Introduction to Number Theory

Labix

October 5, 2024

Abstract

Contents

1 Properties of the Integers

1.1 Divisibility

We begin our study of number theory with divisibility.

Definition 1.1.1: Divisibility

Let $a, b \in \mathbb{Z}$. We define the relation $a|b$ if and only if there exists some $k \in \mathbb{Z}$ such that $b = ak$. We say that a divides b in this case.

The definition is vey simple. The intuition is straight forward as well. Savour this moment as the subject increases its difficulty exponentially.

Proposition 1.1.2

Let $d, m, n \in \mathbb{Z}$. The relation $|$ has the following properties and thus is a partial order in $\mathbb{N}$.

- (Reflexivity) $n|n$
- (Antisymmetry) $m|n$ and $n|m \implies m = n$
- (Transitivity) $d|n$ and $n|m \implies d|m$
- (Linearity) $d|n$ and $d|m \implies d|(an + bm)$ for any $a, b \in \mathbb{Z}$
- $1|n$
- $n|0$

Proof. We prove antisymmetry and transitivity and leave the others for the reader. Let $m, n, d \in \mathbb{Z}$.

- (Antisymmetry) If $m|n$ and $n|m$ then there exists some $k_1, k_2 \in \mathbb{N}$ such that $n = k_1 m$ and $m = k_2 n$ thus $n = k_1 k_2 n$. Then $k_1 k_2 = 1 \implies k_1 = k_2 = 1$ and $m = n$
- (Linearity) If $d|n$ and $n|m$ then there exists $k_1 k_2 \in \mathbb{N}$ such that $n = k_1 d$ and $m = k_2 n$. Then $m = k_2 k_1 d$ thus $d|m$

□

These properties will come up again and again and will be the foundation of number theory. It is safe to say that number theory is built upon the notion of divisibility.

1.2 The Division Algorithm

This section is dedicated to develop the Euclidean algorithm, a means to find the greatest common divisor. The gcd is a central notion in number theory as well.

Definition 1.2.1: Greatest Common Divisor

Suppose that $m, n \in \mathbb{Z}$. A number $d \in \mathbb{N}$ such that

- $d \geq 0$
- $d|m$ and $d|n$
- $e|a$ and $e|b \implies e|d$

is called the greatest common divisor of m and n, denoted $\gcd(m, n)$.

In contrast to the greatest common divisor, we also have the lowest common multiple. Although they work as a pair, we often see the notion of gcd come up more than lcm.

Definition 1.2.2: Lowest Common Multiple

Suppose that $m, n \in \mathbb{Z}$. A number $l \in \mathbb{N}$ such that

- $l \geq 0$
- $m|l$ and $n|l$
- $m|e$ and $n|e \implies l|e$

is called the lowest common multiple of m and n, denoted $\operatorname{lcm}(m, n)$.

Beware that both of these definitions does not imply the uniqueness of such a number. However, with a little work, we will see that both of them are indeed unique. Readers should think about whether the existence of these numbers is guaranteed as well.

Proposition 1.2.3

Let $m, n \in \mathbb{Z}$. $\gcd(m,n)$ and $\text{lcm}(m,n)$ are unique.

Proof. By the third property of both numbers, we must have if c, d are $\gcd(m,n)/\text{lcm}(m,n)$, then $c|d$ and $d|c$ thus $c = d$ and $\gcd(m,n)/\text{lcm}(m,n)$ is unique. □

We will see more on gcd and lcm when we deal with factorization. For now, we turn our heads to the division algorithm. This algorithm proves to us that upon dividing two integers, as long as they are not divisible by one or the other, you can always guarantee a remainder smaller than the divident.

Theorem 1.2.4: The Division Algorithm

Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$ with $b \neq 0$. Then there exists unique $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$.

Proof. We prove existence first by considering three cases.
Cases 1: b is divisible by a. If b is divisible by a then there exists $k \in \mathbb{Z}$ such that $b = ka$ thus $k = q$ and $r = 0$.

Case 2: b is positive and a does not divide b. Let

$$S = \{b - ka \in \mathbb{N} | k \in \mathbb{N}\}$$

Then $S \subseteq \mathbb{N}$ thus we can apply the well-ordering principle to S. Let r be the least natural number in S. Then $r \in S$ implies $r = b - ka$ for some $k \in \mathbb{N}$. Thus $b = ka + r$ for some k and r. We show that $r < a$. Suppose for a contradiction that $r \geq a$. Then $u = r - a \in \mathbb{N}$ and

$$b = ka + r \implies b = ka + (u - a) \implies b = (k-1)a + u$$

thus $u \in S$ and $u < r$, contradicting the fact that r is the least element in S. Thus $r \leq a$. If $r = a$, then

$$b = ka + a \implies b = (k+1)a$$

which means that $a|b$ which is false in our case. Thus we must have $r < a$.

Case 3: b is negative and a does not divide b. Then apply the exact same argument to the number $-b$ to get $(-b) = ka + r$ and $b = -ka - r$. Let $k' = -k - 1$ and $r' = -r + a$. Then

$$b = -ka - r = k'a + a + r' - a = k'a + r'$$

Since we have $0 \leq r < a$, we have $-a < -r \leq 0$ and $0 < r' \leq a$. Again $r' \neq a$ or else $a|b$ which contradicts our assumption.

We now prove uniqueness. Suppose that $b = aq_1 + r_1$ and $b = aq_2 + r_2$. Then $r_1 - r_2 = a(q_2 - q_1)$. We know that $-a < r_1 - r_2 < a$ thus $-a < a(q_2 - q_1) < a$ and $-1 < q_2 - q_1 < 1$ which is impossible for integers q_1, q_2 unless $q_1 = q_2$. If $q_1 = q_2$ then $r_1 = r_2$ and we are done. □

The division algorithm does not require b to be larger than a. In fact, if a is larger than b, then the division algorithm simply gives a itself as the remainder. Before we reach our conclusion, we need one more proposition.

Proposition 1.2.5

Suppose that $m \geq n > 0$ are natural numbers with $m = qn + r$ for some $q, r \in \mathbb{N}$. Then

$$\gcd(m, n) = \gcd(n, r)$$

Proof. Suppose that $d = \gcd(m, n)$. Then we know that $d < n$ from definition. We want to show that d satisfies the three results of a gcd but in terms of n and r. Since $d|n$ and $d|m$, by linearity we must have $d|r$.

