Elliptic curves

(1) Prove that the elliptic curve

$$E: \quad y^2 = x^3 - x$$

has no points of order 4 over $\mathbb{Q}$ under the "chord-tangent law". (Hint. First determine the points of order 2, and then determine the conditions which are required for a point P to have the property that $2P$ is one of these points.)

(2) The number 5 is congruent. Use the results from the lecture to produce 4 rational points $(x, y) \in \mathbb{Q}^2$ with $y \neq 0$ on the elliptic curve

$$E(5): \quad y^2 = x^3 - 25x.$$

(3) Let D be a positive integer. Prove that if there is a point $(x, y) \in \mathbb{Q}^2$ for which

$$y^2 = x^3 - D^2 x$$

and $y \neq 0$, then D is a congruent number.

(4) How many rational right triangles with area 5 can one directly construct using just these 4 points? Construct them.

(5) Prove that there are infinitely many rational right triangles with area 5.

(6) Consider the elliptic curve

$$E: \quad y^2 = x^3 + 1.$$

For primes p let $a_E(p) := p - N(p)$, where

$$N(p) := \#\{(x, y) \pmod{p} \ : \ y^2 \equiv x^3 + 1 \pmod{p}\}.$$

a) Compute $a_E(p)$ for the primes $p \in \{5, 7, 11, 13, 17, 19\}$.

b) Compute the coefficients $A(n)$, for $n \leq 20$, of the infinite product

$$\sum_{n=1}^{\infty} A(n) q^n := q \prod_{n=1}^{\infty} (1 - q^{6n})^4 = q - 4q^7 + \dots.$$

(Hint. Use the Euler and Jacobi identities from the "partitions" lecture.).
c) Compare $A(p)$ and $a_E(p)$ for the primes $p \in \{5, 7, 11, 13, 17, 19\}$.

d) For primes $p \equiv 2 \pmod{3}$, prove your speculation (i.e. $A(p) = a_E(p)$ for all primes $p \geq 5$). (Hint. First show that $A(p) = 0$ for such p. Then show that $N(p) = p$ for these p using a group homomorphism $x \to x^3$ on the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.)