How can you tell if you have an elliptic curve?

- Given a curve $y^2 = x^3 + bx + c = p(x)$ over a field F, how can we tell if its an elliptic curve? We need to know if $p(x)$ has multiple roots.

How can you tell if you have an elliptic curve?

- Given a curve $y^2 = x^3 + bx + c = p(x)$ over a field F, how can we tell if its an elliptic curve? We need to know if $p(x)$ has multiple roots.
- This is done with something called the discriminant. In this case, the discriminant is

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_3 - x_2)$$

where the x_i's are the roots of p possibly in a larger field.

How can you tell if you have an elliptic curve?

- Given a curve $y^2 = x^3 + bx + c = p(x)$ over a field F, how can we tell if its an elliptic curve? We need to know if $p(x)$ has multiple roots.
- This is done with something called the discriminant. In this case, the discriminant is

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_3 - x_2)$$

  where the x_i's are the roots of p possibly in a larger field.
- Clearly the discriminant is 0 iff p has multiple roots.

How can you tell if you have an elliptic curve?

- Given a curve $y^2 = x^3 + bx + c = p(x)$ over a field F, how can we tell if its an elliptic curve? We need to know if $p(x)$ has multiple roots.
- This is done with something called the discriminant. In this case, the discriminant is

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_3 - x_2)$$

  where the x_i's are the roots of p possibly in a larger field.
- Clearly the discriminant is 0 iff p has multiple roots.
- For a polynomial in the form given, one can compute that

$$\Delta = -4b^3 - 27c$$

  and so you can determine if you have an elliptic curve directly from the coefficients.

Example of El Gamal with ECC

- Given the elliptic curve $y^2 = x^3 - x + 1$ over F_7. Check that this is actually an elliptic curve.

Example of El Gamal with ECC

- Given the elliptic curve $y^2 = x^3 - x + 1$ over F_7. Check that this is actually an elliptic curve.
- Bob let's $g = (1, 1)$ and $b = (0, -1)$. We calculate that $3g = b$ so Bob is using $n = 3$.

Example of El Gamal with ECC

- Given the elliptic curve $y^2 = x^3 - x + 1$ over F_7. Check that this is actually an elliptic curve.
- Bob let's $g = (1, 1)$ and $b = (0, -1)$. We calculate that $3g = b$ so Bob is using $n = 3$.
- Now if Alice sends $r = t = (6, 1)$ then Bob calculates $m = t - 3r = -2r$ since $r = t$ and $2r = (3, 2)$ (Check!) so the message was $-2r = (3, 5)$ whatever that means.

Using Hasse's theorem

Theorem (Hasse, Lang-Weil)

If E is an elliptic curve over a finite field F_q and we write $E(F_q)$ for the points on this curve then

$$||E(F_q)| - (q+1)| \leq 2\sqrt{q}.$$

Using Hasse's theorem

Theorem (Hasse, Lang-Weil)

If E is an elliptic curve over a finite field F_q and we write $E(F_q)$ for the points on this curve then

$$||E(F_q)| - (q+1)| \leq 2\sqrt{q}.$$

- Now suppose we have the elliptic curve $y^2 = x^3 - 4x + 16$ over F_{1439}.

Using Hasse's theorem

Theorem (Hasse, Lang-Weil)

If E is an elliptic curve over a finite field F_q and we write $E(F_q)$ for the points on this curve then

$$||E(F_q)| - (q+1)| \leq 2\sqrt{q}.$$

- Now suppose we have the elliptic curve $y^2 = x^3 - 4x + 16$ over F_{1439}.
- $2\sqrt{1439} < 76$ so the number of points on this elliptic curve is between

$$1440 - 76 = 1364 \text{ and } 1440 + 76 = 1516.$$

Using Hasse's theorem

Theorem (Hasse, Lang-Weil)

If E is an elliptic curve over a finite field F_q and we write $E(F_q)$ for the points on this curve then

$$||E(F_q)| - (q+1)| \leq 2\sqrt{q}.$$

- Now suppose we have the elliptic curve $y^2 = x^3 - 4x + 16$ over F_{1439}.
- $2\sqrt{1439} < 76$ so the number of points on this elliptic curve is between

$$1440 - 76 = 1364 \text{ and } 1440 + 76 = 1516.$$

- If they also knew that there was a point on the curve of order 80 then they could conclude that the order of the group was 1440 (which it is) because that is the only multiple of 80 between 1364 and 1516.

Coding the message

- Suppose we have the elliptic curve $y^2 = x^3 + x - 1 = p(x)$ over F_{17} and we wish to code the message $m = 3$.

Coding the message

- Suppose we have the elliptic curve $y^2 = x^3 + x - 1 = p(x)$ over F_{17} and we wish to code the message $m = 3$.
- Notice that $p(3) = 12$ and 12 is not a square in F_{17}.

Coding the message

- Suppose we have the elliptic curve $y^2 = x^3 + x - 1 = p(x)$ over F_{17} and we wish to code the message $m = 3$.
- Notice that $p(3) = 12$ and 12 is not a square in F_{17}.
- If we let $K = 2$ then $2 \cdot 4 < 17$ so we could try $2m$ and $2m + 1$. $p(6) = 0$ in F_{17} and so we could code m as the point $(6, 0)$ together with $K = 2$.

