Elliptic Curves #1

Wednesday, November 4, 2020 11:31 AM

A lot of public key cryptography is based on group theory.

Abelian Groups (look up Abel, the father of group theory)

A set of elements, G, and have an operation (+)

(A1) Closure: if a and b belong to G, then a + b belongs to G.
(A2) Associative: a + (b + c) = (a + b) + c, for all a,b,c in G.
(A3) Identity Element: There exists some element e, such that a + e = a for for elements a in G.
(A4) Inverse Element: For each a in G there is an element a' such that a + a' = a' + a = e.

(A1) - (A4) is a regular group

(A5) Commutative Property: a + b = b + a for all a, b in G

If a group satisfies (A5) it's an Abelian Group.

In Diffie-Hellman, our operation is modular exponentiation mod a prime, p.
My set of elements is {1,2,3,…,p-1}

For Elliptic Curve Crypto, instead of exponentiation, we are going to multiply…

Our objects are going to points with integer coordinates, and we will define something called addition of points. Much like Diffie Hellman, there is going to be a base point a, and we will multiply this point by some integer (really means repeated addition). It will be hard to undo the multiplication much like the discrete log problem where it's hard to undo the exponentiation…

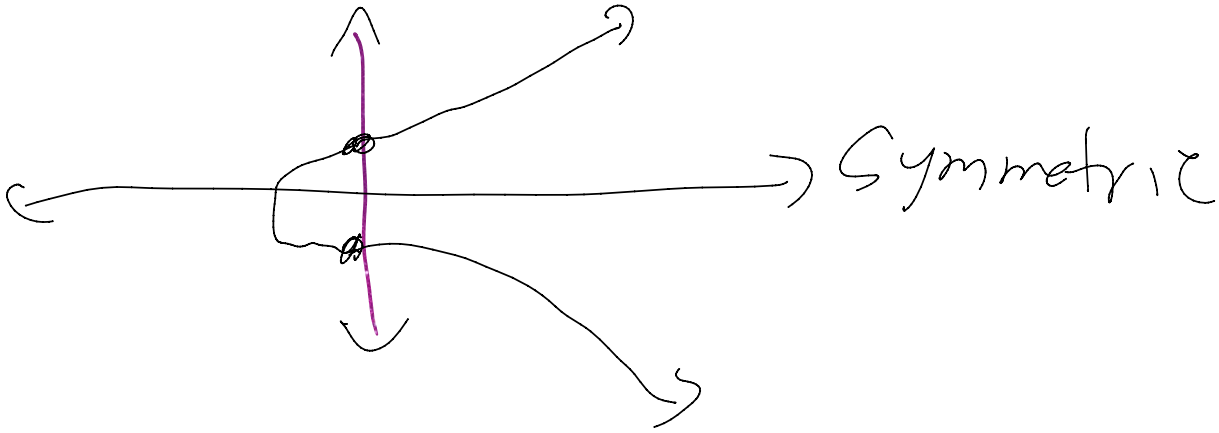
Elliptic Curve (in real numbers)

$y^2 = x^3 + ax + b$ (a general elliptic curve has more terms, but you can do some math tricks to reduce any elliptic curve to a curve with this form.)

So in real numbers, let's say a = 3, b = 5

$y^2 = x^3 + 3x + 5$

Plug in x = 2, $y^2 = 8 + 6 + 5 = 19$ 19, so y = +sqrt(19) or y = -sqrt(19)



For our purposes, you have to pick a and b such that $4a^3 + 27b^2 != 0$

For this, we can plug in arbitrary real values for x that aren't ints and of course, many times, y will not be an integer either!!!

Elliptic Curves (Integer coordinates only)

$y^2 = x^3 + ax + b \pmod p$

New rules: x and y are integers, ranging from 0 to p-1. (a and b are given integers in the same range.)