Now suppose for a contradiction that there exists e such that e is a common divisor of n and r and $e > d$. Then $e|n$ and $e|r$ by definition thus $e|m$ by linearity. $e|m$ and $e|n$ implies that e is a larger common divisor of m and n than d. However this is not possible since d is assumed to be the largest among the common divisors. This is a contradiction thus $d = \gcd(n, r)$ and we are done. □

Theorem 1.2.6: Euclid's Algorithm

Suppose that $m \geq n > 0$ are natural numbers. We have the following inequalities.

$$m = nq_1 + r_1 \text{ with } 0 < r_1 < n$$

$$n = r_1q_2 + r_2 \text{ with } 0 < r_2 < n$$

$$r_1 = r_2q_3 + r_3 \text{ with } 0 < r_3 < n$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{k-2} = r_{k-1}q_k + r_k \text{ with } 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k-1}$$

From this, we have $r_k|r_{k-1}$, $r_k|r_{k-2} \dots r_k|n$ and $r_k|m$.

Proof. The first part of the results is due to the repeated use of the division algorithm. For the second part, we have

$$\gcd(m, n) = \gcd(n, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = r_k$$

and we are done. □

Lemma 1.2.7: Bezout's Lemma

Let $a, b \in \mathbb{Z}$ such that they are not both 0. Then there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b)$$

Proof. Reconstruct x and y using the Euclidean Algorithm. This is possible since $\gcd(m, n) = r_k$ and every $r_1, \dots, r_{k-1}$ has a factor of r_k in it. □

Lemma 1.2.8

Let $a, b \in \mathbb{Z}$ such that they are not both 0. Then the equation

$$ax + by = \gcd(a, b)$$

has an infinite number of integer solutions.

Proof. Using Bezout's Lemma, we conclude that (x_0, y_0) is a solution to the equation. But then

$$(x_0 - bt, y + at)$$

are also solutions for $t \in \mathbb{Z}$ since

$$a(x_0 - bt) + b(y + at) = ax + by = \gcd(a, b)$$

□

1.3 Unique Factorization

Definition 1.3.1: Prime Numbers

We say that $n \in \mathbb{N}$ is a prime number if and only if it has exactly two factors, which is 1 and n. Else n is composite.

Lemma 1.3.2

Every integer is divisible by a prime.

Proof. If the integer is a prime then it divides itself. If the integer is not a prime then it has some other factor $k < n$ not equal to 1 or n. If k is prime then we are done. If k is not prime then there is another non trivial factor $k_1 < k$. Repeat this process until you reach a prime. This is always possible since the integers are well ordered integers between 1 and n are finite. □

Lemma 1.3.3

Every integer $n > 1$ can be written as a product of primes.

Proof. If n is a prime that we are already done. If n is not a prime then we know that it is divisible by a prime p. Then repeat this procedure on $\frac{n}{p}$ until the remaining integer is a prime. □

Theorem 1.3.4

There is an infinite number of primes.

Proof. Suppose for a contradiction that there is only a finite number of primes $p_1, \ldots, p_n$. Then I claim that $p = p_1, \cdots p_n + 1$ is a prime. □

Proposition 1.3.5: Euclid's Lemma

Suppose that $p, m, n \in \mathbb{N}$, with p prime and $m, n > 1$. Suppose that $p|mn$. Then p divides at least one of m or n.

Proposition 1.3.6

Suppose that p is a prime such that $p|a_1 a_2 \cdots a_k$. Then $p|a_i$ for some $i \in \{1, 2, \ldots, k\}$.

Proof. Treat $a_2 \cdots a_k$ as one integer. By Euclid's lemma, p either divides a_1 or $a_2 \cdots a_k$. If p divides a_1 we are done. If it doesn't then $p|a_2 \cdots a_k$. Repeat this procedure until one of a_i is divisible by p or we reach $p|a_{k-1}a_k$. Then by Euclid's lemma $p|a_{k-1}$ or $p|a_k$ and we are done. □

Proposition 1.3.7

Let $d, m, n \in \mathbb{Z}$. If $\gcd(m, d) = 1$, then $d|mn$ implies $d|n$.

Theorem 1.3.8: Fundamental Theorem of Arithmetic

Suppose that $n \neq 0$ is a natural number. Then there exists exactly one prime factorization for every n, meaning that the decomposition

$$n = \prod_{k=1}^{n} p_k^{s_k}$$

where p_k is prime exists and is unique.

Theorem 1.3.9

Suppose that $m, n \in \mathbb{N}$. Suppose that

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_q^{\beta_q}$$

with $p_1 = 2$, $p_2 = 3$, $p_3 = 5 \ldots$. Without loss of generality $r \leq q$. Then

$$\gcd(m, n) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_q^{\min(\alpha_q, \beta_q)}$$

$$\operatorname{lcm}(m, n) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_q^{\max(\alpha_q, \beta_q)}$$

Proof. This is direct from the definition of $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ and the fact that $p_k^{\min(\alpha_k, \beta_k)} | m$ and n but $p_k^{\min(\alpha_k, \beta_k)+1}$ either does not divide m or n. The proof for $\operatorname{lcm}(m, n)$ is similar. □

Theorem 1.3.10

Suppose that m and n are natural numbers. Then

$$\gcd(m, n) \times \operatorname{lcm}(m, n) = m \times n$$

Proof. Since $\min\{a, b\} \cdot \max\{a, b\} = ab$, from the above theorem, we have that $\gcd(m, n) \times \operatorname{lcm}(m, n) = m \times n$ and we are done. □

2 Congruences

2.1 Modular Arithmetic

Definition 2.1.1: Modulo Notation

We say that $a \in \mathbb{Z}$ is congruent to $b \in \mathbb{Z}$ modulo $n \in \mathbb{N}$ if and only if $m|(a-b)$. We write it as $a \equiv b \pmod{n}$.

Proposition 2.1.2

The congruence relation is an equivalence relation. We denote the equivalence class as

$$\mathbb{Z}/n\mathbb{Z}$$

with elements in it as either $m \in \mathbb{Z}/n\mathbb{Z}$, $[m] \in \mathbb{Z}/n\mathbb{Z}$ or $m + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$.

Proof. The three facts
- (Reflexivity) $a \equiv a \pmod{m}$
- (Symmetry) $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$
- (Transitivity) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$

are obvious to prove. □

Group and ring theory play a very important role in abstract algebra. Abstract algebra is practically invented to investigate properties of integers.

Proposition 2.1.3

Suppose that $a, b, c, d \in \mathbb{Z}$. Then
- (Addition) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$
- (Multiplication) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$

and thus $\mathbb{Z}/n\mathbb{Z}$ form a ring.

Proof. Easy expansion involving rewriting the modulo definition into its divisibility equivalence. □

Proposition 2.1.4

If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$ then

$$a \equiv b \pmod{m}$$

Proof. If $ac \equiv bc \pmod{m}$, then $ac = bc + km$ for some $k \in \mathbb{Z}$. Then $c(a-b) = km$. But m does not divide c so m must divide $a - b$. Thus $a \equiv b \pmod{m}$. □

Proposition 2.1.5

If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = d$ then

$$a \equiv b \pmod{m/d}$$

Proof. If $ac \equiv bc \pmod{m}$, then $ac = bc + km$ for some $k \in \mathbb{Z}$. Then $c(a-b) = km$ and $\frac{c}{d}(a-b) = k\frac{m}{d}$. The same thing happens since $\frac{m}{d}$ does not divide $\frac{c}{d}$ so it must divides $a - b$.

