Number Theory

2018A7PS0193P

April 6, 2021

Contents

Chapter 1

Fundamentals

1.1 Notation

For the rest of this course, the following notation will be followed:

1. $\mathbb{N}$ is the set of natural numbers
2. $\mathbb{Z}$ is the set of integers
3. $\mathbb{W}$ is the set of whole numbers, i.e. $\mathbb{W} = \mathbb{N} \cup \{0\}$

1.2 Induction

Often in number theory, we use inductive proofs to prove our arguments. Induction consists of the following steps:

1. Define an induction hypothesis $P(k)$
2. Verify it works for some base case $k = b$. It is possible multiple base cases need to be verified.
3. Assuming $P(k)$ is true, show that it implies that $P(k+1)$ is true

Remember that $P(k)$ is a statement, not a function. You cannot multiply it by some constant or perform any operations on it.

In weak induction (like in the steps given above), we only assume that $P(k)$ is true. However in strong induction, we assume that $P(i)$ is true $\forall i \in [b, k]$, and use this to prove that $P(k+1)$ is true.

Exercise. Prove that the principle of strong induction is true given that the principle of weak induction is true.

Solution. Let us assume that $P(1), ..., P(b)$ is true. If $P(1), ..., P(k)$ are true for some $k \geq b$, then $P(k+1)$ is true. Then, we must show that $P(n)$ is true for all $n \geq 1$.

Let $Q(n)$ be the statement that $P(1), ...P(n)$ are true. Of course, in the base case, $Q(1)$ is true. Let $Q(k)$ be true, where $K \geq 1$. This means that $P(1), ...P(k)$ is true, so $P(k+1)$ must be true. Hence, $Q(k+1)$ is true.

So, by Weak induction, $Q(n)$ is true $\forall n \geq 1$, which implies that $P(n)$ is true $\forall n \geq 1$. ■

1.3 Well Ordering Principle

Theorem 1.1 (Well Ordering Principle)**.** Every non empty set of non-negative integers has a least element.

This is not true about negative integers - consider the case of infinite sets, like the set of all integers. There is no well defined least element.

Lemma 1.2. The well ordering principle is equivalent to the principle of mathematical induction.

Proof. First, let us prove that WOP $\Rightarrow$ PMI. Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$. Suppose that:

- $P(1)$ is true
- $P(k)$ is true implies $P(k+1)$ is true for all $k \in N$.

We have to show that $P(n)$ is true for all $n \in N$. Let :

$$S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$$

This means we must show that $S = \mathbb{N}$. Let $T := \mathbb{N} \backslash S$, i.e. T is the complement. Let as assume that $S \neq \mathbb{N}$.

By WOP, T has a least element, say m. Note that $m \geq 2$ since $1 \in S$. Then, $m - 1 \notin T$ and $m - 1 \in S$. As such, $P(m-1)$ must be true! However, by our initial assumptions, that would mean $P(m)$ is true as well, so $m \in S$. This creates a contradiction, since $m \in T$. Hence, $S = \mathbb{N}$.

Now, let us prove that PMI $\Rightarrow$ WOP.

Consider the statement $P(n)$ that every non empty set of non-negative integers of size n has a least element. It is clear that the base case $P(1)$ is true. Now, let us assume that $P(k)$ is true - what can we say about $P(k+1)$. When we insert an element, we have two cases:

1. The inserted element is less than the least element. In this case, there is a new least element, and $P(k+1)$ is true.
2. The inserted element is not less than the least element. In this case, the least element is the same, and $P(k+1)$ is true.

Hence, by PMI, we can say that $P(n)$ is true $\forall n \in N$, i.e., WOP is true.

Since PMI $\Rightarrow$ WOP and WOP $\Rightarrow$ PMI, PMI $\Leftrightarrow$ WOP. □

1.4 Binomial Theorem

Theorem 1.3 (Binomial Theorem)**.** Let $x, y \in \mathbb{C}$ and let $n \in \mathbb{N}$, then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Corollary 1.3.1.

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Lemma 1.4 (Pascal's Identity)**.**

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Lemma 1.5.

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} = F_n$$

1.5 Pigeonhole Principle

Theorem 1.6. If n items are put into m containers, with $n > m$, then at least one container must contain more than one item.

Chapter 2

Division

2.1 Division Algorithm

Theorem 2.1. Let $a, b \in \mathbb{Z}$ with $b > 0$. Then, there exist unique integers q and r such that $a = bq + r$, $r \in [0, b)$.

Proof. Let $S = \{a - bn : n \in Z, a - bn \geq 0\}$. This set is always non-empty:

- If $a \geq 0$, then $a \in S$
- If $a < 0$, then if $n = a$, we have $a - ab \in S$ since $b \geq 1$.

By WOP, S has a least element, say r. So, there exists $q \in Z$ such that $r = a - bq$. Since $r \in S$, we have $r \geq 0$.

Suppose $r \geq b$. Then:

$$a - b(q+1) = a - bq - b = r - b \geq 0$$

$$\Rightarrow a - b(q+1) \in S$$

$$\Rightarrow r - b \in S$$

However, $r - b < r$, and r is the least element! This gives us a contradiction. So, $r < b$.

As such, we have proved the existence of this solution. Now we must prove it's uniqueness.

Suppose there exists p, r, q', r', such that:

$$a = bq + r, 0 \leq r < b$$

$$a = bq' + r', 0 \leq r' < b$$

Assume WLOG $q \geq q'$. Now,

$$r' - r = b(q - q')$$

If $q > q'$, then $r' - r \geq b$. However, $r' - r < b$. So, this is a contradiction, and $q' = q$. The solution must be unique.

□

Definition 1. If $a, b \in \mathbb{Z}$, we say that a divides b if $b = ak$ for some $k \in \mathbb{Z}$. This is denoted by $a|b$

Some properties of division are:

- If $a|b$, then $\pm a| \pm b$
- If $a|b$ and $b|c$ then $a|c$ (Transitivity)
- If $a|b$ and $a|c$ then $a|bx + cy$ (Linear Combination)
- If $a|b$ and $b \neq 0$, then $|a| \leq |b|$ (Bounds by divisibility)
- $a|b$ and $b|a$, then $b = \pm a$.

Exercise. Prove that $x^a - 1|x^b - 1 \Leftrightarrow a|b$.

