Congruent Numbers Handout Answers

Yingkun Li
UCLA Math Circle
March 11, 2012

(Exercise 1) Give 3 examples of congruent numbers and the rational triangles they correspond to.
Answer: Answers will vary.

(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.
Answer: The difference is the area n

(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?
Answer: $(a, b, c) = (10, 24, 26)$. In general, we have $(a, b, c) = (|t - r|, |t + r|, 2s)$.

(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.
Answer: Answer will vary.

(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 $y \neq 0$?
Answer: $(a, b, c) = (4, 15/2, 17/2)$. In general, $(a, b, c) = (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y})$.

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]

Answer: (a) No. (b) Yes.

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?
Answer: The points are in the form $a \cdot [15 : 0 : 1] + b \cdot [-9 : 36 : 1]$. The equation of the line is $3X + 2Y - 45Z = 0$.

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

Exercise 7 What is the coordinate of a point in $\mathbb{RP}^2$ not coming from $\mathbb{R}^2$ under (1)? These points are usually called "points at infinity".
Answer: These are points of the form $[u, v, 0]$ with u, v real numbers and $uv \neq 0$. In fact, these points all lie on the same line $Z = 0$.

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?
Answer: The point is $[0 : 1 : 0]$.

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 $Y^2Z = X^3 - 15^2XZ^2$.
Answer: Under (1), the point (-9, 36) is [-9:36:1].

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]?
Answer: [-9:-36:1] and [0:-1:0] = [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}?
Answer: [-15/4:225/8:1].

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)
Answer: Equation of the tangent line is $X - 15Z = 0$.

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?
Answer: The intersection is [0:1:0]. This agrees with the theorem since the intersection has multiplicity 3.

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* <u>*addition operation*</u> *"+" 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)
Answer: [-15/4:-225/8:1].

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 $O + O$?
Answer: They are both O.

Exercise 15a What is the coordinate of $P + (-P)$ for any point P on E_n?
Answer: It is $O = [0 : 1 : 0]$.

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

Exercise 16 (May need calculus) What is the coordinate of $2Q$ when $Q = [-9 : 36 : 1]$ on E_{15}?
Answer: It is [289/16:-2737/64:1].

Exercise 17 Show that the addition operation above is well-defined, commutative, and associative.
Answer: By the theorem above, a line intersects the elliptic curve E_n at exactly three points (not necessarily distinct). So the sum of two points is well-defined. Since the order of the three points do not change the line, this operation is commutative and associative.

Exercise 18 Show that the set of rational points on E_n is closed under addition and inverse operations.
Answer: If two points on E_n have rational coordinates, then the line it determines has rational coefficients as well. Thus, the last intersection point must have rational coordinates since it is the third solution of a rational cubic equation with two other rational roots.

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 $n = 20$.

Answer: When $n = 20$, $C_n = D_n = 0$ and the theorem holds.

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

Answer: When $n = 1$, $A_n = B_n = 2$ and $2A_n \neq B_n$. So 1 is not a congruent number.