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 simply the study of integers. This course analyzes some interesting relationships between integers, and the implications of these relationships. The course can be thought of as being split into three main sections, the first being solving $x^2 \equiv a \ (mod\ p)$, the second $x^2 + y^2 = n$, and finally, $x^2 - Dy^2 = 1$. 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

Pythagorean Triplets

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:

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

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 $c^2 = a^2 + b^2$ 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
If (a, b, c) form a PPT so that $c^2 = a^2 + b^2$, then 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:

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

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 $(c - b)$ and $(c + b)$ 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.

Chapter 2

Euler's Formula

2.1 Fermat's Little Theorem

Definition 2.1.0.1 (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 2.1.0.1
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 2.1.0.2 (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 2.1.0.2 (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: $a = 3$**,** $p = 5$

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

2.2 Euler's Totient Function

Definition 2.2.0.1 (Euler's Phi/Totient Function)
Let $m \in \mathbb{N}$. Define $\phi(m) := \#$ elements in R_m
$$\phi(m) = \# \text{ elements in } \{b \in \mathbb{Z}\colon\ 1 \leq b \leq m,\ gcd(b, m) = 1\}$$

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 2.2.0.1 (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 2.2.0.2
If $gcd(a, m) = 1$, then the following sets are congruent in $mod\ m$

$$a \cdot R_m = ab_1, ab_2, ..., ab_{\phi(m)}$$
$$R_m = b_1, b_2, ..., b_{\phi(m)}$$

In other words, $R_m \equiv a \cdot R_m\ (mod\ m)$

Proof (Lemma 1.2.0.4)
It suffices to prove that any two numbers ab_j, ab_j are congruent to m if and only iff $i = j$, since this will show that $ab_1, ..., ab_{\phi(m)}$ all have a different module m.

Suppose $ab_i = ab_j\ (mod\ m)$. Since $gcd(a, m) = 1$, we can cancel out a, so $b_i \equiv b_j\ (mod\ m)$. But since $1 \leq b_i, b_j \leq m$, this implies that $i = j$.

Thus, we have that $R_m \equiv a \cdot R_m\ (mod\ m)$. ■

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:

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

■

Example: Compute the remainder of 5^{10000} divided by 9

$gcd(5, 9) = 1$, so we use Euler's formula.
Notice that $\phi(9) = 6$
So, by Euler, $5^6 \equiv 1\ (mod\ 9)$

$$\text{Notice that } 5^{10000} = (5^6)^{1666} \cdot 5^4$$
$$5^{10000} \equiv 1^{1666} \cdot 625 \ (mod\ 9)$$
$$5^{10000} \equiv 4 \ (mod\ 9)$$
$$\text{So the remainder is 4.}$$

To give some motivation for the next theorem, notice how in order to use Euler's formula, we need to determine $\phi(m)$, which of course becomes very difficult when m gets large. So we need a trick to determining $\phi(m)$ for large m.

Theorem 2.2.0.3 (Phi Function Theorem)
If $m, n \in \mathbb{Z}$ and $gcd(m, n) = 1$, then we have that $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

Using this theorem in conjunction with what we know about $\phi(p)$ and $\phi(p^k)$ for prime numbers p, we can calculate $\phi(m)$ for large m values much faster by first putting m in its prime factorized form, and then calculating ϕ for each base number in m, and then multiplying the values together.

Example: Compute $\phi(1000)$

$$\begin{aligned}\phi(1000) &= \phi(2^3 \cdot 5^3)\\ &= \phi(2^3) \cdot \phi(5^3)\\ &= (2^3 - 2^2) \cdot (5^3 - 5^2)\\ &= 400\end{aligned}$$

Proof (Phi Function Theorem)
We need to show that $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ when $n, m \in \mathbb{Z}$ and $gcd(m, n) = 1$. Recall that $\phi(m)$ is just the number of elements in the reduced residue set R_m. The proof is easier if we compare R_{mn} to $R_m \times R_n$.

$$R_{mn} = \{b \in \mathbb{Z} : 1 \leq b \leq m \cdot n,\ gcd(b, m \cdot n) = 1\}$$
$$R_m = \{c \in \mathbb{Z} : 1 \leq c \leq m,\ gcd(c, m) = 1\}$$
$$R_n = \{d \in \mathbb{Z} : 1 \leq d \leq n,\ gcd(d, n) = 1\}$$
$$R_m \times R_n = \{(c, d) : c, d \in \mathbb{Z},\ 1 \leq c \leq m,\ 1 \leq d \leq n,\ gcd(c, m) = 1,\ gcd(d, n) = 1\}$$

We need to show that the size of R_{mn} is equal to the size of $R_m \times R_n$. If we can construct a bijection between these two sets, then that would imply that they are of equal size as required.

Define a map:

$$f : R_{mn} \to R_m \times R_n$$
$$b \mapsto (c, d)$$
$$c \equiv b \ (mod\ m)$$
$$d \equiv b \ (mod\ n)$$

Proof (Phi Function Theorem cont.)
Since b is coprime to $m \cdot n$, b is coprime to both m and n, thus the mapping is well defined. The bijection is followed by the *Chinese Remainder Theorem (CRT)*.
Since CRT says that any

$$\begin{cases} x \equiv c \ (mod\ m) \\ x \equiv d \ (mod\ n) \end{cases}$$

has a *unique* solution $x \equiv x_0 \ (mod\ m \cdot n)$, then,

$$\begin{cases} x_0 \equiv c \ (mod\ m) \\ x_0 \equiv d \ (mod\ n) \end{cases}$$

So a bijection between the two sets exists, and thus we have the they are equal in size, as required. ■

Corollary 2.2.0.3.1

$$\phi(m) = m \cdot \prod_{i=1}^{t} (1 - \frac{1}{p_i})$$

Example: Compute $\phi(1000)$

$$\begin{aligned} 1000 &= 2^3 \cdot 5^3 \\ \phi(1000) &= 1000(1 - \frac{1}{2})(1 - \frac{1}{5}) \\ &= 400 \end{aligned}$$

Proof (Corollary)
This result is found by dividing by the common factor of p^k for each base number in the prime factorized form of m, since

$$\phi(m) = \prod_{i=1}^{t} (p^{k_i} - p^{k_i - 1})$$

Where i is the index of the current prime number in the prime factorized form of m. Simply rearranging this formula will give you the result of the corollary. ■

Chapter 3

Congruence Relations

3.1 Successive Squaring algorithm

Question: Compute the remainder r of when 9^{53} is divided by 67. In other words, solve for r in $9^{53} \equiv r$ (mod 67).

Motivation: Using theorems we know, such as the *congruence power theorem* from MATH135, we are required to use 53 as an exponent, which is far too large for us to compute. Thus, a better method is needed for computing these remainder problems for large exponents.

Theorem 3.1.0.1 (Method of Successive Squaring To Compute a^k mod m)
Step 1: Write k as a sum of powers of 2
Step 2: Make a table of the powers of a modulo m using successive squaring
Then,

$$a^k \equiv \prod_{i=1}^{t} (A_i)^{u_i} \mod m$$

Now that we have the resources to answer the question, lets go through the question.

Question: Compute the remainder r of when 9^{53} is divided by 67. In other words, solve for r in $9^{53} \equiv r$ (mod 67).

Answer
Step 1: (Write the exponent as a sum of powers of 2)

$$53 = 2^5 + 21$$
$$53 = 2^5 + 2^4 + 2^2 + 2^0$$

The largest exponent is 5 in the rewritten number, and so for the next step, we will go up to $9^{2^5} = 9^{32}$

Step 2: (Create a table of the powers of 9 modulo 67)

$$\begin{array}{rcrcrl} 9^1 \equiv & 9 & & & \equiv 9 (mod\ 67) \\ 9^2 \equiv & 81 & & & \equiv 14 (mod\ 67) \\ 9^4 \equiv & (14^2) \equiv & 196 & & \equiv 62 (mod\ 67) \\ 9^8 \equiv & (62^2) \equiv & 3844 & & \equiv 25 (mod\ 67) \\ 9^{16} \equiv & (25^2) \equiv & 625 & & \equiv 22 (mod\ 67) \\ 9^{32} \equiv & (22^2) \equiv & 484 & & \equiv 15 (mod\ 67) \end{array}$$

Notice that,

$$9^{53} \equiv 9^{32} \cdot 9^{16} \cdot 9^4 \cdot 9^1 \ (mod\ 67)$$
$$9^{53} \equiv 15 \cdot 22 \cdot 62 \cdot 9 \ (mod\ 67)$$
$$9^{53} \equiv 24 \ (mod\ 67)$$

Thus we have that the remainder when 9^{53} is divided by 67, is 24. ■

3.2 Bases in Congruence Relations

Question: Let $k, m \in \mathbb{N}$, $b \in \mathbb{Z}$. Solve the congruence relation for x:
$$x^k \equiv b \ (mod\ m)$$
Note that so far we know how to solve for k if we are given x, b and m, but now we are looking to solve for x when given k, b and m.

We can very easily solve it if $k = 1$, so lets suppose $k > 1$.

Theorem 3.2.0.1 (Solving For x in Congruence Relations)
Let $b, k, m \in \mathbb{Z}$, $k \geq 1$, $m \geq 1$ such that we have that $gcd(b, m) = 1$ and $gcd(k, \phi(m)) = 1$. Then, the following steps will give a solution to
$$x^k \equiv b \ (mod\ m)$$
Step 1: Compute $\phi(m)$

Step 2: Find positive integers $u, v \in \mathbb{N}$ that satisfy $k \cdot u - \phi(m) \cdot v = 1$. Note: this step is from the linear diophantine equation theorem, which states that $a \cdot x + b \cdot y = c$ has a solution if $gcd(a, b) \mid c$. We can find solutions to this using the *Euclidean Algorithm*

Step 3: $x = b^u \ (mod\ m)$ is a solution to the relation

Proof
It's enough to show that $x = b^u$ is a solution.

$$(b^u)^k = b^{ku} = b^{1+\phi(m)v} = (b^{\phi(m)})^v b$$

By Euler's formula, $b^{\phi(m)} \equiv 1 \ (mod\ m)$, so,

$$(b^u)^k \equiv 1^v b \equiv b \ (mod\ m)$$

So, $x = b^u$ is a solution to the equation. ■

Remark: This theorem gives us a way to find the k^{th} root of b modulus m.

Example: Solve $x^{25} \equiv 7 \ (mod\ 135)$.

Answer
Notice that $gcd(7, 135) = 1$ and $gcd(25, \phi(135)) = 1$
The conditions for our theorem are met, so we may use it.

We have the following linear diophantine equation:

$$25 \cdot u + 72 \cdot v = 1$$

Solved by $E.Z.A$, gives $u = 49, v = 17$.

By our theorem, we have that $x = 7^{49}$ is a solution. We can perform 7^{49} $(mod\ 135)$ to find a smaller solution to our equation using successive squaring. Since an example of successive squaring is given on the previous page, this will be skipped. The answer after successive squaring is 52 (this is different than the answer given in class (88), but this is the correct answer), and so we know that $52^{25} \equiv 7 \ (mod\ 135)$, as required.

Example: Solve $x^4 \equiv 7 \ (mod\ 15)$

Answer
Notice that $gcd(7, 15) = 1$ and $gcd(4, \phi(15)) = 4 \neq 1$, so we cannot use our theorem.

We can, however, use the *Splitting Module Theorem* from MATH 135.
By SMT, $x^4 \equiv 7 \ (mod\ 15)$ if and only if $x^4 \equiv 7 \ (mod\ 5)$ and $x^4 \equiv 7 \ (mod\ 3)$.

Consider $x^4 \equiv 7 \ (mod\ 5)$.
Notice that if x is a solution, it must be coprime to 5, since $gcd(5, 7) = 1$. So, by FlT, we have that $x^4 \equiv 1 \ (mod\ 5)$, however, $7 \equiv 2 \ (mod\ 5)$, which is a contradiction, and so $x^4 \equiv 7$ $(mod\ 5)$ has no solution.
Thus, $x^4 \equiv 7 \ (mod\ 15)$ has no solution by SMT.

