Congruent Numbers Handout

Yingkun Li
UCLA Math Circle
March 11, 2012

Let's recall a few definitions from the talk.

- A triangle whose sides are all rational numbers is called a *rational triangle*.
- A positive integer is called *congruent number* if it is the area of rational triangle.
- For any real number a, b, an elliptic curve $E_{a,b}$ is the set of points (x, y) in the plane satisfying the equation $y^2 = x^3 + ax + b$. We will primarily be interested in the cases when $a = -n^2$ and $b = 0$ for an integer n. For example, $E_{1,0} : y^2 = x^3 - x$.

In this handout, we will explore the connection between these numbers and curves through exercises.

(Exercise 1) Give 3 examples of congruent numbers and the rational triangles they correspond to.

(Exercise 2a) Given a rational triangle with sides (a, b, c) and area n, show that the following three squares form an arithmetic progression:

$$\left(\frac{b-a}{2}\right)^2, \left(\frac{c}{2}\right)^2, \left(\frac{b+a}{2}\right)^2.$$

What is the difference between consecutive terms? Construct the sequence using one of the three examples you gave above.

(Exercise 2b) Suppose you are given an arithmetic progression

$$49, 169, 289$$

Can you find a rational triangle with sides (a, b, c) such that the procedure in exercise 2a produces this progression? What about any arithmetic progression r^2, s^2, t^2 with r, s, t distinct rational numbers?

From the exercise above, you can probably figure out the origin of name "congruent numbers". The following exercises show the connection between congruent numbers and elliptic curve. We will use E_n to denote the elliptic curve defined by the equation $y^2 = x^3 - n^2x$. If a point $P = (x_0, y_0)$ in the Cartesian coordinate plane satisfies the equation $y^2 = x^3 - n^2x$, we say that the point P lies on the curve E_n.

(Exercise 3a) Given a rational triangle with sides (a, b, c) verify that the point $(\frac{nb}{c-a}, \frac{2n^2}{c-a})$ is on the curve E_n. Use one of the examples you gave in exercise 1 to find this point.

(Exercise 3b) Construct a rational triangle with sides (a, b, c) such that the procedure in the exercise 3b produce the point $(-9, 36)$ on the curve E_{15}. What is the construction for any point (x, y) on E_n with x, y rational numbers and $y \neq 0$?

Here are some exercises about the projective plane, which we denote by $\mathbb{RP}^2$. Recall that points in $\mathbb{RP}^2$ are labeled by homogeneous coordinates $[x : y : z]$, where x, y, z are real numbers with nonzero product, i.e. $xyz \neq 0$. Two coordinates are the same if one can be scaled to the other by a nonzero real number. For example $[1 : 2 : 3]$, $[-\pi, -2\pi, -3\pi]$ and [2:4:6] all represent the same point in $\mathbb{RP}^2$. We can consider the Cartesian plane $\mathbb{R}^2$ as inside of the real projective plane $\mathbb{RP}^2$ via

$$\begin{aligned} \mathbb{R}^2 &\to \mathbb{RP}^2 \\ (x, y) &\mapsto [x : y : 1] \end{aligned} \tag{1}$$

Exercise 4 Three points in $\mathbb{RP}^2$, $p_i = [x_i : y_i : z_i], i = 1, 2, 3$, are collinear if there exist nonzero real numbers a, b, c such that

$$ax_1 + bx_2 + cx_3 = ay_1 + by_2 + cy_3 = az_1 + bz_2 + cz_3 = 0.$$

Are the following three points collinear?

a. [1:0:0], [0:1:0], [0:0:1]

b. [3:2:1], [4:5:6], [1:1:1]

Exercise 5 Describe all the points collinear with the points [15:0:1],[-9:36:1]. If the coordinate of the point is denoted by $[X, Y, Z]$, what is the equation satisfied by X, Y, Z?

Exercise 6 What is the equation of the line passing through [1:0:0] and [0:1:0] in $\mathbb{RP}^2$?

Exercise 7 What is the coordinate of a point in $\mathbb{RP}^2$ <u>not</u> coming from $\mathbb{R}^2$ under (1)? These points are usually called "points at infinity".

