

# MATH 788Y: BASIC ARITHMETIC OF ELLIPTIC CURVES

TTh 12:30PM- 1:45PM, LC 303B, SPRING 2005

INSTRUCTOR: GANG YU

As a branch of number theory, the theory of Diophantine equations deals with the solution of polynomials in either integers or rationals. The most famous example maybe is Fermat's Last Theorem. This theorem says that if  $n \geq 3$  is an integer, then the equation

$$X^n + Y^n = Z^n$$

has no solutions in non-zero integers  $X, Y, Z$ . Equivalently, the only solutions in rational numbers to the equation

$$x^n + y^n = 1$$

are those with either  $x = 0$  or  $y = 0$ . Fermat's Last Theorem is now known to be true, due to the works of K. Ribet (1990), A. Wiles (1995) and R. Taylor and A. Wiles (1995). The final resolution of Fermat's Last Theorem relies on proving the modularity of a family of elliptic curves defined over the rationals  $\mathbb{Q}$ . An elliptic curve  $E/\mathbb{Q}$  can always be described by an equation (the so-called *Weierstrass form* of  $E$ )

$$E : y^2 = x^3 + ax + b = P(x) \tag{1}$$

where  $a, b \in \mathbb{Z}$  and  $P(x)$  does not have a double root.

The theory of elliptic curves is varied and amazingly vast. It has been very useful in applications. Besides yielding a proof of Fermat's Last Theorem, the theory of elliptic curves also has real world applications. For example, deciphering a public key cipher (invented by Rivest, Shamir and Adleman) depends virtuely on the factorization of a given large composite integer. Factorization algorithms are one of the major concerns of computational number theory. Using techniques from number theory, various algorithms have been devised, such as the continued fraction method, the ideal class group method, and the quadratic sieve method. But one of the best methods currently available is Lenstra's Elliptic Curve Algorithm, which as the name suggests relies on the theory of elliptic curves.

Returning to the special Diophantine equation (1), naturally one may ask:

- (a) Does (1) have any solutions in integers?
- (b) Does (1) have any solutions in rational numbers?
- (c) Does (1) have infinitely many solutions in integers?
- (d) Does (1) have infinitely many solutions in rational numbers?

It turns out that, except for (c), the answer varies as equation (1) varies. It is very nice that the set of rational points on  $E$ , along with an identity, forms an abelian group, called the *Mordell-Weil group* of  $E$  over  $\mathbb{Q}$ , usually denoted by  $E(\mathbb{Q})$ . Thus, the answer to question (d) depends on whether  $E(\mathbb{Q})$  has positive rank. While Mazur shows that the torsion part of  $E(\mathbb{Q})$  can be one of only 15 possibilities, a result of Nuge'll says that all torsion points are with both  $x$  and  $y$  being integers and can be found out according to a simple criterion.

In this course, we will introduce some very basic arithmetic aspects of elliptic curves defined over  $\mathbb{Q}$  and finite fields  $\mathbb{F}_p$ , including the group structure of  $E(\mathbb{Q})$ , the finiteness of the rank of  $E(\mathbb{Q})$ —this is a special case of the Mordell-Weil Theorem, Hasse's estimate on the order of  $E(\mathbb{F}_p)$ , and the elliptic curve  $L$ -functions. If time permits, some applications, such as Lenstra's Elliptic Curve Algorithm, will be introduced.

This course will be accessible to mathematics graduate and undergraduate students having some basic knowledge of elementary number theory.