3.3 Sums of Divisors with Phi

Question: Let $n \in \mathbb{N}$, and $d_1, d_2, ..., d_k$ be all positive divisors of n. What is the sum of $\phi(d_1) + \phi(d_2) + ... + \phi(d_k)$?

Answer
The sum is equal to n. This will be proven as a theorem, but for now lets consider the summation when n is prime.

Let $n = p$, where p is prime.
$d_1 = 1$, $d_2 = p$ are the only divisors by the properties of primes. Thus we have,

$$\phi(1) + \phi(p) = 1 + p - 1 = p = n$$

Let $n = p^k$, where p is prime.
$d_1 = 1$, $d_2 = p$, $d_3 = p^2$, ..., $d_k = p^k$ are the only divisors of n.

$$\phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^k)$$
$$= 1 + (p-1) + (p^2 - p) + ... + \phi(p^k - p^{k-1})$$
Notice the cancellation,
$$= p^k = n$$

We've shown that when n is prime or has a prime base, the sum of Euler's phi function of the divisors of n is equal to n. This will be helpful since every integer can be expressed as a product of primes.

Theorem 3.3.0.1 (Euler's Phi Function Summation Formula)
For $n \in \mathbb{N}$ and $d \geq 1$,

$$\sum_{d|n} \phi(d) = n$$

Proof
Let $F = \sum_{d|n} \phi(d)$.

If we can show for $m, n \in \mathbb{N}$, if $gcd(m, n) = 1$, then $F(m \cdot n) = F(m) \cdot F(n)$, then we are done, since we can express any number as a product of primes, and we know that $F(p^K) = p^k$ for any prime p.

Let $m = p_1^{d_1} p_2^{d_2} ... p_k^{d_k}$, and let $n = \gamma_1^{t_1} \gamma_2^{t_2} ... \gamma_j^{t_j}$
Notice how since $gcd(m, n) = 1$, all p_k are different from γ_j. By the *Divisors From Prime Factorization Theorem*, any divisor d of $m \cdot n$ has the form of a subset of the product of primes multiplied together, i.e, if we let $e = p_1^{\omega_1} p_2^{\omega_2} ... p_l^{\omega_l}$ and $f = \gamma_1^{i_1} \gamma_2^{i_2} ... \gamma_w^{i_w}$, where $e \mid m$ and $f \mid n$, then $d = e \cdot f$.

Thus, any divisor d of $m \cdot n$ is a product of e (a positive divisor of m) and f (a positive divisor of n), where $gcd(e, f) = 1$ since $gcd(m, n) = 1$.

Proof (cont.)
The converse of this is also true. If e is a positive divisor of m, and f is a positive divisor of n, then $e \cdot f$ is a positive divisor of $m \cdot n$, with $gcd(e, f) = 1$.

To sum up what we have so far, let $\{e_1, e_2, ..., e_s\}$ be the set of all positive divisors of m, and let $\{f_1, f_2, ..., f_u\}$ be the set of all positive divisors of n. Then, $\{e_i \cdot f_j : 1 \leq i \leq s, 1 \leq j \leq u\}$ is the set of all positive divisors of $m \cdot n$. Notice that all $gcd(e_i, f_j)$ are coprime by definition.

$$F(m \cdot n) = \sum_{i=1}^{s} \sum_{f=1}^{u} \phi(e_i \cdot f_j)$$

$$= \sum_{i=1}^{s} \sum_{f=1}^{u} \phi(e_i) \cdot \phi(f_j$$

$$= \sum_{i=1}^{s} \phi(e_i) \cdot \sum_{f=1}^{u} \phi(f_j)$$

$$= F(m) \cdot F(n)$$

■

3.4 Primitive Roots Modulo p

Question: Let $m \in \mathbb{N}$. For some $a \in Z$, where $gcd(a, m) = 1$, what is the smallest positive integer k such that $a^k \equiv 1 \ (mod\ m)$?

We know by Euler that $k = \phi(m)$ is a solution to the equation, so we can say that the smallest integer k always exists, and $k \leq \phi(m)$.

Definition 3.4.0.1 (Exponent of a modulo m)
Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$, where $gcd(a, m) = 1$. The smallest exponent e such that $a^e \equiv 1 \ (mod\ m)$ is called the exponent of a modulo m, and is denoted by $e_m(a)$. Note that $e_m(a) \leq \phi(m)$.

Example: Compute $e_7(5)$. i.e., find the smallest integer e such that $5^e \equiv 1 \ (mod\ 7)$.

Answer
First, compute $\phi(7) = 6$, so the possible values of $e_7(5)$ are between 1 and 6.

$$5^1 \equiv 5 \not\equiv 1 \ (mod\ 7)$$
$$5^2 \equiv 25 \equiv 4 \ (mod\ 7)$$
$$5^3 \equiv 4 \cdot 5 \equiv 6 \ (mod\ 7)$$
$$5^4 \equiv 6 \cdot 5 \equiv 2 \ (mod\ 7)$$
$$5^5 \equiv 2 \cdot 5 \equiv 3 \ (mod\ 7)$$
$$5^6 \equiv 3 \cdot 5 \equiv 1 \ (mod\ 7)$$

So, the smallest exponent e which solves the congruence relation $5^e \equiv 1 \ (mod\ 7)$ is the maximum value it could have been, i.e, equal to $\phi(7) = 6$.

To give some motivation for the next proposition, notice how long it would take to calculate $e_m(a)$ for large values of $\phi(m)$. Surely, not all positive integers between 1 and $\phi(m)$ are possible values for e, so let's try to reduce the values from this range even further.

Proposition 3.4.0.1 (Exponent Divisibility Property)
Let $a, m \in \mathbb{Z}$, with $gcd(a, m) = 1$, and suppose there is a solution to the equation $a^n \equiv 1 \ (mod\ m)$ for some $n \in \mathbb{N}$. Then, we have that

$$e_m(a) \mid n$$

In particular,

$$e_m(a) \mid \phi(m)$$

Remark: In our last example in which we calculated $e_7(5)$, we had to calculate the value of 5^n modulo 7 for all $1 \leq n \leq \phi(7)$. If we can prove this proposition, we would have only needed to calculate the value of 5^n modulo 7 for the divisors of $\phi(7)$, so 1,2 and 3.

Proof (Exponent Divisibility Property)
By definition, $a^{e_m(a)} \equiv 1 \ (mod\ \text{m})$. Let $d = gcd(e_m(a), n) = e_m(a)$, since $e_m(a)$ is primitive.

By the *Linear Diophantine Equation Theorem*, there exists two positive integers u, v such that $e_m(a) \cdot u - n \cdot v = d$. Then, $a^{e_m(a) \cdot u} = (a^{e_m(a)})^u \equiv 1^u \equiv 1 \ (mod\ \text{m})$

$$1 \equiv a^{e_m(a) \cdot u} = a^{n \cdot u + d} = (a^n)^u \cdot a^d \equiv 1^u \cdot a^d \equiv a^d \ (mod\ \text{m})$$

But, by definition, $d = e_m(a)$, and so we have $e_m(a) \mid n$ as required. ■

Definition 3.4.0.2 (Primitive Roots mod m)
Let $m \in \mathbb{Z}$ and let there exist a positive integer e_m such that, for all $a \in \mathbb{Z}$ where $gcd(a, m) = 1$, we have that $a^{e_m} \equiv 1 \ (mod\ m)$, and e_m is the smallest positive integer satisfying this property.

Then, a positive integer g such that $gcd(g, m) = 1$ is called the primitive root mod m if $e_m(g) = e_m$

In particular, if $m = p$ for a prime p, $e_p = p - 1$. A primitive root g of p satisfies $e_p(g) = p - 1$.

Theorem 3.4.0.2
For any prime p, there exists a primitive root modulo p. In other words, for any prime p, there exists $g \in \mathbb{Z}$ such that $e_p(g) = p - 1 = \phi(p)$.

Remark: The definition for primitive roots here is different than the one in the textbook, however, they are the same for primes, which is what we will be focusing on in this course.

We would like to prove this theorem, but we need to define a useful function and lemma first.

Definition 3.4.0.3
Let p be prime and n be a divisor of $\phi(p) = p - 1$. We define

$$\psi(n) := \#\{a : \ 1 \leq a < p, \ e_p(a) = n\}$$

In other words, $\psi(n)$ gives the number of values of $a < p$ which satisfies the equation $a^n \equiv 1 \ (mod\ p)$

Remark: The primitive root theorem is equivalent to $\psi(p-1) \geq 1$, so we will prove this instead.

Examples: Let $p = 7$

$$\psi(1) = \#\{1\} = 1 \text{ since } 1^1 \equiv 1 \ (mod\ 7) \text{ is the only solution under 7.}$$
$$\psi(2) = \#\{6\} = 1 \text{ since } 6^2 \equiv 1 \ (mod\ 7) \text{ is the only solution under 7.}$$
$$\psi(3) = \#\{2, 4\} = 2 \text{ since } 2^3 \equiv 1 \ (mod\ 7) \text{ and } 4^3 \equiv 1 \ (mod\ 7)$$

Notice that it seems to be true that $\phi(n) = \psi(n)$. We can easily verify for the examples we've done that this holds, but it's difficult to show it holds for all n, p. If it is true, then $\psi(p-1) = \phi(p-1) \geq 1$, proving the theorem is true. We need to introduce a theorem which will help us prove this.

Theorem 3.4.0.3 (Lagrange's Theorem)
Given a polynomial $f(x)$ of degree $n, n \in \mathbb{N}$, the number of solutions to the congruence relation $f(x) \equiv 0\ (mod\ p)$ for a prime p is at most n.

Proof
Let $x = a_1,\ 1 \leq a_1 < p$ be a solution to $f(x) \equiv 0\ (mod\ p)$. We will be referring to the following congruence relation often, and so let $\star$ represent $f(x) \equiv 0\ (mod\ p)$.

The factor theorem from MATH135 says that for any $c \in F$, we have
$$(x - c) \mid f(x) \iff f(c) = 0$$
Where F is a field. In our case, $F = \mathbb{Z}/p\mathbb{Z}$ for prime p, which is a field (this notation is the proper notation, it means the set of integers in modulo p).

So, since a_1 is a solution, we have that $(x - a_1) \mid f(x)$. If we repeat the process n times, we're left with the following
$$f(x) \equiv (x - a_1)(x - a_2)...(x - a_n)g_n(x)$$
Where $a_1, a_2, ..., a_n$ are solutions to $\star$. We need to show that there cannot be any more solutions, so lets assume we have another solution a^0 to $\star$. Then, we have
$$0 \equiv f(a^0) = (a^0 - a_1)(a^0 - a_2)...(a^0 - a_n)g_n(a^o)\ (mod\ p)$$
Since we are in the field $\mathbb{Z}/p\mathbb{Z}$, it is also a domain (if $ab = 0$ then $a = 0$ or $b = 0$). Thus, we have that at least one factor of $f(a^0)$ is equal to 0, but we defined a^0 to be a unique solution, so none of $(a^0 - a_n) = 0$. This means that $g_n(x) \equiv 0\ (mod\ p)$.

By the factor theorem,
$$(x - a^0) \mid g(a^0)$$
and also,
$$f(x) \equiv (x - a_1)(x - a_2)...(x - a_n)(x - a^0)g_n(x)\ (mod\ p)$$

This has degree $n+1$, contradicting our assumption from the theorem that the degree of the polynomial was n. Thus, the number of solutions to $f(x) \equiv 0\ (mod\ p)$ is at most n.

Example: Consider $x^5 \equiv 1\ (mod\ 11)$
The solutions are, $x = 1, 3, 4, 5, 9$, so there are 5 solutions, and a degree of 5.

Lemma 3.4.0.4
Let p be a prime number. If $n \mid (p-1)$, then the congruence $x^n - 1 \equiv 0\ (mod\ p)$ has exactly n solutions.