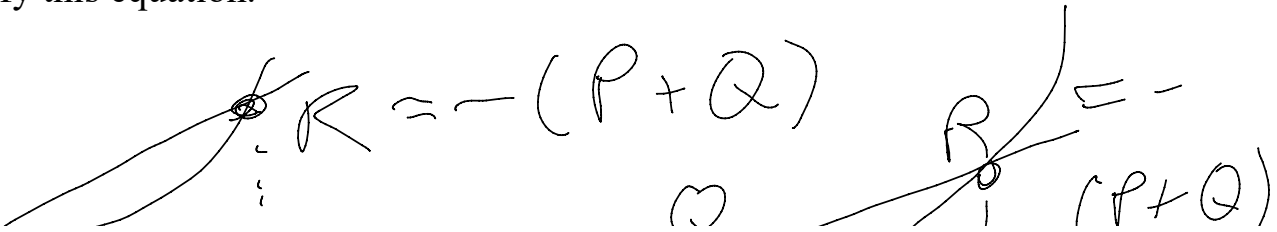
$4a^3 + 27b^2 != 0 \pmod p$

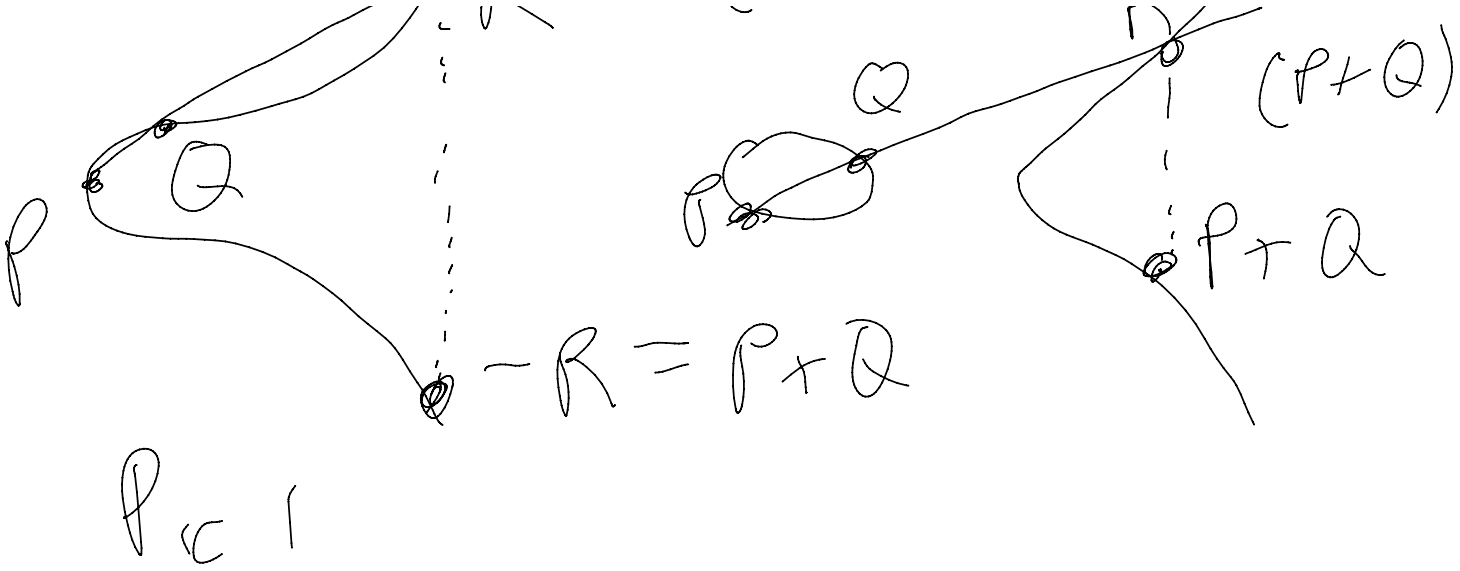
Let's say a = 1 , b = 1, p = 23

$y^2 = x^3 + x + 1 \pmod{23}$

x = 0, y = 1 or 22 (0, 1), (0, 22)
x = 1, y = 7 or 16 (1, 7), (1, 16)
x = 3, y = 10 or 13 (3, 10), (3, 13)
etc.

Ultimately, our Abelian Group is the set of ordered pairs (x, y), that satisfy this equation.

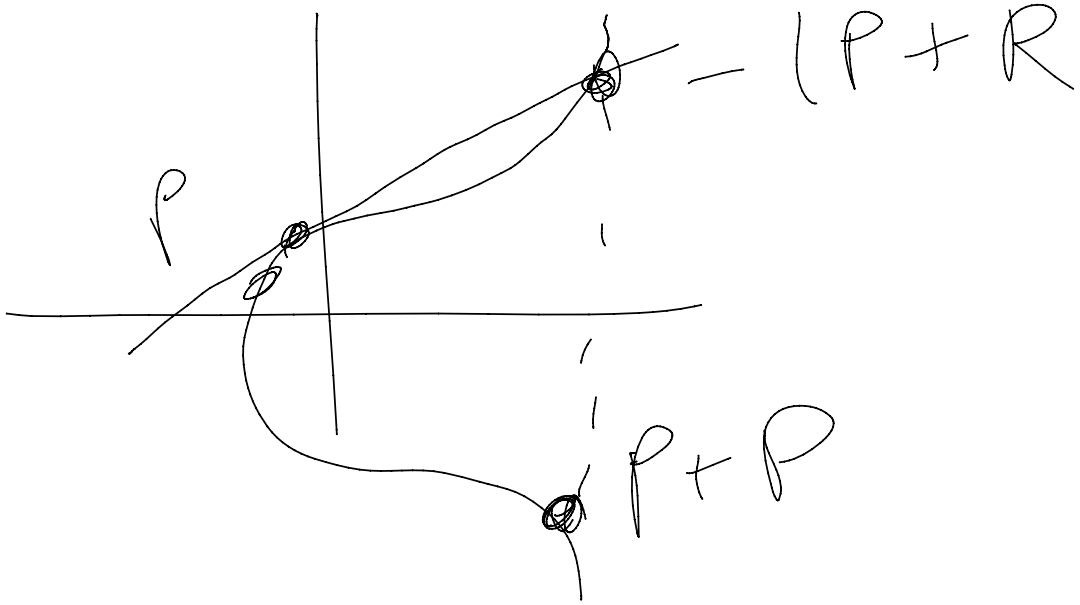




To add 2 points P and Q on the curve do this:

