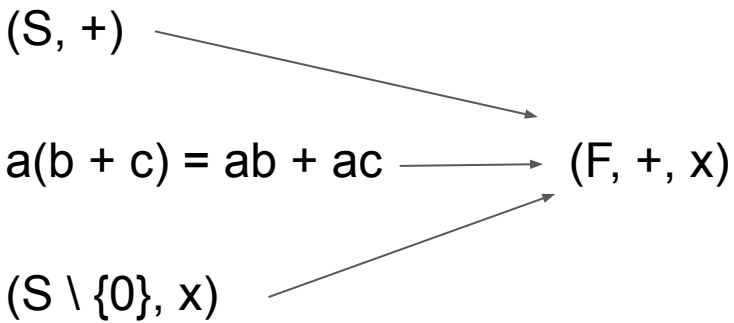
Chapter 2

Basic Operations

Abelian group

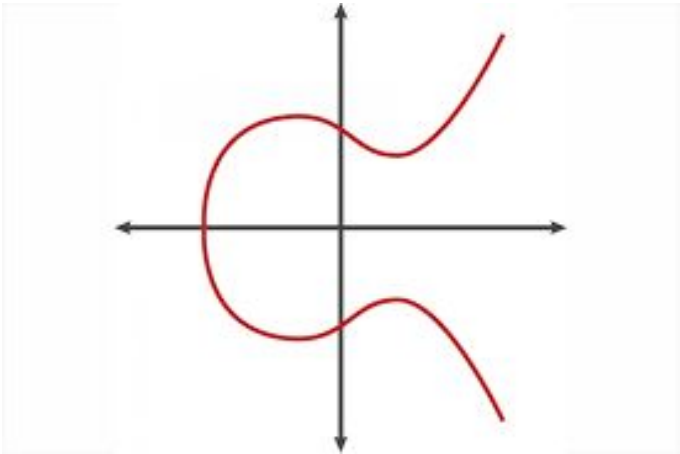
Field



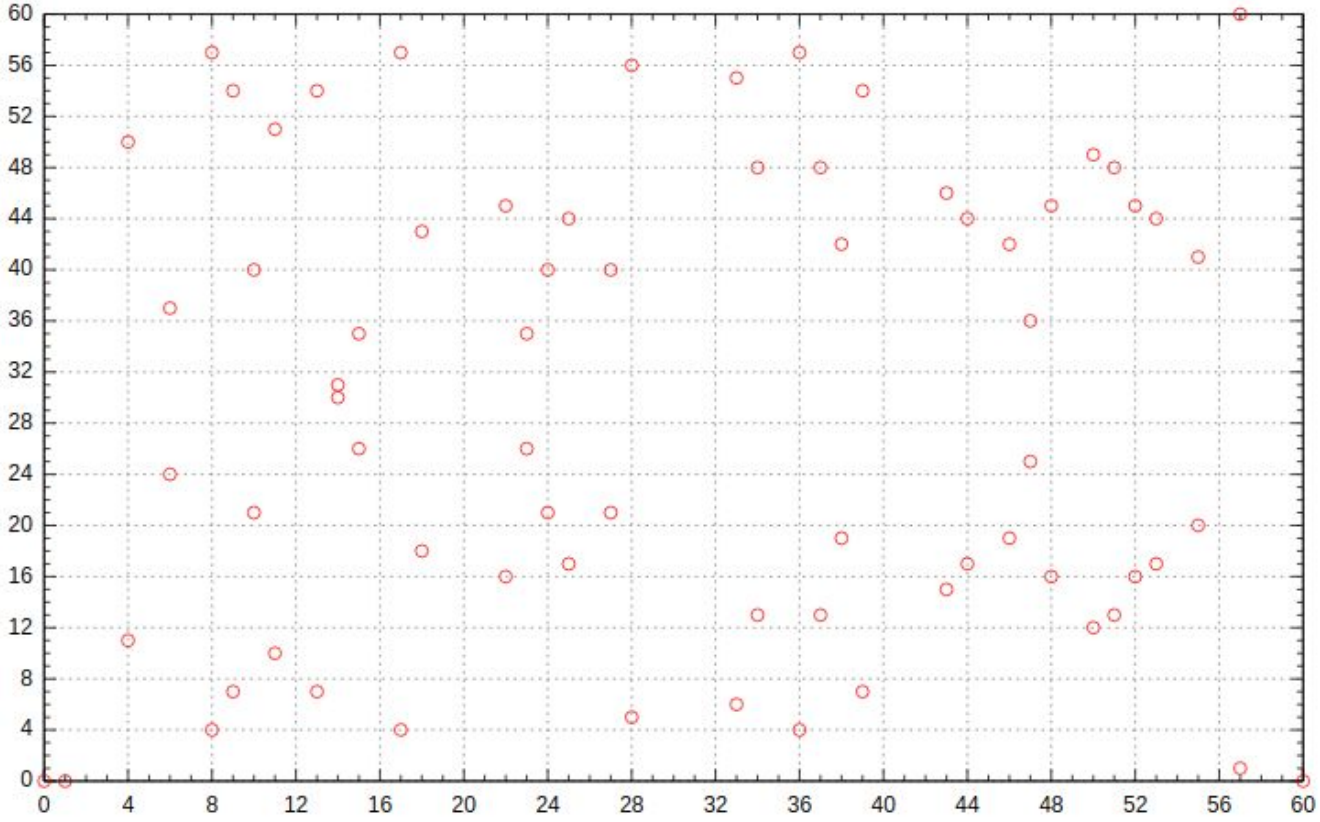
Section 2.2 - Elliptic Curves

- Montgomery elliptic curves are curves of the form: $By^2 = x^3 + Ax^2 + x$
- We also importantly consider a “point at infinity”, ∞, to be part of the curve

Elliptic curve over the real numbers



An elliptic curve over the finite field, F_{61}



Group structure of elliptic curves

Collectively supplementing the points on the elliptic curve with a binary addition operation yields an abelian group!

Define the additive identity to be the point at infinity, ∞. So, for a point P on the elliptic curve, $P + \infty = \infty + P = P$.

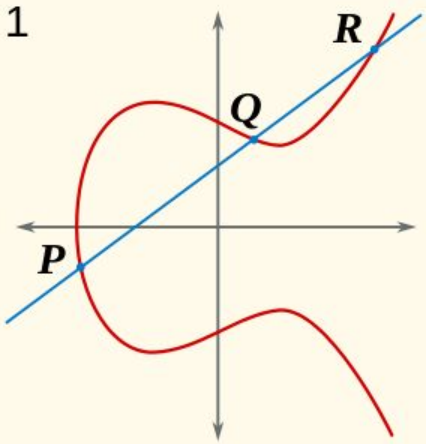
To add two points on the curve, draw a line of intersection through the points. The third point of intersection is defined as the negation of the sum of the points. This is because we define the sum of three points of intersection on a line as ∞.