Solution. First, let us prove that if $a|b$, then $x^a - 1|x^b - 1$. Let $b = qa$. Then,

$$x^b - 1 = (x^a)^q - 1^q = (x^a - 1)((x^a)^{q-1} + \cdots + x^a + 1)$$

So, $x^b - 1|x^a - 1$. Now to prove the converse. Let $b = aq + r$. Assume $a \nmid b$, then $0 < r < a$. Then,

$$x^b - 1 = x^b - x^r + x^r - 1 = x^r(x^{aq} - 1) + x^r - 1$$

$x^a - 1|x^{qa} - 1$, so $x^r - 1$ is the remainder. Since $r < a$, $x^a - 1 \nmid x^r - 1$. This would mean that $x^a - 1 \nmid x^b - 1$, which is a contradiction. So, $r = 0$. Hence proved. ■

2.2 Base b representations

Theorem 2.2. Let $b \in \mathbb{N}$ with $b \geq 2$. Then every positive integer can be expressed uniquely as

$$N = a_k b^k + ... + a_1 b + a_0$$

where $k \geq 0, a_k \neq 0$ and $0 \leq a_i < b$ for $i = 0, ...k$. This is denoted by $N = (a_k, ...a_1 a_0)_b$

Proof. By the division algorithm, there exist unique integers q_0 and a_0 such that:

$$N = q_0 b + a_0, a_0 \in [0, b)$$

Note that $q_0 < N$. If $q_0 \neq 0$ we apply the division algorithm again to find unique integers q_1 and a_q such that:

$$q_0 = q_1 b + a_1, a_1 \in [0, b)$$

Then,

$$N = (q_1 b + a_1)b + a_0 = q_1 b^2 + a_1 b + a_0$$

We continue till we get a quotient $q_k = 0$. This will terminate since $q_k < ... < q_2 < q_1 < q_0 < N$, forming a decreasing sequence of non-negative integers and eventually reaching zero. From this, we get:

$$N = a_k b^k + ... + a_1 b + a_0$$

Hence, the solution always exists.

Suppose N has two distinct expansions. We can write it as:

$$\begin{aligned} N &= a_k b^k + ... + a_1 b + a_0 \\ &= c_k b^k + ... + c_1 b + c_0 \end{aligned}$$

where $0 \leq a_i, c_j < b$ for all i, j. Let $d_i = a_i - c_i$. Then, $\sum_{i=0}^{k} d_i b^i = 0$. The d_i cannot all be zero as the two expansions are assumed distinct. Let j be the least integer, $0 \leq j \leq k$, such that $d_j \neq 0$. Then, $\sum_{i=j}^{k} d_i b^i = 0$. Dividing by b^j, we find that $\sum_{i=j}^{k} d_i b^{i-j} = 0$. Thus,

$$d_j + b \left(\sum_{i=j+1}^{k} d_i b^{i-j-1} \right) = 0$$

This implies that the $b|d_j$ and since $d_j \neq 0$, we get that $b = |b| \leq |d_j|$. However, $|d_j| < b$. Hence, we have a contradiction, and the two expansions cannot be distinct. Hence, the solution is also always unique. □

Lemma 2.3. If $N = (a_k...a_1a_0)_b$, then:

$$bN = (a_k...a_1a_00)_b$$

$$\left\lfloor \frac{N}{b} \right\rfloor = (a_k...a_1)_b$$

This is a trivial result, which can be thought of as a left or right bitwise shift.

Lemma 2.4 (Particular case of Legendre's formula)**.** Let $n \in \mathbb{N}$ and let e denote the highest power of 2 dividing $n!$. Then

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$$

This is always a finite sum. This can alternatively expressed as, if $n = (a_k...a_1a_0)_2$, then:

$$e = n - (a_k + ... + a_1 + a_0)$$

Proof. It is clear that e is the sum of the no. of positive multiples of 2^i which are $\leq n$, for all i. So, this can be calculated by:

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$$

□

Thus, if r denotes the number of ones in the binary expansion of n, then 2^{n-r} is the highest power of 2 dividing $n!$. Further,

- $2^n \nmid n!$ for $n \in \mathbb{N}$
- $2^{n-1}|n!$ if and only if n is a power of 2.

Chapter 3

Properties of Numbers

3.1 Prime and Composite Numbers

Definition 2. A positive integer $p > 1$ is called prime if its only positive divisors are 1 and p. A positive integer which is not prime is called composite.

The number 1 is neither prime nor composite.

Lemma 3.1. Every integer $n \geq 2$ has a prime factor.

Proof. Let $P(n)$ be the statement that n has a prime factor. Then $P(2)$ is true, since 2 is a prime factor of 2. Let $k \geq 2$. Assume $P(2)...P(k)$ are true.

If $k+1$ is prime, then $k+1$ is a prime factor of itself. So $P(k+1)$ is true.

If $k+1$ is composite, then there exists $d \in [2, k]$ such that $d|k+1$. By the induction hypothesis, d has a prime factor p. Since $p|d$ and $d|k+1$, $p|k+1$. So p is a prime factor of $k+1$, and $P(k+1)$ is true. By PSI, $P(n)$ is true for all $n \geq 2$. □

Theorem 3.2 (Euclid)**.** There are infinitely many primes.

Proof. Suppose there are finitely many primes $p_1, ..., p_k$. Let

$$N = p_1...p_k + 1$$

Since $N \geq 2$, it must have a prime factor. Hence, there exists $i \in [1, k]$ such that $p_i|N$. Since $p_i|N$ and $p_i|p_1p_2...p_k$, we get that $p_i|N - p_1p_2...p_k$, i.e., $p_i|1$. However, $p_i \geq 2$, which gives us a contradiction. So, there must be infinitely many primes. □

Exercise. For $n \geq 1$, let p_n be the nth prime. Prove that

$$p_n \leq 2^{2^{n-1}}$$

Solution. Let $P(n)$ be the statement that $p_n \leq 2^{2^{n-1}}$. It is clear that this is true for the base case $P(1)$. Let us assume that $P(1), ..., P(k)$ is true for $k \geq 1$. We observed in Euclid's proof that $p_1...p_k + 1$ is not divisible by any of $p_1...p_k$. Hence if p_i denotes a prime factor of $p_1...p_k + 1$, then $i \geq k+1$.

$$p_{k+1} \leq p_i \leq p_1...p_k + 1$$

Using the inductive hypothesis, we find that

$$\begin{aligned} p_{k+1} &\leq p_1...p_k + 1 \leq 2.2^2.2^{2^2}...2^{2^{k-1}} + 1 \\ &= 2^{\sum_{j=0}^{k-1} 2^j} + 1 = 2^{2^k - 1} + 1 \leq 2^{2^k} \end{aligned}$$

So, $P(k+1)$ is true. So, by PSI, the result has been proven. ■

Exercise. Prove that there are infinitely many primes of the form $6n+5$.

Solution. Suppose that there are finitely many primes of the form $6n+5$, called $p_1, \cdots pp_n$. Consider $q = 6p_1 \cdots p_n + 5$.

For our first case, consider that q is a prime. This would mean there is a new prime of the form $6n+5$, which would be a contradiction.

Now consider that q is a composite number. All odd primes besides 3 are of the form $6n+1$ or $6n+5$. We can prove (by checking) that the product of two numbers of the form $6n+1$ will only be of the form $6n+1$. Hence, at least one of the prime factors of q must be of the form $6n+5$. However, the primes p_i cannot divide q. Hence, this is a contradiction, since there must be a new prime. ■

Definition 3. The product of the first n prime numbers is called the n^{th} primorial and is denoted by $p_n\#$.

Definition 4. Euclid numbers are integers of the form $E_n = p_n\# + 1$.

All Euclid numbers are not primes - E_6 is not a prime!

