MAT 373 Homework 9

Justyce Countryman

March 25, 2024

Problem 1: If p is a prime, prove that for any integer a:

$$p \mid a^p + (p-1)!a \text{ and } p \mid (p-1)!a^p + a$$

Hint: By Wilson's Theorem, $a^p + (p-1)!a \equiv a^p - a \pmod{p}$.

Proof. Suppose p is a prime and a is any integer. With the usage of Fermat's Little Theorem, we are able to mention that $a^p \equiv a \pmod{p}$, and by Wilson's Theorem, we can also say that $(p-1)! \equiv -1 \pmod{p}$. Additionally, by manipulating Wilson's Theorem, we can state that $a^p + (p-1)!a \equiv a^p - a \pmod{p}$. All of this information tells us the following:

$$p \mid a^p - a$$

$$p \mid (p-1)! + 1$$

$$p \mid a^p + (p-1)!a - a^p + a$$

We know that p also divides any linear combination of these statements and a^p is an integer since a is any integer, p is a prime, and thus also an integer, and the exponentiation of two integers yields another integer, so we can say:

$$p \mid 1[a^p - a] + 1[a^p + (p-1)!a - a^p + a]$$

which simplifies to:

$$p \mid a^p - a + a^p + (p-1)!a - a^p + a = a^p + (p-1)!a$$

$$p \mid a^p + (p-1)!a$$

and:

$$p \mid a^p[(p-1)! + 1] - 1[a^p - a]$$

which simplifies to:

$$p \mid a^p(p-1)! + a^p - a^p + a$$

$$p \mid (p-1)!a^p + a$$

As a result, we now know that $p \mid a^p + (p-1)!a$ and $p \mid (p-1)!a^p + a$.

□

Problem 2: Find all Primitive Pythagorean Triplets (PPT) where one of the sides is 108.

We know that (x, y, z) forms a PPT if and only if there are integers s, t such that one of them is even and the other is odd with $\gcd(s, t) = 1$ and $x = 2st$, $y = s^2 - t^2$, and $z = s^2 + t^2$.

Additionally, we know $x = 2st$ is an even integer because the product of an even and odd yields an even, and multiplying that value by 2 still gives an even integer. We also see that y and z must be odd integers since $x^2 + y^2 = z^2$. Thus, since we have 108, an even, as one of the sides, we now know $x = 2st = 108$, which tells us that $st = 54$.

Looking at all positive combinations of s and t (since negative combinations would be redundant) that when multiplied together make 54, we can notice the following:

$s = 54, t = 1$, s is even, t is odd, and $\gcd(54,\ 1) = 1$
$s = 27, t = 2$, s is odd, t is even, and $\gcd(27,\ 2) = 1$
$s = 18, t = 3$, s is even, t is odd, but $\gcd(54,\ 1) = 3$
$s = 9, t = 6$, s is odd, t is even, but $\gcd(27,\ 2) = 3$

As a result, the possible combinations of (s, t) that will let (x, y, z) form unique PPTs are $(54, 1)$ and $(27, 2)$.

Applying the formulas for x, y, and z for both (s, t) combinations gives us:

$x = 2(54)(1) = 108$
$y = (54)^2 - (1)^2 = 2915$
$z = (54)^2 + (1)^2 = 2917$
and:
$x = 2(27)(2) = 108$
$y = (27)^2 - (2)^2 = 725$
$z = (27)^2 + (2)^2 = 733$

Therefore, all PPTs where one of the sides is 108 include $(108, 2915, 2917)$ and $(108, 725, 733)$.

Problem 3: Show that no PPT has 2003 as a "hypotenuse" ($z \neq 2003$)

Proof. For the purposes of contradiction, let's suppose that there is a PPT that has 2003 as a "hypotenuse". This tells us that $(x, y, 2003)$, for some positive integers x, y, forms a PPT and $x^2 + y^2 = 2003^2$ and $\gcd(x, y) = \gcd(y, 2003) = \gcd(x, 2003) = 1$. However, 2003 is a prime, so its only divisors are 1 and itself. Additionally, since we have a PPT, we also have $x = 2st, y = s^2 - y^2$, and $z = s^2 + t^2$ for some integers s, t, where one is even and the other is odd.

In terms of this problem, we can redefine $z = s^2 + t^2$ as:

$$2003 = s^2 + t^2$$

$$s^2 = 2003 - t^2$$

$$s = \pm\sqrt{2003 - t^2}$$

This creates a contradiction because 2003 is a prime, which tells us that 2003 is not a perfect square, which means that we cannot get an integer s from any integer t. As a result, it is impossible to have 2003 as a "hypotenuse." □

Problem 4: Let (x, y, z) be a PPT. Prove $5|xyz$. Hint: Use Fermat's Little Theorem

Proof. Suppose (x, y, z) is a PPT. We then know that $\gcd(x, y) = \gcd(y, z) = \gcd(x, z) = 1$ and $x^2 + y^2 = z^2$.

We can see that at most one of x, y, or z can be divisible by 5 because any more would cause x, y, and z to no longer be pairwise relatively prime, which would not follow the definition of PPTs.

