MAT 373 Homework 11

Justyce Countryman

April 10, 2024

Problem 1: Let p be a prime which is the sum of two square, say $p = a^2 + b^2$, prove $\gcd(a, b) = 1$.

Proof. Suppose for the sake of contradiction that a and b are not relatively prime, meaning $\gcd(a, b) = d \neq 1$ for some positive integer d. This information allows us to say that there exists integers x, y such that $a = dx$ and $b = dy$. Let's plug in this information into $p = a^2 + b^2$:

$$p = (dx)^2 + (dy)^2 = d^2x^2 + d^2y^2$$

$$p = d^2(x^2 + y^2)$$

The above equation tells us that p is divisible by d^2. Since p is a prime, this is only possible if $d^2 = 1$ or $d^2 = p$.

We can say $d > 1$ since d is a positive integer and we assumed it cannot be 1, so $d^2 \neq 1$.

Additionally, if we suppose $d^2 = p$, then $d = \pm\sqrt{p}$. d has to be a positive integer, so that leaves us with $d = \sqrt{p}$. However, the square root of any prime is irrational, so d will never be a positive integer, which creates a contradiction.

Thus if p is a prime which is the sum of two squares ($p = a^2 + b^2$), then $\gcd(a, b) = 1$.

□

Problem 2: Find all PPTs which have a side of length p, where p is a prime of the form $4k + 3$, justify your answer.

Since we are dealing with PPTs, we already know:

$$x = 2st$$

$$y = s^2 - t^2 = (s - t)(s + t)$$

$$z = s^2 + t^2$$

such that s, t are integers with one of s, t being even and the other odd.

We know the following from class:

$$4k + 3 \equiv 3 \pmod 4 \tag{1}$$

$$s^2 + t^2 \not\equiv 3 \pmod 4 \tag{2}$$

such that $k \in \mathbb{Z}$, but we are only interested in the values of k that make $4k + 3$ a prime.

We know x is even, y, z are odd, and all primes of the form $4k + 3$ are odd, so no PPT can have $x = 4k + 3$. Also, equation (2) tells us that no PPT can have $z = 4k + 3$. So $y = 4k + 3 = (s - t)(s + t)$.

Also from class, we found out that $s - t$ and $s + t$ are relatively prime. This information simplifies our problem down to the following system since $4k + 3$ is a prime:

$$s + t = 4k + 3 \tag{3}$$

$$s - t = 1 \tag{4}$$

Adding (3) and (4) together helps us solve for s:

$$2s = 4k + 4$$

$$s = 2k + 2$$

In order to satisfy the system previously described, $t = 2k + 1$.
Finally, we can solve for x, y, z:

$$x = 2(2k + 2)(2k + 1)$$

$$y = (2k + 2)^2 - (2k + 1)^2$$

$$z = (2k + 2)^2 + (2k + 1)^2$$

As a result, all PPTs which have a side of length p, where p is a prime of the form $4k + 3$, are of the form $(2(2k + 2)(2k + 1), (2k + 2)^2 - (2k + 1)^2, (2k + 2)^2 + (2k + 1)^2)$.

Problem 3: Determine exactly how many PPTs there are with a side of length p where p is a prime of the form $4k + 1$.

Since we are talking about PPTs, we can consider:

$$x = 2st$$

$$y = s^2 - t^2$$

$$z = s^2 + t^2$$

such that s, t are integers with one of s, t being even and the other odd.

We know x is even, y, z are odd, and all primes of the form $4k + 1$, where k is some positive integer, are odd, so no PPT can have $x = 4k + 1$.

We also know that $4k + 1 \equiv 1 \pmod 4$ for all possible k. It is also possible for $s^2 + t^2 \equiv 1 \pmod 4$ since the remainder of any square number (mod 4) is either 0 or 1, so the possibility of $z = 4k + 1$ exists.

As a result, primes of the form $4k + 1$ can only be the y or z part of the PPT. This means that for every prime of the form $4k+1$, there are two unique PPTs that include that prime. From class, we also determined that there are infinite primes of the form $4k + 1$, so there must also be an infinite number of PPTs with a side containing a prime of the form $4k + 1$.

Problem 4: Find the next calendar year after this year which is, and which is not the sum of two squares.

Starting with 2025, let's find its canonical prime factorization form.

$$2025 = 5^1 \cdot 405$$

$$2025 = 5^1 \cdot 5^1 \cdot 81$$
$$2025 = 5^1 \cdot 5^1 \cdot 9 \cdot 9$$
$$2025 = 5^1 \cdot 5^1 \cdot 3^2 \cdot 3^2$$
$$2025 = 5^2 \cdot 3^4$$

Based on an theorem (not proven in class yet), we need to look at the primes in our prime factorization which are congruent to 3 (mod 4) and check if they have an even exponent. If this is true, then the positive integer being represented can be written as a sum of two squares, otherwise it is not possible.

In our prime factorization of 2025, we only have to check 3^4, which has an even exponent. Thus, we know that 2025 can be written as a sum of two squares.

Next, let's try 2026:

$$2026 = 2^1 \cdot 1013^1$$

Neither 2 nor 1013 is congruent to 3 (mod 4), so 2026 can also be written as a sum of two squares

Now let's look at 2027:

$$2027 = 2027^1$$

$2027 \equiv 3 \pmod 4$, so we have to check 2027^1, which has an odd exponent. This information tells us that 2027 cannot be written as a sum of two squares.

Therefore, the next calendar year after this year which is, and which is not, the sum of two squares are 2025 and 2027 respectively.