Thus $a \equiv b \pmod{m/d}$ and we are done. □

2.2 Linear Congruences

Lemma 2.2.1

If $\gcd(a, m)$ does not divide b, then

$$ax \equiv b \pmod{m}$$

has no solutions.

Proof. This lemma is equivalent to asking whether

$$ax - my = b$$

has integer solutions, which has no solution according to Bezout's lemma. □

Lemma 2.2.2

If $(a, m) = 1$, then

$$ax \equiv b \pmod{m}$$

has exactly one solution modulo m.

Proof. The question is equivalent to finding integers x, y such that $ax = by + m$ holds. Rewriting this gives $ax - by = m$ which is Bezout's lemma. Thus existence of solution is guaranteed.

We need to show that there are no other solutions modulo m. □

Corollary 2.2.3

Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then a has an inverse modulo m if and only if $\gcd(a, m) = 1$.

Proof. From the above lemma, we know that if $\gcd(a, m) = 1$ then $ax \equiv 1 \pmod{m}$ has exactly one solution thus we are done.

If $ax \equiv 1 \pmod{m}$ has a unique solution, then $ax = 1 + km$ for some $k \in \mathbb{Z}$. This is just rewriting bezout's lemma with $ax - km = 1$ thus we know that this means that $\gcd(a, m) = 1$. □

Lemma 2.2.4

Let $d = (a, m)$. If $d|b$, then

$$ax \equiv b \pmod{m}$$

has exactly d solutions.

Theorem 2.2.5: Chinese Remainder Theorem

Let $m_1, \ldots, m_k \in \mathbb{N}$ be pairwise coprime and let $a_1, \ldots, a_k \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$, unique to modulo $\prod_{i=1}^{k} m_k$ such that

$$x \equiv a_i \pmod{m_i}$$

for $1 \leq i \leq k$. This solution is given by

$$x = \sum_{t=1}^{k} a_t M_t y_t$$

where $M_t = \prod_{j \neq t} m_j$ and $M_t y_t \equiv 1 \pmod{m_t}$. Any other integer z is a solution to the answer as long as $x \equiv z \pmod{m_1 \times \cdots \times m_k}$

Proof. We show that x is indeed congruent to a_i modulo m_i for $1 \leq i \leq k$. Note that for $t \neq i$, m_i is a factor of M_t. Thus for $t \neq i$, $a_t M_t y_t \equiv 0 \pmod{m_i}$. Thus

$$\begin{aligned} x &\equiv \sum_{t=1}^{k} a_t M_t y_t \pmod{m_i} \\ &\equiv a_i M_i y_i \\ &\equiv a_i \end{aligned}$$

Since $M_i y_i \equiv 1 \pmod{m_i}$.

Now we show uniqueness. Suppose that x, y are two solutions, then $x - y$ is divisible by $m_1, \ldots, m_k$. As $m - 1, \ldots, m_k$ are coprime, we have that $m_1 \cdots m_k | x - y$ thus x is in fact congruent to y. □

In practice, you are suppose to find y_i by yourself using the fact that $M_i y_i \equiv 1 \pmod{m_i}$. An algorithm for solving for the system of linear congruences is given as follows:

Step 1: Convert the system of linear congruences $a_i x \equiv b_i \pmod{m_i}$ into the form $x_i \equiv c_i \pmod{m_i}$ by finding the inverse of a_i modulo m_i.
Step 2: Compute $M_t = \frac{1}{m_t} \Pi_{i=1}^{k} m_k$
Step 3: Find y_t from $M_t y_t \equiv 1 (\text{mod } m_i)$
Step 4: Find x from $x = \sum_{t=1}^{k} a_t M_t y_t$

2.3 Multiplicative Functions

Definition 2.3.1: Multiplicative Functions

We say that $f : \mathbb{Z} \to \mathbb{Z}$ is a multiplcative function if $(m, n) = 1$ implies $f(mn) = f(m)f(n)$.

Definition 2.3.2: Sum and Number of Divisors

Let $n \in \mathbb{N}$. Denote

$$d(n) = \sum_{d|n} 1$$

the number of positive divisots of n and

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

the sum of the positive divisors of n.

Theorem 2.3.3

$d(n)$ and $\phi(n)$ are multiplicative. Meaning if $n = \prod_{i=1}^{k} p_i^{r_i}$ is the prime decomposition of

$x \in \mathbb{N}$, then

$$d(n) = \prod_{i=1}^{k} d(p_i^{r_i})$$

and

$$\sigma(n) = \prod_{i=1}^{k} \sigma(p_i^{r_i})$$

Definition 2.3.4: Euler's Totient Function

Let $n \in \mathbb{N}$. Define the euler totient function to be

$$\phi(n) = \sum_{\substack{(d,m)=1 \\ d \leq m}} 1 = |\{k \in \mathbb{N} | \gcd(k,n) = 1, 1 \leq k \leq n\}|$$

the number of positive integers less than or equal to itself that is relatively prime. In particular, $\phi(m)$ is the order of the group $(\mathbb{Z}/m\mathbb{Z})^\times$

It is clear that the order of the group $(\mathbb{Z}/m\mathbb{Z})^\times$ has to exclude all elements in $\mathbb{Z}/m\mathbb{Z}$ that has a multplicative inverse as a ring, which is exactly the elements $k + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ with $\gcd(k,m) = 1$

Theorem 2.3.5: Euler's Theorem

Suppose that $m \geq 1$ and $(a,m) = 1$. Then

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

Proof. Easy proof by considering Lagrange's theorem. □

Lemma 2.3.6

Let p be a prime. Then

$$\phi(p^n) = p^{n-1}(p-1)$$

Proof. $\phi(p) = p - 1$ is trivial since a prime is coprime to all numbers except 1. Let $n \geq 1$, Then the positive integers less than and not coprime with p^n are exactly $p, 2p, 3p, \ldots, p^{n-1}p$. There are p^{n-1} of them. Thus we have that

$$\begin{aligned}\phi(p^n) &= \text{all numbers less than } p^n - \text{ less than and not coprime with } p^n \\ &= p^n - p^{n-1} \\ &= p^{n-1}(p-1)\end{aligned}$$

□

Theorem 2.3.7

$\phi(n)$ is multiplicative. Meaning if $n = \prod_{i=1}^{k} p_i^{r_i}$ is the prime decomposition of $x \in \mathbb{N}$, then