Theorem 3.3. Every composite number n has a prime factor $\leq \lfloor \sqrt{n} \rfloor$

Proof. Since n is composite, there exists integers $k, l \in (1, n)$ such that

$$n = kl$$

If $k > \sqrt{n}$ and $l > \sqrt{n}$ then $kl > n$, which is false. So, one of them must be less than or equal to $\sqrt{n}$. □

So, if $n > 1$ has no prime factors $\leq \lfloor \sqrt{n} \rfloor$, then n is prime. We can use this as a test of primality.

It is faster to do this using the Sieve of Eratosthenes. Using this, we can test primality of the first n integers in $O(n \log \log n)$ instead of $O(n\sqrt{n})$. This is a pretty well known algorithm so it's left to the reader to see it on cp-algorithms.

Theorem 3.4. There is no non-constant polynomial $f(x)$ with integer coefficients such that $f(n)$ is prime for all integer n.

Proof. Suppose such a polynomial $f(x)$ exists:

$$f(x) = a_k x^k + ... + a_1 x + a_0, k \geq 1, a_k \neq 0$$

Let $b \in \mathbb{Z}$. Then $f(b)$ is a prime number, say p. Let $t \in \mathbb{Z}$. We have:

$$\begin{aligned} f(b + tp) &= a_k(b + tp)^k + ... + a_1(b + tp) + a_0 \\ &= (a_k b^k + ...a_1 b + a_0) + p \cdot g(t) \\ &= f(b) + p \cdot g(t) = p(1 + g(t)) \end{aligned}$$

where $g(t)$ is a polynomial in t. Since $p|f(b + tp)$ and it must be prime, so $f(b + tp) = p$. This implies that f assumes the value p infinitely many times. This is a contradiction, since a polynomial of degree k cannot assume the same value ¿ k times. □

3.2 Prime Counting function

Let x be a positive real number. We define :

$$\pi(x) = \sum_{p \leq x} 1$$

where p denotes a prime. So $\pi(x)$ counts the number of primes $\leq x$. This is called the prime counting function.

Theorem 3.5 (Prime Number Theorem)**.**

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1$$

This essentially states that $\pi(x)\sim\frac{x}{\log x}$. The proof is too complicated to be covered in this course.

3.3 Gaps between Primes

The following lemma states that we can find a gap between primes of any arbitrary length.

Lemma 3.6. For every $n\in\mathbb{N}$, there are n consecutive integers that are all composite.

Proof. Consider the numbers:

$$(n+1)!+2,(n+1)!+3,...,(n+1)!+(n+1)$$

It is clear that for $n\geq 1$, $2|(n+1)!+2$. However, $(n+1)!+2\neq 2$. So, $(n+1)!+2$ cannot be prime, and must be composite. We can extend this to each of the given numbers, and prove that they are all composite. □

Definition 5. A pair (p,q) of primes with $p<q$ is called a twin prime pair if $q-p=2$.

It is unknown how many twin primes exist. It is conjectured that there are infinitely many twin primes, but this has not yet been proved.

Theorem 3.7 (Bertrand's Postulate)**.** For every integer $n\geq 2$, there is always at least one prime between n and $2n$.

This was verified by Bertrand but proved by Chebyshev. It is sometimes called Chebyshev's theorem. The proof of this result goes beyond the scope of this course.

Remark. Do not use this result unless mentioned that we can, in the exam .

Exercise. Using Bertrand's postulate, prove that for $n\geq 2$:

$$p_n<2^n$$

Solution. Consider the statement $P(n)$ that $p_n<2^n$. This is true for the base case that $P(2)$. Now assume that $P(k)$ is true. This means:

$$p_k<2^k$$

From Bertrand's postulate,

$$k < p_k < 2k$$

$$k + 1 \leq p_k$$

We also know from Bertrand's postulate that:

$$k + 1 < p_{k+1} < 2(k + 1)$$

$$p_{k+1} < 2p_k$$

So, from the induction hypothesis,

$$p_{k+1} < 2.2^k$$

$$p_{k+1} < 2^{k+1}$$

Hence, $P(k) \Rightarrow P(k + 1)$. From PMI, $P(n)$ is true $\forall n \geq 2$. ■

Exercise. Prove that if $2^m + 1$ is prime, then $m = 2^n$ for some n.

Solution. Here, we use the following lemma - if k is odd, then $x^k + 1$ is divisible by $x + 1$. Suppose that m has an odd factor k. Then, we can express m as kp. So,

$$2^{kp} + 1 = (2^p)^k + 1$$

From our lemma, this is divisible by $2^p + 1$ which is a number other than 1 and itself. This means $2^m + 1$ cannot be prime if it has an odd factor, and hence m must be a power of 2. ■

3.4 Fermat Numbers

Definition 6. Fermat numbers are f_n such that:

$$f_n = 2^{2^n} + 1$$

Lemma 3.8 (Recursive definition)**.**

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2$$

This result is obvious from expanding the RHS, so the proof is not given here.

Exercise. Prove that f_n, $n \geq 2$, all end in 7.

Solution. Let $P(n)$ be the statement that f_n ends in 7. This is true for our base case $P(2)$. Let us assume that $P(k-1)$ is true, i.e. $f_k \mod 10 = 7$. So, by the recursive definition:

$$\begin{aligned} f_k &= f_{k-1}^2 - 2f_{k-1} + 2 \mod 10 \\ &= 7^2 - 2 * 7 + 2 \mod 10 \\ &= 7 \mod 10 \end{aligned}$$

So, by PMI, $P(n)$ is true for all $n \geq 2$. ■

Lemma 3.9 (Duncan's Identity)**.**

$$f_0 f_1 ... f_{n-1} = f_n - 2$$

Proof. Let $P(n)$ be the statement that this is true for f_n. This is clearly true for the base case $P(1)$. Let us assume $P(k)$ is true, i.e.

$$f_0 f_1 ... f_{k-1} = f_k - 2$$

$$f_0 f_1 ... f_k = f_k(f_k - 2) = f_k^2 - 2f_k = f_{k+1} - 2$$

The above result comes from the recursive definition. Since $P(k+1)$ follows from $P(k)$, by PMI, Duncan's identity is true. □

Theorem 3.10. Every prime factor of f_n, $n \geq 2$, is of the form $k \cdot 2^{n+2} + 1$.

Proof. To be discussed later in the course. □

This theorem can be helpful to quickly find the primality of f_n. For instance, f_4 is prime - we can see this by checking all the numbers of the form $2^6 k + 1$ which are less than $\sqrt{f_4}$. This cuts down the search space and makes primality checking faster.

3.5 Fibonacci Numbers

Definition 7. Fibonacci numbers are numbers of the form:

$$F_n = F_{n-1} + F_{n-2}$$

where $F_1 = 1, F_2 = 1$

Lemma 3.11.

$$\sum_{i=1}^{k} F_i = F_{k+2} - 1$$

Lemma 3.12 (Cassini's Formula)**.**

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n, n \geq 2$$

The proofs of lemmas 3.11 and 3.12 come directly from induction, so I am not discussing the proof here.

