PMATH 340: Elementary Number Theory

Notes Taken By:
Evan Bernard

Class Taught By:
Professor Wentang Kuo

Winter 2020
University of Waterloo

Contents

Abstract

Number Theory is quite simply the study of integers. This course analyzes some interesting relationships between integers, and the implications of these relationships. You are expected to be familiar with what was taught in MATH 135, including but not limited to, *linear Diophantine equations, euclidean algorithm, congruence* and the *Chinese remainder theorem.*

Chapter 1

idk what to call this chapter yet

1.1 Integral Pythagorean Triplets

Question: Find all integral Pythagorean triples.

In other words, find all integer triples a, b, c, such that a, b, c satisfy the Pythagorean formula, $c^2 = a^2 + b^2$. We may assume that $a, b > 0$ since if $a = 0$ or $b = 0$ then the solutions are known.

Find all triplets a, b, c such that $a, b, c \in \mathbb{N}$ and $c^2 = a^2 + b^2$

Examples:

$$\begin{gathered}5^2 = 3^2 + 4^2\\ 13^2 = 5^2 + 12^2\\ 17^2 = 8^2 + 15^2\\ 25^2 = 7^2 + 24^2\end{gathered}$$

Note that, given a Pythagorean triple a, b, c, and an integer d, then da, db, dc form another Pythagorean triplet.

Definition 1.1.0.1
A Primitive Pythagorean triplet, or PPT, is a triple of natural numbers a, b, c so that $a, b, c \in \mathbb{N}$ and $gcd(a, b, c) = 1$ since otherwise, you can divide by a common factor and find a smaller triplet.

We can now rewrite the question into a simpler question, which reduces the question into the essential component of it: Find all primitive Pythagorean triples.

Proposition 1.1.0.1
c is odd.

Proof
Suppose c is even. Then $c = 2k$ for $k \in \mathbb{N}$
Case 1: both a and b are even.
Then $gcd(a, b, c) = 2 \neq 1$ thus a, b, c are not PPT
Case 2: both a and b are odd.
Then there exists $x, y \in \mathbb{Z}$ such that $a = 2x + 1$ and $b = 2y + 1$, and since $c^2 = a^2 + b^2$, we have that:

$$\begin{gathered} c^2 = (2x+1)^2 + (2y+1)^2 \\ 4z^2 = 4(x^2 + xy^2 + y) + 2 \\ 4(z^2 - x^2 - x - y^2 - y) = 2 \\ 2(z^2 - x^2 - x - y^2 - y) = 1 \end{gathered}$$

This is a contradiction, and thus, our first assumption is invalid. Therefore c must be an odd integer.

So far, we know that if a, b, c is a PPT, then c is odd and without loss of generality, we may assume that a is even and b is odd.

By rearranging the Pythagorean formula, we get:

$$a = \sqrt{(c-b)(c+b)}$$

Proposition 1.1.0.2
If a is odd, then $(c-b)(c+b)$ are squares.

Proof
Let p be a prime divisor of a. Then,

$$\begin{gathered} p^2 \mid a^2 \\ p^2 \mid (c+b)(c-b) \end{gathered}$$

Suppose p divides one of $(c+b)$ and $(c-b)$ but not both, then $(c+b)$ and $(c-b)$ are squares by the *Unique Factorization Theorem.*
Therefore it is enough to show that $gcd(c+b, c-b) = 1$.
Let $d = gcd(c+b, c-b)$, then we have the following:

$$\begin{aligned} d &\mid c+b \\ d &\mid c-b \\ \implies d &\mid (c+b)+(c-b) = 2c \\ \implies d &\mid (c+b)-(c-b) = 2b \end{aligned}$$

Proof (Cont.)
Thus, we have that,

$$d \mid gcd(2b, 2c)$$
$$d \mid 2gcd(b, c)$$
$$d = 1 \text{ or } d = 2$$

Suppose $d = 2$, we know that,

$$d \mid (c-b) \text{ and } d \mid (c-b)(c+b) = a^2$$
$$\implies 2 \mid a^2$$
$$\implies 2 \mid a$$
$$\implies \text{ a is even}$$

But we assumed that a was odd, so d must be equal to 1. Since $d = gcd(c+b, c-b)$ and $d = 1$, $(c-b)$ and $(c+b)$ are coprime, and so are squares by the*Unique Factorization Theorem.*

Since we have that $(c-b)$ and $(c+b)$ are coprime and squares, we also have that $\exists s, t \in \mathbb{N}$ where $gcd(s, t) = 1$ and $c - b = t^2$ and $c + b = s^2$

$$\implies c = \frac{s^2 + t^2}{2}$$
$$b = \frac{s^2 - t^2}{2}$$
$$a^2 = c^2 - b^2 = s^2 \cdot t^2$$
$$\implies a = s \cdot t$$

Theorem 1.1.0.3 (Pythagorean Triple Theorem)
Every primitive Pythagorean triple (a, b, c), where a, c are odd, b is even, can be obtained by $a = s \cdot t$, $b = \dfrac{s^2 - t^2}{2}$, $c = \dfrac{s^2 + t^2}{2}$, where $s, t \in \mathbb{N}, s > t$, and s, t are odd and coprime $(gcd(s, t) = 1)$.