Proof
Let $p-1=nk$.
We have that

$$x^{p-1}-1=x^{nk}-1=(x^n)^k-1$$
$$=(x^n-1)((x^n)^{k-1}+(x^n)^{k-2}+...+(x^n)^2+(x^n)^1+1)$$

By FlT, the congruence $x^{p-1}-1\equiv 0\ (mod\ p)$ has $p-1$ solutions, ie. $(1,2,3,...,p-1)$. Since $x^n-1\equiv 0\ (mod\ p)$ has at most n solutions by the previous theorem, and $(x^n)^{k-1}+(x^n)^{k-2}+...+(x^n)^2+(x^n)^1+1\equiv 0\ (mod\ p)$ has at most $n(k-1)$ solutions, $x^n-1\equiv 0\ (mod\ p)$ must have exactly n solutions. ■

To sum up what we've done, we've proven the following proposition:

Proposition 3.4.0.5
If $n\mid p-1$ and $d_1,d_2,...,d_r=n$ are all the divisors of n, then $\psi(d_1)+\psi(d_2)+...+\psi(d_r)=n$.

Recall that ϕ also satisfies the above equation. Now we can finally use these propositions to prove the following theorem:

Theorem 3.4.0.6
For all $n\in\mathbb{Z}$, we have that $\psi(n)=\phi(n)$

Proof
Let p be a prime
Clearly, $\phi(1)=1=\psi(1)$.
Let q be a prime factor of $p-1$. Then, by the above proposition, $\psi(1)+\psi(q)=q$. Thus, $\psi(q)=q-\psi(1)=q-\phi(1)=q-1=\phi(q)$.

Let qr be a divisor of $p-1$, where q,r are prime. Then, by the above proposition,
$$\psi(qr)=qr-\psi(q)-\psi(r)-\psi(1)=qr-\phi(q)-\phi(r)-\phi(1)=\phi(qr)$$
Since we can express every n as the product of primes, we have that $\phi(n)=\psi(n)$ for all $n\in\mathbb{Z}$. ■

Definition 3.4.0.4 (Index of a mod p for base g)
Let p be a prime and g and primitive root of p (ie. $a^g\equiv 1\ (mod\ p)$ for all $a\in\mathbb{Z}$). Let a be a non-zero number modulo p. Then, there is a unique number i such that $1\le i\le p-1$ such that $a\equiv g^i\ (mod\ p)$. The exponent i is called the index of a modulo p for the base g. Assuming that p and g have been specified, we write $I(a)$ for the index.

Proposition 3.4.0.7
Let g be a primitive root of p. Then, every non-zero number modulo p is congruent to a power of g. More precisely, for any number $1 \leq a < p$, we can pick exactly one of the powers $g, g^2, g^3, ..., g^{p-1}$ as being congruent to a modulo p.

Example: Let $p = 13$, and $g = 2$. Then,

I	1	2	3	4	5	6	7	8	9	10	11	12
2^I $(mod\ 13)$	2	4	8	3	6	12	11	9	5	10	7	1

Read back the numbers to get the indices.

a	1	2	3	4	5	6	7	8	9	10	11	12
$I(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Theorem 3.4.0.8 (Index Rules Theorem)
Let p be a prime and g a primitive root of p. Then,

- $I(ab) \equiv I(a) + I(b)$ $(mod\ p-1)$ (product rule)
- $I(a^k) \equiv k \cdot I(a)$ $(mod\ p-1)$ (power rule)

Proof (Index Rules)
Let g be a primitive root of p. By definition, we have that $g^{I(a)} \equiv a$ $(mod\ p)$ and $g^{I(b)} \equiv b$ $(mod\ p)$

$$\begin{gathered} g^{I(ab)} \equiv ab\ (mod\ p) \\ ab \equiv g^{I(a)} g^{I(b)}\ (mod\ p) \\ \implies g^{I(ab)} \equiv g^{I(a)+I(b)}\ (mod\ p) \\ \implies g^{I(ab)-(I(a)+I(b))} \equiv 1\ (mod\ p) \\ \implies I(ab) - (I(a) + I(b)) \equiv 0\ (mod\ p) \end{gathered}$$

■

Example: Let $p = 13, g = 2$, compute $12 \cdot 11 \bmod 13$

Answer
Solving $12 \cdot 11 \equiv x \ (mod\ 13)$

$$I(12 \cdot 11) \equiv I(12) + I(11) \ (mod\ 12)$$
$$I(12) + I(11) \equiv 6 + 7 \ (mod\ 12)$$
$$6 + 7 \equiv 1 \ (mod\ 12)$$

So, we have

$$12 \cdot 11 \equiv 2^{I(12 \cdot 11)} \ (mod\ 13)$$
$$12 \cdot 11 \equiv 2 \ (mod\ 13)$$

Example: Let $p = 13, g = 2$, compute $11^{100} \bmod 13$

Answer
Solving $11^{100} \equiv x \ (mod\ 13)$

$$I(11^{100}) \equiv 100 I(11) \ (mod\ 12)$$
$$I(11^{100}) \equiv 100 \cdot 7 \ (mod\ 12)$$
$$I(11^{100}) \equiv 4 \ (mod\ 12)$$

So, we have

$$11^{100} \equiv 2^{I(11^{100})} \ (mod\ 13)$$
$$11^{100} \equiv 2^4 \ (mod\ 13)$$
$$11^{100} \equiv 3 \ (mod\ 13)$$

Example: Let $p = 13, g = 2$, solve the linear congruence $11x \equiv 2 \ (mod\ 13)$

Answer
Take the index of both sides,

$$I(11x) \equiv I(2) \ (mod\ 12)$$
$$I(11) + I(x) \equiv I(2) \ (mod\ 12)$$
$$7 + I(x) \equiv 1 \ (mod\ 12)$$
$$I(x) \equiv 6 \ (mod\ 12)$$
$$\implies x \equiv 12 \ (mod\ 13)$$

Remark: It turns out that it does not matter which primitive root we use, taking the primitive root $g = 7$, for example, produces the same set of solutions. It seems like using indices can greatly simplify the computation of linear congruence, however to use such a method, the index table must first be calculated.

Chapter 4

Squares Modulo P

4.1 Quadratic Residues

Question: Given a number a, and prime p, does the congruence $x^2 \equiv a \ (mod\ p)$ have a solution?

Example: is 3 congruent to a perfect square modulo 11? ie. does $x^2 \equiv 3 \ (mod\ 11)$ have a solution?

Answer
As a naive first attempt, we will just calculate the congruence relation for all unique values of x.

$$\begin{array}{rr} 1^2 \equiv 1 \ (mod\ 11) & 10^2 \equiv 1 \ (mod\ 11) \\ 2^2 \equiv 4 \ (mod\ 11) & 9^2 \equiv 4 \ (mod\ 11) \\ 3^2 \equiv 9 \ (mod\ 11) & 8^2 \equiv 9 \ (mod\ 11) \\ 4^2 \equiv 5 \ (mod\ 11) & 7^2 \equiv 5 \ (mod\ 11) \\ 5^2 \equiv 3 \ (mod\ 11) & 6^2 \equiv 3 \ (mod\ 11) \end{array}$$

Clearly, when $x = 5, 6$, the relation $x^2 \equiv 3 \ (mod\ 11)$ holds.

It's no coincidence that $1^2 \equiv 10^2 \ (mod\ 11)$ and $2^2 \equiv 9^2 \ (mod\ 11)$ etc. It follows from the fact that we're taking $(p-b)^2$ for some b. Expanding that gives $p^2 - 2pb + b^2$, which is congruent to b^2 in mod p. Hence, for $p - a = b$, we have that $a^2 \equiv b^2 \ (mod\ p)$.

Definition 4.1.0.1 (Quadratic Residue and Non-Residue)
Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. If $x^2 \equiv a \ (mod\ p)$ has a solution, then a is called a quadratic residue modulo p. We use the notation QR. If $x^2 \equiv a \ (mod\ p)$ does not have a solution, then we call a a quadratic non-residue modulo p, and give the notation NR.

Example: The quadratic residues in modulo 11 are 1,3,4,5,9 since all of $x^2 \equiv a \ (mod\ p)$ have solutions for $a = 1, 3, 4, 5, 9$.

It turns out that determining the solution of $x^2 \equiv a \ (mod\ p)$ is very difficult, so we need some observations which will help us in finding the answer.

Proposition 4.1.0.1
Let p be an odd prime. Then, there are exactly

$$\frac{p-1}{2} \text{ quadratic residues modulo } p\text{, and}$$
$$\frac{p-1}{2} \text{ quadratic non-residues modulo } p$$

Proof
The quadratic residues modulo p are congruent to $1^2, 2^2, ..., ((p-1)/2)^2$. To prove that there are exactly $(p-1)/2$ quadratic residues modulo p, it is sufficient to prove that $1^2, 2^2, ..., ((p-1)/2)^2$ are distinct modulo p.

Suppose that $1 \leq b_2 \leq b_1 \leq \frac{p-1}{2}$ and $b_1^2 \equiv b_2^2 \ (mod\ p)$. Then, we have that $p \mid b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2)$, and since p is prime, either $p \mid (b_1 - b_2)$ or $p \mid (b_1 + b_2)$.
But $2 \leq b_1 + b_2 \leq \frac{p-1}{2} + \frac{p-1}{2} = p - 1 < p$, so $p \nmid (b_1 + b_2)$

Thus, $p \mid (b_1 - b_2)$. But $0 \leq (b_1 - b_2) \leq \frac{p-1}{2} < p$, so we must have that $b_1 - b_2 = 0$ if $p \mid (b_1 - b_2)$. Hence we have that $b_1 = b_2$.

We have shown that all quadratic residues modulo p are of the form $1^2, 2^2, ..., ((p-1)/2)^2$ are distinct, and thus there are exactly $\frac{p-1}{2}$ of them. ■

Question: Suppose $a_1, a_2 \in \mathbb{Z}$. Can we determine whether or not $a_1 \cdot a_2$ is a quadratic residue on the basis of a_1 and a_2?

Theorem 4.1.0.2 (Quadratic Residue Rules V1)
Let p be an odd prime. We have the following, where QR denotes an integer which is a quadratic residue modulo p, and NR an integer which is a quadratic non-residue.

$$QR \cdot QR = QR$$
$$QR \cdot NR = NR$$
$$NR \cdot NR = QR$$

Proof (Quadratic Residue Rules V1)
We have 3 statements to prove:

1. $QR \cdot QR = QR$
2. $QR \cdot NR = NR$
3. $NR \cdot NR = QR$

We will begin by proving (1). Suppose we have two quadratic residues modulo p, namely a_1, a_2. By definition, for some integers b_1, b_2,

$$b_1{}^2 \equiv a_1 \ (mod\ p) \text{ and } b_2{}^2 \equiv a_2 \ (mod\ p)$$
$$\implies b_1^2 b_2^2 \equiv a_1 a_2 \ (mod\ p)$$
$$\implies (b_1 b_2)^2 \equiv a_1 a_2 \ (mod\ p)$$

Thus, $a_1 a_2$ is a QR modulo p, as required.

Now, lets prove (2). Suppose we have a QR and NR a_1, a_2 respectively, modulo p. Assume that $a_1 a_2$ is a QR modulo p. Then, we have that,

$$\exists b_2 \in \mathbb{Z} \text{ such that } b_2{}^2 \equiv a_1 a_2 \ (mod\ p)$$
$$\text{But, since } a_1 \text{ is a QR modulo } p,$$
$$\exists b_1 \in \mathbb{Z} \text{ such that } b_1{}^2 \equiv a_1 \ (mod\ p)$$
$$\implies b_2{}^2 \equiv b_1^2 a_2 \ (mod\ p)$$
$$\implies b_2^2 (b_1^2)^{-1} \equiv b_1^2 a_2 (b_1^2)^{-1} \equiv a_2 \ (mod\ p)$$

Thus, a_2 is a QR, which contradicts our assumption.

