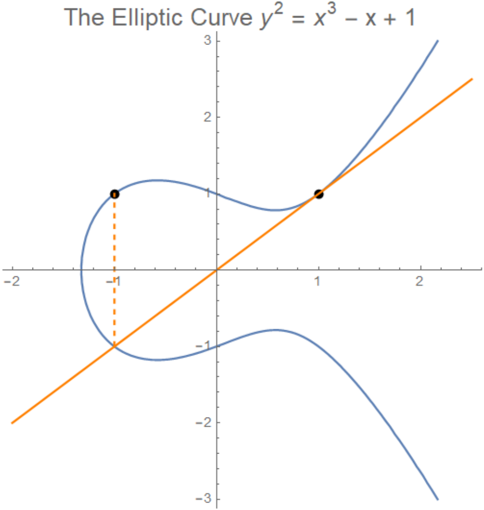
We can compute the slope of the tangent line to E at P using some calculus[5].

---

[5]Finally, a useful application of implicit differentiation!

The Addition Law, X: Marks The Spot

Here's a picture to illustrate this "doubling law":



The Addition Law, XI: This One Goes To Eleven

Now, for those of you who know what a group is, in fact this addition law makes the set of points on the elliptic curve into an abelian group.

- The addition law is associative: $(P + Q) + R = P + (Q + R)$ for any P, Q, R.
- The addition law is commutative: $P + Q = Q + P$ for any P, Q.
- There is an identity: $P + \infty = P$ for any P.
- There exist inverses: $P + (-P) = \infty$ for any P.

Scaling Points, I

Now, what does any of this have to do with factoring integers? We're getting there, but hold on for just a bit more.

- The main idea, interestingly enough, involves thinking about what happens if we repeatedly add a point P to itself: namely, the points P, $P+P$, $P+P+P$, $P+P+P+P$, and so on.
- For shorthand, let's write $nP = \underbrace{P + P + \cdots + P}_{n \text{ terms}}$.
- Most of the time, the multiples of P rapidly get very complicated. For $P = (1,1)$ on $y^2 = x^3 - x + 1$, for example, they are $2P = (1/4, -7/8)$, $3P = (56, 419)$, $4P = (-223/784, 24655/21952)$, and so on.
- These multiples will just get more and more complicated as we keep going.

Scaling Points, II

But sometimes, multiples start repeating. For example, consider the elliptic curve $y^2 = x^3 + 1$.

- For $P = (-1, 0)$, we can compute $2P = \infty$, $3P = (-1, 0)$, $4P = \infty$, $5P = (-1, 0)$, and so on. The multiples of P just alternate between P and the identity ∞.
- For $Q = (0, 1)$, on the other hand, we can compute $2Q = (0, -1)$, $3Q = \infty$, $4Q = (0, 1)$, $5Q = (0, -1)$, $6Q = \infty$, and so on. The multiples of Q cycle between $(0, 1)$, $(0, -1)$, and ∞.
- Now, what do you think happens if we look at the multiples of $P + Q = (2, -3)$?

Scaling Points, II

But sometimes, multiples start repeating. For example, consider the elliptic curve $y^2 = x^3 + 1$.

- For $P = (-1, 0)$, we can compute $2P = \infty$, $3P = (-1, 0)$, $4P = \infty$, $5P = (-1, 0)$, and so on. The multiples of P just alternate between P and the identity ∞.
- For $Q = (0, 1)$, on the other hand, we can compute $2Q = (0, -1)$, $3Q = \infty$, $4Q = (0, 1)$, $5Q = (0, -1)$, $6Q = \infty$, and so on. The multiples of Q cycle between $(0, 1)$, $(0, -1)$, and ∞.
- Now, what do you think happens if we look at the multiples of $P + Q = (2, -3)$?
- In fact, they will repeat every 6 times: $2(P + Q) = (0, -1)$, $3(P + Q) = (-1, 0)$, $4(P + Q) = (0, 1)$, $5(P + Q) = (0, 1)$, and $6(P + Q) = \infty$. After this we just start cycling back at $(0, -1)$ again.

Scaling Points, III

We can see that if some multiple of a point is ∞, then all of the later multiples will just repeat the earlier ones.

- In the event that some multiple of P is the identity element ∞, the smallest positive n for which $nP = \infty$ is called the order of n.
- On the previous slide, the order of P was 2, while the order of Q was 3.

Elliptic Curves Modulo Primes, I

Up until this point, we've been thinking about elliptic curves with integer coefficients, with equations like $y^2 = x^3 + Ax + B$. We could also think of this equation modulo a prime number p, however.

- For those unfamiliar with modular arithmetic, this just means that the two sides have the same remainder when we divide them both by p.
- For example, the point $(4, 1)$ lies on $E : y^2 = x^3 + x - 2$ modulo 5, because $y^2 = 1$ and $x^3 + x - 2 = 66$, and 1 and 66 have the same remainder when we divide them by 5.
- In fact, because there are only 5 possible values for x and y when we divide them by 5, we can actually just work out all of the points on E modulo 5: they are $(1, 0)$, $(4, 1)$, $(4, 4)$, and of course ∞.