Additionally, we know that for any integer a, if a^2 is divisible by 5^2, a^2 and a are divisible by 5. This idea tells us that if x, y, and z are not divisible by 5, then x^2, y^2, and z^2 are all not divisible by $5^2 = 25$ and since $5|25$, x^2, y^2, and z^2 would also not be divisible by 5.
If we look at all remainders for any square number (mod 5), we see the following:

$$a^2 \equiv 0 \pmod 5 \rightarrow (0)^2 = 0$$

$$a^2 \equiv 1 \pmod 5 \rightarrow (1)^2 = 1$$

$$a^2 \equiv 2 \pmod 5 \rightarrow (2)^2 = 4$$

$$a^2 \equiv 3 \pmod 5 \rightarrow (3)^2 - 5(1) = 4$$

$$a^2 \equiv 4 \pmod 5 \rightarrow (4)^2 - 5(3) = 1$$

We see that the only possible residues (or remainders) of any square number (mod 5) are 0, 1, and 4.

In order for $x^2 + y^2 = z^2$ to hold and to satisfy the definition of PPT, we need to have the remainder of either x^2 or y^2 as 1 and the other as 4. This case would ensure that z is divisible by 5, but this equation can be manipulated to make either x, y, or z divisible by 5 through the consideration of the equations $x^2 = z^2 - y^2$ and $y^2 = z^2 - x^2$, and noticing the following remainders for any negative square number (mod 5):

$$-a^2 \equiv 0 \pmod 5 \implies a^2 \equiv 0 \pmod 5 \rightarrow (0)^2 = 0$$

$$-a^2 \equiv 1 \pmod 5 \implies a^2 \equiv -1 \pmod 5 \implies a^2 \equiv 4 \pmod 5 \rightarrow (4)^2 - (5)3 = 1$$

$$-a^2 \equiv 2 \pmod 5 \implies a^2 \equiv -2 \pmod 5 \implies a^2 \equiv 3 \pmod 5 \rightarrow (3)^2 - 5(1) = 4$$

$$-a^2 \equiv 3 \pmod 5 \implies a^2 \equiv -3 \pmod 5 \implies a^2 \equiv 2 \pmod 5 \rightarrow (2)^2 = 4$$

$$-a^2 \equiv 4 \pmod 5 \implies a^2 \equiv -4 \pmod 5 \implies a^2 \equiv 1 \pmod 5 \rightarrow (1)^2 = 1$$

We now see that in order for either $x^2 = z^2 - y^2$ or $y^2 = z^2 - x^2$ to follow and for the definition of PPT to still be satisfied, their respective right-hand sides must consist of a remainder of 1 and a remainder of 4 so that either x or y is divisible by 5. As a result, we now know that at least one of x, y, z must be divisible by 5. However, recall that we can only have at most one of x, y, or z divisible by 5. Therefore, exactly one of x, y, or z is divisible by 5.

Now let's consider all cases of either x, y, or z being divisible by 5:

Case 1: x is divisible by 5:

We know we have $x \equiv 0 \pmod 5$, but we can also utilize Fermat's Little Theorem (FLT) to also give us $y^4 \equiv 1 \pmod 5$ and $z^4 \equiv 1 \pmod 5$. Because all of these congruence contain the same modulo, we can say:

$$x \cdot y^4 \cdot z^4 \equiv 0 \cdot 1 \cdot 1 \pmod 5$$

$$xy^4z^4 \equiv 0 \pmod 5$$

$$(y^3z^3)xyz \equiv 0 \pmod 5$$

So $5|(y^3z^3)xyz$ and we already know $5 \nmid y$ and $5 \nmid z$, so since $\gcd(5,\ y) = \gcd(5,\ z) = 1$, so we also know $\gcd(5,\ y^3) = \gcd(5,\ z^3) = \gcd(5,\ y^3z^3) = 1$. With this information, now we know $5|xyz$.

Case 2: y is divisible by 5:

Applying the same logic as case 1 along with FLT tells us that we have $y \equiv 0 \pmod 5$, $x^4 \equiv 1 \pmod 5$ and $z^4 \equiv 1 \pmod 5$. Which allows to see that $x^4yz^4 \equiv 1 \pmod 5$ and $(x^3z^3)xyz \equiv 0 \pmod 5$. Since $5 \nmid x$ and $5 \nmid z$, $\gcd(5,\ x^3) = \gcd(5,\ z^3) = \gcd(5,\ x^3z^3) = 1$. With this information, we get $5|xyz$ again.

Case 3: z is divisible by 5:

Yet again using the same logic as case 1 along with FLT tells us that we have $z \equiv 0$ (mod 5), $x^4 \equiv 1 \pmod 5$ and $y^4 \equiv 1 \pmod 5$. We see $x^4y^4z \equiv 1 \pmod 5$ and $(x^3y^3)xyz \equiv 0$ (mod 5). Since $5 \nmid x$ and $5 \nmid y$, $\gcd(5,\ x^3) = \gcd(5,\ y^3) = \gcd(5,\ x^3y^3) = 1$, and thus we still get $5|xyz$.

Now that all possible cases have been considered and validated, we now know that if (x, y, z) is a PPT, then $5|xyz$. $\square$