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{r_i})$$

Proof. We appeal to the Chinese Remainder Theorem for Rings. We have that $(p\mathbb{Z})$ and $(q\mathbb{Z})$ are coprime ideals in $\mathbb{Z}$ since $(p\mathbb{Z}) + (q\mathbb{Z}) = (1) = \mathbb{Z}$ from the fact that there exists $x, y \in \mathbb{Z}$ such that $px + qy = 1$ from Bezout's lemma. Notice also that $(p\mathbb{Z}) \cap (q\mathbb{Z}) = (pq\mathbb{Z})$We can thus apply the Chinese Remainder Theorem for Rings and have that

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$$

Now notice that in ring products, $(r, s) \in R \times S$ is a unit if and only if r is a unit in R and s is a unit in S. Thus we have that the number of units in $\mathbb{Z}/pq\mathbb{Z}$ is exactly the product of the number of units in $p\mathbb{Z}$ and the number of units in $q\mathbb{Z}$. Since the number of units in a $\mathbb{Z}/m\mathbb{Z}$ is exactly $\phi(m)$, we are done. □

Corollary 2.3.8

If $n = \prod_{i=1}^{k} p_i^{r_i}$ is the prime decomposition of $x \in \mathbb{N}$, then

$$\phi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Proof. This is direct from the fact that ϕ is multiplicative and that $\phi(p^n) = p^{n-1}(p-1)$. □

Theorem 2.3.9

If $n \geq 1$, then

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

2.4 Special Congruences

Lemma 2.4.1

If $\gcd(a, m) = 1$, then the least residues of $a, 2a, \ldots, (m-1)a$ are

$$1, 2, \ldots, m-1$$

in some order.

Proof. We show that no two residues in the set $\{a, 2a, \ldots, (m-1)a\}$ is congruent to complete the proof. Suppose for a contrary that there exists $1 \leq r, s \leq m-1$ such that $ra \equiv sa \pmod{p}$. Then $(r-s)a \equiv \pmod{p}$ and $\gcd(a, m) = 1$ implies $r \equiv s \pmod{p}$. Thus r and s in fact are the same element in the set $\{a, 2a, \ldots, (m-1)a\}$ and we are done. □

Theorem 2.4.2: Fermat's Theorem

If p is a prime and $\gcd(a, p) = 1$. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof. Using the above lemma, we find that

$$a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot \cdots \cdot (p-1) \pmod{p}$$
$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

Since $(p-1)!$ and p are relatively prime, we can cancel it out to get

$$a^{p-1} \equiv 1 \pmod{p}$$

□

We will see a vast generalization of Fermat's theorem soon involving general modulo instead of primes. It involves the notion of groups.

Lemma 2.4.3

The congruence equation

$$x^2 \equiv 1 \pmod{p}$$

has exactly two solutions, 1 and $p-1$.

Proof. It is easy to check that 1 and $p-1$ are indeed solutions of the congruence equation. Now let r be a solution to the linear congruence. Then

$$(r-1)(r+1) \equiv 0 \pmod{p}$$

Hence either $p|r+1$ or $p|r-1$. This means that either $r \equiv -1 \pmod{p}$ or $r \equiv 1 \pmod{p}$ thus we are done. □

Lemma 2.4.4

Let p be an odd prime. For every $a \in \{1, \dots, p-1\}$, there exists a unique $b \in \{1, \dots, p-1\}$ such that $ab \equiv 1 \pmod{p}$ such that eventually we can pair up the numbers in $\{1, \dots, p-1\}$ so that they are inverses of each other.

Moreover, the only elements with inverse as itself is precisely 1 and $p-1$.

Proof. Notice that since p is a prime, $\gcd(a, p) = 1$ for any a in the set. We have proven that this guarantees an inverse for a that is unique up to modulo p. The above lemma has also shown that $x^2 \equiv 1 \pmod{p}$ precisely have two solutions. □

Theorem 2.4.5: Wilson's Theorem

p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}$$

Proof. From the above lemma, we pair up elements in the set $\{1, \dots, p-1\}$ so that multiplication in the congruence relation gives 1. Then we have that

$$\begin{aligned}(p-1)! &\equiv 1 \cdot 1 \cdot (p-1) \pmod{p} \\ &\equiv -1\end{aligned}$$

Now suppose that $(p-1)! \equiv -1 \pmod{p}$. Suppose for a contradiction that p is not prime. Then $p = ab$ for some $a, b \in \mathbb{N}$ where $a, b < p$. Then since $(p-1)!$ necessarily contains one multiple of a and b, $(p-1)!$ will contain a copy of p in it and thus is divisible by p, a contradiction. □

We will see a proof of similar style when we encounter Euler's Criterion.

Lemma 2.4.6

Let p be prime. Let $1 \leq k < p$ be a positive integer. Then

$$\binom{p}{k} \equiv 0 \pmod{p}$$

Proof. Clear there is a factor of p in $\frac{p!}{k!(p-k)!}$ since p is a prime and p is not contained in $k!$ or $(p-k)!$. □

Notice that the proof goes wrong if we relax the conditions to general numbers instead of prime numbers because divisors of p in this case could lie in $k!$ or $(p-k)!$.

Lemma 2.4.7: Power-Up Lemma

Let p be a prime. Let $k \in \mathbb{N}$. Suppose that $a \equiv b \pmod{p^k}$. Then

$$a^p \equiv b^p \pmod{p^{k+1}}$$

Proof. Suppose that $a = b + cp^k$ for some $c \in \mathbb{Z}$. Then we have that

$$\begin{aligned} a^p &\equiv (b+cp^k)^p \pmod{p^{k+1}} \\ &\equiv \sum_{k=0}^{p} \binom{p}{k} b^k c^{p-k} p^{k(p-k)} \pmod{p^{k+1}} \\ &\equiv b^p \pmod{p^{k+1}} \end{aligned}$$

using the binomial theorem. □

Corollary 2.4.8

Let p an odd prime. Let $k \geq 2$ be an integer. Then

$$(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \pmod{p^k}$$

where $a \in \mathbb{Z}$.

2.5 Order and Primitive Roots

Definition 2.5.1: Order

Let $m \in \mathbb{Z}$ and $a \in \mathbb{Z}$ such that $\gcd(a,m) = 1$. Define the order of a modulo m to be the smallest natural number d such that

$$a^d \equiv 1 \pmod{m}$$

In particular, the order of a modulo m is equivalent to saying the order of $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Theorem 2.5.2

Let $\gcd(a,m) = 1$ and a has order d modulo m. Then $a^n \equiv 1 \pmod{m}$ if and only if $d|n$.