Finally, lets prove (3). Let A be the set of all QR's modulo p, and B be the set of all NR's modulo p. As we've seen, $|A| = |B| = (p-1)/2$. It's also clear that $A \cap B = \emptyset$, and $A \cup B = R_p$. Let c be a NR. Since $cA = \{ca : a \in A\}$, and each element in A is a QR, by (2), cA is a set of NR's, thus $cA \subseteq B$. But, we have that $|A| = |B|$, and $|cA| = |A|$, so we must have that $cA = B$. By a similar argument, we can also get that $cR_p = R_p$.

$$A \cup B = R_p \text{ and } A \cap B = \emptyset$$
$$B = R_p - A$$
$$cB = c(R_p - A)$$
$$cB = cR_p - cA$$
$$cB = R_p - B$$
$$cB = A$$

So, any NR c times an NR in B is in the set A, this is a QR, as required. ∎

4.2 Legendre Symbol

Definition 4.2.0.1 (Legendre Symbol)
Let p be an odd prime, and $gcd(a, p) = 1$. The Legendre symbol of a modulo p is given by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 : a \in QR \\ -1 : a \in NR \end{cases}$$

Examples: $\left(\frac{7}{11}\right) = -1$, since 7 is an NR modulo 11. $\left(\frac{9}{11}\right) = 1$, since 9 is a QR modulo 11.

Theorem 4.2.0.1 (Quadratic Residue Rules V2)
For all $a, b \in \mathbb{Z}$ such that $a \not\equiv 0\ (mod\ p)$, $b \not\equiv 0\ (mod\ p)$, and an odd prime p,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof (Quadratic Residue Rules V2)
Each case can be seen by the multiplication rules from Quadratic Residue Rules V1, and so will be omitted here.

Examples:

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)(1) = -1$$

Thus, $x^2 \equiv 6\ (mod\ 11)$ has no solutions.

$$\left(\frac{24}{11}\right) = \left(\frac{2^3}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{2}{11}\right)^2\left(\frac{3}{11}\right) = (-1)^3(1) = -1$$

Thus, $x^2 \equiv 24\ (mod\ 11)$ has no solution

What about when we have a negative a value? ie. compute $\left(\frac{-5}{11}\right)$

$$\left(\frac{-5}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{5}{11}\right) = ?$$

Lets try to find a pattern in the solutions to $x^2 \equiv -1\ (mod\ p)$, so we can determine if a negative a value has a solution by factoring out the -1.

p	3	5	7	11	13	17	19	23	29	31
$\left(\frac{-1}{p}\right)$	-1	1	-1	-1	1	1	-1	-1	1	-1

It seems as though $\left(\frac{-1}{p}\right) = 1$ when $p \equiv 1\ (mod\ 4)$, and $\left(\frac{-1}{p}\right) = -1$ otherwise. Note that the only possible congruence value is 3, since p is odd. This leads us to the following theorem, which we will prove with the help of Euler's Criterion.

Theorem 4.2.0.2 (Quadratic Reciprocity Part 1)
Let p be an odd prime.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 : p \equiv 1\ (mod\ 4) \\ -1 : p \equiv 3\ (mod\ 4) \end{cases}$$

Before we can prove this, we first need Euler's Criterion.

4.3 Euler's Criterion

Theorem 4.3.0.1 (Euler's Criterion)
Let p be an odd prime, and $a \not\equiv 0\ (mod\ p)$. Then,

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\ (mod\ p)$$

Proof (Euler's Criterion)
We have 2 cases, when a is a QR, and when a is a NR.

Case 1: Suppose a is a QR. Then, by definition, $b^2 \equiv a\ (mod\ p)$ for some $b \in \mathbb{Z}$, so $\left(\frac{a}{p}\right) = 1$. We have,

$$a^{\frac{p-1}{2}}$$
$$\equiv (b^2)^{(p-1)/2}$$
$$\equiv b^{p-1}, \text{ so by } FlT,$$
$$a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right)\ (mod\ p)$$

as required.

Case 2: Suppose a is a NR. Then, by definition, $\left(\frac{a}{p}\right) = -1$. Consider the following, which will be denoted

$$(*)\text{: } x^{\frac{p-1}{2}} - 1 \equiv 0\ (mod\ p)$$

Proof (cont.)
We know by case 1 that $(*)$ is satisfied when x is a QR, and we will now show that in fact, the only set of solutions to $(*)$ is the same as the set of integers in QR. We know that there are $\frac{p-1}{2}$ distinct elements in QR, so $(*)$ has <u>at least</u> $\frac{p-1}{2}$ solutions. By a theorem proved earlier this term, since $(*)$ has degree $\frac{p-1}{2}$, there are <u>at most</u> $\frac{p-1}{2}$ solutions. Thus, there are exactly $\frac{p-1}{2}$ solutions to $(*)$, and each solution is a QR. So, a is a solution to $(*)$, if and only if a is QR.
Let a be a NR. By FlT, we have

$$0 \equiv a^{p-1} - 1 \ (mod\ p)$$
$$0 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \ (mod\ p)$$

But, since a is a NR, a cannot be a solution to $(*)$ as we have shown, and so $(a^{\frac{p-1}{2}} - 1)$ is not congruent to 0 modulo p, so we can freely divide both sides of the congruence relation

$$0 \equiv a^{\frac{p-1}{2}} + 1 \ (mod\ p)$$
$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \ (mod\ p)$$

So, for every a, we have that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ (mod\ p)$, as required. ■

Proof (Quadratic Reciprocity Part 1)
By Euler's criterion, we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \ (mod\ p)$$

We have two cases, one where Legendre's symbol evaluates to 1 and another which evaluates to -1.
<u>Case 1:</u> $\left(\frac{-1}{p}\right) = -1$, then we must have that $(p-1)/2$ is odd

$$(p-1)/2 = 2k + 1 \text{ for some } k \in \mathbb{Z}$$
$$p - 1 = 4k + 2$$
$$p = 4k + 3$$

So, if p is congruent to 3 modulo 4, then $\left(\frac{-1}{p}\right) = -1$

<u>Case 2:</u> $\left(\frac{-1}{p}\right) = 1$, then we must have that $(p-1)/2$ is even, and by a similar argument, we get that p must be congruent to 1 modulo 4, as required. ■

Now that we are able to calculate Legendre's Symbol for a numerator of -1 and we know that it is closed under multiplication, we should try to find a way to calculate it for prime numerators, that way we can take any integer and factor it into a workable equation.

Question: What is $\left(\frac{q}{p}\right)$ when q is prime? Let's first check the case where $q = 2$.

Theorem 4.3.0.2 (Quadratic Reciprocity Part 2)
Let p be an odd prime. Then,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 : p \equiv 1, 7 \ (mod\ 8) \\ -1 : p \equiv 3, 5 \ (mod\ 8) \end{cases}$$

Example: Compute $\left(\frac{2}{11}\right)$. We know that $11 \equiv 3 \ (mod\ 8)$, thus, $\left(\frac{2}{11}\right) = -1$ Notice that if we multiply the set of integers between 1 and $\frac{p-1}{2}$ by 2, we get $\{2, 4, 6, 8, 10\}$, and if we reduce the numbers greater than $\frac{p-1}{2}$ in modulo 11, we get the set $\{2, 4, -5, -3, -1\}$, which is the same as our original set, with some elements negated and in a different order. So, we can get that

$$(2 \cdot 1)(2 \cdot 2)(2 \cdot 3)(2 \cdot 4)(2 \cdot 5) \equiv 2 \cdot 4 \cdot -5 \cdot -3 \cdot -1 \ (mod\ 11)$$
$$2^{(11-1)/2} \cdot 5! \equiv (-1)^3 \cdot 5!$$
$$2^{(11-1)/2} \equiv (-1)^3$$

Theorem 4.3.0.3 (Gauss' Lemma)
Let p be an odd prime, $a \in \mathbb{Z}$, and $a \not\equiv 0 \ (mod\ p)$. Take the numbers $a, 2a, 3a, ..., \frac{p-1}{2}a$ and reduce each of them modulo p to get a number lying between $\frac{-(p-1)}{2}$ and $\frac{p-1}{2}$. If s is the number of resulting numbers less than 0, then we have

$$\left(\frac{a}{p}\right) = (-1)^s$$

Proof (Gauss' Lemma)
For $1 \leq i \leq \frac{p-1}{2}$, let $ia \equiv ui \ (mod\ p)$ such that $\frac{-(p-1)}{2} \leq ui \leq \frac{p-1}{2}$. Note that s is the number of elements $u_1, u_2, ...u_{(p-1)/2}$ which are less than 0.

Claim: $\{|u_1|, |u_2|, ..., |u_{(p-1)/2}|\} = \{1, 2, ..., \frac{p-1}{2}\}$
Proof of claim: It is sufficient to show that no two elements in the set $\{|u_1|, |u_2|, ..., |u_{(p-1)/2}|\}$ are the same. Thus, we need to show that if $u_i = \pm u_j$ then $i = j$.
<u>Case 1:</u> $u_i = u_j$, then $ia \equiv u_j \equiv u_i \equiv ja \ (mod\ p)$ by definition, and since $gcd(a, p) = 1$, we have $i \equiv j \ (mod\ p)$, which implies $i = j$ because of the range of i and j.
<u>Claim 2:</u> $u_i = -u_j$, then,

$$ia \equiv u_i \ (mod\ p)$$
$$ja \equiv -u_i \ (mod\ p)$$

Adding these equations together, we get that

$$(i + j)a \equiv 0 \ (mod\ p)$$
$$i + j \equiv 0 \ (mod\ p)$$

Proof (cont.)
But, we have that $1 \leq i, j \leq \frac{p-1}{2}$, so we can't have that they are congruent to 0 modulo p, a contradiction. Thus, we only have to worry about case 1, which implies $i = j$, as required.

So, we have the following:

$$a \cdot 2a \cdot 3a ... \cdot \tfrac{p-1}{2}a \equiv u_1 \cdot u_2 ... \cdot u_{\frac{p-1}{2}} \ (mod\ p)$$
$$a^{\frac{p-1}{2}}(\tfrac{p-1}{2})! \equiv (-1)^s \cdot \tfrac{p-1}{2}! \ (mod\ p)$$
$$a^{\frac{p-1}{2}} \equiv \left(\tfrac{a}{p}\right) \equiv (-1)^s \ (mod\ p)$$

As required. ■

Now we have the ability to prove Quadratic Reciprocity Part 2, and we will do so by comparing our results from Gauss' Lemma for different values of p modulo 8.

Proof (Quadratic Reciprocity Part 2)
By Gauss' Lemma, we need to count the number of negative elements in the set

$$\{2 \cdot 1, 2 \cdot 2, 2 \cdot 3, ..., 2 \cdot \tfrac{p-1}{2}\}$$

In other words, we need to count the number of elements in the set which are larger than $\frac{p}{2}$. Consider $2j$ for some $1 \leq j \leq \frac{p-1}{2}$. j is less than $\frac{p}{2}$ exactly when $j \leq \frac{p}{4}$. Hence, there are exactly $\lfloor \frac{p}{4} \rfloor$ many integers in the set. So we have that $s = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$. Thus, by Gauss, we have the following:

$$\left(\tfrac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}$$

<u>Case 1:</u> $p \equiv \pm 1 \ (mod\ 8)$, then we have that $p = 8k \pm 1$, for some a$k \in \mathbb{Z}$. Plugging in our value for p, we get that $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ is an even integer, thus we have $\left(\frac{2}{p}\right) = 1$ when $p \equiv \pm 1$ $(mod\ 8)$.
<u>Case 2:</u> $p \equiv \pm 3 \ (mod\ 8)$, we follow similar steps as above to find that s will end up be an odd integer, thus $\left(\frac{2}{p}\right) = -1$, as required. ■

Doing a similar calculation, we can easily see that when $p \equiv \pm 1 \ (mod\ 8)$, $(-1)^{\frac{p^2-1}{8}} = 1$, and when $p \equiv \pm 3 \ (mod\ 8)$, $(-1)^{\frac{p^2-1}{8}} = -1$, as required.

