Example from Monday

- The elliptic curve and its derivative were

$$y^2 = x^3 + 2x + 4 = p(x) \text{ and } y' = \frac{3x^2 + 2}{2y}$$

  over F_5.
- The squares in F_5 are $0, 1$ and 4.
-

x	0	1	2	3	4
$p(x)$	4	2	1	2	1

- So the points on the curve are $(0, 2), (0, 3), (2, 1), (2, 4), (4, 1), (4, 4)$ and 0.
- The tangent line at $P = (0, 2)$ has slope 3 and so the line is $y = 3x + 2$. The third point on this line and the curve is $(4, 4)$ so $2P = (4, 1)$.

Example from Monday, cont'd

- Similarly the slope between P and $2P$ is 1 so the line between them is $y = x + 2$. The third point on the line and the curve is then $(2, 4)$ and so $3P = (2, 1)$.
- We also have $4P = (2, 4), 5P = (4, 4)$ and $6P = (0, 3)$. Of course we knew that the order of $(0, 2)$ is 7.

El Gamal cryptosystem with elliptic curves

- The complication here is the elliptic curve; the cryptosystem is the same as in the case of discrete log.
- That is, Bob makes the following triple public: an elliptic curve over some finite field, an element of the group g and some multiple of g called $b = ng$. Bob knows n but does not make it public.
- If Alice wants to send a message m to Bob she chooses a random number k, computes $t = m + kb$ and $r = kg$ and sends the pair (t, r) to Bob.
- Bob is able to recover m since he can compute $nr = kng = kb$ and subtract it from t to get m.

A few complications

- We have to say a couple of things about how this will all be implemented. As before, the finite field will have to be given in some concrete fashion involving the specification of the characteristic (some prime) and an irreducible polynomial.
- Once we know what the finite field looks like we can specify the elliptic curve by just giving the equation. g and b can also be given as pairs of elements from the field.
- How many points are on the elliptic curve? How big is the group?

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

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

How do we code a message using an elliptic curve

- The simple answer is to use the x-coordinate to code the message. The problem is that for any given x, the chance that there will be any y at all such that (x, y) is on the curve is only about 50%.
- Here is how to deal with this in the case we are dealing with a finite field F_p where p is a large prime.
- Pick a reasonable large number K and agree to code your messages using numbers m such that $K(m+1) < p$.
- Now consider $x_j = Km + j$ where $j = 0, \ldots, K-1$.
- The chances that x_j is the x-coordinate of something on your curve is about 1/2 and these probabilities are roughly independent as you vary j so the chance that none of the x_j is the x-coordinate of a point on your curve is about $1/2^K$ which for large K is essentially 0.
- To recover the message from the point (x, y) coding the message, compute the integer part of x/K.

Attacks on elliptic curve cryptosystems

- ECC is a discrete log cryptosystem and so any of the attacks we saw before are also valid here: Pohlig-Hellman, Baby step - Giant step and index calculus.
- One complicating factor for the hackers is that some of these algorithms require you to know the size of the group in order to implement the attack.
- Pohlig-Hellman for instance assumes you can factor the size of the group. Index calculus also assumes you know the size of the group in order to implement its attack.
- The attacker has the added burden if they want to use these attacks of figuring out the size of the group.
- As I said before, Baby step - Giant step is a generic algorithm for this attack against any cyclic group and will work with any N which is an upper bound on the size of the square root of the group so the Hasse, Lang-Weil theorem provides a reasonably upper bound for this attack.

Test information

- The third test will Wednesday, Nov. 28 at 1:30 (during class) in the T13, room 123.
- The test will be 50 minutes long.
- The topics covered will be those found in the lecture notes as well as chapter 7, sections 7. 1, 7.2 except 7.2.4, 7.4 and 7.5 and chapter 16, sections 16.1, 16.2 and 16.5.
- You are allowed to have the standard McMaster calculator, Casio fx-991 (no communication capability). No other aids are allowed. Please bring your ID with you.
- The best gauge of the level of the test is to look at the lecture notes, homework and practice problems.
- There will be a review class on Monday, Nov. 26 in-class.
- I will post practice problems from the text on the website soon.