Proof. Suppose that $a^n \equiv 1 \pmod{m}$. By the division algorithm, we have that $n = dq + r$ for

some $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Then

$$\begin{aligned} a^n &\equiv a^{dq+r} \pmod{m} \\ &\equiv (a^d)^q \cdot a^r \pmod{m} \\ &\equiv a^r \pmod{m} \end{aligned}$$

This mean that $a^r \equiv 1 \pmod{m}$ which means $r = 0$ since $r < d$ and d is the order of a.

Now suppose that $d|n$. Then

$$\begin{aligned} a^n &\equiv (a^d)^{n/d} \pmod{m} \\ &\equiv 1 \pmod{m} \end{aligned}$$

Thus we are done. □

Lemma 2.5.3

If $\gcd(a, m) = 1$ and a has order d modulo m, then $d|\phi(m)$.

Proof. Apply Euler's theorem and the above theorem. □

Theorem 2.5.4

If the order of a modulo m is t then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

Proof. Suppose that $a^r \equiv a^s \pmod{m}$. WLOG let $r \geq s$. Then $a^{r-s} \equiv 1 \pmod{m}$ which is true if and only if $r - s$ is a multiple of t. The process can be reversed for the if part. □

Theorem 2.5.5

Let a have order d modulo m. Let $u \in \mathbb{N}$. Then

$$\text{ord}_m(a^k) = \frac{\text{ord}_m(a)}{\gcd(k, \text{ord}_m(a))}$$

Proof. This is proven in groups and rings. □

Definition 2.5.6: Primitive Root

We say that a is a primitive root of m if $(a, m) = 1$ and the order of a modulo m is $\phi(m)$. In particular, a being a primitive root of m is equivalent to saying that a generates $(\mathbb{Z}/m\mathbb{Z})^\times$

Corollary 2.5.7

If p is a prime then there are exactly $\phi(p-1)$ primitive roots modulo p.

Proof. □

Theorem 2.5.8

If g is a primitive root of m, then g^t is a primitive root modulo p if and only if $(t, \phi(m)) = 1$.

Notice that this is a rather strong statement. Once we are successful in finding one primitive root, we will be able to find all other primitive roots.

Proposition 2.5.9

Let $n \in \mathbb{N}$ such that there exists at least one primitive root modulo n. Then the number of primitive roots modulo n is exactly $\phi(\phi(n))$.

Proof. Notice that from the above theorem, g^t is a primitive root modulo p if and only if $\gcd(t, \phi(m)) = 1$. Thus we need to count how many numbers are coprime to $\phi(m)$, which is exactly $\phi(\phi(m))$. □

Theorem 2.5.10

Let p be an odd prime. Then there exists a primitive root $g \in \mathbb{Z}$ modulo p such that g^{p-1} does not equal to 1 congruent to p^2. Moreover, any such g is a primitive root modulo any power of p.

Theorem 2.5.11

Let $m \geq 2$ be an integer. If $m = 2$ or 4 or $m = p^k$ or $m = 2p^k$ for some $k \in \mathbb{N}$ and p and odd prime, then there exists a primitive root modulo p. Otherwise, there isn't.

To show that g is a primitive root of p, we usually use the definition, which is to show that the order of g is $\phi(p)$. And to do this, we consider all factors of $\phi(p)$ and simply show that powers of g of those factors are not the identity.

3 Quadratic Congruences

3.1 Quadratic Residues

Proposition 3.1.1

Let $A, B, C \in \mathbb{Z}$. Solving

$$Ax^2 + Bx + C \equiv 0 \pmod{p}$$

is equivalent to solving $y^2 \equiv a \pmod{m}$ where y is linear to x, given that p is a prime number.

Proof. Take A to be indivisible by p. Else the quadratic congruence deforms into a linear congruence. Then A must have a moduo inverse since p is a prime. Then we can write the congruence as $x^2 + A'Bx + A'C \equiv 0 \pmod{p}$. If $A'B$ is even, we can complete the square and we are done. If $A'B$ is odd, then replace $A'B$ with $p + A'B$ and it is even. □

Definition 3.1.2: Quadratic Residue

If there exists x_0 to be the solution to $x^2 \equiv a \pmod{m}$, then a is said to be a quadratic residue modulo m. If there are no solutions, then a is said to be a quadratic non-residue modulo m

Proposition 3.1.3

Suppose that p is an odd prime. If p does not divide a then $x^2 \equiv a \pmod{m}$ has either two or zero solutions modulo m.

Definition 3.1.4: Legendre Symbol

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre Symbol is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a\text{is a quadratic non-residue modulo } p \end{cases}$$

Theorem 3.1.5: Euler's Criterion

Let p be prime. Let $a \in \mathbb{Z}$ with $p \nmid a$. Then

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

Proof. By Wilson's theorem, we have that $(p-1)! \equiv -1 \pmod{p}$. Thus we just have to prove that

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

First suppose that $\left(\frac{a}{p}\right) = 1$. Let x be the intger that solves this quadratic residue. Notice that

$$\begin{aligned} x(p-x) &\equiv -x^2 \pmod{p} \\ &\equiv -a \pmod{p} \end{aligned}$$

Now also notice that since p does not divide a, for all numbers between 1 and $p-1$ except the x and $p-x$ that solves the quadratic congruence, we can pair them up so that multiplication between the two elements yield a. This means that we have

$$\begin{aligned}(p-1)! &\equiv -a \prod_{\substack{1\leq k\leq p-1\\ k\notin\{x,p-x\}}} k \pmod p\\ &\equiv -a\cdot a^{\frac{p-3}{2}} \pmod p\\ &\equiv -a^{\frac{p-1}{2}} \pmod p\end{aligned}$$

Thus we are done.

Now suppose that $\left(\frac{a}{p}\right)=-1$. Then similar to the above, we get $p-1$ pairs since none are quadratic residues thus

$$(p-1)!\equiv a^{\frac{p-1}{2}} \pmod p$$

Thus we are done. □

This criterion is a powerful statement in the sense that we can know whether a is a quadratic residue of p by direct computation.

Proposition 3.1.6

Let p be an odd prime. Let $a,b\in\mathbb{Z}$. Then

- If $a\equiv b \pmod p$, then $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$
- $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Corollary 3.1.7

Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right)=\begin{cases}-1 & \text{if } p\equiv 3 \pmod 4\\ 1 & \text{if } p\equiv 1 \pmod 4\end{cases}$$

Proof. A simple application of Euler's criterion. □

Proposition 3.1.8: Gauss's Lemma

Let p be an odd prime. Let a be an integer such that $\gcd(a,p)=1$. Consider the integers $a,2a,3a,\ldots,\frac{p-1}{2}a$ and their least positive residues modulo p. Let n be the number of these residues that are greater than $\frac{p}{2}$. Then

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

Proof. Define a set $P_1=\{1,\ldots,\frac{p-1}{2}\}$ and $P_2=\{\frac{p+1}{2},\ldots,p-1\}=\{\frac{1-p}{2},\ldots,-1\}$. We only consider modulo relations thus they are equivalent sets. Let $k_1,k_2\in P_1$ be distinct. Notice that $1\leq k_1+k_2\leq p-1$. Without loss of generality take $k_1>k_2$. Then since p does not divide k_1+k_2 and k_1-k_2, and that p does not divide a, then p does not divide $k_1a\pm k_2a$ by Euclid's lemma.

