Math 215 Spring 2023 Number Theory II

Elliptic Curves

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

4-21-2023

Outline

Definition of Elliptic Curves

An elliptic curve is a cubic curve of the form $y^2 = x^3 + ax + b$.

Every irreducible cubic curve (cannot be factored into smaller polynomials) can be transformed to this form as long as the coefficients are not in a field of characteristic 2 or 3.

The adjective *elliptic* was attached to these curves because they come from integrals used to find arc-length of an ellipse.

Highlights

1. The *Frey elliptic curve* $y^2 = x(x + A^p)(y - B^p)$ was used to prove that the **Fermat equation** $x^p + y^p = z^p$ has no solutions. (Hence no solutions for $x^n + y^n = z^n$ for any $n \in \mathbb{Z}$).

2. Rational points on elliptic curves are used in *Elliptic Curve Cryptography* and *Elliptic Curve Factorization.*

3. The points on elliptic curves yield interesting results on number fields just as the points on the unit circle yield the *cyclotomic extensions.* They can also be used to construct new field extensions with interesting properties.

Some Properties

1. The elliptic functions can be used to parametrize elliptic curves over complex field and they are doubly periodic. (Similar to exponential functions parametrizing the circle).
2. Over complex numbers the curve is topologically same as the torus of genus 1 (donut with 1 hole).
3. Elliptic curves can be studied over $\mathbb{R}, \mathbb{Q}$, or $\mathbb{F}_p$ for various p and there are amazing connections between all of these.

Group Operation on Unit Circle

Recall the following group operation on the rational points on a unit circle (HW3, NT1, Fall 2022) :

If $P = (\cos(2\pi a), \sin(2\pi a))$ and $Q = (\cos(2\pi b), \sin(2\pi b))$ are two rational points then let

$$P + Q = (\cos 2\pi(a+b), \sin 2\pi(a+b)).$$

What is the inverse element and what is the identity element? Is it an abelian group?

What is the order of an element P if $a = m/n$ written in the reduced form (i.e, with m, n relatively prime) ?

NOTE: Remember that we also found other rational points by drawing a line from a point (for example $(-1, 0)$ to the circle).

contd: Group operation on the circle

Let the rational points be $P = (\cos(2\pi a), \sin(2\pi a)) = (r, s)$, $Q = (\cos(2\pi b), \sin(2\pi b)) = (u, v)$.
$P + Q = (\cos 2\pi(a+b), \sin 2\pi(a+b)) = (ru - sv, rv + su)$.
Since sums and products of rational numbers is rational, $P + Q$ is rational as well. The identity is $(1, 0)$ and it is easy to check. The inverse of any rational point $P = (\cos(2\pi a), \sin(2\pi a))$ will be $P^{-1} = (\cos(-2\pi a), \sin(-2\pi a))$ so that $P + P^{-1} = (1, 0)$.
Associativity follows from that of addition because eventually $P + Q + R$ equals $(\cos 2\pi(a+b+c), \sin 2\pi(a+b+c))$ where $R = (\cos 2\pi c, \sin 2\pi c)$.

If $a = m/n$ then $P = (\cos 2\pi a, \sin 2\pi a)$ has order n because $P^n = P + P + ... + P$ (n *times*) $= (\cos 2\pi(na), \sin 2\pi(na)) = (\cos 2\pi m, \sin 2\pi m) = (1, 0)$ because m is an integer.

Group operation on $y^2 = x^3 + 17$.

Outline of Silverman's exposition on rational points of the elliptic curve $y^2 = x^3 + 17$:

1. $(-2, 3), (2, 5), (-1, 4)$ are some rational points.
2. The intersection of line of slope 1 from $(-2, 3)$ with the curve gives $(-1, 4)$ and $(4, 9)$.
3. The line of slope 3 does not give rational points, though.
4. If we join two rational points, then the third intersection is guaranteed to be rational, for example join $(-2, 3)$ and $(2, 5)$.
5. Group operation: $P + Q$ is given by reflection of third intersection about the x-axis.

Some results on rational points

1. **Mordell-Weil**: The group of rational points of a non-singular elliptic curve is a *finitely generated* abelian group. Same is true if the points are allowed to be in an *extension of* $\mathbb{Q}$.
2. **Mazur** The subgroup of points of finite order (torsion points) can only be one of finitely many isomorphism types.
3. **Faltings** Any curve of genus bigger than 1 can only have finitely many rational points (or points in a finite extension of $\mathbb{Q}$).
4. **Bhargava, Shankar 2010** The average rank of the free subgroup of group of rational points is bounded.