Elliptic Curves Modulo Primes, II

Here's a simple observation:

Observation

Every point on an elliptic curve modulo a prime p has finite order.

Elliptic Curves Modulo Primes, II

Here's a simple observation:

Observation

Every point on an elliptic curve modulo a prime p has finite order.

- Why? Well, there are only p possible values for each coordinate of a point (x, y), so (counting ∞) there's a maximum of $p^2 + 1$ possible points on E.
- Then the multiples of any point P must start repeating, since there's only finitely many options.
- If $aP = bP$ for some $a < b$, adding $-aP$ to both sides shows that $(b - a)P = \infty$. This means some multiple of P is the identity.

Elliptic Curves Modulo Primes, III

Now, here's a marvellous observation:

Observation

The addition law still works perfectly well on an elliptic curve modulo a prime p.

Elliptic Curves Modulo Primes, III

Now, here's a marvellous observation:

Observation

The addition law still works perfectly well on an elliptic curve modulo a prime p.

- Why? Well, we can just write out the addition law as an algebraic formula.
- Explicitly, if $y = mx + b$ is the line through $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ (or the equation of the tangent line, when $P = Q$), then $P + Q = (m^2 - x_1 - x_2, m(m^2 - x_1 - x_2) + b)$.
- Everything in the formula still makes sense modulo p: the only potential concern is that the formula involves a quotient: specifically, in finding the slope m of the line.

Elliptic Curves Modulo Primes, IV

So let's think carefully about the slope of a line modulo p, which will be some kind of quotient a/b.

- If you try out some examples, you will eventally notice that most of the time, you can use some trickery to convert a quotient a/b into an integer modulo p.
- For example, $1/3 = 6/3 = 2$ modulo 5, or $3/4 = 24/4 = 6$ modulo 7.
- In fact, when p is prime, in general any rational number a/b is equivalent to an integer modulo p, as long as b is not divisible by p.
- So we can simplify any slope as long as the denominator doesn't reduce to 0 modulo p. But if the denominator is zero, that just means the line is vertical, in which case the sum we're trying to compute is just ∞.

Elliptic Curves Modulo ~~Primes, V~~ Nonprimes, VI

Now, this business about the addition law still working perfectly well modulo p really does rely on p specifically being a prime number.

- If we try things modulo a composite number n, say $n = 6$, this simplification doesn't always work.
- For example, try finding a way to simplify the slope $2/3$ modulo 6 so that it comes out to be an integer by adding or subtracting multiples of 6 from the numerator and denominator.
- Here are some other bad ones: $1/3$, $1/2$, $3/4$, $7/8$, $5/9$, ...

Elliptic Curves Modulo ~~Primes, V~~ Nonprimes, VI

Now, this business about the addition law still working perfectly well modulo p really does rely on p specifically being a prime number.

- If we try things modulo a composite number n, say $n = 6$, this simplification doesn't always work.
- For example, try finding a way to simplify the slope $2/3$ modulo 6 so that it comes out to be an integer by adding or subtracting multiples of 6 from the numerator and denominator.
- Here are some other bad ones: $1/3$, $1/2$, $3/4$, $7/8$, $5/9$, ...
- In general, if the denominator has a common factor with n (but isn't just 0 mod n), then the resulting slope makes no sense.

This seems like a big problem, right?

Elliptic Curve Factorization, I: We're Almost Done

Believe it or not, this "problem" is actually the key to factoring integers with elliptic curves. Here's the idea:

- Suppose n is a composite integer.
- Pick any elliptic curve E with a point $P \neq \infty$ on E modulo n. (We can do this easily if we select the point and value of A first, and then just compute the needed B that makes $y^2 = x^3 + Ax + B$.)
- Now start computing the multiples of P, with everything done modulo n: compute $2P$, $3P$, $4P$, ...
- If in the middle of the calculation, we get an illegal denominator, then it has a common factor with n that isn't n itself.
- Taking the gcd of this "bad" denominator with n then yields a nontrivial factor of n.

Elliptic Curve Factorization, II: I'm Almost Through

Here's an example with the point $P = (1, 3)$ on $E : y^2 = x^3 + 4x + 4$ modulo 21.

Elliptic Curve Factorization, II: I'm Almost Through

Here's an example with the point $P = (1, 3)$ on
$E : y^2 = x^3 + 4x + 4$ modulo 21.

- To find $2P$ we first compute the slope of the slope of the tangent line, which is $\dfrac{3(1)^2 + 4}{2 \cdot 3} = \dfrac{7}{6}$ by some implicit differentiation.
- But this ratio is not defined modulo 21 since 6 is not relatively prime to 21.
- Per the procedure we compute $\gcd(21, 6) = 3$, and voilà: we have a factor of 21.

