Exercise: 1 is not a Congruent Number

William stein

July 31, 2012

If you can do this exercise, you will prove that 1 is not a congruent number, hence that the area of a rational right triangle can not be a perfect square. Along the way, you will also prove Fermat's Last Theorem for exponent 4 (and something even stronger).

1. Suppose a, b, c are relatively prime integers with $a^2+b^2=c^2$ (relatively prime means that no prime number simultaneously divides all three of a, b, c). Then there exist integers x and y with $x > y$ relatively prime such that $c = x^2 + y^2$ and either $a = x^2 - y^2$, $b = 2xy$ or $a = 2xy$, $b = x^2 - y^2$. [Hint: use that the unit circle $X^2+Y^2 = 1$ is parametrized by $X = \frac{1-t^2}{1+t^2}$, $Y = \frac{2t}{1+t^2}$.]

2. Fermat's Last Theorem for exponent 4 asserts that any solution to the equation $x^4 + y^4 = z^4$ with $x, y, z \in \mathbf{Z}$ satisfies $xyz = 0$. Prove Fermat's Last Theorem for exponent 4, as follows:

   (a) Show that if the equation $x^2 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$, then Fermat's Last Theorem for exponent 4 is true.

   (b) Show that if n, k, m are integers with $n^2 + k^4 = m^4$ and p is a prime that divides both k and m, then p^2 divides n. Thus by dividing both sides by p^4, we see that there exists an integer solution with n, k, m not all divisible by p.

   (c) (*) Prove that $x^2 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$ as follows. Suppose $n^2 + k^4 = m^4$ is a solution with $m > 0$ minimal among all solutions. Show that there exists a solution with m smaller using Exercise 1 (consider two cases as below). This is called Fermat's "method of infinite descent."

      i. **Case one:** $m^2 = x^2 + y^2, n = 2xy, k^2 = x^2 - y^2$. [Hint: Consider m^2k^2, which should make the solution clear in this case.]

ii. **Case two:** $m^2 = x^2 + y^2, n = x^2 - y^2, k^2 = 2xy$. [Hint: Since $2xy$ is a perfect square, we have $x = 2u^2$ and $y = v^2$ (the other way around is similar). From the Pythagorean triple $m^2 = x^2 + y^2$, we have $x = 2rs$ and $y = r^2 - s^2$, and $m = r^2 + s^2$. Since $2u^2 = 2rs$, we have $r = g^2$ and $s = h^2$. Substituting these, along with $y = v^2$, into $y = r^2 - s^2$ gives $v^2 = g^4 - h^4$, hence $v^2 + h^4 = g^4$, with $g < m$.]

3. (*) Prove that 1 is not a congruent number by showing that the elliptic curve $y^2 = x^3 - x$ has no rational solutions except $(0, \pm 1)$ and $(0, 0)$, as follows:

   (a) Write $y = \frac{p}{q}$ and $x = \frac{r}{s}$, where p, q, r, s are all positive integers and $\gcd(p, q) = \gcd(r, s) = 1$. Prove that $s \mid q$, so $q = sk$ for some $k \in \mathbf{Z}$.

   (b) Prove that $s = k^2$ by substituting $y = p/(sk), x = r/s$ into $y^2 = x^3 - x$ and putting both sides of the equation in lowest terms. Substitute $s - k^2$ to see that $p^2 = r^3 - rk^4$.

   (c) Prove that r is a perfect square by supposing that there is a prime ℓ such that $\text{ord}_\ell(r)$ is odd (i.e., the power of ℓ in the factorization of r is odd), and analyzing ord_ℓ of both sides of $p^2 = r^3 - rk^4$.

   (d) Write $r = m^2$, and substitute to see that $p^2 = m^6 - m^2k^4$. Prove that $m \mid p$.

   (e) Divide through by m^2 and deduce a contradiction to Exercise 2.