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 $(x, y) \in \mathbb{Q}^2$. 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 $n = 4$.

Answer.

(a) Set $u = x^2$ and $v = y^2$. Take $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$. Then $a^2 + b^2 = c^2$ and

$$\frac{1}{2}ab = \left(u^2 - v^2\right) uv = \left(x^4 - y^4\right) x^2 y^2 = x^2 y^2 z^2,$$

where we used that $x^4 - y^4 = z^2$. This proves (i).

Now set $\lambda = xyz$ (which is nonzero since x, y, z are nonzero). Take $A = a/\lambda$, $B = b/\lambda$, and $C = c/\lambda$. Then (A, B, C) satisfies the required conditions.

(b) We prove the contrapositive. That is, we will show that if 1 is congruent then there exists $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$ and $x^4 - y^4 = z^2$. Assuming that 1 is congruent, let $(a, b, c) \in \mathbb{Q}$ be such that

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{ab}{2} = 1.$$

Now let $\lambda \in \mathbb{Z}$ be such that $(A, B, C) = (a\lambda, b\lambda, c\lambda)$ is a primitive pythagorean triple. Note that $AB = ab\lambda^2 = 2\lambda^2$. Now set

$$x = A + B, \qquad \text{and} \qquad y = A - B.$$

Notice that x and y are both nonzero since $A \neq B$. We calculate directly that

$$\begin{aligned} x^4 - y^4 &= (A+B)^4 - (A-B)^3 \\ &= 8A^3B + 8AB^3 \\ &= 8AB(A^2+B^2) \\ &= 16\lambda^2C^2 = (4\lambda C)^2. \end{aligned}$$

Thus, setting $z = 4\lambda C$ gives the desired solution.

(c) Suppose that a counterexample to Fermat's Last Theorem for $n = 4$ exists, meaning there exist nonzero integers a, b, c such that $a^4 + b^4 = c^4$. Now set $x = c$, $z = b^2$ and $y = a$. This gives

$$x^4 - y^4 = c^4 - a^4 = b^4 = (b^2)^2 = z^2.$$

Since x, y, z are nonzero this contradicts Fermat's result. Hence no such counterexample exists.

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

Answer.

(a) If

$$x^2 + bx + c = (x-\alpha_1)(x-\alpha_2) = x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2,$$

it follows that $b = -(\alpha_1 + \alpha_2)$ and $c = \alpha_1\alpha_2$. Therefore,

$$b^2 - 4c = (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2 = (\alpha_1 - \alpha_2)^2$$

as desired.

(b) We see similarly to part (a) that if

$$\begin{aligned} x^3 + ax^2 + bx + c &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \\ &= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

then

$$a = -\alpha_1 - \alpha_2 - \alpha_3, \quad b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \quad c = -\alpha_1\alpha_2\alpha_3.$$

A lengthy calculation gives the desired formula.

(c) In Table 1, for each possibility of E, we give the possible nonzero values of y_0, where (x_0, y_0) is a point of finite order on $E(\mathbb{Q})$.

E	$y^2 = x^3 - 2$	$y^2 = x^3 + 8$	$y^2 = x^3 + 4$	$y^2 = x^3 - 43x + 166$
$\Delta(E)$	$-3(2 \cdot 3)^2$	$-3(3 \cdot 2 \cdot 2 \cdot 2)$	$-3(3 \cdot 2 \cdot 2)^2$	$- \cdot 2 \cdot 13(2^7)^2$
$\pm y_0$	$2, 3, 6$	$2, 3, 4, 6, 8, 12, 24$	$2, 3, 4, 6, 12$	$2, 2^2, \ldots, 2^7$

Table 1: Possible nonzero y_0-values for points of finite order on E

Plugging these values into each of the corresponding equations, we find that for (i) (besides the identity element), there are no finite order points, for (ii) the points

$$(-2, 0), (-1, \pm 3), (2, \pm 4)$$

all lie on the curve.