Since this is true for arbitrary k_1, k_2, taking modulo p for general ka for $k \in P_1$ will allow ka to lie within the set $P_1 \cup P_2$. Also notice that taking distinct elements for k will result in a distinct modulo. Suppose that among these k, m of them fall into P_1 and n of them fall into P_2. Say they fall into $A \subset P_1$ and $B \subset P_2$ respectively (Observe that $P_1 \cap P_2 = \emptyset$ implies $A \cap B = \emptyset$, also $A \cup B = P_1$). Recalling that P_2 has two equivalent definitions, we have

$$\begin{aligned}\prod_{k=1}^{\frac{p-1}{2}}(ka) &\equiv \left(\prod_{\substack{1\leq k\leq \frac{p-1}{2}\\ k\in A}} k\right) \times \left((-1)^n \prod_{\substack{1\leq k\leq \frac{p-1}{2}\\ k\in B}} k\right) \pmod p \\ &\equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} \pmod p\end{aligned}$$

and also

$$\prod_{k=1}^{\frac{p-1}{2}}(ka) \equiv a^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \pmod p$$

Finally, notice that the product is invertible modulo p, thus we can cancel it on both sides to get

$$(-1)^n \equiv a^{\frac{p-1}{2}} \pmod p$$

and we are done. □

Lemma 3.1.9

Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \pmod 8 \\ 1 & \text{if } p \equiv \pm 1 \pmod 8 \end{cases}$$

Proof. We apply Gauss's lemma direct by counting the number of elements in $\{2, 4, \ldots, p-1\}$ that upon taking modulo p, ends in the set $\{\frac{p+1}{2}, \ldots, p-1\}$. But these are precisely the elements $\frac{p+1}{2}, \ldots, p-1$, which has $\lfloor \frac{p+1}{4} \rfloor$ elements. The result follows immediately. □

Theorem 3.1.10: The Quadratic Reciprocity Theorem

Let $p \neq q$ be odd primes. Then

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right) & \text{otherwise} \end{cases}$$

3.2 Primitive Roots and Quadratic Residues

Proposition 3.2.1

Let p be a prime. If g is a primitive root modulo p then g is a quadratic non-resuidue of p.

Proof. Trivially if there exists x such that $x^2 \equiv g \pmod p$, then since the order of x divides $\phi(p)$, the order of g divides $\frac{\phi(p)}{2}$. But the order of a primitive root must be $\phi(p)$. □

Definition 3.2.2: Fermat Primes

We say that n is a Fermat prime if n is prime and $n = 2^{2^k} + 1$ for some $k \in \mathbb{N}$.

Theorem 3.2.3

If p is a Fermat prime then g is a primitive root modulo p if and only if g is a quadratic non-residue of p.

4 Diophantine Equations

4.1 Introduction to Diophantine Equations

Definition 4.1.1: Diophantine Equations

Diophantine Equations are polynomial equations in two or more unknowns with integer coefficients, where we only consider integer solutions.

We will consider diophantine equations of the form:

$z = x^2 + y^2$ and the cases with three squares and four squares.
$z^2 = x^2 + y^2$ the pythagoreas triples.
$ax^2 + by^2 = cz^2$ which is ternary quadratic equations.

4.2 Lattices

Definition 4.2.1: Lattice

Let $n \in \mathbb{N} \setminus \{0\}$. We say that Λ is a lattice in $\mathbb{R}^n$ if

$$\Lambda = \left\{ \sum_{k=1}^{n} a_k v_k \middle| v_k \in \mathbb{Z} \right\}$$

where $v_1, \ldots, v_n$ are linearly independet vectors. In this case, we say that $v_1, \ldots, v_n$ forms a basis for Λ.

Theorem 4.2.2: Minkowski's Theorem

Let Λ be a lattice in $\mathbb{R}^n$. Let $S \subseteq \mathbb{R}^n$ be a symmetric, convex set whose volumes exceeds $2^n \det(\Lambda)$. Then S contains a non-zero lattice point.

Corollary 4.2.3: Strong Minkowski's Theorem

Let Λ be a lattice in $\mathbb{R}^n$. Let $S \subseteq \mathbb{R}^n$ be a symmetric, convex, compact set whose volumes is greater than or equal to $2^n \det(\Lambda)$. Then S contains a non-zero lattice point.

4.3 Sum of Squares

We discuss numbers that can be written as a sum of two squares, in other words, solving the diophantine equation $z = x^2 + y^2$.

Theorem 4.3.1

Let $p \equiv 1 \pmod 4$ be prime. Then p is a sum of two squares.

Proof. We know that -1 is a quadratic residue of p. So let m be an integer such that $m^2 \equiv -1 \pmod p$. Define a lattice by $\Lambda = \text{span}\{(1, m), (0, p)\}$. Consider another set

$$S = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 < 2p\}$$

Clearly S is symmetric and convex. It also has volume $2\pi p$ thus is larger than 2^2 times the volume of Λ which is $\det(\Lambda) = p$. By Minkowski's theorem, there exists $(x, y) = a(1, m) + b(0, p) \in \Lambda$ for some a, b such that $(x, y) \in S$ which is nonzero.

Since

$$\begin{aligned} x^2 + y^2 &\equiv a^2 + a^2m^2 \pmod{p} \\ &\equiv a^2(1 + m^2) \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Since $x^2 + y^2 < 2p$, naturall we have $x^2 + y^2 = p$. □

Lemma 4.3.2

If $a, b \in \mathbb{N}$ are each sum of two squares, then so is ab.

Proof. A simple proof involving algebraic manipulations. □

Lemma 4.3.3

Let $x, y \in \mathbb{Z}$ and suppose a prime $p \equiv 3 \pmod{4}$ divides $x^2 + y^2$. Then $p|x$ and $p|y$.

Corollary 4.3.4

If $n \in \mathbb{N}$ is a sum of two squares and $p \equiv 3 \pmod{4}$ is a prime divisor of n, then $p^2|n$ and $\frac{n}{p^2}$ is a sum of two squares.

Theorem 4.3.5: Two Square Theorem

Let $n \in \mathbb{N}$. Then n can be expressed as a sum of two squares if and only if for every prime

$$p \equiv 3 \pmod{4}$$

in the prime decomposition of n, p has an even power in the factorization.

We turn to discuss diophnatine equations of the form $w = x^2 + y^2 + z^2$

Theorem 4.3.6: Three Square Theorem

A positive integer is a sum of three squares if and only if its not of the form $4^a(8b+7)$ where $a, b \in \mathbb{N} \cup \{0\}$.