To summarize what we have done so far, we have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 : p \equiv 1 \ (mod\ 4) \\ -1 : p \equiv 3 \ (mod\ 4) \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 : p \equiv \pm 1 \ (mod\ 8) \\ -1 : p \equiv \pm 3 \ (mod\ 8) \end{cases}$$

We would like to have a way to calculate $\left(\frac{q}{p}\right)$ for any q, and we can do so by splitting q into it's prime factors, so we'll need to compute the result for odd primes q.

4.4 Quadratic Reciprocity

Theorem 4.4.0.1 (Quadratic Reciprocity)
Let p, q be distinct odd primes

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Example: Compute $\left(\frac{90}{101}\right)$.

$$\left(\frac{90}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{3^2}{101}\right)\left(\frac{5}{101}\right)$$
$$101 \equiv 5 \ (mod\ 8), \text{ so } \left(\frac{2}{101}\right) = -1$$
$$\text{Clearly, 3 is a solution for } x^2 \equiv 3^2 \ (mod\ 101), \text{ so } \left(\frac{3^2}{101}\right) = 1$$
$$\left(\frac{90}{101}\right) = -\left(\frac{5}{101}\right)$$
$$\text{By quadratic reciprocity,}$$
$$= -\left(\frac{101}{5}\right) \cdot (-1)^{\frac{101-1}{2} \cdot \frac{5-1}{2}}$$
$$= -\left(\frac{1}{5}\right) \cdot 1$$
$$\left(\frac{90}{101}\right) = -1$$

Before we can try to prove Quadratic Reciprocity, we will need a lemma.

Lemma 4.4.0.2
Let p be an odd prime, and a an odd integer where $a \not\equiv 0 \ (mod\ p)$. Then, we have

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

where $T(a, p)$ is defined by

$$T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \tfrac{ja}{p} \rfloor$$

Proof (Of Lemma)
Let $1 \leq j \leq \frac{p-1}{2}$. we have

$$(*) : ja = p\lfloor \frac{ja}{p} \rfloor + r_j$$

for $0 \leq r_j \leq p-1$, by the division algorithm. Let u_j be the number between $\frac{-(p-1}{2}$ and $\frac{p-1}{2}$ such that $ja \equiv u_j \ (mod\ p)$. Then, we have

$$r_j = u_j \text{ if } 0 \leq r_j \leq \frac{p-1}{2}$$
$$r_j = p + u_j \text{ if } \frac{p-1}{2} \leq p-1$$

Let s be the number of u_j which are less than 0, and let t be the number of u_j which are greater than 0. We can then re-index r_j and u_j

let $u_1, ..., u_s$ be the u which are less than 0,
and $u_{s+1}, ..., u_{s+t}$ be the u which are greater than 0

Summing $(*)$ for all $1 \leq j \leq \frac{p-1}{2}$, we have

$$(1) : \sum_{j=1}^{\frac{p-1}{2}} ja = p \cdot \left(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor \right) + \left(\sum_{j=1}^{s} (p + u_j) \right) + \left(\sum_{j=1}^{t} u_{j+s} \right)$$

But, we know from the proof in the previous section that

$$\{|u_1|, |u_2|, ..., \left|u_{(p-1)/2}\right|\} = \{1, 2, ..., \tfrac{p-1}{2}\}$$

and thus we have

$$(2) : \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{s} -u_j + \sum_{i=1}^{t} u_{s+i}$$

So, if we take $(1) - (2)$, we get

$$(a-1) \cdot \left(\sum_{j=1}^{\frac{p-1}{2}} j \right) = \sum_{j=1}^{s} (p + 2u_j) + p \cdot T(a,p)$$

Taking this equation in modulo 2, it reduces to

$$0 \equiv s + T(a,p) \ (mod\ 2)$$

$$\implies T(a,p) \equiv s \ (mod\ 2)$$

So finally, we get

$$(-1)^s = (-1)^{T(a,p)}$$

as required. ■

So far we have proved a lemma which will be useful in the proving of quadratic reciprocity. Lets use what we've proved in an example

Example: Compute $\left(\frac{11}{7}\right)$

Answer
We will need to calculate $T(11,7)$ and use the lemma

$$T(11,7) = \sum_{j=1}^{\frac{7-1}{2}} \lfloor \tfrac{11j}{7} \rfloor = \lfloor \tfrac{11}{7} \rfloor + \lfloor \tfrac{22}{7} \rfloor + \lfloor \tfrac{33}{7} \rfloor$$
$$T(11,7) = 1 + 3 + 4 = 8$$
Using the lemma, we get
$$\left(\frac{11}{7}\right) = (-1)^8 = 1$$

Example: Compute $\left(\frac{7}{11}\right)$

Answer
We will need to calculate $T(7,11)$ and use the lemma

$$T(7,11) = \sum_{j=1}^{\frac{11-1}{2}} \lfloor \tfrac{7j}{11} \rfloor = \lfloor \tfrac{7}{11} \rfloor + \lfloor \tfrac{14}{11} \rfloor + \lfloor \tfrac{21}{11} \rfloor + \lfloor \tfrac{28}{11} \rfloor + \lfloor \tfrac{35}{11} \rfloor$$
$$T(7,11) = 0 + 1 + 1 + 2 + 3 = 7$$
Using the lemma, we get
$$\left(\frac{7}{11}\right) = (-1)^7 = -1$$

Observation: We can see that $8 + 7 = 15 = 3 \cdot 5 = \frac{7-1}{2} \cdot \frac{11-1}{2}$. In other words, we have that $T(11,7) + T(7,11) = \frac{7-1}{2} \cdot \frac{11-1}{2}$

Notice that if we take the equation of a line $11x = 7y$, it turns out that $T(11,7)$ is equal to the number of integral points to the right of the line, as can be seen easier by $1+3+4$, 1 is the number of integral points under $x = 1$, 3 is the number of integral points under $x = 2$, and 4 is the number of integral points under $x = 3$. This can be seen by drawing a graph with the line $11x = 7y$. This observation is the key to proving quadratic reciprocity. Which we will now do.

Proof (Quadratic Reciprocity)
Compute $\left(\frac{q}{p}\right)$.

$$T(q,p) = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor \text{ and } T(p,q) = \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor$$

Now consider the line $qx = py$, and the integral points to the rights of the line, where $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{q-1}{2}$. Notice that there are a total of $\frac{p-1}{2} \cdot \frac{q-1}{2}$ integral points in the rectangle bounded by the line and the range. We will be arguing that every integral point is in exactly one of $T(q,p)$ or $T(p,q)$, thus proving that their sum is equal to $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

There are $\lfloor \frac{qj}{p} \rfloor$ many integral points to the right of the line in the range with j being the x coordinate. So, summing for all $j = x$ in the range, we get $\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{qj}{p} \rfloor$ which is equal to $T(q,p)$. Similarly, there are $\lfloor \frac{pj}{q} \rfloor$ many integral points to the left of the line for all $j = y$ in the range, which is equal to $T(p,q)$.

Thus, we have that every point is in one of $T(q,p)$ or $T(p,q)$, proving that

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

If we take (-1) as the base, we then get

$$(-1)^{T(q,p)+T(p,q)} = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}}$$

Following the result of the lemma previously proven, we get this is equal to

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

And notice that this is an equivalent way of writing Quadratic Reciprocity. ■

Example: Compute $\left(\frac{713}{1009}\right)$

Answer
First, notice that 1009 is prime, and so we are free to use the theorems we've just proven. We can factor 713 into two primes $713 = 23 \cdot 31$

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right) \cdot \left(\frac{31}{1009}\right) \text{ and by QR,}$$
$$\left(\frac{713}{1009}\right) = \left(\frac{1009}{23}\right) \cdot (-1)^{504 \cdot 11} \cdot \left(\frac{1009}{31}\right) \cdot (-1)^{504 \cdot 15}$$
$$\left(\frac{713}{1009}\right) = \left(\frac{1009}{23}\right) \cdot \left(\frac{1009}{31}\right)$$
$$\left(\frac{713}{1009}\right) = \left(\frac{20}{23}\right) \cdot \left(\frac{17}{31}\right)$$
$$\left(\frac{713}{1009}\right) = \left(\frac{2^2}{23}\right) \cdot \left(\frac{5}{23}\right) \cdot \left(\frac{17}{31}\right)$$

Answer (cont.)
Notice that $\left(\frac{2^2}{23}\right) = 1$

$$\left(\frac{713}{1009}\right) = \left(\frac{5}{23}\right) \cdot \left(\frac{17}{31}\right)$$
$$\left(\frac{713}{1009}\right) = \left(\frac{23}{5}\right) \cdot \left(\frac{31}{17}\right) \text{ by QR}$$
$$\left(\frac{713}{1009}\right) = \left(\frac{3}{5}\right) \cdot \left(\frac{14}{17}\right)$$
$$\text{Notice that } \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1 \text{ by QR part 2}$$
$$\left(\frac{713}{1009}\right) = -1 \cdot \left(\frac{2}{17}\right) \cdot \left(\frac{7}{17}\right)$$
$$\text{Notice that } \left(\frac{2}{17}\right) = 1 \text{ since } 17 \equiv 1 \ (mod\ 8) \text{ by QR part 2}$$
$$\left(\frac{713}{1009}\right) = -1 \cdot \left(\frac{17}{7}\right) = -1 \cdot \left(\frac{3}{7}\right)$$
$$\left(\frac{713}{1009}\right) = -1 \cdot \left(\frac{7}{3}\right) \cdot (-1)^3 = -1 \cdot -1 \cdot \left(\frac{1}{3}\right)$$
$$\left(\frac{713}{1009}\right) = \left(\frac{1}{3}\right) = 1$$

Definition 4.4.0.1 (Jacobi Symbol)
Let $n \geq 3$ be an odd integer, $a \in \mathbb{Z}$, such that $gcd(a, n) = 1$, and let n have a prime decomposition $n = p_1^{\delta_1} p_2^{\delta_2} ... p_k^{\delta_k}$. Then, we define the Jacobi symbol as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\delta_1} \left(\frac{a}{p_2}\right)^{\delta_2} \cdots \left(\frac{a}{p_k}\right)^{\delta_k}$$

Where each of $\left(\frac{a}{p_i}\right)$ is a legendre symbol.

Remark: Notice how when n is prime, we have that the Jacobi symbol is equal to the legendre symbol. The Jacobi symbol $\left(\frac{a}{n}\right)$ being equal to 1 does **not** mean $x^2 \equiv a \ (mod\ n)$ has an integer solution, unlike the legendre symbol.

Theorem 4.4.0.3 (Jacobi Symbol Theorem)
Let $m, n \geq 3$ be odd integers, and $a, b \in \mathbb{Z}$ such that $gcd(a, n) = gcd(b, n) = gcd(m, n) = 1$.
Then we have the following:

1. If $a \equiv b\ (mod\ n)$, then we have $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
4. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$
5. $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

Most of these items can be proven directly from rules we have derived about the legendre symbols, and so will be omitted.

Example: Compute $\left(\frac{37603}{48611}\right)$, note that 48611 is prime.

Answer
Since 48611 is prime, the Jacobi symbol is equal to the legendre symbol.

$$\begin{aligned}
\left(\frac{37603}{48611}\right) &= \left(\frac{48611}{37603}\right) \cdot (-1)^{\frac{48611-1}{2}\cdot\frac{37603-1}{2}} \\
&= -\left(\frac{11008}{37603}\right) = -\left(\frac{2^8 \cdot 43}{37603}\right) = -\left(\frac{43}{37603}\right) \\
&= -\left(\frac{37603}{43}\right) \cdot (-1)^{\frac{37603-1}{2}\cdot\frac{43-1}{2}} \\
&= \left(\frac{21}{43}\right) = \left(\frac{43}{21}\right) \cdot (-1)^{\frac{21-1}{2}\cdot\frac{43-1}{2}} \\
&= \left(\frac{1}{21}\right) = 1
\end{aligned}$$

Chapter 5

Integer Points on a Circle

5.1 $x^2 + y^2 = p$

The goal of this chapter is to develop tools to find integer solutions to the equation $x^2 + y^2 = n$, given some $n \in \mathbb{Z}$. Not unlike finding integer solutions to $x^2 \equiv a \ (mod\ p)$, we will be starting off by trying to find a function which determines if an integer solution exists. Let's first consider prime n values.

p	2	3	5	7	11	13	17	19	23	29
Solution	$1, 1$	No	$1, 2$	No	No	$2, 3$	$1, 4$	No	No	$2, 5$

We can see that there seems to be a pattern; $x^2 + y^2 = p$ has a solution when p is congruent to 1 modulo 4, or $p = 2$.