Coding the message

- Suppose we have the elliptic curve $y^2 = x^3 + x - 1 = p(x)$ over F_{17} and we wish to code the message $m = 3$.
- Notice that $p(3) = 12$ and 12 is not a square in F_{17}.
- If we let $K = 2$ then $2 \cdot 4 < 17$ so we could try $2m$ and $2m + 1$. $p(6) = 0$ in F_{17} and so we could code m as the point $(6, 0)$ together with $K = 2$.
- If we let $K = 3$ then still $3 \cdot 4 < 17$ and we could try 9, 10 and 11. $p(9) = p(10) = 6$ which is not a square but $p(11) = 15 = 10^2$ in F_{17} and so we could code m using $(11, 10)$ or $(11, -10)$ as long as we passed along the information $K = 3$ as well.

- Here is a clever idea due to Lenstra on how to use elliptic curves to do factoring.

Factoring with elliptic curves

- Here is a clever idea due to Lenstra on how to use elliptic curves to do factoring.
- Fix some elliiptic curve $y^2 = x^3 + bx + c$ where b and c are integers.

Factoring with elliptic curves

- Here is a clever idea due to Lenstra on how to use elliptic curves to do factoring.
- Fix some elliiptic curve $y^2 = x^3 + bx + c$ where b and c are integers.
- Now it makes sense to consider this curve over F_p for primes p as long as p doesn't divide the discriminant; for technical reasons we will also want $p \neq 2, 3$.

Factoring with elliptic curves

- Here is a clever idea due to Lenstra on how to use elliptic curves to do factoring.
- Fix some elliiptic curve $y^2 = x^3 + bx + c$ where b and c are integers.
- Now it makes sense to consider this curve over F_p for primes p as long as p doesn't divide the discriminant; for technical reasons we will also want $p \neq 2, 3$.
- What if we don't know if n is prime or not and we try to treat our curve over Z_n? Not much will go wrong unless we try to divide by some non-zero $a \in Z_n$ where $\gcd(a, n) \neq 1$.

Factoring with elliptic curves

- Here is a clever idea due to Lenstra on how to use elliptic curves to do factoring.
- Fix some elliiptic curve $y^2 = x^3 + bx + c$ where b and c are integers.
- Now it makes sense to consider this curve over F_p for primes p as long as p doesn't divide the discriminant; for technical reasons we will also want $p \neq 2, 3$.
- What if we don't know if n is prime or not and we try to treat our curve over Z_n? Not much will go wrong unless we try to divide by some non-zero $a \in Z_n$ where $\gcd(a, n) \neq 1$.
- But this is the point! If this gcd is not 1 then we have found a divisor of n.

Example of factoring with elliptic curves

- Let's factor 77. Consider the curve $y^2 = x^3 - x + 1$. The discriminant is -23 and so this will give an elliptic curve as long as our characteristic is not 23.

Example of factoring with elliptic curves

- Let's factor 77. Consider the curve $y^2 = x^3 - x + 1$. The discriminant is -23 and so this will give an elliptic curve as long as our characteristic is not 23.
- Look at the point $P = (3, 5)$ and let's try to compute the order of this point mod 77. Of course 77 is not prime so this might not work

Example of factoring with elliptic curves

- Let's factor 77. Consider the curve $y^2 = x^3 - x + 1$. The discriminant is -23 and so this will give an elliptic curve as long as our characteristic is not 23.
- Look at the point $P = (3, 5)$ and let's try to compute the order of this point mod 77. Of course 77 is not prime so this might not work
- We compute $2P = (10, 23)$ - we do this using the formal derivative and this is where characteristic not 2 matters in order to get the slope of the tangent line.

Example of factoring with elliptic curves

- Let's factor 77. Consider the curve $y^2 = x^3 - x + 1$. The discriminant is -23 and so this will give an elliptic curve as long as our characteristic is not 23.
- Look at the point $P = (3, 5)$ and let's try to compute the order of this point mod 77. Of course 77 is not prime so this might not work
- We compute $2P = (10, 23)$ - we do this using the formal derivative and this is where characteristic not 2 matters in order to get the slope of the tangent line.
- Now to compute $3P$ we need the slope between P and $2P$ which is formally $18/7$ so we dutifully try to compute the inverse of 7 mod 77 by using the Euclidean algorithm and we discover that 7 is a factor of 77.

Example of factoring with elliptic curves

- Let's factor 77. Consider the curve $y^2 = x^3 - x + 1$. The discriminant is -23 and so this will give an elliptic curve as long as our characteristic is not 23.
- Look at the point $P = (3, 5)$ and let's try to compute the order of this point mod 77. Of course 77 is not prime so this might not work
- We compute $2P = (10, 23)$ - we do this using the formal derivative and this is where characteristic not 2 matters in order to get the slope of the tangent line.
- Now to compute $3P$ we need the slope between P and $2P$ which is formally $18/7$ so we dutifully try to compute the inverse of 7 mod 77 by using the Euclidean algorithm and we discover that 7 is a factor of 77.
- Why did this work? If we look at P mod 7 and P mod 11 it is a good exercise to show that the orders are 3 and 5.

Example of factoring with elliptic curves

- Let's factor 77. Consider the curve $y^2 = x^3 - x + 1$. The discriminant is -23 and so this will give an elliptic curve as long as our characteristic is not 23.
- Look at the point $P = (3, 5)$ and let's try to compute the order of this point mod 77. Of course 77 is not prime so this might not work
- We compute $2P = (10, 23)$ - we do this using the formal derivative and this is where characteristic not 2 matters in order to get the slope of the tangent line.
- Now to compute $3P$ we need the slope between P and $2P$ which is formally $18/7$ so we dutifully try to compute the inverse of 7 mod 77 by using the Euclidean algorithm and we discover that 7 is a factor of 77.
- Why did this work? If we look at P mod 7 and P mod 11 it is a good exercise to show that the orders are 3 and 5.
- Since the order mod 7 is 3, you run into trouble computing the slope once you have computed $2P$.