Finally we also consider the case with four squares.

Lemma 4.3.7

If $a, b \in \mathbb{N}$ are each sum of four squares, then so is ab.

Proof. A matter of algebra manipulation. □

Theorem 4.3.8: Lagrange's Four Square Theorem

Any positive integer is a sum of four squares.

Proof. By the above lemma and the fact that $2 = 1^2 + 1^2 + 0 + 0$, we just have to show that any odd prime has a decomposition into a sum of four squares. Let p be an odd prime. We show that there exists $x^2 + y^2 + w^2 + z^2$ divisible by p and lies between $(0, 2p)$, which

completes the proof.

Define two sets $A = \{a^2 | a \in \mathbb{Z}/p\mathbb{Z}\}$ and $B = \{-(1+b^2) | b \in \mathbb{Z}/p\mathbb{Z}\}$. They each have cardinality $\frac{p-1}{2}$ and thus must intersect at say $a_0 \in A$ and $-(1+b_0^2) \in B$. Then we have the modulo equation

$$a^2 + b^2 \equiv -1 \pmod{p}$$

Now define

$$\Lambda = \{(x, y, w, z) \in \mathbb{Z}^4 | z \equiv ax + by \pmod{p} \text{ and } w \equiv ay - bx \pmod{p}\}$$

Then

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 &\equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \pmod{p} \\ &\equiv x^2 + y^2 + (a^2 + b^2)x^2 + (a^2 + b^2)y^2 \pmod{p} \\ &\equiv (a^2 + b^2 + 1)(x^2 + y^2) \pmod{p} \\ &\equiv (a^2 + b^2 + 1)(x^2 + y^2) \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

We now show that Λ can be applied the Minkowski theorem (The symmetric convex set is defined below). Notice that

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ a \\ -b \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ b \\ a \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ p \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ p \end{pmatrix} \right\}$$

forms a basis for the lattice Λ, and that $\det(\Lambda) = p^2$. Now

$$D = \{(x, y, z, w) \in \mathbb{R}^4 | x^2 + y^2 + z^2 + w^2 < 2p\}$$

is symmetric and convex. It also has volume

$$\frac{\pi^2}{2}(\sqrt{2p})^4 = 2\pi^2 p^2 > 2^4 \det(\Lambda) = 2^4 p^2$$

Applying Minkowski's theorem gives a nonzero element of Λ thus we are done. □

In general, to find out the sum of four squares of a natural number, we first try and find the biggest square contained in the number, then try and find a three or two square decomposition. If it does not work, try the second biggest square and vice versa.

4.4 Gaussian Integers

We study the ring of Gaussian integers here, which is actually a type of field extension. We attempt to classify all primes in the ring of Gaussian Integers.

Definition 4.4.1: Gaussian Integers

Define the ring of Gaussian integers to be

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

Define the norm of $z = a + bi \in \mathbb{Z}[i]$ to be $N(z) = a^2 + b^2$.

Notice that $\mathbb{Z} \leq \mathbb{Z}[i]$. In fact, the Guassian integers are simply complex numbers with integer coefficients. We are trying to extend the notion of divisibility and prime numbers to an algebraically complete field. Moreover, by the definition of norm, we are in fact discussing equations of the form $x^2 + y^2 = z$.

Proposition 4.4.2

The ring of Gaussian integers is a Euclidean domain, and thus is also a PID and UFD.

Recall that we have the notion of division in a commutative ring. As ina analysis, we have defined the notion of distance in the complex numbers.

Definition 4.4.3: Gaussian Primes

We say that $z \in \mathbb{Z}[i]$ is a Gaussian prime if $z \neq 0$, z is not a unit and that for any $x, y \in \mathbb{Z}[i]$ such that $z|xy$, then either $z|x$ or $z|y$.

This is precisely the definition of a prime or irreducible element in integral domains.

Proposition 4.4.4

Let $z \in \mathbb{Z}[i]$ be a Gaussian prime. Then any unit multiple of z is also a Gaussian prime, as well as $\overline{z}$

Lemma 4.4.5

Let $z \in \mathbb{Z}[i]$ and $N(z)$ is a prime number in $\mathbb{Z}$. Then z is a Gaussian prime.

Theorem 4.4.6

Let $z \in \mathbb{Z}[i]$. Then z is a Gaussian prime if and only if z is in one of the following forms:

- $1 + i$
- p is a prime in $\mathbb{Z}$ such that $p \equiv 3 \pmod 4$
- $N(z)$ is a prime in $\mathbb{Z}$ such that $N(z) \equiv 1 \pmod 4$
- Any unit multple of the above

Below gives a list of ways to detect whether p is a prime for $z \in \mathbb{Z}[i]$.

Proposition 4.4.7

Let $z \in \mathbb{Z}[i]$. Let $p \in \mathbb{Z}$ be a prime divisor of $N(z)$.

- If $p = 2$ then $1 + i|z$
- If $p \equiv 3 \pmod 4$ then $p|z$
- If $p = x^2 + y^2$ with $x, y \in \mathbb{Z}$ then either $x + yi$ or $x - yi$ divides z

4.5 Pythagorean Triples

Definition 4.5.1: Pythagorean Triples

A pythagorean triple is a solution $(x, y, z) \in (\mathbb{N} \setminus \{0\})^3$ such that $x^2 + y^2 = z^2$. A pythagorean triple is said to be primitive if $\gcd(x, y, z) = 1$.

Lemma 4.5.2

Exactly one of x, y, z in a pythagorean triple is even.

Proof. Obviously all three cannot be odd numbers at the same time. If they both are even then by taking modulo 2 we see that $0 \equiv 1 \pmod 2$ which is a contradiction. □

Lemma 4.5.3

If x, y, z is a pythagorean triple then z is odd.

Proof. For odd or even x, y such that not both are even, $x^2 + y^2 \equiv 1 \pmod 2$. □

Lemma 4.5.4

Let $r, s, t \in \mathbb{N}$ such that $r^2 = st$. If $\gcd(s, t) = 1$, then s, t are both perfect squares.

Proof. Result is clear from the fact that s and t have no common prime numbers in their decomposition, and that every prime in the prime decomposition of r^2 must have an even number of power. □

Theorem 4.5.5

Let $(x, y, z) \in (\mathbb{N} \setminus \{0\})^3$. Then (x, y, z) is a pythagorean triple if and only if $x = u^2 - v^2$, $y = 2uv$ and $z = u^2 + v^2$ for some coprime $u, v \in \mathbb{N} \setminus \{0\}$ such that at least one of u, v is even and that $u > v$.