For (ii), we similarly find that the only possible points of finite order is $(0, 2)$ and $(0, -2)$. It is easy to see that both points are inflection points, hence $E(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/3\mathbb{Z}$.

For (iii), although $(-2, 0)$, $(1, \pm 3)$ and $(2, \pm 4)$ are all integral points on the curve, we claim that $E(\mathbb{Q})_{\text{tor}} = \{\mathcal{O}, (-2, 0)\} \simeq \mathbb{Z}/2\mathbb{Z}$. Clearly $(-2, 0)$ is a point of order two on $E(\mathbb{Q})$. If either of the other 4 points were also of finite order, then the line between any of them and $(-2, 0)$ would interect $E(\mathbb{Q})$ at another point of finite order. However, the coordinates of all such points are readily checked to be nonintegral, hence by the Nagel-Lutz Theorem, they are not of finite order. This proves the claim.

Finally, for (iv), from the table we find the following possibilities of finite order points:

$$(-5, \pm 2^4), \quad (3, \pm 2^3), \quad (11, 2^5).$$

In fact, one can show that for $P = (-5, 16)$, $Q = (3, 8)$ and $R = (11, 32)$,

$$R + P = -P, \quad Q + R = P, \quad \text{and} \quad 2R = Q.$$

From this it follows that

n	0	1	2	3	4	5	6
nR	$\mathcal{O}$	R	Q	P	$-P$	$-Q$	$-R$

In other words, $E(\mathbb{Q})_{\text{tor}} = \{nR \mid 0 \leq n \leq 6\} \simeq \mathbb{Z}/7\mathbb{Z}$.

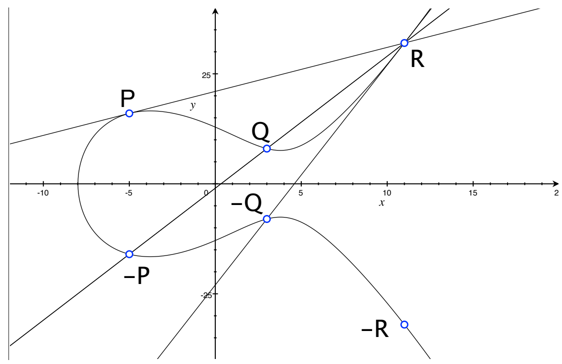

Figure 1: Rational points of finite order on $E : y^2 = x^3 - 43x + 166$

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 $P - Q$.

Answer. We note that

$$4^2 = (-2)^3 + 24 \qquad \text{and} \qquad 5^2 = 1^3 + 24,$$

showing that both points are on the curve.

(a) We first compute the line through $P = (x_1, y_1) = (-2, 4)$ and $Q = (x_2, y_2) = (1, 5)$. For example, the slope of this line is $m = \frac{5-4}{1-(-2)} = \frac{1}{3}$. Plugging in $(1, 5)$ into $y = \frac{1}{3}x + b$ gives $b = 5 - \frac{1}{3} = \frac{14}{3}$, so that the line though P and Q is

$$\ell\colon y = \frac{1}{3}x + \frac{14}{3} = \frac{1}{3}(x + 14).$$

Therefore, the points of intersection between ℓ and E are the solutions of the two equations

$$y = \frac{1}{3}(x + 14) \tag{1}$$
$$y^2 = x^3 + 24. \tag{2}$$

Substituting (1) into (2) we find

$$\left(\frac{1}{3}(x + 14)\right)^2 = x^3 + 24 \iff \frac{1}{9}\left(x^2 + 28x + 196\right) = x^3 + 24,$$

that is,

$$x^3 - \frac{1}{9}x^2 - \frac{28}{9}x - \frac{20}{9} = 0.$$

Now, the sum of the x-values of the three solutions must equal $-h$, where h is the coefficient of the x^2 term. That is, letting $P + Q = (x_3, y_3)$ we must have $(-2) + 1 + x_3 = \frac{1}{9}$ and we find $x_3 = \frac{10}{9}$. Plugging this into (1) gives $y = \frac{136}{9}$. However, we actually want the negative value of this. That is, $(x_3, y_3) = (\frac{10}{9}, -\frac{136}{9})$.

