Math/CS 103 Professor: Padraic Bartlett

Minilecture 12: Groups and Elliptic Curves

Week 9 *UCSB 2014*

On a recent HW, we defined the concept of a **group**:

Definition. A **group** is the following object: a set G along with an operation $\cdot$ that satisfies the following properties:

- **Closure**: For all a, b in G, $a \cdot b$ is in G.
- **Associativity**: For all a, b and c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Identity element**: There exists an element e in G such that for all a in G, $e \cdot a = a \cdot e = a$.
- **Inverse element**: For each a in G, there is an element b in G such that $a \cdot b = b \cdot a = e$, where e is an identity element.

On said HW, you found several examples of groups:

1. $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$, the collection of integers $\{0, \ldots n-1\}$ with the group operation given by addition mod n, is a group for any n.
2. $\langle (\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot \rangle$, the collection of integers $\{1, \ldots n-1\}$ with the group operation given by multiplication mod n, is a group whenever n is a prime number.

You also proved that groups satisfy certain properties:

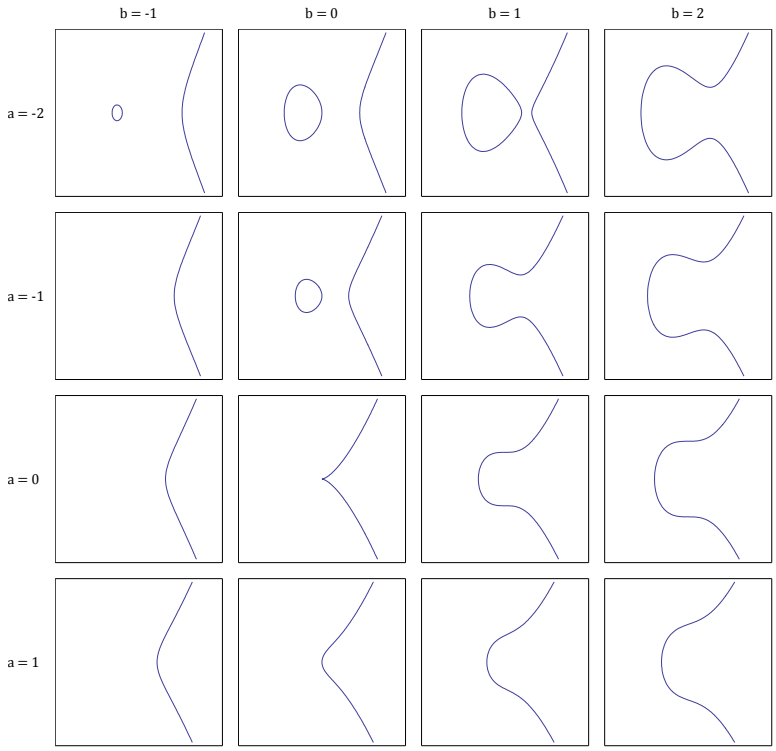
Proposition. Let G be a group with group operation $\cdot$ and identity element e. For any a in this group, let a^k denote the object $\overbrace{a \cdot a \cdot \ldots \cdot a}^{k \text{ times}}$. Let n be the number of elements in this group. Then

$$a^n = e.$$

In this minilecture, I want to introduce one particularly interesting and useful group: the **elliptic curve group**! Consider the following definitions:

Definition. An **elliptic curve** with coefficients $a, b \neq 0$, for the purposes of this class, is the collection of all points (x, y) satisfying the equation

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



Pictures of several elliptic curves with various parameters a, b. Blatantly stolen from Wikipedia.

Notice the following property:

Proposition. Take any two points P, Q on an elliptic curve, and draw a straight line through these two points. Then there are two possibilities: either this line intersects no other points of our elliptic curve, or it intersects our elliptic curve at exactly one other point R.

(If you let $P = Q$, you can make this statement still true by interpreting the "straight line" through those two points to be the tangent line to our curve at that point.)

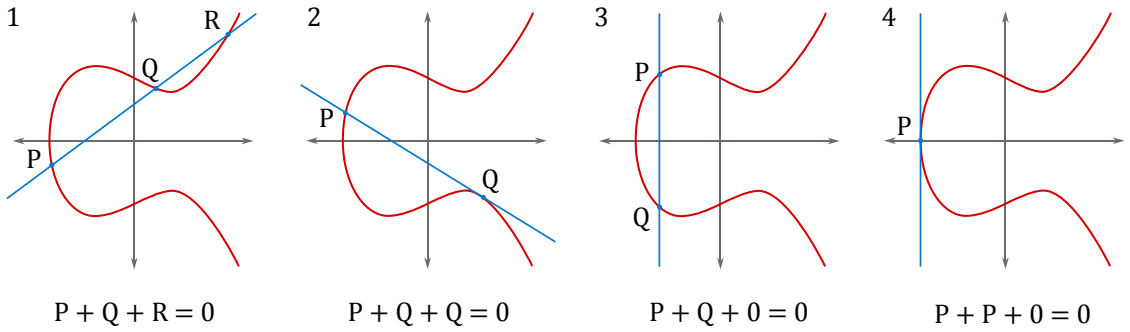
The proof of this is on your HW!

Using this property, we can define an "operation" on the points of our elliptic curve:

Definition. Take some fixed elliptic curve $y^2 = x^3 + ax + b$. Add to the collection of these points a "point at infinity," O. Given this collection of points, consider the following operation: given any two points P, Q, construct a straight line through P and Q. (If $P = Q$, then take a tangent line through P. If P or Q is O, simply set our line to be the single point given by whichever point is not O. Finally, if both $P, Q = O$, just assume that your line is "at infinity," and consists of only the point O.)

If this line goes through a third point on our curve, call that point R. If it does not go through a third point, set $R = O$.

We define our operation as follows: for any such triple P, Q, R, define $P + Q = -R$, and for any point $R = (x, y)$, define $-R = (x, -y)$.



Pictures of points being added on an elliptic curve. Again, pictures stolen from Wikipedia.

Questions on the HW: does this define a group? Does it do so for any curve $y^2 = x^3 + ax + b$?