Proof. Suppose that (x, y, z) is a pythagorean triple with y even. Since y is even, $y = 2r$ for some $r \in \mathbb{N}$. Thus $y^2 = 4r^2$. From $y^2 = z^2 - x^2$, we have that $4r^2 = (z + x)(z - x)$. Since x, z are both odd, $z + x$ and $z - x$ are both even. Thus $z + x = 2s$ and $z - x = 2t$ for some $s, t \in \mathbb{N}$. Solving the the system gives $z = s + t$ and $x = s - t$. Now we have that $4r^2 = 4st$ thus $r^2 = st$.

I claim that s and t here are relatively prime. Suppose for a contradiction that there exists $d \in \mathbb{N}$ such that $d|s$ and $d|t$. From the system of equations, we see that $d|z$ and $d|x$. But we already assumed that x, y, z are relatively prime. Thus the contradiction arises. Now we can apply the above lemma to see that $s = u^2$ and $t = v^2$ for some $u, v \in \mathbb{N}$. Thus $y = \sqrt{4r^2} = \sqrt{4st} = 2uv$. From the system of equations we also have that $z = u^2 + v^2$ and $x = u^2 - v^2$ and we are done.

The only if part is simple in substituting the expressions and seeing that they are indeed equal. It remains to show that u and v are coprime. □

Theorem 4.5.6

The equation $x^4 + y^4 = z^2$ has no solutions over $\mathbb{N} \setminus \{0\}$.

Proof. Notice that this equation is just $(x^2)^2 + (y^2)^2 = z^2$ which is just a question of pythagorean triples. Suppose that x^2, y^2, z is a primitive pythagorean triple that satisfies the equation. By the solution of pythagorean triples, there exists coprime u, v with $u > v$ such that $x^2 = u^2 - v^2$, $y = 2uv$, $z^2 = u^2 + v^2$.

I claim that in fact u must be odd and v even. Because if this was the case, then $x^2 = u^2 - v^2 \equiv -1 \pmod 4$ which is impossible. Rearranging this equation gives $x^2 + v^2 = u^2$, which is another pythagorean triple. So using the solution gives a pair (m, n) such that $x = m^2 - n^2$, $v = 2mn$, $u = m^2 + n^2$.

Now since $y^2 = 2uv$ where u, v are coprime and u is odd, we can deduce that u is a square and v is twice a square, say $u = r^2$ and $v = 2s^2$. Thus we can rewrite equations for u, v as $2s^2 = 2mn$ and $r^2 = m^2 + n^2$. Finally, since $2s^2 = 2mn$ and m, n coprime, they must both be

squares as well, say $m = M^2$ and $n = N^2$. Thus M, N, r is yet another triple satisfying $M^4 + N^4 = r^2$. This complete the infinite descent and we are done. □

We give partial solutions to the general equation $x^n + y^n = z^n$.

Corollary 4.5.7

If n is a multiple of 4 then then the equation $x^n + y^n = z^n$ has no solution over $\mathbb{N} \setminus \{0\}$.

Proof. Take $n = 4k$, then $x^n + y^n = z^n$ is just $(x^k)^4 + (y^k)^4 = (z^{2k})^2$ which is the theorem above in disguise. □

Theorem 4.5.8

Let p be an odd prime such that $q = 2p + 1$ is prime. Then the equation

$$x^p + y^p = z^p$$

has no integer solutions for which p does not divide xyz.

Theorem 4.5.9

Let p be an odd prime. Assume that there exists $x, y, z \in \mathbb{Z}$ such that

$$x^p + y^p + z^p = 0$$

where x, y, z each is indivisble by p. Then

$$2^{p-1} \equiv 1 \pmod{p^2}$$

4.6 Ternary Quadratic Equation

Definition 4.6.1: Squarefree

We say that a number is squarefree if it is not a square of an integer.

Theorem 4.6.2

Let $a, b, c \in \mathbb{N} \setminus \{0\}$ be squarefree and pairwise coprime. Then the equation

$$ax^2 + by^2 = cz^2$$

has a non-trivial integer solution if and only if

- bc is a quadratic residue modulo a
- ac is a quadratic residue modulo b
- $-ab$ is a quadratic residue modulo c

Proof. Firstly suppose that (x, y, z) is a non-trivial solution to $ax^2 + by^2 = cz^2$ that is coprime. Multiplying by c gives

$$acx^2 + bcy^2 = (cz)^2$$

Taking modulo a gives

$$bcy^2 \equiv (cz)^2 \pmod{4}$$

I claim that $\gcd(a, y) = 1$. Indeed suppose for a contradiction that $p|a$ and $p|y$. Then $p|cz^2$. Since $\gcd(a, c) = 1$ we must have $p|z$, which is a contradiction. Thus $\gcd(a, y) = 1$. This

means that we can take the inverse of y modulo a and get

$$bc \equiv (y^{-1}cz)^2 \pmod{a}$$

Similarly, the other quadratic resdiues are proven in the same way.

Now for the other direction, we use the strong form of Minkwoski's theorem. Let $r, s, t \in \mathbb{Z}$ solve the quadratic congruences for bc, ac and $-ab$ respectively. Suppose that

$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 | by \equiv rz \pmod{a}, cz \equiv sx \pmod{b}, ax \equiv ty \pmod{c}\}$$

Then we must have

$$bry \equiv r^2 z \equiv bcz \pmod{a}$$

Thus as $\gcd(a, b) = 1$ we have $ry \equiv cz \pmod{a}$. Thus

$$\begin{aligned} ax^2 + by^2 - cz^2 \equiv by^2 - cz^2 \equiv & \pmod{a} \\ \equiv rzy - cz^2 & \pmod{a} \\ \equiv z(ry - cz) & \pmod{a} \\ \equiv 0 & \pmod{a} \end{aligned}$$

Similarly, we can show that $ax^2 + by^2 - cz^2$ is divisible by b and c. As a, b, c are pariwise coprime, we must have

$$ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}$$

Thus we can write the congruences in Λ into

$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 | z \equiv r_a^{-1} by \pmod{a}, z \equiv c_b^{-1} sx \pmod{b}, x \equiv a_c^{-1} ty \pmod{c}\}$$

where r_a^{-1} denotes the inverse of r modulo a and so on.

By the CRT, we can write the congruences into $y \equiv \nu x \pmod{c}$ and thus

$$z \equiv \tau x + \rho y \pmod{ab}$$

for some $\nu, \tau, \rho \in \mathbb{Z}$. Now, □

4.7 Waring's Problem

Definition 4.7.1: Warring's Problem

Let $k \in \mathbb{N}$. Consider the equation

$$n = \sum_{i=1}^{s} x_i^k$$

for any $n \in \mathbb{N}$. Warring's problem consists of finding $g(k)$, the least $s \in \mathbb{N}$ for which any $n \in \mathbb{N}$ can be expressed as a sum of s powers of k.