An alternative approach is to use the formula (which amounts to the same thing that we just did)

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1. \tag{3}$$

We will use the formulas to now compute $P - Q$. Let $P - Q = (x_4, y_4)$. Since $-Q = (x_2, -y_2) = (1, -5)$ and $P - Q = P + (-Q)$ we find the slope is

$$m = \frac{-5-4}{1-(-2)} = -3.$$

Therefore, using (3) we find

$$\begin{aligned} x_4 &= m^2 - x_1 - x_2 = 9 - (-2) - 1 = 10 \quad \text{and} \\ y_4 &= m(x_1 - x_4) - y_1 = -3(-2-10) - 4 = 32. \end{aligned}$$

Thus, $P - Q = (10, 32)$.

(b) Let ℓ be the tangent line to the point P. Using implicit differentiation we find

$$2y\,dy = 3x^2 dx.$$

Substituting $P = (-2, 4)$, we find the slope of ℓ is

$$\frac{dy}{dx} = \frac{3x^2}{2y} = \frac{12}{8} = \frac{3}{2}.$$

Therefore, the equation of ℓ is $\ell\colon y = \frac{3}{2}x + \frac{7}{2}$ (where we also found the $\frac{7}{2}$ however we like). The points of intersection are now solutions to the equations

$$y = \frac{1}{2}(3x+7) \tag{4}$$

$$y^2 = x^3 + 24. \tag{5}$$

Substituting (4) into (5) we find

$$\left(\frac{1}{2}(3x+7)\right)^2 = x^3 + 24 \iff \frac{1}{4}\left(9x^2 + 42x + 49\right) = x^3 + 24,$$

or

$$x^3 - \frac{9}{4}x^2 - \frac{21}{2}x - \frac{49}{4} = 0.$$

Again, the x-values of the solutions must sum to $\frac{9}{4}$. Setting $2P = (x_5, y_5)$ this means $(-2) + (-2) + x_5 = \frac{9}{4}$, or $x_5 = \frac{25}{4}$. Plugging this into (4) gives the y-value of $\frac{103}{8}$, of which we want the negative. Thus, $2P = (x_5, y_5) = (\frac{25}{4}, -\frac{103}{8})$. Again, the formulas from part (a) could have been used.

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 $\#E(\mathbb{F}_p) = p + 1$.

Answer.

(a) We have $p \equiv 2 \pmod 3$ implies $p - 1 \equiv 1 \pmod 3$. That is, $p - 1 \not\equiv 0 \pmod 3$, which means $3 \nmid (p-1)$. Moreover, since $2 \nmid 3$, we must have $\gcd(3, p-1) = 1$. Therefore, there exists $m, n \in \mathbb{Z}$ such that $3m + (p-1)n = 1$. That is, there exists an $m \in \mathbb{Z}$ such that $3m \equiv 1 \pmod{p-1}$.

(b) By part (a) there is an $\ell \in \mathbb{Z}$ such that $3m = 1 + (p-1)\ell$ (in fact, $\ell = -n$ for the n in the previous solution). Suppose $a^3 \equiv b \pmod p$. Then $b^m \equiv a^{3m} \equiv aa^{(p-1)\ell} \equiv a \pmod p$ since $a^{p-1} \equiv 1 \pmod p$. Meanwhile, if we assume $a \equiv b^m \pmod p$, then $a^3 \equiv b^{3m} \equiv bb^{(p-1)\ell} \equiv b \pmod p$.

(c) The previous parts imply that for each y there is a unique x with $x^3 \equiv y^2 - 1 \pmod p$. (For example, $x^3 \equiv y^2 - 1 \pmod p \iff (y^2-1)^3 \equiv x \pmod p \iff x \equiv (y^2-1)^3 \pmod p$, so each y gives a unique x. If there was an x^2 term we could not state this.) Since $0 \leq y \leq p - 1$, there are p many choices for y. Adding the point at infinity gives $p + 1$ many points. $\square$

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.