Lemma 3.13.

$$F_{n+m} = F_m F_{n+1} + F_{m-1}F_n, m \geq 2, n \geq 1$$

Proof. This is a non-trivial case of induction. Let us fix $m \in \mathbb{N}$, and do induction on n. For $n = 1$, the RHS is:

$$F_{m-1}F_1 + F_m F_2 = F_{m-1} + F_m = F_{m+1}$$

This is also true for $n = 2$. Assume that the result is true for $k = 3, 4, ..., n$. We want to show that the result is true for $k = n + 1$. For $k = n - 1$,

$$F_{m+n-1} = F_{m-1}F_{n-1} + F_m F_n$$

For $k = n$,

$$F_{m+n} = F_{m-1}F_n + F_m F_{n+1}$$

Add both sides, we get:

$$F_{m+n-1} + F_{m+n} = F_{m+n+1} = F_{m-1}F_{n+1} + F_m F_{n+2}$$

Hence Proved. □

3.6 Lucas Numbers

Definition 8. Lucas numbers are numbers L_n such that:

$$L_n = L_{n-1} + L_{n-2}$$

where L$_1 = 1, L_2 = 3$.

Theorem 3.14 (Binet's formulas)**.** Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

$$L_n = \alpha^n + \beta^n$$

Proof. TODO □

Chapter 4

Greatest Common Divisor and Least Common Multiple

4.1 Greatest Common Divisor

Definition 9. Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor of a and b is the positive integer d such that:

- $d|a$ and $d|b$
- If c is a positive integer such that $c|a$ and $c|b$, then $c \leq d$.

This is generally denoted by (a, b).

The GCD of two non-zero numbers always exists and is unique. Observe that $(a, b) = (a, -b) = (-a, b) = (-a, -b)$. If $a \neq 0$, then $(a, 0) = |a|$.

Definition 10. $a, b \in \mathbb{Z}$ are relatively prime (coprime) if $(a, b) = 1$.

Exercise. Prove that $(F_n, F_{n+1}) = 1$ for $n \geq 1$.

Solution. From Cassini's formula, we know that:

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n$$

Let $d = (F_n, F_{n+1})$. Since $d|F_n$ and $d|F_{n+1}$, we have $d|F_{n-1}F_{n+1} - F_n^2$. So $d|(-1)^n$. This means that $|d| \leq |(-1)^n|$. Since d is a positive number, $d = 1$. ■

Exercise. Prove that $(f_m, f_n) = 1$ for distinct non-negative m, n.

Solution. Suppose $m < n$. Let $d = (f_m, f_n)$. Since $d|f_m$ and $d|f_n$, $d|f_n - (f_0 ... f_m .. f_{n-1})$. From Duncan's identity, this implies that $d|2$. Since $d > 0$,, $d = 1$ or $d = 2$. However, Fermat numbers are always odd - so $d \neq 2$. This implies that $d = 1$. ■

Theorem 4.1. Let $a, b \in \mathbb{Z}$, not both zero. Then there exist integers x_0, y_0 such that:

$$(a, b) = ax_0 + by_0$$

Proof. Consider the set $S = \{ax + by > 0 : a, b \in \mathbb{Z}\}$. Let $d = \min S$. Suppose that d does not divide a. Then by division algorithm:

$$a = qd + r$$

$$qd = a - r$$

$$q(ax + by) = a - r$$

$$r = a(1 - qx) - bqy$$

So, r is a linear combination of a and b, and since $r > 0$, $r \in S$. From division algorithm, $r < d$, which contradicts the fact that $d = \min S$. So, by contradiction, d divides a (and by similiar argument, d divides b). We also know that any common divisor of a and b must divide d. This is obvious since if $a = uc$ and $b = vc$, then $d = ax + by = c(ux + vy)$, so $c|d$. From these two facts, it is clear that d is the GCD, and is of the form $ax + by$. □

Exercise. Let $a, b \in \mathbb{N}$. If $b = aq + r$, then $(a, b) = (a, r)$.

Solution. Let $d = (a, b)$ and $e = (b, r)$. We need to show that $d = e$. Since $d|a$ and $d|b$, $d|a - bq = r$. So d is a common divisor of b and r. Hence $d \leq e$. Similarly, as $e|b$ and $e|r$, e divides $bq + r = q$. Thus e is a common divisor of a and b, so $e \leq d$. Thus, $e = d$. ■

Exercise. Let $a, b, c \in \mathbb{N}$. Prove that $(ac, bc) = c(a, b)$.

Solution. Let $d = (a, b)$. Then $d|a$ and $d|b$, so $d|ca$ and $d|cb$. There exist integers x, y such that:

$$d = ax + by$$

$$cd = (ac)x + (bc)y$$

If e is a positive integer such that $e|ac$ and $e|bc$, then $e|(ac)x + (bc)y$, i.e. $e|cd$. So, cd is the GCD of ac and bc. ■

Theorem 4.2. Let $a, v \in \mathbb{Z}$, not both zero. Then $(a, b) = 1$ if and only if there exist integers x_0, y_0 such that $ax_0 + by_0 = 1$.

Proof. If $(a, b) = 1$, there must exist x_0, y_0 such that $ax_0 + by_0 = 1$, from Theorem 4.1. Conversely, suppose there exists $x_0, y_0 \in \mathbb{Z}$, such that

$$ax_0 + by_0 = 1$$

Let $d = (a, b)$. Then $d|ax_0 + by_0$, which means that $d|1|$. Since $d \in \mathbb{N}$, $d = 1$. □

Corollary 4.2.1. Let $d = (a, b)$. Then, $(\frac{a}{d}, \frac{b}{d}) = 1$

Corollary 4.2.2. If $(a, b) = 1$, and a and b both divide c, then $ab|c$.

Theorem 4.3 (Euclid's Lemma)**.** If $a|bc$ and $(a, b) = 1$, then $a|c$.

Proof.

$$ax + by = 1$$

$$acx + bcy = c$$

Since $a|acx$ and $a|bcy$, so $a|c$. □

Exercise. Let $m, n \in \mathbb{N}, m > 2$. If $F_m|F_n$, prove that $m|n$.

Solution. We know that:

$$F_n = F_{n-m}F_{m-1} + F_{n-m+1}F_m$$

Since $F_m|F_n$ and $F_m|F_{n-m+1}F_m$, we get $F_m|F_n - F_{n-m+1}F_m$ and hence $F_m|F_{n-m}F_{m-1}$. But, we also know that $(F_m, F_{m-1}) = 1$. By Euclid's Lemma, $F_m|F_{n-m}$.

From the division algorithm, let $n = mq + r$. Suppose $r > 0$. From our previous result, $F_m|F_{n-m}$, so $F_m|F_{n-2m}...F_m|F_r$. This means that $F_m \leq F_r$. But $r < m$, so $F_r < F_m$. This is a contradiction. So $r = 0$. Hence proved. ■

Definition 11. Let $n \geq 2$ and let $a_1, ...a_n \in \mathbb{Z}$, not all zero. The GCD of $a_1, ..., a_n$ is the largest positive integer that divides each a_i. This is denoted by $a_1, ..., a_n$.