Example: $s = 3$**,** $t = 1$

$$b = \frac{3^2 - 1^2}{2} = 4$$
$$c = \frac{3^2 + 1^2}{2} = 5$$
$$a = 3 \cdot 1 = 3$$
$$\text{A } PPT \text{ is } (3, 4, 5)$$

It's Important to note that this does not guarantee the result to be a PPT for any s and t satisfying the conditions, however, every PPT will have an s and t decomposition.

1.2 Euler's Formula

Definition 1.2.0.1 (Congruence)
Let $a, b, m \in \mathbb{Z}, m \in \mathbb{N}$. We say that a is *congruent* to b modulo m, if $m \mid (b - a)$. We use the following notation:

$$a \equiv b \ (mod\ m)$$

Theorem 1.2.0.1
If $a, b, c \in \mathbb{Z}, m \in \mathbb{N}$ and $gcd(c, m) = 1$, then,

$$a \cdot c \equiv b \cdot c \ (mod\ m)$$
$$\implies a \equiv b \ (mod\ m)$$

Question: Given $a \in \mathbb{Z}, m \in \mathbb{N}$, find an integer $\gamma \in \mathbb{N}$, such that $a^\gamma \equiv 1 \ (mod\ m)$

Theorem 1.2.0.2 (Fermat's Little Theorem *(FlT)*)
$\forall a, p \in \mathbb{Z}$, prime p, $gcd(a, p) = 1$ then,

$$a^{p-1} \equiv 1 \ (mod\ p)$$

So part of the question is trivial with FlT, namely, when m is prime then we can simply let γ be $m - 1$ and we've found a solution to the problem.

Finding an integer γ satisfying the equation for any integer m however, is much more difficult.

Definition 1.2.0.2 (Reduced Residue Class Set)
Let $m \in \mathbb{N}$, we define the reduced residue class set as:

$$R_m = \{b \in \mathbb{Z}\colon\ 1 \leq b \leq m,\ gcd(b, m) = 1\}$$

Example:

The residue class set R_p for a prime number p is the following:

$$R_p = \{1, 2, 3, 4, ..., p - 1\}$$

Recall that the key step for proving FlT is to see that:

$$\{1, 2, 3, ..., p - 1\} \equiv \{a, 2a, 3a, ...(p - 1)a\} \ (mod\ p) \text{ for } p \nmid a.$$

Example: $a = 3$**,** $p = 5$

$$R_5 = \{1, 2, 3, 4\}$$
abusing notation,
$$3 \cdot R_5 = \{3, 6, 9, 12\}$$

and notice that when we take the mod 5 of each element, we get,
$3 \cdot R_5 \ mod\ 5 \equiv \{3, 1, 4, 2\}$
which is exactly R_5 in a different order

Definition 1.2.0.3 (Euler's Phi (Totient) Function)
Let $m \in \mathbb{N}$. Define $\phi(m) :=$ # elements in R_m

$$\phi(m) = \text{\# elements in } \{b \in \mathbb{Z}\text{: } 1 \leq b \leq m,\ gcd(b, m) = 1\}$$

Example 1: $\phi(p) = p - 1$
Since $R_p = \{1, 2, 3, ...p - 1\}$, there are $p - 1$ elements in R_p

Example 2: $\phi(p^k) = p^k - p^{k-1}$
Constructing R_{p^k}, it's clear that there would be p^k elements in the set if we were to include the values of b which don't satisfy the condition that $gcd(b, p^k) = 1$. The question now is how many values of b are there which don't satisfy the condition? The only time $gcd(b, p^k) \neq 1$ is when $b \mid p^k$. Since p is prime, this is also when b is a multiple of p. There are exactly p^{k-1} multiples of p, and so the value of Euler's Phi Function is $p^k - p^{k-1}$.

Theorem 1.2.0.3 (Euler's Formula)
Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $gcd(a, m) = 1$. Then,

$$a^{\phi(m)} \equiv 1\ (mod\ m).$$

Remark: By Euler's formula, we can see that when $m = p$ is prime then $a^{p-1} \equiv 1\ (mod\ p)$, so FlT is just a special case of Euler's formula.

Lemma 1.2.0.4
$R_m \equiv a \cdot R_m\ (mod\ m)$

Proof (Lemma 1.2.0.4)
We will do this proof on friday, for now we will assume it's true to prove Euler's formula.

Proof (Euler's Formula)
By Lemma 1.2.0.4, we have that,

$$R_m \equiv a \cdot R_m \ (mod\ m)$$

Suppose we have that,

$$R_m = \{b \in \mathbb{Z}\colon\ 1 \leq b \leq m,\ gcd(b, m) = 1\}$$
$$a \cdot R_m = \{a \cdot b \in \mathbb{Z}\colon\ 1 \leq a \cdot b \leq m,\ gcd(b, m) = 1\}$$

Now consider what we get if we take the product of all terms in these sets. Notice that,

$$\prod_{b \in R_m} b \equiv \prod_{b \in R_m} a \cdot b \mod m$$

Thus we have that,

$$\prod_{b \in R_m} b \equiv a^{\phi(m)} \cdot \prod_{b \in R_m} b \mod m$$

and since $\forall\ b \in R_m$, $gcd(b, m) = 1$, we're able to cancel out the cartesian products and are left with the following:

$$1 \equiv a^{\phi(m)} \ (mod\ m)$$