Answer.

(a) We prove the contrapositive. To do so, assume that C has a singular point. This means that both $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ simultaneously vanish at some point (x_0, y_0) on C. Since $\frac{\partial F}{\partial y} = 2y = 0$ at y_0, we must have $y_0 = 0$. Meanwhile, since $\frac{\partial F}{\partial x} = f'(x) = 0$ at $x = x_0$, we have $f'(x_0) = 0$. Finally, since (x_0, y_0) is on C, we have that $0 = y_0^2 - f(x_0) = -f(x_0)$ so that $f(x_0) = 0$. Since $f(x_0) = f'(x_0) = 0$ it must be that f has a multiple root at x_0. That is, C is not an elliptic curve.

(b) Again, we prove the contrapositive. Supppose that $f(x)$ has a multiple root at some point α. That is, $(\alpha, 0)$ is a point on C. On one hand, this implies that $f'(\alpha) = 0$

so that $\frac{\partial F}{\partial x}$ vanishes at $(\alpha, 0)$. On the other hand, since $\frac{\partial F}{\partial y} = 2y$ also vanishes at this point. Thus, C is singular (i.e. not nonsingular).

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.

Answer. Suppose that $\mathbf{u}$ and $\mathbf{v}$ are nonzero vectors in 3-space. We recall the following facts.

- The cross product $\mathbf{u} \times \mathbf{v}$ is a vector which is perpendicular to both $\mathbf{u}$ and $\mathbf{v}$. It is the zero vector if and only if $\mathbf{u} = t\mathbf{v}$ for some nonzero t. (In other words, $\mathbf{u} \times \mathbf{v} = \mathbf{0}$ if and only if $\mathbf{u}$ and $\mathbf{v}$ are colinear.)

- The vectors $\mathbf{u}$ and $\mathbf{v}$ are perpendicular to each other if and only if their dot product $\mathbf{u} \cdot \mathbf{u} = 0$.

- If $P, Q, R \in k^3$ are not colinear, there is a uniqe plane containing them.

Note that the projective line $\mathbb{P}_k^2$ can be identified with the set of lines in k^3 passing through the origin. In other words, points in $\mathbb{P}_k^2$ are given by $\{t\mathbf{u} \mid t \in k\}$ for some nonzero vector $\mathbf{u} \in k^3$.

(a) Let $[a:b:c]$ and $[d:e:f]$ be unique points in $\mathbb{P}_k^2$. Then the points (a,b,c), (d,e,f) and $(0,0,0)$ in k^3 are not colinear so by the third point above, there is a unique plane in k^3 containing the three points. Any equation for this plane $\alpha X + \beta Y + \gamma Z = 0$ defines a line in $\mathbb{P}_k^2$.

(b) A line $L = L_{\alpha,\beta,\gamma}$ in $\mathbb{P}_k^2$ is given by an equation of the form $\alpha X + \beta Y + \gamma Z = 0$ with α, β, γ not all zero. So, by the second bullet point above, the point $\{t\mathbf{u} \mid t \in k\}$ lies on $L_{\alpha,\beta,\gamma}$ if and only if (α, β, γ) is perpendicular to $\mathbf{u}$. Let $L_{\alpha',\beta',\gamma'}$ be another (different) line in $\mathbb{P}_k^2$. That means (α, β, γ) and $(\alpha', \beta', \gamma')$ are noncolinear nonzero vectors. Let

$$\mathbf{u} = (\alpha, \beta, \gamma) \times (\alpha', \beta', \gamma').$$

By the first bullet point, $\mathbf{u}$ lies on both lines. On the other hand, again applying the first bullet point, $\mathbf{v}$ lies on both lines only if it is a nonzero multiple of $\mathbf{u}$. Hence there is a unique point in $\mathbb{P}_k^2$ on both lines.