To get the correct sum, reflect this point over the x-axis.

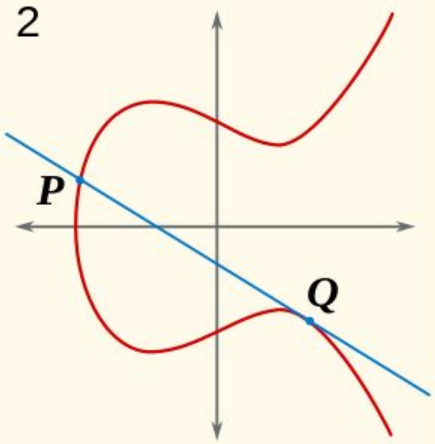
Note the third point may be ∞ if the line is vertical

Elliptic Curves

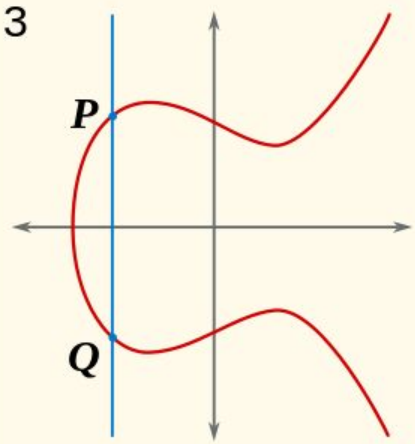
Point addition



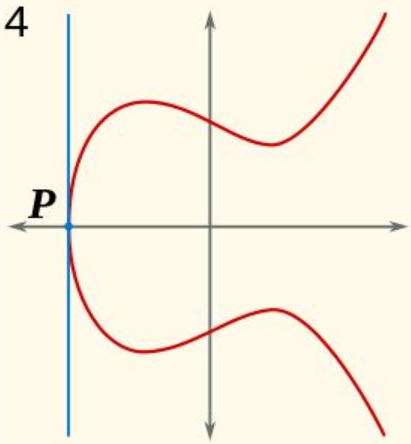
$P + Q + R = 0$



$P + Q + Q = 0$



$P + Q + 0 = 0$



$P + P + 0 = 0$

Discrete logarithm problem

Scalar multiplication can be defined using repeated point doubling and addition

It is denoted: [k]P

Since we are dealing with repeated applications of an abelian group's operation, we can naturally define a discrete log problem:

Given a point P and a scalar multiple [k]P, find k

Now knowing how "strangely" addition works and how unrelated the sum of points seem to the original points, you can imagine how difficult solving the discrete log problem will be for large k