This has the following properties:

- $(a_1, a_2...a_n)$ is the least positive integer that is a linear combination of $a_1...a_n$.

- $(a_1, ..., a_n) = ((a_1, ..., a_{n-1}), a_n)$
- If $d|a_1...a_n$ and $(d, a_i) = 1$ for all $i \in [1, n-1]$, then $d|a_n$.
- If $a_1, ..., a_n$ are pairwise relatively prime, then $(a_1, ..., a_n) = 1$.

4.2 Euclidean Algorithm

We are given $a, b \in \mathbb{Z}$, not both zero, and want to compute (a, b). The algorithm to do this works as follows:

1. If a or b are negative, replace with their absolute value.
2. If $a > b$, then swap a and b.
3. If $a = 0$, then $(a, b) = b$.
4. If $a > 0$, write $b = aq + r$. Then,

   $$(a, b) = (r, a)$$

   Go to step 3 with $a = r$ and $b = a$ respectively.

This is called the Euclidean Algorithm.

To express (a, b) as a linear combination of a and b where $0 \leq a \leq b$, we create a table with four columns with headings x, y, r, q. We denote the rows as $R_{-1}, R_0, R_1, ...R_{i-1}$ and the entries in R_i as x_i, y_i, r_i, q_i. $R_{-1} = (0, 1, b, 0)$ and $R_0 = (1, 0, a, 0)$. Suppose we have filled till R_{i-1} for some $i \geq 1$. To fill R_i, we first compute q_i, which is the quotient obtained on dividing r_{i-2} by r_{i-1}. Next, $R_i = R_{i-2} - q_i R_{i-1}$. We continue this until $r = 0$. Then, the GCD is the value of r in the row before, and the coefficients are the values of x and y in the row before. This is known as the Extended Euclidean Algorithm.

Theorem 4.4 (Lame's theorem)**.** Let $b \geq a \geq 2$. The number of divisions required to compute (a, b) by the Euclidean algorithm is at most 5 times the number of decimal digits in a.

Proof. Suppose that a contains k decimal digits and takes n divisions to compute (a, b). We need to show that $n \leq 5k$. Let $r_0 = b, r_1 = a$. Applying Division algorithm repeatedly, we have:

$$r_0 = r_1 q_1 + r_2, 0 < r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2$$

$$\cdots$$

$$r_{n-1} = r_n \cdot q_n + 0$$

We can prove that $q_i \geq 1$ for $1 \leq i \leq n-1$ and $q_n \geq 2$. This is because if q_n is 1, then $r_{n-1} = r_n$, which is a contradiction. If $q_i = 0$, then $r_{i-1} = r_{i+1}$, which is also a contradiction. We claim that $r_{n-i} \geq F_{i+2}$ for $1 \leq i \leq n-1$. This is true for the base case, where $r_{n-1} \geq F_3 = 2$.

$$\begin{aligned} r_{n-j} &= r_{n-(j-1)}q_{n-(j-1)} + r_{n-(j-2)} \\ &\geq r_{n-(j-1)} + r_{n-(j-2)} \\ &\geq F_{j+1} + F_j = F_j + 2 \end{aligned}$$

In particular, $a = r_1 \geq F_{n+1}$. Now $10^k > a \geq F_{n+1}\alpha^{n-1}$, where $\alpha = \frac{1+\sqrt{5}}{2}$ and $n \geq 3$. Taking logarithms and using the fact that $\log \alpha > 1/5$, we get that $n \leq 5k$. □

Exercise. Prove that for all $a, m, n \in \mathbb{N}$,

$$(a^n - 1, a^m - 1) = a^{(n,m)} - 1$$

Solution. Let $f_n = a^n - 1$. Our goal is to prove that $(f_n, f_m) = f_{(n,m)}$.

$$\begin{aligned} f_n &= a^n - 1 \\ &= a^{n-m}(a^m - 1) + a^{n-m} - 1 \\ &= f_{n-m} + kf_m \end{aligned}$$

So now, when performing Euclid's algorithm to find the GCD, $(f_n, f_m) = (f_{n-m}, f_m)$. This occurs recursively, and as we can see it is also performing Euclid's algorithm in the subscript. Hence, $(f_n, f_m) = f_{(n,m)}$. ■

4.3 Least Common Multiple

Definition 12. Let $a, b \in \mathbb{N}$. We say that a positive integer l is the least common multiple of a and b if

- a and b both divide l
- c is a positive integer divisible by both a and b, then $l \leq c$.

It is generally denoted by $[a, b]$.

Exercise. Prove that $(a, b)[a, b] = ab$.

Solution. Let $d = (a, b)$ and let $k = ab/d$. Obviously, $k \in \mathbb{N}$. We have to show that $k = [a, b]$. We first prove that a and b both divide k. Write

$$a = da_1, b = db_1, a_1, b_1 \in \mathbb{Z}$$

Then, $k = \frac{ab}{d} = ab_1 = ba_1$. Hence a and b both divide k. Suppose c is a positive integer divisible by both a and b. Write

$$c = aa', c = bb', a', b' \in \mathbb{Z}$$

Since $d = (a, b)$, there exists integers x and y such that:

$$d = ax + by$$

Then

$$\frac{c}{k} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \frac{c}{b}x + \frac{c}{a}y = b'x + a'y \in \mathbb{Z}$$

Hence k divides c. Since $c \neq 0$, this implies $k \leq c$. Therefore, by definition, $k = [a, b]$ and $(a, b)[a, b] = ab$. ■

4.4 Fundamental Theorem of Arithmetic

Theorem 4.5 (Fundamental Theorem of Arithmetic)**.** Every integer $n \geq 2$ can be written as a product of primes and the factorization into primes is unique up to the order of the factors.

Proof. Let $P(n)$ be the statement that n can be written as a product of primes. $P(2)$ is true, since it is a prime. Let $k \geq 2$ and $P(2), \cdots, P(k)$ is true. If $k + 1$ is prime, then $P(k + 1)$ is immediately true. If it is composite, then $k + 1$ is of the form $a \cdot b$ where $2 \leq a, b \geq k$. By induction hypothesis, since $P(a)$ and $P(b)$ is true, $P(k + 1)$ is also true.

Suppose that

$$n = p_1 p_2 .. p_r = q_1 ... q_s$$

Assume $r \leq s$. Since if $p_1 | q_1 ... q_s$, $p_1 = q_i$ for some $i, 1 \leq i \leq s$. We can cancel this out and keep doing this till we get

$$1 = q_{i_1} q_{i_2} q_{i_{s-r}}$$

However, q_i is a prime. This is a contradiction unless $s = r$. Hence uniqueness is proved. □

The largest power x such that $p^x|a$ for a prime p is called the multiplicity of p in a.

Chapter 5

Linear Diophantine Equations

5.1 Linear Diophantine Equations in Two Variables

Linear Diophantine equations in two variables are of the form:

$$ax + by = c$$

An integer solution exists if and only if $(a, b)|c$. In this case, for any initial solution x_0, y_0, the general solution is given by:

$$x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n$$

where $d = (a, b)$ and $n \in \mathbb{Z}$. The initial solution x_0, y_0 can be found using the Extended Euclidean Algorithm.