1. Draw a line between P and Q. Record where it intersects the curve at a 3rd point. Call this R. R = - (P+Q)
2. Reflect the point R about the line of symmetry to give you -R = P+Q, and this is your result.

The procedure for adding is different if the points you are adding are different or the same. (Imagine doing P + P…)



1. There is a special point O which serves as the additive identity. So O = -O. and for any point on the curve P + O = P, and we assume that P does not

equal O. (Really weird, O doesn't get coordinates.)
2. The negative of a point P(x, y) is -P(x, p-y), where p is the prime number we are modding by.

How do I add two points, P, Q. Do the case where P and Q are different points and have different x coordinates.

Points $P(x_p, y_p)$, $Q(x_q, y_q)$

delta = $(y_q - y_p)/(x_q - x_p)$, this is the slope formula, and we want this because we need to calculate a line intersection and this is the slope of our line. **In real numbers, we just use fractions, but with mod a prime, the division represents modInverse!!! (If the numerator and denominator share a common factor, it turns out that you can mathematicallay cancel that common factor. But after that, you still have to do modInverse.)**

Let R = P + Q, then we have

x_r = delta*delta - x_p - x_q mod prime
y_r = -y_P + delta(x_p - x_r) mod prime

Let's apply these and add two points P and Q.

$y^2 = x^3 + x + 1$ (mod 23)

P(3, 10), Q(9, 7), They call this curve $E_{23}(1, 1)$ ($E_p(a, b)$)

Delta = $(y_q - y_p)/(x_q - x_p) = (7 - 10)/(9 - 3) = -3/6 = -1/2$ (mod 23)

So what we really want to calculate is

$(-1)(2^{-1}) = (-1)(12) = -12 = 11$ mod 23

$2^{-1} = 12$ mod 23, since 2 x 12 = 24 = 1 mod 23.

x_r = delta*delta - x_p - x_q = 11*11 - 3 - 9 = 109 = 17 (mod 23)
y_r = -y_P + delta(x_p - x_r) = -10 + 11(3 - 17) = -10 -154 = -164 = 20 mod 23
Thus P + Q = **(17, 20).**

Here we are defining R to be the sum instead of the negative of the sum. I am not sure why the book does this…

Formula for adding P + P

We don't calculate a delta this time, since we can't divide by a difference in x.

$$x_r = \left(\frac{3x_p^2 + a}{2y_p}\right)^2 - 2x_p$$

$$y_r = \left(\frac{3x_p^2 + a}{2y_p}\right)(x_p - x_R) - y_p$$

$$y^2 = x^3 + ax + b$$

$$2yy' = 3x^2 + a$$

$$y' = \frac{3x^2 + a}{2y}, \text{ tangent slope!}$$

P = (3, 10), $y^2 = x^3 + x + 1 \pmod{23}$, a = 1, b = 1, p=23

$$x_R = \left(\frac{3x_p^2 + a}{2y_p}\right)^2 - 2x_p$$

$$= \left(\frac{27 + 1}{20}\right)^2 - 6$$

23 = 4 x 5 + 3
5 = 1 x 3 + 2
3 = 1 x 2 + 1

3 - 2 = 1

$$= \left(\frac{28}{20}\right)^2 - 6$$

$$= \left(\frac{7}{5}\right)^2 - 6$$

$$= (7 \times 5^{-1} \bmod 23)^2 - 6 \bmod 23$$

$$= ((7 \times 14 \bmod 23)^2 - 6) \bmod 23$$

$$= ((98 \bmod 23)^2 - 6) \bmod 23$$

$$= (6^2 - 6)$$

$$= 30 = 7 \bmod 23$$

$$y_R = \left(\frac{3x_p^2 + 9}{2y_p}\right)(x_p - x_R) - y_p$$

$$= 6(3 - 7) - 10$$

SAVE!

$$= -24 - 10$$

3 - 2 = 1
3 - (5 - 3) = 1 1
2 x 3 - 5 = 1 1
2(23 - 4x5) - 5 = 1
2 x 23 - 9 x 5 = 1
-9 x 5 = 1 mod 23
$5^{-1} = -9 = 14$

$$\equiv -24 - 10$$

$$\equiv -34 \equiv 12 \pmod{23}$$

$$2P = (7, 12)$$