Homework Set Twelve

Due Thursday, July 21.

Question 1. We say that $n \in \mathbb{N}$ is *congruent* if there exists $(a, b, c) \in \mathbb{Q}^3$ such that

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad n = \frac{ab}{2}.$$

In other words, there exists a right triangle with rational sides whose area equals n. Recall that Fermat's Last Theorem states that if $n \geq 3$ then $a^n + b^n = c^n$ has no solution $(a, b, c) \in \mathbb{Q}^3$ with $abc \neq 0$.

(a) Suppose there are nonzero integers x, y, z such that $x^4 - y^4 = z^2$.

 (i) Find $(a, b, c) \in \mathbb{N}^3$ in terms of x and y such that $a^2 + b^2 = c^2$ and $\frac{ab}{2} = (xyz)^2$. (Hint: take $u = x^2$ and $v = y^2$ and recall what you've learned when working with primitive pythagorean triples.)

 (ii) Find $(A, B, C) \in \mathbb{Q}^3$ such that $A^2 + B^2 = C^2$ and $\frac{1}{2}AB = 1$. (Hint: These should be in terms of combinations of a, b, c, x, y, z.) Use this to deduce that if 1 is congruent there exists $(r, s, t) \in \mathbb{Q}^2$ such that $xyz \neq 0$ and $x^4 - y^4 = z^2$ has a integers x, y, z such that $xyz \neq 0$.

(b) (BONUS) Suppose that $x^4 - y^4 = z^2$ has no solutions $(x, y, z) \in \mathbb{Z}^2$ with $xyz \neq 0$. Use this to prove that the number 1 is not congruent.

(c) (BONUS) Fermat proved that $x^4 - y^4 = z^2$ has no nontrivial solutions thus establishing, by the above, that 1 is not congruent. Show that this also implies Fermat's Last Theorem in the case of $n = 4$.

Question 2. A cubic curve E given by the equation

$$y^2 = x^3 + ax^2 + bx + c$$

defines an elliptic curve if and only if $\Delta(E) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$. (We call $\Delta(E)$ the *discriminant of* E.)

(a) Let $g(x) = x^2 + bx + c$. Prove that if $g(x) = (x - \alpha_1)(x - \alpha_2)$ then $(\alpha_1 - \alpha_2)^2 = b^2 - 4c$. (This is called the *discriminant of* g.)

(b) (BONUS) Prove that if $f(x) = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ then

$$\Delta(E) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

(c) A theorem of Nagell-Lutz says that if $(x_0, y_0) \in E(\mathbb{Q})$ is a point of finite order then $x_0, y_0 \in \mathbb{Z}$ and either $y_0 = 0$ or $y_0^2 \mid \Delta(E)$. Use this to find all points of finite order for each of the following elliptic curves.

 (i) $y^2 = x^3 - 2$

 (ii) $y^2 = x^3 + 8$

(iii) $y^2 = x^3 + 4$

(iv) (BONUS) $y^2 = x^3 - 43x + 166$.

Question 3. Consider the elliptic curve $E\colon y^2 = x^3 + 24$ over the real numbers. Check that $P = (-2, 4)$ and $Q = (1, 5)$ are on E and compute $P + Q$ and $P - Q$.

Question 4. Suppose p is a prime and $p \equiv 2 \pmod 3$.

(a) Show there exists an integer m such that $3m \equiv 1 \pmod{p-1}$.

(b) Use the previous part to show that every integer modulo p has a unique cube root. That is, show that for every $a \in \mathbb{Z}$ there exists $b \in \mathbb{Z}$ such that $a \equiv b^3 \pmod p$.

(c) Consider the elliptic curve $E\colon y^2 \equiv x^3 + 1$. Use the previous information to prove that $\#E(\mathbb{F}_p) = p + 1$.

Question 5. We associate to any $F(x, y) \in \mathbb{C}[x]$ the curve

$$C_F = C := \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}.$$

Definition. The curve C is is said to be *nonsingular at* $P_0 = (x_0, y_0)$ if $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ do not vanish simultaneously at (x_0, y_0). The curve is called *nonsingular* if it is nonsingular at every point.

Suppose that $f(x) = x^3 + ax^2 + bx + c$ for some $a, b, c \in \mathbb{C}$.

(a) (BONUS) Recall that a cubic curve $C\colon y^2 = f(x)$ (defined as above for $F(x, y) = y^2 - f(x)$) is an *elliptic curve* if f has no repeated roots. Prove that every such elliptic curve is nonsingular.

(b) (BONUS) Suppose that the curve C defined by $F(x, y) = y^2 - f(x)$ is nonsingular. Prove that C is an elliptic curve.

Question 6. Let k be a field. Let $\mathbb{P}_k^2 = \{(a, b, c) \in k^2 \mid (a, b, c) \neq (0, 0, 0)\}$, and recall that a *line* in $\mathbb{P}_k^2$ is defined to be the set of solutions to an equation of the form

$$\alpha X + \beta Y + \gamma Z = 0$$

with $\alpha, \beta, \gamma \in k$ not all zero.

(a) (BONUS) Prove directly from this definition that two distinct points in $\mathbb{P}_k^2$ are contained in a unique line.

(b) (BONUS) Similarly, prove that any two distinct lines in $\mathbb{P}_k^2$ intersect in a unique point.