5.2 Fibonacci Linear Diophantine Equation

Theorem 5.1. Let $k \in \mathbb{N}, c \in \mathbb{Z}$. The linear Diophantine equation:

$$F_{k+1}x + F_k y = c$$

is always solvable. If k is even, the complete solution is given by:

$$x = F_{k-1}c + F_k n, y = -F_k c - F_{k+1}n$$

If k is odd, the complete solution is given by:

$$x = -F_{k-1}c + F_k n, y = F_k c - F_{k+1}n$$

Proof. $(F_k, F_{k+1}) = 1$, so the solution always exists. If k is even, then:

$$x_0 = F_{k-1}c, y_0 = -F_k c$$

always solves it (prove it via Cassini's Formula). If k is odd, then:

$$x_0 = -F_{k-1}c, y = F_k c$$

always solves it. □

5.3 Linear Diophantine Equations in Many Variables

Theorem 5.2. Let $a_1, ..., a_k$ be integers, not all zero. The Diophantine equation:

$$a_1x_1 + ... + a_kx_k = x$$

has an integer solution if and only if $(a_1, ..., a_k)|c$. In that case, there are infinitely many solutions.

Exercise. Find the complete solution to:

$$6x + 8y + 12z = 10$$

Solution. $(6, 8, 12) = 2$, and $2|10$, so this equation is solvable. Let us consider the "subequation" $8y + 12z$. Since it is a linear combination of 8 and 12, it must be a multiple of $(8, 12) = 4$. So,

$$8y + 12z = 4u$$

This gives us a new equation:

$$6x + 4u = 10$$

The general solution of this is given by:

$$x = 1 + 2n, u = 1 - 3n$$

Substituting u in the first equation,

$$8x + 12y = 4(1 - 3n)$$

This equation is also solvable, and we can find it's general solution as well. Since $4 = 2.8 + (-1).12$, we get $4(1 - 3n) = (2 - 6n)8 + (-1 - 3n)12$. Finally, we can write the complete solution:

$$x = 1 + 2n$$

$$y = 2 - 6n + 3m$$

$$z = -1 + 3n - 2m$$

■

Exercise. Suppose we have a coin system. Let's say we use 4 rupee and 9 rupee coins only. Then which amounts can be exchanged? For instance, 1 rupee cannot be exchanged; 17 rupees can be exchanged.

Solution. This problem can be expressed as - what numbers can be expressed as a linear combination of 4 and 9 with positive coefficients.

In fact, only finitely many integers cannot be exchanged. Generally, if $p, q \in \mathbb{N}$ with $(p, q) = 1$, then the largest integer which cannot be represented as $ap + bq$ with $a, b \in \mathbb{Z}, a, b \geq 0$ is $pq - p - q$.

Let $x = ap + bq$. Since $(p, q) = 1$, each multiple of q leaves a different remainder when divided by p which does not change when one adds multiples of p to it. This means that if x leaves a remainder r when divided by q, there has been some ap that leaves the same remainder. The last remainder to be taken is q with $p(q - 1)$.

TO FIX ■

Chapter 6

Congruence

6.1 Introduction

Definition 13. Let $m \in \mathbb{N}$. Two integers a, b are said to be congruent modulo m if $m|a-b$. This is denoted by $a \equiv b \mod m$

Congruence has the following properties:

- $a \equiv a \mod m$
- $a \equiv b \mod m$, then $b \equiv a \mod m$
- $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$

As such, it is an equivalence relation. The set of all integers congruent to a modulo m is denoted by $[a]$, and is called the congruence class of $a \mod m$

Lemma 6.1. Two integers are congruent modulo m if and only if a, b have the same remainder upon division by m

Proof. Suppose a and b have the same remainder upon division by m. Then:

$$a = mq_1 + r$$

$$b = mq_2 + r$$

$$a - b = m(q_1 - q_2) + 0$$

$$m|a - b \Rightarrow a \equiv b \mod m$$

Suppose $a \equiv b \mod m$. This means that $a - b = mk, k \in \mathbb{Z}$. By division algorithm, there exist unique integers q, r such that:

$$b = mq + r, 0 \leq r < m$$

$$a = m(q + k) + r$$

Since $0 \leq r < m$, r is the remainder of a upon division by m. So, they have the same remainder. Hence proved. □

So, every integer a is congruent to it's remainder r modulo m. We call r the least residue of a modulo m. Every integer is congruent to exactly one of the least residues $0, 1, ..., m - 1$ modulo m. Hence,

$$\mathbb{Z} = \bigcup_{i=0}^{m-1} [i]_m$$

Lemma 6.2. Suppose $a \equiv b \mod m$ and $c \equiv d \mod m$. Then:

- $a \pm c \equiv b \pm d \mod m$
- $ac \equiv bd \mod m$
- $a^n \equiv b^n \mod m$

Lemma 6.3. Let p be a prime and let $a \in \mathbb{Z}$ with $(a, p) = 1$. Then the least residues of:

$$a, 2a, \cdots, (p - 1)a$$

modulo p are a permutation of the integers $1, 2, \cdots, p - 1$.

Proof. Let $i \in \{1, 2, ..., p - 1\}$. Suppose $ia \equiv 0 \mod p$. Then, $i \equiv 0 \mod p$, which is false. So, ia cannot be congruent to 0 modulo p.

Let $i, j \in \{1, 2, \cdots, p - 1\}, i \neq j$. Suppose that $ia \equiv ja \mod p$. Since $(a, p) = 1$, $i \equiv j \mod p$. However, $|i - j| \leq p - 1$. Then, $p||i - j|$ if and only if $i = j$, but this is a contradiction. Hence, ia for $i \in \{1, 2, \cdots, p - 1\}$ are all incongruent to one another. Hence, they will all have different least residues, none of which are equal to 0. So, the least residues must be a permutation of $\{1, 2, \cdots, p - 1\}$. □

Exercise. Find the remainder when $1! + 2! + ... + 100!$ is divided by 15.

Solution. If $n \geq 5$, then $n!$ is divisible by 15. So, $n! \equiv 0 \mod 15$. Hence, this sum modulo 15 is equivalent to $1! + 2! + 3! + 4!$ modulo 15. So, the remainder is 3. ■

Exercise. Find the positive integers n for which $\sum_{k=1}^{n} k!$ is a square.

Solution. If $k \geq 5$, then $k! \equiv 0 \mod 10$. So,

$$\sum_{k=1}^{n} k! \equiv 1! + 2! + 3! + 4! \mod 10$$

Squares are congruent to 0,1,4,5,6 or 9 modulo 10. However, for $n \geq 5$, this sum is 3 modulo 10. So, n must be less than 5. We can now try each of these cases by hand. From this, we find $n = 1$ or $n = 3$. ■

Definition 14. A set $a_1, ..., a_m$ is said to be a complete set of residues modulo m if every integer is congruent modulo m to exactly one of them.

A set of m integers form a complete set of residues modulo m if and only if no two of the integers are congruent modulo m.

