Exercises for the congruent number problem

Maosheng Xiong

1. Prove Euclid's formula (300 BC): Given (a, b, c) positive integers, pairwise coprime, and $a^2+b^2 = c^2$ (such (a, b, c) is called a primitive Pythagorian triple). Then there is a pair of coprime positive integers (p, q) with $p + q$ odd, such that

$$a = 2pq, \quad b = p^2 - q^2, \quad c = p^2 + q^2.$$

2. Prove that 2 is not a congruent number, following Fermat's method of infinite descent.

3. The rational point $P = (1, 2)$ is on the elliptic curve

$$E: \quad y^2 = x^3 - 5x + 8.$$

Using the tangent line and the secant line construction, verify that

(i)

$$2P = P + P = \left(-\frac{7}{4}, -\frac{27}{8}\right).$$

(ii) Let $Q = \left(-\frac{7}{4}, -\frac{27}{8}\right)$, then

$$3P = P + Q = \left(\frac{553}{121}, -\frac{11950}{1331}\right).$$

4. Given a positive rational number t. A rational number n is called t-congruent if there are positive rational numbers a, b, c such that

$$a^2 = b^2 + c^2 - 2bc\frac{t^2 - 1}{t^2 + 1}, \quad \text{and } 2n = bc\frac{2t}{t^2 + 1}.$$

Prove that n is t-congruent if and only if the following:

(i) Either both n/t and $t^2 + 1$ are nonzero rational squares,

(ii) or the elliptic curve

$$C_{n,t}: \quad y^2 = x(x - n/t)(x + nt)$$

has a rational point (x, y) with $y \neq 0$.