A BRIEF EXPOSITION ON THE GROUP STRUCTURE OF ELLIPTIC CURVE CRYPTOGRAPHY

JESUS GARCIA

May 10, 2020

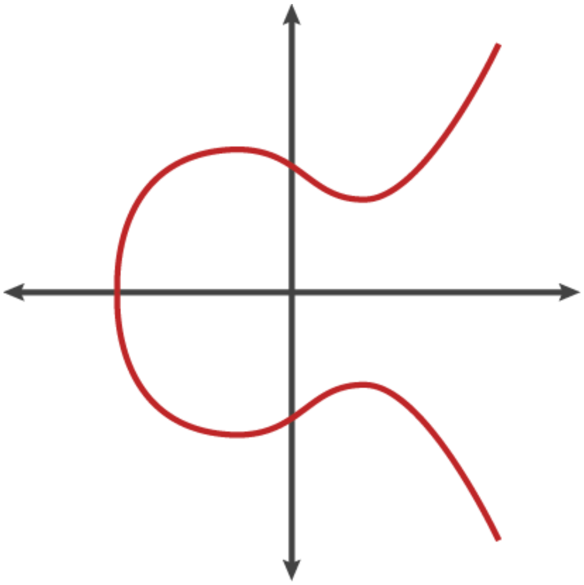
1. Introduction

Elliptic Curve Cryptography(ECC) is an implementation of public-key cryptography that is found on the algebraic structure(this is what we are going to survey) of elliptic curves. Popular schemes of public key cryptography include RSA(1977) and Diffie-Hellman. Although ECC provides security like RSA however, the attractiveness in ECC lies in the fact that it uses much smaller key sizes than that of RSA. Although the implementation details of ECC may be interesting, we will be looking at the group and algebraic structure of elliptic curves.

2. Elliptic Curves

You may be wondering what an elliptic curve is or what it may look like. Many have likened it to the Lululemon logo tipped on its side.

2.1. **Ex.** Here is an elliptic curve (see Figure 2.1):



An elliptic curve consists of a set of points that satisfies the following equation:

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

Note that changing the values of a and b will yield different curves. More importantly, note that the elliptic curves are symmetric about the x-axis.

In addition to our equation we **must** include a "point at infinity" or an ideal point to be on our curve. We can denote this ideal point as **0**. Hence, we can redefine our elliptic curve like so:

$$\{(x, y) \in \mathbb{R}^2 \ |y^2 = x^3 + ax + b\} \cup \{0\}$$

Before we can go any further we must briefly go over groups and their structure for any arbitrary group.

2.2. **A Refresher On Groups.**

Definition 2.1. A **Group** is a set G with a binary operation *: $G * G \to G$. Such that:

- **Identity**: There is some element $e \in G$ (called the identity) Such that:
  $e * g = g * e = g$ for all $g \in G$ (You may think of this at the "do nothing" operation)
- **Inverses**: For every $g \in G$ there is an element g^-1 (called g inverse) such that:
  $$g * g^{-1} = g^{-1} * g = e \text{ for all } g \in G.$$
- **Associativity**: For any three elements $g, h, i \in G$:
  $$(g * h) * i = g * (h * i)$$

Definition 2.2. A Group G is **commutative or abelian** if:

$$ab = ba \text{ for all a,b} \in G$$

Note that only **some** groups may have the additional property of being **communative or abelian**.

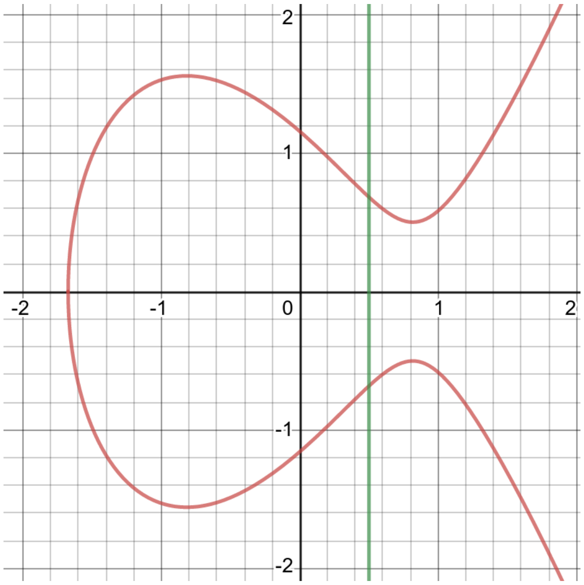
3. Group Structure for Elliptic Curves

In this section we will demonstrate the group structure for elliptic curves.