Exercise. Let $m \in \mathbb{N}$ with $m \geq 3$. Prove that the set $\{1^2, 2^2, ..., m^2\}$ doesn't form a complete set of residues modulo m.

Solution. If they do not form a complete set of residues modulo m, then two of the integers must be congruent modulo m. Since $m - 1 \equiv -1 \mod m$, we have:

$$(m-1)^2 \equiv 1 \mod m$$

Thus, this set cannot form a complete set of residues modulo m. ■

Exercise. Find all positive integers x, y, z such that:

$$3^x + 4^y + 5^z$$

Solution. Let us first consider this modulo 4. Then,

$$3^x \equiv 1 \mod 4$$

We can prove that this is only possible if x is even. $3 \equiv 3 \mod 4$ and $3^2 \equiv 1 \mod 4$. This repeats again and again, and can be proved by induction.

Now let us consider this modulo 4. Then,

$$1 \equiv 2^z \mod 3$$

From the same argument above, we get that z must be even too.

From this, we get a new equation:

$$3^{2x_1} + 2^{2y} = 5^{2z_1}$$

$$2^{2y} = 5^{2z_1} - 3^{2x_1} = (5^{z_1} + 3^{x_1})(5^{z_1} - 3^{x_1})$$

From the fundamental theorem of arithmetic, we know that:

$$5^{z_1} + 3^{x_1} = 2^s, s \geq 0$$

$$5^{z_1} - 3^{x_1} = 2^t, t \geq 0$$

From this set of equations,

$$5^{z_1} = \frac{2^t + 2^s}{2} = 2^{t-1}(2^{s-t} + 1)$$

Since the LHS is odd, $t = 1$. So,

$$5^{z_1} = 2^{s-1} + 1 \text{ and } 3^{x_1} = 2^{s-1} - 1$$

By considering the 3^{x_1} modulo 3, we get that:

$$2^{s-1} \equiv 1 \mod 3$$

This once again implies that $s - 1$ is even.

$$3^{x_1} = 2^{2s_1} - 1 = (2^{s_1} - 1)(2^{s_1} + 1)$$

Once again we apply the fundamental theorem of arithmetic, and get the equations

$$2^{s_1} - 1 = 3^a$$

$$2^{s_1} + 1 = 3^b$$

$$3^b - 3^a = 2$$

This implies that $b = 1, a = 0$. From this we know that $s_1 = 1$ and $s = 3$. These results also tell us that $z = 2$ and $x = 2$.

$$3^2 + 4^y = 5^2$$

$$4^y = 5^2 - 3^2 = 16$$

Hence, the only positive integers satisfying the equation are $x = y = z = 2$. ■

Exercise. Show that $x^2 + 2y^2 = 8z + 5$ has no integral solution.

Solution. This equation is solvable if and only if there $\exists x, y$ such that

$$x^2 + 2y^2 \equiv 5 \mod 8$$

If a is an integer, we can show that $a^2 \equiv 0, 1, 4 \mod 8$. So if x and y are integers, x^2 is equivalent to $0, 1, 4$, and $2y^2$ is equivalent to $0, 2$. The sum cannot be equivalent to 5. Hence, no integral solution exists. ■

Exercise. Show that the sequence 71,771,7771,... has no perfect squares.

Solution. Remember that a perfect square is equivalent to either 0 or 1 modulo 4. We now prove that the i^{th} term r_i of the given sequence is such that $r_i \equiv 3 \mod 4$.

Let $P(n)$ be a statement that the term r_i is such that $r_i \equiv 3 \mod 4$. This is true for a $i = 1$, since $71 \equiv 3 \mod 4$. Assume $P(k)$ is true. We can express r_{i+1} by the recurrence:

$$\begin{aligned} r_{i+1} &= 10r_i + 61 \\ r_{i+1} &\equiv 10 \cdot 3 + 1 \mod 4 \\ r_{i+1} &= 3 \mod 4 \end{aligned}$$

By PMI, $P(n)$ is true $\forall n \geq 1$. Hence, no member of this sequence may be a perfect square.

As an aside, remember that there is no perfect square that can end with two odd digits. ■

6.2 Square and Multiply Algorithm

Let a, l, m be integers ≥ 2. We want to compute $a^l \mod m$. To do this, we could use the following steps:

1. Write the base-2 expansion on $l = (a_l \cdots a_1 a_0)_2$, where $k \geq 0, a_k \neq 0, 0 \leq a_i < 2$.
2. Compute $a^{2^i} \mod m$ for $0 \leq i \leq k$. This can be done in $O(k)$ via squaring.
3. Multiply the $a^{2^i} \mod m$ for all i with $a_i = 1$ to get the result.

6.3 Cancellation in Congruences

Theorem 6.4. Let $a, b, c, m \in \mathbb{Z}$ with $m \geq 2$. Then,

- If $ac \equiv bc \mod m$ and $(c, m) = 1$, then $a \equiv b \mod m$.
- Let $d = (c, m)$. If $ac \equiv bc \mod m$ then $a \equiv b \mod \frac{m}{d}$.

Proof. We have $m|(a-b)c$, which implies that $\frac{m}{d}|(a-b)\frac{c}{d}$. Since $(\frac{m}{d}, \frac{c}{d}) = 1$, we get that $\frac{m}{d}|(a-b)$. This is the second result. The first result is a consequence of the second. □

6.4 Combining Congruences with different moduli

Theorem 6.5. Let $a, b, m_1, ..., m_k \in \mathbb{Z}$ with $m_1, m_2, ..., m_k \geq 2$. If

$$a \equiv b \mod m_1$$

$$a \equiv b \mod m_2$$

$$\cdots$$

$$a \equiv b \mod m_k$$

then $a \equiv b \mod [m_1, m_2, \cdots, m_k]$

6.5 Linear Congruences

Let $a, b, m \in \mathbb{Z}, m \geq 2$. Then $ax \equiv b \mod m$ is called a linear congruence. Our goal is to find possible x that satisfy the given congruence.

Theorem 6.6. Let $a, b, m \in Z$ and $d = (a, m)$. The linear congruence $ax \equiv b \mod m$ has a solution if and only if $d|b$. If $d|b$, then there are d mutually incongruent solutions modulo m.

Proof. The linear congruence $ax \equiv b \mod m$ can be expressed as a linear Diophantine equation:

$$ax = b + my$$

$$ax - my = b$$

Hence, it has a solution if and only if that LDE is solvable. This means that the linear congruence is also only solvable if and only if $(a, m)|b$.

Suppose $d|b$. Then, there are infinitely many solutions to the LDE. If (x_0, y_0) is a particular solution, then the complete solution is given by

$$x = x_0 + \frac{m}{d}n, y = y_0 + \frac{a}{d}n$$

Then, we will get the solutions:

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + d\frac{m}{d}, ...$$

Here we can see that after that last term, all the solutions will be congruent to one of the first d terms. Hence, if the first d solutions are incongruent, we will have proved our theorem.