Elliptic Curve Factorization, III: You're Almost Free

Now, of course, it's probably not at all clear why we would expect this procedure to work, or why it would even be efficient.

Elliptic Curve Factorization, III: You're Almost Free

Now, of course, it's probably not at all clear why we would expect this procedure to work, or why it would even be efficient.

- In fact, we don't want to compute all of the multiples of P: this will be too slow.
- We just want to compute a bunch of them that are "highly divisible": what we do is just find the multiples $2!P$, $3!P$, $4!P$, $5!P$, $6!P$, ..., and just keep track during the calculations if we end up with any bad denominators of our slopes.
- This is fairly quick because we can just use the recursion $Q_1 = P$, $Q_j = jQ_{j-1}$.

Elliptic Curve Factorization, IV: Yes, There's More

Here's an example with $n = 170999$ using $P = (1, 4)$ on $y^2 = x^3 + 4x + 11$.

- We compute the points Q_j successively using the recursion $Q_1 = P$, $Q_j = jQ_{j-1}$ on the E modulo n until we obtain a bad denominator.

j	1	2	3	4
Q_j	$(1, 4)$	$(109545, 75144)$	$(81282, 86818)$	$(100818, 143145)$
Factor?	no	no	no	no
j	5	6	7	8
Q_j	$(152033, 116998)$	$(87978, 17295)$	$(104368, 99929)$	$(126411, 167685)$
Factor?	no	no	no	no
j	9	10		
Q_j	$(79623, 108587)$	–		
Factor?	no	557		

Elliptic Curve Factorization, V: Stay Alive

Here's an example with $n = 170999$ using $P = (1, 4)$ on $y^2 = x^3 + 4x + 11$.

- Here, finding $10Q_9$ will require dividing by a denominator that is not relatively prime to n.
- The exact details of the computation will depend on the method used to compute $10Q_9$, but successive doubling will yield $2Q_9 = (147257, 97701)$ and $8Q_9 = (160625, 116187)$.
- Attempting to add these two points will require using a line with slope $m = \dfrac{116187 - 97701}{160625 - 147257} = \dfrac{18486}{13368}$, and $\gcd(13368, 170999) = 557$.
- And so, we find the factor 557 of 170999.

Elliptic Curve Factorization, VI: Pick Up Sticks

So why does this procedure work? Here's some reasons:

- If $n = pq$, the factorization algorithm will succeed after M steps when the order of P as a point on E modulo p divides $M!$ (so $M!P = \infty$ modulo p) but the order as a point on E modulo q does not divide $M!$ (so $M!P \neq \infty$ modulo q).
- It is unlikely that these two things will occur at exactly the same value of M, so what we are essentially seeking is for the order of P on E modulo p to divide $M!$.
- A result from group theory (Lagrange's theorem) implies that the order of P on E modulo p divides the total number of points on E modulo p, so as long as the number of points on E modulo p only has small prime factors, it will divide $M!$ for small M, and the factorization will succeed quickly.
- Finally, by trying different randomly-chosen curves E, we are fairly likely to be able to get one whose number of points has prime factors that are all fairly small relative to n. (Whew!)

Elliptic Curve Factorization, VII: I Ran Out Of Jokes

Okay, enough details, let's put it to the test. Below I chose a dozen random 5-digit primes. Pick two and multiply them together with a calculator or computer. Then I'll see if I can get my implementation of elliptic curve factorization to factor the product you give me.

- 11701.
- 17623.
- 20533.
- 22697.
- 38287.
- 46549.
- 51767.
- 54629.
- 62603.
- 73967.
- 80953.
- 93281.

Or if you like, you can find some other composite number, and I'll give it a try.

Some Other Tidbits

There are lots of other interesting things to say about elliptic curve factorization (and very much else to say about elliptic curves in general). Here are some:

- Elliptic curve factorization is fastest at finding "small" factors, around 10-50 digits or so, of large composite integers.
- Elliptic curves can also be used to do cryptography: in fact, public-key elliptic curve cryptography is now a bit more commonly used than RSA, because ECC can use much smaller key sizes for an equivalent level of security.
- And finally, just to tease some pure mathematics, elliptic curves are also a fundamental ingredient in Wiles's proof of Fermat's Last Theorem[6].

[6] To learn more about elliptic curves, take Math 7359: Elliptic Curves and Modular Forms

Thanks!

Thanks to Zach Greenfield and the other math club organizers for providing me the opportunity to speak here today!

Please also allow me to advertise the Putnam Club, which meets Wednesdays from 6pm-7:30pm in 509 Lake. We get together to (try to) solve some problems from old Putnam exams, and also eat pizza. If you like competition math and/or problem-solving, come check us out!

I hope you enjoyed my talk, and I'd like to thank you for attending! Enjoy your weekend!