Theorem 5.1.0.1
$x^2 + y^2 = p$ for some prime p has a solution if and only if $p = 2$, or $p \equiv 1 \ (mod\ 4)$.

Proof
($\Longrightarrow$) Assume that $x^2 + y^2 = p$ has an integer solution for some prime p. Note that when $p = 2$, we are done, so we may assume p is odd, and want to show that $p \equiv 1 \ (mod\ 4)$.

$$x, y \equiv 0, 1, 2, 3 \ (mod\ 4)$$
$$x^2, y^2 \equiv 0, 1 \ (mod\ 4)$$
$$x^2 + y^2 \equiv 0, 1, 2 \ (mod\ 4)$$

Case 1: $x^2 + y^2 \equiv 0 \ (mod\ 4)$. This implies that p is divisible by 4 or is equal to 0, a contradiction.
Case 2: $x^2 + y^2 \equiv 1 \ (mod\ 4)$. We are done, since we have $p \equiv 1 \ (mod\ 4)$.
Case 3: $x^2 + y^2 \equiv 2 \ (mod\ 4)$. This implies that $p = 4k + 2$ for some $k \in \mathbb{Z}$, so $p = 2(2k + 1)$, so p is even, meaning $p = 2$.

Proof (Cont.)
There another way of proving the forward direction, which goes as follows:

($\implies$) Assume $x^2+y^2 = p$ has a solution for some prime p. We may assume p is an odd prime since $1^2 + 1^2 = 2$ is the only solution which gives $p = 2$. Notice that we have $0 < x, y < p$, $\sqrt{p}$ is irrational for any prime p. Therefore, we have that $gcd(x, p) = gcd(y, p) = 1$, and so taking the equation in modulo p,

$$x^2 + y^2 \equiv 0 \ (mod\ p)$$
$$x^2 \equiv -y^2 \ (mod\ p) \text{ for some } x, y \in \mathbb{Z}$$

This is equivalent to

$$\begin{aligned} \left(\frac{x^2}{p}\right) = \left(\frac{-y^2}{p}\right) = 1 \\ \implies \left(\frac{-1}{p}\right) \cdot \left(\frac{y^2}{p}\right) = 1 \text{ by QR} \\ \implies \left(\frac{-1}{p}\right) = 1 \\ \implies p \equiv 1 \ (mod\ 4) \end{aligned}$$

So, we must have that p is congruent to 1 mod 4 when we have a solution to $x^2 + y^2 = p$ for a prime p, as required.

($\impliedby$) Assume $p = 2$ or $p \equiv 1 \ (mod\ 4)$, we need to show that $x^2 + y^2 = p$ has integer solutions. If $p = 2$, we have the solution of $x = y = 1$, so we may assume that $p \equiv 1 \ (mod\ 4)$. So, we have

$$\left(\frac{-1}{p}\right) = 1$$
$$\exists A \in \mathbb{N} \text{ s.t. } A^2 \equiv -1 \ (mod\ p), \text{ for } 0 < A < p$$
$$A^2 + 1^2 \equiv 0 \ (mod\ p)$$
$$\exists M \in \mathbb{N} \text{ s.t. } A^2 + 1^2 = Mp, \text{ for } 0 < M < p$$

If $M = 1$, then we have guaranteed a solution to $x^2 + y^2 = p$, namely $(x, y) = (A, 1)$. So, we can use the *Method Of Descent* to inductively reduce M in the equation $A^2 + 1^2 = Mp$ until $M = 1$, thus guaranteeing the existence of a solution to $x^2 + y^2 = p$. ■

5.2 Method Of Descent

Theorem 5.2.0.1 (Method Of Descent (Euler, Fermat))
Let p be an odd prime. Assume that there exists $A, B, M \in \mathbb{N}$ where $1 < M$, and $0 < A, B, M < p$ such that $A^2 + B^2 = Mp$. Then, there exists $a, b, m \in \mathbb{N}$ where $0 < a, b, m < p$, and $m < M$ such that $a^2 + b^2 = mp$.

The main idea behind the proof of this theorem (or, more accurately, algorithm), is the following identity:

Theorem 5.2.0.2
$(u^2+v^2)(A^2+B^2) = (uA+vB)^2 + (vA-uB)^2$

Proof
This can be easily seen by expanding both sides, but a more interesting proof comes from using complex numbers. Let $z = u + iv$ and $w = B + Ai$, noticing that $\mathbb{N} \subset \mathbb{C}$

$$|zw| = |z||w|$$
$$|zw|^2 = |z|^2|w|^2$$
$$|(u+vi)(B+Ai)|^2 = (uA+vB)^2(vA-uB)^2 = (v^2+u^2)(A^2+B^2)$$

as required. ■

Example: Use the Method Of Descent to find a smaller value of M where $A^2 + B^2 = Mp$ and $A = 387$, $B = 1$, $M = 170$, $p = 881$.

Answer
We need to find some $a, b, m \in \mathbb{N}$ such that $a^2 + b^2 = mp$ where $m < M$ given the values above.

1. Write $387^2 + 1^2 = 170 \cdot 881$, notice that $0 < 170 < 881$
2. Chose numbers with

$$47 \equiv 387 \ (mod\ 170)$$
$$1 \equiv 1 \ (mod\ 170)$$
$$\text{notice } \frac{-170}{2} \leq 47, 1 \leq \frac{170}{2}$$

   Then, we have $47 \cdot 1 \equiv 387 \cdot 1 \ (mod\ 170)$, and $47 \cdot 387 + 1 \cdot 1 \equiv 0 \ (mod\ 170)$, from the original equation
3. Observe that

$$47^2 + 1^2 \equiv 387^2 + 1^2 \equiv 0 \ (mod\ 170), \text{ so}$$
$$47^2 + 1^2 = 13 \cdot 170$$
$$387^2 + 1^1 = 881 \cdot 170$$

Answer

4. Now we can use the identity to get

$$\begin{gathered}(47^2+1^2)(387^2+1^2)=(13)(170^2)(881)\\ =(47\cdot 387+1\cdot 1)^2+(387\cdot 1-47\cdot 1)^2\end{gathered}$$

5. Since $47\cdot 387+1\cdot 1\equiv 387\cdot 1-47\cdot 1\equiv 0\ (mod\ 170)$, we can cancel out 170

$$(\tfrac{(47)(387)+(1)(1)}{170})^2+(\tfrac{(387)(1)-(47)(1)}{170})^2=13\cdot 881$$

So, we have that

$$107^2+2^2=13\cdot 881$$

and $13<170$, as required.

Following similar steps as shown in this example, we can prove the Method of Descent for general equations $A^2+B^2=Mp$.

Proof (Method of Descent)
Consider $A^2+B^2=Mp$ for a prime p, where $0<A,B<p$, and $1<M<p$. We can choose numbers a,b such that

$$\begin{gathered}a\equiv A\ (mod\ M)\\ b\equiv B\ (mod\ M)\\ \tfrac{M}{2}\leq a,b\leq\tfrac{M}{2}\end{gathered}$$

By the congruence properties, we have that

$$\begin{gathered}aB\equiv bA\ (mod\ M)\\ aA+bB\equiv A^2+B^2\equiv 0\ (mod\ M)\\ a^2+b^2\equiv A^2+B^2\equiv 0\ (mod\ M)\\ \implies a^2+b^2=mM \text{ for some } m\in\mathbb{Z}\end{gathered}$$

Consider the product $(a^2+b^2)(A^2+B^2)$. By the identity, we have $(a^2+b^2)(A^2+B^2)=(aA+bB)^2+(aB-bA)^2=M^2mp$. Dividing by M^2, we get

$$(\tfrac{aA+bB}{M})^2+(\tfrac{aB-bA}{M})^2=mp.$$

But $aA+bB\equiv 0\ (mod\ M)$, so $\frac{aA+bB}{M}$ is an integer, and similarly, since $aB\equiv bA\ (mod\ M)$, $\frac{aB-bA}{M}$ is also an integer. Thus, we've found some m which satisfies $a^2+b^2=mp$, so now we need to show that $m<M$ to finish the proof.

$$\begin{gathered}m=\tfrac{a^2+b^2}{M}\\ \leq\tfrac{(\frac{M}{2})^2+(\frac{M}{2})^2}{M} \text{ by the range defined for } a,b\\ =\tfrac{M}{2}<M\end{gathered}$$

So, m satisfies the equation and is also strictly less than M, as required. ■

We've shown that the Method of Descent is valid, so our proof that there exists some integer solution to $x^2 + y^2 = p$ for a prime p if and only if $p = 2$ or $p \equiv 1 \ (mod\ 4)$ is sound. We will now focus on whether or not an integer solution exists to $x^2 + y^2 = n$ for some integer n, not necessarily prime.

5.3 $x^2 + y^2 = n$

Given a positive integer n, determine whether or not there exists some $a, b \in \mathbb{Z}$ such that $a^2+b^2 = n$. Notice that we may assume that $gcd(a, b) = 1$, since otherwise we are able to factor out the common divisor.

Let n be a positive integer of the form $n = p_1 p_2 ... p_r M^2$ where M is a positive integer and $p_1, ..., p_r$ are distinct primes.

Theorem 5.3.0.1
Let $n \in \mathbb{N}$.

1. We can factor n into $n = p_1 ... p_r M^2 m$, where $p_1, ..., p_r$ are distinct primes which are either 2 or congruent to 1 modulo 4. Then, n is a sum of squares.
2. n can be written as $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ where $gcd(a, b) = 1$ if and only if either
   (a) n is odd and every prime divisor of n is congruent to 1 modulo 4
   (b) n is even and $\frac{n}{2}$ is odd and every prime divisor of $\frac{n}{2}$ is congruent to 1 modulo 4

Proof
Proof of 1:
We will prove this part via induction on r. The base case is that $r = 0$, in which case we have that $n = M^2 = M^2 + 0^2$, as required. We will assume that the statement holds for some $r = k$. Now consider $r = k + 1$.

$$n = p_1 ... p_k M^2 p_{k+1}$$
But n/p_{k+1} can be written as $u^2 + v^2$ by our hypothesis,
$$n = (u^2 + v^2) p_{k+1}$$
$p_{k+1} = A^2 + B^2$ by assumption and the theorem for $x^2 + y^2 = p$
$$n = (u^2 + v^2)(A^2 + B^2)$$
$$n = (uA + Bv)^2 + (uB - vA)^2$$

Thus, n is the sum of squares, as required. ■

Proof (Cont.)
Proof of 2:
($\Longrightarrow$) Assume that $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, where $gcd(a, b) = 1$. We have two cases.
Case 1: n is odd.
Then, we know that none of $p_1, ..., p_r$ are equal to 2. We need to show that $p_i \equiv 1 \ (mod\ 4)$ for all i in the range. We know that $n = a^2 + b^2 \equiv 0 \ (mod\ p_i)$, thus,

$$\begin{aligned} \left(\frac{a}{p_i}\right)^2 &\equiv \left(\frac{-b}{p_i}\right)^2 \ (mod\ p_i) \\ \Longrightarrow\ 1 &\equiv \left(\frac{-1}{p_i}\right) \ (mod\ p_i) \\ \Longrightarrow\ p_i &\equiv 1 \ (mod\ 4) \end{aligned}$$