We define a group G over elliptic curves:

- The elements of the group G are the set of all points of an elliptic curve.
- **Binary operation**: Addition is the group binary operation given by three aligned, non-zero points P,Q,R:
  $$P + Q + R = 0 \text{ for any non-zero P,Q,R} \in G$$
- **identity**: The point at infinity **0**. i.e:
  $$p + 0 = p = 0 + p \text{ for all p(points)} \in G$$
- **inverses**: The **inverse**(p^{-1}) of the point p is the point reflected accross the x-axis. i.e:
  $$p * p^{-1} = 0 = p^{-1} + p \text{ for all p} \in G$$

3.1. **Ex.** Here is an elliptic curve: $y^2 = x^3 + ax + b$, we see that it is intersected by the line x=.5. The two points that x=.5 crosses are inverses. (see Figure 3.1):



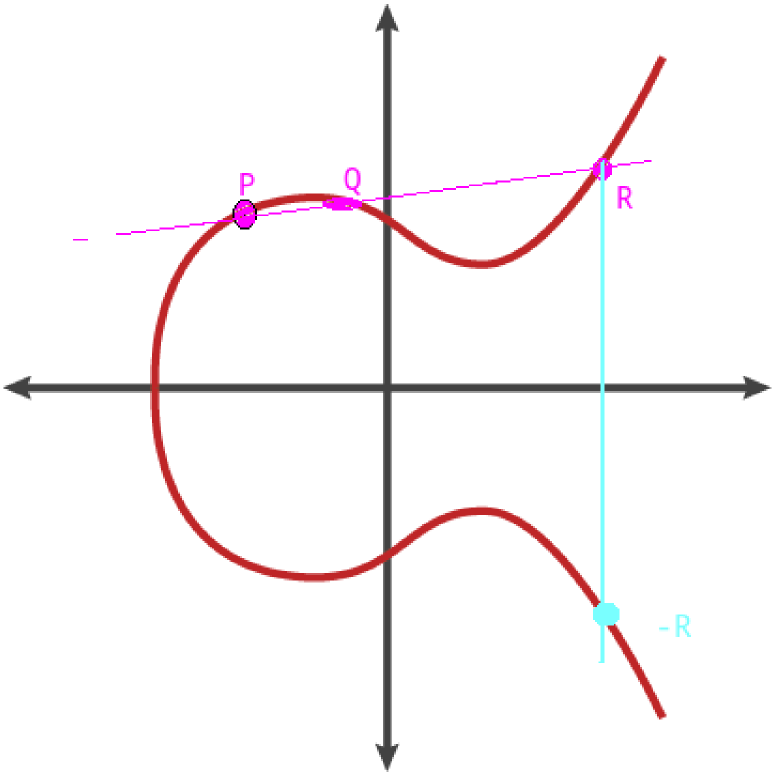
- **Associativity**If P,Q,R are aligned then we have:

$$\begin{gathered} P + (Q + R) = \\ = Q + (P + R) \\ = R + (P + Q) \\ \ldots \\ = 0 \end{gathered}$$

We have necessarily shown that the binary operation + is associative **and** commutative.
Thus, the group G is necessarily abelian!

3.2. **Geometric Addition.** Since we have shown that G is indeed an abelian group, we may redefine the equation: $P + Q + R = 0$ to $P + Q = -R$!
If we draw a line intersecting through P and Q, the line will intersect a third point on the curve, denoted R.

3.3. **Ex.** Here is an elliptic curve demonstrating the property explained above(see Figure 3.3):


P
Q
R
-R