Exercise 8a The equation of the elliptic curve E_n in the homogeneous coordinate is $Y^2Z = X^3 - n^2XZ^2$. Which point at infinity lies on the curve E_n?

Exercise 8b The point $(-9, 36) \in \mathbb{R}^2$ is on the curve E_{15}. What is this point in homogeneous coordinate under (1)? Verify that this point satisfies the equation $Y^2Z = X^3 - 15^2XZ^2$.

From the last exercise, we see that a point at infinity in $\mathbb{R}^2$ lies on the elliptic curve. Thus, it is more convenient to study elliptic curves E_n in the projective plane $\mathbb{RP}^2$. So from now on all the points (x, y) on E_n will be described using homogeneous coordinates $[x : y : 1]$.

Next, we will explain how to add and subtract the rational points on the elliptic curve E_n. Here, we will need to quote the following special case of Bézout's theorem.

Theorem 1. *Counting multiplicity, a line and an elliptic curve have three intersections in* $\mathbb{RP}^2$.

Exercise 9 The *negative* of a point $P = [X : Y : Z]$ on E_n is defined by to $-P := [X : -Y : Z]$. What is the negative of $[-9 : 36 : 1]$? What about [0:1:0]?

Exercise 10 Given two points $P = [15 : 0 : 1], Q = [-9 : 36 : 1]$ on E_{15}, they determine a line in $\mathbb{RP}^2$ (see exercise 5). What are all the intersections between this line and the elliptic curve E_{15}?

Exercise 11 What is the equation of the line tangent to E_{15} at the point $P = [15 : 0 : 1]$? What are all the intersections between this line and the curve E_{15}? Does that agree with the theorem above? (Hint: Draw the graph of E_{15} in the plane)

Exercise 12 What are the intersections between the line in exercise 6 and the elliptic curve E_n? Does this agree with the theorem above?

Definition 1. *Let ℓ be a line in $\mathbb{RP}^2$ and intersects the elliptic curve E_n at points P_1, P_2, P_3 with multiplicity m_1, m_2, m_3 respectively. We define the addition operation "$+$" on these point by*

$$m_1P_1 + m_2P_2 = -m_3P_3.$$

Exercise 13 What is the sum of the points $P = [15 : 0 : 1]$ and $Q = [-9 : 36 : 1]$ on E_{15}? (Hint: use exercise 10)

Exercise 14 Denote the point $O = [0 : 1 : 0]$. From exercise 8, we know that O lies on any elliptic curve E_n. What is $-O$ and $O + O$?

Exercise 15a What is the coordinate of $P + (-P)$ for any point P on E_n?

Exercise 15b What is the coordinate of $2P$ when $P = [15 : 0 : 1]$ on E_{15}?

Exercise 16 (May need calculus) What is the coordinate of $2Q$ when $Q = [-9 : 36 : 1]$ on E_{15}?

Exercise 17 Show that the addition operation above is well-defined, commutative, and associative.

Exercise 18 Show that the set of rational points on E_n is closed under addition and inverse operations.

Using the exercises above, one can put a group structure on the rational points on E_n. It is a deep theorem that this group is finitely generated. The rank of this group, i.e. the number of generators, is a mysterious quantity. One can ask many questions about it, few of which can be answered. The

Birch & Swinnerton-Dyer conjecture connects the rank with the order of vanishing of a function $L_E(s)$ at $s = 1$. Under a weak version of the conjecture, Jerrold Tunnell gave a quick algorithm to test if an integer n is a congruent number.

Theorem 2 (Tunnell, 1982)**.** *For a given integer n, define the following sets*

$$\begin{aligned} A_n &= \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\}, \\ B_n &= \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\}, \\ C_n &= \#\{x, y, z \in \mathbb{Z} | n = 8x^2 + 2y^2 + 64z^2\}, \\ D_n &= \#\{x, y, z \in \mathbb{Z} | n = 8x^2 + y^2 + 16z^2\}. \end{aligned}$$

If n is an odd congruent number, then $2A_n = B_n$. If n is an even congruent number, then $2C_n = D_n$. The converse is also true under a weak version of the BSD conjecture for the elliptic curve E_n.

Exercise 19 Verify the theorem for the congruent number $n = 20$.

Exercise 20 Use Tunnell's theorem to show that 1 is <u>not</u> a congruent number.