Case 2: n is even.
Then we may write $n = 2k = a^2 + b^2$ for some $k \in \mathbb{Z}$. Taking this equality in modulo 2, we get that either $a, b \equiv 1 \ (mod\ 2)$ or $a, b \equiv 0 \ (mod\ 2)$, since otherwise n wouldn't be even. Thus, we may write

$$\begin{gathered} a = 2u + 1 \\ b = 2v + 1 \text{ for some } u, v \in \mathbb{Z} \\ n = a^2 + b^2 = (2u + 1)^2 + (2v + 1)^2 \\ n = 4(u^2 + u + v^2 + v) + 2 \end{gathered}$$

So, 4 does not divide n, so $\frac{n}{2}$ is odd, and every prime divisor of n is congruent to 1 modulo 4, as required.
($\Longleftarrow$) Assume each prime divisor of n is congruent to 1 modulo 4. Then, by the theorem proved earlier in the chapter, we may write n as the sum of squares. ■

Theorem 5.3.0.2 (Pythagorean Hypotenuse Proposition)
A number c appears as the hypotenuse of a primitive Pythagorean triple (a, b, c), where a is odd, b is even and c is odd, if and only if c is a product of odd primes $p \equiv 1 \ (mod\ 4)$

Proof
We know that $a^2 + b^2 = c$, $gcd(a, b) = 1$, and c is odd by our work in the first chapter. Thus, c^2 must be a product of primes congruent to 1 modulo 4, similarly for c. The converse is also clear. ■

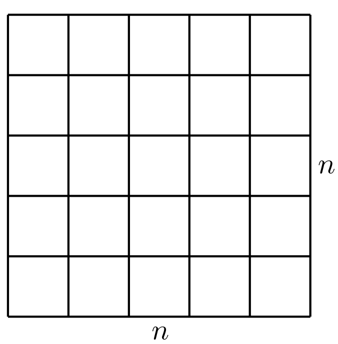
Chapter 6

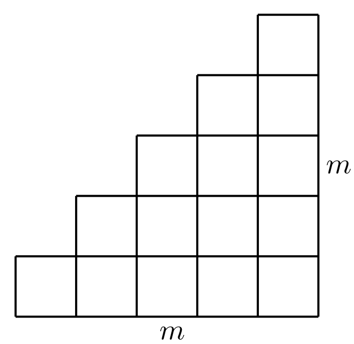
$x^2 - Dy^2 = 1$

6.1 Square and Triangle Numbers

Definition 6.1.0.1 (Square and Triangle Numbers)
An integer N is called a square number if a square with side length of n can be constructed, such that the number of cubes in the square is equal to N. Similarly, M is called a triangle number if a right angle triangle with sides at the right angle equal to m can be constructed such that the number of cubes in the triangle is equal to M.

Example: Here, we have a square number $N = 25$ and a triangle number $M = 15$





Question: Find all the square numbers that are also triangular numbers.

We need to solve $n^2 = \dfrac{m(m+1)}{2}$ in $\mathbb{N}$.

$$\begin{aligned} n^2 &= \frac{m(m+1)}{2} \\ 8n^2 &= 4m^2 + 4m \\ 2(2n)^2 &= (2m+1)^2 - 1 \end{aligned}$$

Setting $x = 2m+1$ and $y = 2n$, we have

$$\begin{aligned} 2y^2 &= x^2 - 1 \\ x^2 - 2y^2 &= 1 \end{aligned}$$

So, if there is a solution $x = 2m+1$ for some m, then y must also be even. Thus, let $m = \frac{x-1}{2}$ and $n = \frac{y}{2}$. So, we need to solve $x^2 - 2y^2 = 1$ in $\mathbb{Z}$ to find all the numbers which are both square and triangle. We can see the first few solutions by inspection:

$$\begin{aligned} m = 1,\, n = 1 &\implies x = 3,\, y = 2 \\ m = 8,\, n = 6 &\implies x = 17,\, y = 12 \\ m = 49,\, n = 35 &\implies x = 99,\, y = 70 \end{aligned}$$

Now to try to figure out the pattern, we will consider the much simpler equation $x^2 - y^2 = 1$

$$\begin{aligned} x^2 - y^2 &= 1 \\ (x-y)(x+y) &= 1 \\ x = \pm 1,\, y &= 0 \end{aligned}$$

So, it's clear that the difficulty of $x^2 - 2y^2 = 1$ arises from the fact that 2 is a non-unit coefficient of y in $\mathbb{Z}[x,y]$, so we cannot factor it in $\mathbb{Z}[x,y]$. What if we allow ourselves to use $\sqrt{2}$? Then, we may factor

$$\begin{aligned} x^2 - 2y^2 &= 1 \\ (x - \sqrt{2}y)(x + \sqrt{2}y) &= 1 \end{aligned}$$

We can find the first solution manually, and we find that $x = 3, y = 2$ is a solution. So, we have $(3 - 2\sqrt{2})(3 + 2\sqrt{2}) = 1$. Notice that we may take this to the k^{th} power and obtain another solution. Taking it to the second power, we get

$$\begin{aligned} (3 - 2\sqrt{2})^2(3 + 2\sqrt{2})^2 &= 1^2 \\ (17 - 12\sqrt{2})(17 + 12\sqrt{2}) &= 1 \\ 17^2 - 2(12)^2 &= 1 \\ \implies x = 17, y &= 12 \end{aligned}$$

So, it's clear that we may find infinitely many solutions by taking $(3-2\sqrt{2})(3+2\sqrt{2}) = 1$ to the power of k, for $k \in \mathbb{N}$. This can be proven explicitly using the binomial theorem, but will be omitted here. The natural question to ask is whether or not doing this for all k will find every solution, and the answer is yes!

Theorem 6.1.0.1

1. Every positive integer solution to the equation $x^2 - 2y^2 = 1$ is obtained by raising $3+2\sqrt{2}$ to different powers. That is, the solutions (x_k, y_k) can be found from $x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k$, $k \in \mathbb{N}$
2. Every square-triangular number $n^2 = \frac{m(m+1)}{2}$ is given by $m = \frac{x_k - 1}{2}$, and $n = \frac{y_k}{2}$

Proof

It's easy to see that raising $(3+2\sqrt{2})$ to some k^{th} power will yield a solution to $x_k^2 - 2y_k^2 = 1$, and we've already shown that every square-triangular number is given by $m = \frac{x_k-1}{2}$ and $n = \frac{y_k}{2}$, so it remains to show that every solution (x_k, y_k) to $x^2 - 2y^2 = 1$ is obtained by taking $(3+2\sqrt{2})$ to some power k. i.e, for every solution (u, v), there exists some $k \in \mathbb{N}$ such that $u + v\sqrt{2} = (3+2\sqrt{2})^k$

Let (u, v) be a solution, so $u^2 - 2v^2 = 1$.
Case 1: $u = 1$, There are no positive solutions
Case 2: $u = 2$, There are no solutions since u^2 is even
Case 3: $u = 3$, we have a solution $(3, 2)$, and $k = 1$ gives $(u + \sqrt{2}v) = (3 + \sqrt{2}2)^k$ So, we may assume that $u > 3$.

Claim: Let u, v be a solution to $x^2 - 2y^2 = 1$ such that $u > 3$. Then, we can find two positive integers t, s where $s < u$ such that $u + v\sqrt{2} = (3+2\sqrt{2})(s + t\sqrt{2})$. Note that this is a descent argument.

Proof of Claim: We can always write $u + v\sqrt{2} = (3+2\sqrt{2})(s+t\sqrt{2})$. In fact, multiplying by $(3-2\sqrt{2})$, we get

$$\begin{gathered}(3-2\sqrt{2})(u+v\sqrt{2}) = (3-2\sqrt{2})(3+2\sqrt{2})(s+t\sqrt{2}) \\ = (s+t\sqrt{2}), \text{ thus,} \\ (3u-4v) + (3v-2u)\sqrt{2} = s + t\sqrt{2}\end{gathered}$$

So, we can set

$$s = 3u - 4v \text{ and } t = 3v - 2u$$

to get that $u + v\sqrt{2} = (3+2\sqrt{2})(s+t\sqrt{2})$, as required. Moreover, $s^2 - 2t^2 = 1$, which can be seen directly. We now need to show the following

1. $s, t > 0$
2. $s < u$

Proof (Cont.)
For 1., note that $u^2 - 2v^2 = 1$, so $u^2 = 1 + 2v^2$, and $u > v\sqrt{2}$. Thus, $\frac{u}{v} > \sqrt{2}$, but we have that

$$s = 3u - 4v$$
$$s = 3v(\tfrac{u}{v} - \tfrac{4}{3}) > 3v(1.414... - 1.333...) > 0$$

With a very similar argument, you can see that $t > 0$, thus we have that t, s are positive integers, as required.

For 2., note that

$$\begin{aligned} u + \sqrt{2}v &= (3 + 2\sqrt{2})(s + t\sqrt{2}) \\ &= (3s + 4t) + (2s + 3t)\sqrt{2} \\ \implies u &= 3s + 4t, v = 2s + 3t \end{aligned}$$

Notice that $u > s$ and $v > t$ since $s, t > 0$, so $s < u$ as required.

6.2 Pell Equation

Definition 6.2.0.1 (Pell Equation)
A Pell equation is an equation of the form $x^2 - Dy^2 = 1$, where $D \in \mathbb{N}$ is not a perfect square.

Notice that if D were a perfect square, it would be easy to factor the left hand side into a product of linear polynomials, and subsequently find integer solutions.

Example: $D = 2$ gives the Pell equation $x^2 - 2y^2 = 1$, which as we've just shown, has the set of integer solutions obtained by raising $3 + 2\sqrt{2}$ to all positive integers.

Theorem 6.2.0.1
If we have some solution (x_0, y_0) to a Pell equation $x^2 - Dy^2 = 1$ for some non perfect square D, then we have infinitely many solutions to that equation.

Proof
We know that $(x_0 - \sqrt{D}y_0)(x_0 + \sqrt{D}y_0) = 1$, so we can raise the equation to the k^{th} power for some $k \in \mathbb{N}$, and we get

$$\begin{aligned} 1 &= (x_0 - \sqrt{D}y_0)(x_0 + \sqrt{D}y_0) \\ 1^k = 1 &= (x_0 - \sqrt{D}y_0)^k(x_0 + \sqrt{D}y_0)^k \\ &= (x_k - \sqrt{D}y_k)(x_k + \sqrt{D}y_k) \\ &= x_k^2 - Dy_k^2 \end{aligned}$$

Thus, (x_k, y_k) is a solution to $x^2 - Dy^2 = 1$, showing that if we have one solution to a Pell equation, then we have infinitely many solutions.

Example: Let $D = 313$. The smallest positive integer solution to $x^2 - 313y^2 = 1$ is
$$x = 32188120829134849,\ y = 1819380158564160$$

Observations: Intuitively, if we have very large $x, y \in \mathbb{N}$, then $x - \sqrt{D}y$ is very small. So if we re-arrange the Pell equation, we see that

$$\frac{1}{x + \sqrt{D}y} \text{ is very small}$$

Multiplying by $\frac{1}{y}$, we see that

$$\frac{x}{y} - \sqrt{D} = \frac{1}{x + \sqrt{D}y}\frac{1}{y} \text{ is even smaller}$$

So, when x, y are very large solutions to $x^2 - Dy^2 = 1$, then $\frac{x}{y}$ is a good approximation to $\sqrt{D}$. Notice that since x, y are positive integers, we get that

$$\left|\frac{x}{y} - \sqrt{D}\right| \leq \frac{1}{\sqrt{D}y^2}$$

Observation: For any $y \in \mathbb{N}$, if we take x to be the integer closest to $\sqrt{D}y$, then

$$\left|x - \sqrt{D}y\right| \leq \frac{1}{2} \implies \left|\frac{x}{y} - \sqrt{D}\right| \leq \frac{1}{2y}$$

Theorem 6.2.0.2 (The Pigeonhole Principle)
Finite Version: If we have more pigeons than pigeonholes, then at least one pigeonhole has two pigeons.
Infinite Version: If we have finitely many pigeon holes and infinitely many pigeons, then at least one pigeonhole has infinitely many pigeons.

Theorem 6.2.0.3 (Dirichlet Diophantine Approximation Theorem)
Suppose that $D \in \mathbb{N}$ and D is not a perfect square. Then, there are infinitely many pairs of (x, y) such that

$$\left|\frac{x}{y} - \sqrt{D}\right| \leq \frac{1}{y^2}$$

Remark: This actually holds for any irrational number d, but we insist here that $d = \sqrt{D}$ for some non perfect square D

Claim: Let $Y \in \mathbb{N}$. Then, there exists a pair (x, y), where $x, y \in \mathbb{N}$ such that $x - y\sqrt{D} \leq \frac{1}{Y}$, with $1 \leq y \leq Y$

Proof (of Claim)
We set up Y pigeon holes. Start with the interval $[0, 1]$, and divide it into Y sub interval, so we have the first interval $[0, \frac{1}{Y}]$, the second interval $[\frac{1}{Y}, \frac{2}{Y}]$, and the last interval $[\frac{Y-1}{Y}, 1]$. We will now argue that we must have some (x, y) in the same interval, which will imply the result we are looking for.

We may write

$$0\sqrt{D} = N_0 + F_0 = \lfloor 0\sqrt{D} \rfloor + F_0 \text{ so } 0 \leq F_0 \leq 1$$
$$1\sqrt{D} = N_1 + F_1$$
$$t\sqrt{D} = N_t + F_t$$

Notice that we may also write the fraction parts F_t as

$$F_t = t\sqrt{D} - N_t$$
$$F_t = t\sqrt{D} - \lfloor t\sqrt{D} \rfloor$$

So, for $0 \leq t \leq Y$, we can look at the set of fraction parts, $\{F_0, F_1, ..., F_Y\}$, noticing that we have $(Y + 1)$ fraction parts, and all of the fraction parts are in the range $0 \leq F_i \leq Y$, and we only have Y intervals. Thus, by the finite version of the pigeonhole argument, we must have at least 2 elements in one interval. Namely, there exists $0 \leq m < n \leq Y$ such that $F_n, F_m \in [\frac{s-1}{Y}, \frac{s}{Y}]$. Thus,

$$|F_m - F_n| < \frac{1}{Y}$$

So, expanding the fraction parts, we get that we can find a solution

$$x = (N_n - N_m)$$
$$y = (n - m)$$

such that $x - y\sqrt{D} < \frac{1}{Y}$, as required. ■

Proof (DDAT)
Using induction, the base case is $n = 1$, and we we are done.

Assume that we have found some solution (x_i, y_i), $1 \leq i \leq n$ such that $\left|x_i - y_i\sqrt{D}\right| \leq \frac{1}{y_i}$.

Let Y_{n+1} be the positive integer such that $\frac{1}{Y_{n+1}}$ is smaller than any $\left|x - y\sqrt{D}\right|$, where $x, y \in \mathbb{N}$, $1 \leq y \leq max\{y_1, y_2, ..., y_n\}$. By the claim, there exists x_{n+1}, y_{n+1} such that $|x_{n+1} - y_{n+1}| < \frac{1}{Y_{n+1}}$, where $y_{n+1} \leq Y_{n+1}$. By the choice of Y_{n+1}, we know that $y_{n+1} > max\{y_1, ..., y_n\}$. In particular, $y_{n+1} \neq y_i$ for all $0 \leq i \leq n$. So, (x_{n+1}, y_{n+1}) is different than (x_i, y_i) for all $1 \leq i \leq n$.

Thus, the statement is true for $n + 1$. So, by POSI, the statement is true for all n. ■

By DDAT, we have infinitely many pairs (x, y) such that

$$\left|x - y\sqrt{D}\right| \leq \frac{1}{y}$$

If we multiply both sides by $\left|x + y\sqrt{D}\right|$, we get

$$\left|x^2 - Dy^2\right| \leq \frac{x + y\sqrt{D}}{y} = \frac{x}{y} + \sqrt{D}$$

Moreover, we know that

$$\left|\tfrac{x}{y} - \sqrt{D}\right| \leq \tfrac{1}{y^2}$$

$$\tfrac{x}{y} \leq \sqrt{D} + \tfrac{1}{y^2} \leq 2\sqrt{D}$$

To sum up, we have

$$(x^2 - Dy^2) \leq \frac{x}{y} + \sqrt{D} \leq 3\sqrt{D}$$

Remember, we want to solve $x^2 - \sqrt{D}y^2 = 1$, so we need to work our way down from being less than or equal to $3\sqrt{D}$ to being equal to 1. To start, we'll use a pigeonhole argument. Consider the set of pigeons

$$S_1 = \{x^2 - Dy^2 : x, y \in \mathbb{N}, \left|x^2 - Dy^2\right| \leq 3\sqrt{D}\}$$

Clearly, each element in S_1 is bounded by $3\sqrt{D}$. Now consider $2A + 1$ pigeonholes, where $A = \lceil 3\sqrt{D} \rceil$, with the set of pigeonholes being of the form

$$S_2 = \{-A, -A + 1, ..., 0, 1, ..., A\}$$

So, by DDAT, we have infinitely many elements in the set S_1, and only a finite number of elements in the set S_2, so by the pigeonhole argument, there must be some element in S_2 which has an infinite number of pigeons in it. More precisely, there exists some $M \in \mathbb{Z}$, $-A \leq M \leq A$, $M \neq 0$ such that there are infinitely many positive integer pairs (x, y) which satisfy $x^2 - Dy^2 = M$.

Before continuing with the proof, lets look at a concrete example.

Example: Consider $D = 13$ and $M = 4$. Find some $x, y \in \mathbb{N}$ such that $x^2 - Dy^2 = 1$.

Answer
We have that $x^2 - 13y^2 = 4$ has solutions $(x, y) = (11, 3), (119, 33), (14159, 3927)$. Now we would like to find a solution to $x^2 - 13y^2 = 1$. The idea to do this is to divide one "bigger" solution by a different solution. Considering the solutions $(11, 3), (119, 33)$, we get

$$11^2 - 13(3^2) = 4$$
$$(11 - 3\sqrt{13})(11 + 3\sqrt{13})$$
$$(119 - 33\sqrt{13})(119 + 33\sqrt{13})$$

Notice that we have

$$\frac{(119 - 33\sqrt{13})(119 + 33\sqrt{13})}{(11 - 3\sqrt{13})(11 + 3\sqrt{13})} = \frac{4}{4} = 1$$

The division of $x_1 - y_1\sqrt{D}$ by $x_2 - y_2\sqrt{D}$ clearly gives an expression of the form $x_3 - y_3\sqrt{D}$, and similarly, the division of the conjugates will give an expression of the form $x_3 + y_3\sqrt{D}$. Thus, performing the division of one solution on another will give a solution to $x^2 - Dy^2 = 1$. The only issue is, we cannot guarantee that it will produce integer values for x, y. For example, let's divide $119 - 33^2\sqrt{13}$ by $11 - 3\sqrt{13}$.

$$\begin{aligned}\frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}} &= \frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}}\frac{11 + 3\sqrt{13}}{11 + 3\sqrt{13}}\\ &= \frac{22 - 6\sqrt{13}}{4}\end{aligned}$$

We can check that $x, y = (\frac{22}{4}, \frac{6}{4})$ is indeed a solution to $x^2 - 13y^2 = 1$, but x, y are not integers. Let's try dividing the solution $(14159, 3927)$ by the solution $(11, 3)$. The details will be omitted here, but one can check for themselves that the division yields $649 - 180\sqrt{13}$, thus we have an integer solution $(649, 180)$ to $x^2 - 13y^2 = 1$. Why did the division of this solution work? Well, when multiplying the numerator by the conjugate of the denominator, if we have that $c^2 - Dy^2 = M$, we have the general form

$$\frac{a - b\sqrt{D}}{c - d\sqrt{D}} \cdot \frac{c + d\sqrt{D}}{c + d\sqrt{D}} = \frac{ac - bdD + (ad - cb)\sqrt{D}}{M}$$

So, to get an integer solution, we must have that $M \mid (ac - bdD)$ and $M \mid (ad - cb)$ Thus, we get the following

$$c \equiv a \ (mod\ M)$$
$$d \equiv b \ (mod\ M)$$

In our example we see that indeed, $11 \equiv 14159 \ (mod\ 4)$ and $3 \equiv 3927 \ (mod\ 4)$, which is why we yield an integer solution of $(649, 180)$ to $x^2 - 13y^2 = 1$ by the division.

Theorem 6.2.0.4
Let $D \in \mathbb{N}$, where D is not a perfect square. Then, the pell equation $x^2 - Dy^2 = 1$ has a positive integer solution.

Proof
By our previous work, there exists some $M \in \mathbb{Z}$, $M \neq 0$ such that there are infinitely many positive integer pairs (x, y) which satisfy $x^2 - Dy^2 = M$. So, consider the solution

$$x_i \equiv x_j \ (mod\ M)$$
$$y_i \equiv y_j \ (mod\ M)$$

Most of the proof will be omitted here, but the key is to manipulate the fraction

$$\frac{x_i - y_i\sqrt{D}}{x_j - y_j\sqrt{D}}$$

by multiplying by the conjugate, and replacing x_i with x_j in modulo M, to see that the quotient of $x_i - y_i\sqrt{D}$ on $x_j - y_j\sqrt{D}$ has integer values for x, y, and thus we can find a positive integer solution to the Pell equation. ■

Remark: We've shown that given the Pell equation $x^2 - Dy^2 = 1$, we can find a positive integer solution, and thus can find infinitely many solutions by taking $(x_0 + y_0\sqrt{D})$ to the k^{th} power, where (x_0, y_0) is a solution. The natural thing to wonder is the general form of any solution to the equation, and it turns out that any positive integer solution to the equation can be obtained by taking the 'smallest' positive integer solution (x, y) to some positive power.

Theorem 6.2.0.5 (Pell Equation Theorem)
Let $D \in \mathbb{N}$, such that D is not a perfect square. Then, the pell equation $x^2 - Dy^2 = 1$ always has a positive integer solution, and if we let (x_1, y_1) be the smallest positive integer solution in terms of x_1, then the set of all positive integer solutions to $x^2 - Dy^2 = 1$ is

$$\{(x_k, y_k) : x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k, k \in \mathbb{N}\}$$

Proof
We've already shown that the equation has a positive integer solution (x_1, y_1), and we can find infinitely many other positive integer solutions generated by $(x_1 + y_1\sqrt{D})$, so it remains to show that all positive integer solutions to the equation can be expressed as a power of $x_1 + y_1\sqrt{D}$. We do so by a descent argument.

Claim: Let (u, v) be a positive integer solution to $x^2 - Dy^2 = 1$, where $u \geq x_1$. Then we can find two positive integers $s, t \in \mathbb{Z}$ such that $s < u$, and

$$u + v\sqrt{D} = (x_1 + y_1\sqrt{D})(s + t\sqrt{D})$$

Proof (cont.)
Notice that if we can prove the claim, then (s, t) is also a positive integer solution to $x^2 - Dy^2 = 1$, with $s < x_1$, so we can therefore find this new, smaller solution inductively to get the smallest positive integer solution, which shows that all solutions are powers of $(x_1 + y_1\sqrt{D})$.

We can always write
$$u + v\sqrt{D} = (x_1 + y_1\sqrt{D})(s + t\sqrt{D})$$
Now, multiplying both sides by $x_1 - y_1\sqrt{D}$,
$$\begin{aligned}(x_1 - y_1\sqrt{D})(u + v\sqrt{D}) &= (x_1^2 - Dy^2)(s + t\sqrt{D}) \\ &= s + t\sqrt{D} \text{ thus,} \\ s &= ux_1 - vy_1 D \in \mathbb{Z} \\ t &= x_1 v - uy_1 \in \mathbb{Z}\end{aligned}$$

Now we just need to show that both s and t are positive. This will be omitted, but it's easy to see this, since we have explicit expressions for s and t. So, s, t are positive integer solutions smaller than the previous solution, and thus we can express any solution as the power of the smallest integer solution, as required. ■

Due to COVID-19, we no longer have classes and so the course concludes here. The content covered in this document is up to assignment 8.