Assume

$$\begin{aligned} x_0 + \frac{m}{d}n_1 &\equiv x_0 + \frac{m}{d}n_2 && \mod m \\ \frac{m}{d}n_1 &\equiv \frac{m}{d}n_2 && \mod m \\ n_1 &\equiv n_2 && \mod d \text{ (From Theorem 6.3)} \end{aligned}$$

This means that two solutions will only be congruent if n_1 and n_2 are congruent modulo d. So, $ax \equiv b \mod m$ has d mutually incongruent solutions:

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d}$$

□

6.6 System of Linear Congruences

Let $a_1, ..., a_k \in Z$. Let $n_1, ..., n_k$ be integers ≥ 2. We want to find integers x that satisfy the system of linear congruences

$$x \equiv a_1 \mod n_1$$
$$\cdots$$
$$x \equiv a_k \mod n_k$$

Theorem 6.7 (Chinese Remainder Theorem)**.** If $n_1, \cdots, n_k$ are pairwise coprime, then the system:

$$x \equiv a_1 \mod n_1$$
$$\cdots$$
$$x \equiv a_k \mod n_k$$

has a unique solution modulo $n_1 n_2 \cdots n_k$

Proof. Let $n = n_1 n_2 \cdots n_k$. For $i = 1, \cdots, k$ let $N_i = \frac{n}{n_i}$. Note that $(N_i, n_i) = 1$. Let the unique solution of the congruence

$$N_i x \equiv 1 \mod n_i$$

be x_i.

Let us prove that $x = a_1 N_1 x_1 + \cdots + a_k N_k x_k$ satisfies the given system of congruences. First, let us prove that it satisfies the first congruence. Since $N_i \equiv 0 \mod n_1$ for $i = 2, \cdots, k$, we get:

$$x \equiv a_1 N_1 x_1 + 0 \mod n_1$$

We have already assumed that $N_1 x_1 \equiv 1 \mod n_1$. So,

$$x \equiv a_1 \mod n_1$$

Hence proved. The same argument can be made for all the congruences.

Now let us prove that the solution is unique. Suppose x, y satisfy the system of congruences. Then

$$x \equiv a_1 \equiv y \mod n_1$$

$$\ldots$$

$$x \equiv a_1 \equiv y \mod n_k$$

$$x \equiv y \mod [n_1, n_2, ..., n_k]$$

Since $(n_i, n_j) = 1$, $x \equiv y \mod n_1 n_2 ... n_k$. Hence the solution is unique. □

Exercise. Solve the following system of congruences:

$$x \equiv 11 \mod 12$$

$$x \equiv 1 \mod 5$$

$$x \equiv 0 \mod 7$$

Solution.

$$n = 12 \times 5 \times 7 = 420$$

$$N_1 = \frac{n}{12} = 35$$

$$N_2 = 84$$

$$N_3 = 60$$

First, let us solve $N_1 x \equiv 1 \mod n_1$. Then,

$$35x \equiv 1 \mod 12$$

$$x \equiv -1 mod 12$$

Let $x_1 = -1$. The same way, we find $x_2 = -1$ and $x_3 = 0$. So,

$$x = 11 \times 35 \times (-1) + 1 \times 84 \times (-1) + 0$$

$$x \equiv 371 \mod 420$$

■

6.7 Modular Inverse

Definition 15. Let p be a prime and let $a \in Z$ with $(a, p) = 1$. Then a is invertible modulo p and it's inverse is a number x such that:

$$a \cdot x \equiv 1 \mod p$$

Lemma 6.8. *a is self-invertible modulo p if and only if $a \equiv \pm 1 \mod p$.*

Proof. By definition of being "self invertible",

$$a^2 \equiv 1 \mod p$$

$$(a-1)(a+1) \equiv 0 \mod p$$

So, $(a-1) \equiv 0 \mod p$ or $(a+1) \equiv 0 \mod p$. From this, $a \equiv \pm 1 \mod p$. □

Theorem 6.9 (Wilson's Theorem)**.** *If p is a prime number, then $(p-1)! \equiv -1 \mod p$*

Proof. If $p = 2$, then $(p-1)! = 1$, which is $-1 \mod p$.

Suppose $p > 2$. We group the $p-3$ integers, namely $2, \cdots, p-2$ into pairs of inverses (a, b) such that $ab \equiv 1 \mod p$. Hence,

$$(p-1)! \equiv 1.2.3 \cdots (p-2)(p-1) \equiv (p-1) \equiv -1 \mod p$$

□

The following are some consequences of Wilson's theorem:

- The product of $p-1$ integers between any two consecutive multiples of p is congruent to -1 modulo p.
- Let p be a prime and $0 \le r \le p-1$. Then :

$$r!(p-1-r)! + (-1)^r \equiv 0 \mod p$$

Exercise. Let p be a prime and let $n \in \mathbb{N}$. Prove that

$$\frac{(np)!}{n!p^n} \equiv (-1)^n \mod p$$

Solution.

$$\begin{aligned}\frac{(np)!}{n!p^n} &= \frac{(np)!}{p\cdot(2p)\cdots(np)} \\ &= (1\cdot 2\cdots(p-1))((p+1)(p+2)\cdots(2p-1))\cdots(((n-1)p+1)\cdots(np-1)) \\ &\equiv (-1)\cdot(-1)\cdots(-1) \mod p \\ &\equiv (-1)^n \mod p\end{aligned}$$

■

6.8 Fermat's Little Theorem

Theorem 6.10 (Fermat's Little Theorem)**.** Let p be a prime and let $a \in \mathbb{Z}$ with $(a,p) = 1$. Then,

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

Proof. From Lemma 6.3,

$$\begin{aligned}a\cdot 2a\cdots(p-1)a &\equiv 1\cdot 2\cdots(p-1) &&\mod p \\ (p-1)!a^{p-1} &\equiv (p-1)! &&\mod p \\ a^{p-1} &\equiv 1 &&\mod p\end{aligned}$$

The last step follows from the fact that $(p,(p-1)!) = 1$. □

An important consequence of this result is that the inverse of any number a modulo p is a^{p-2}. By using this result, we can solve any congruence of the form:

$$ax \equiv b \mod p$$

by multiplying both sides by the inverse of a, getting the equation:

$$x \equiv a^{p-2}b \mod p$$

Theorem 6.11. Let p be a prime and let $a \in \mathbb{Z}$. Then:

$$a^p \equiv a \mod p$$

Proof. If $(a, p) = 1$, then by Fermat's little theorem,

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

$$a^p \equiv a \mod p$$

If $(a, p) \neq 1$, then $p|a$. Hence $a \equiv a^p \equiv 0 \mod p$. □

Theorem 6.11 gives us the base for Fermat's test for non primality. Let $n \in \mathbb{N}$. If $a^n \not\equiv a \mod n$, then n must be composite. Clearly, the converse does not hold - if $a^n \equiv a \mod n$, this is not proof that n is prime! Composite numbers that follow the result in Fermat's little theorem are called Carmichael numbers.

Theorem 6.12. Let $p_1, p_2, \cdots p_k$ be distinct prime numbers. Let $a \in \mathbb{N}$ and let

$$l = [p_1 - 1, p_2 - 1, \cdots, p_k - 1]$$

Then,

$$a^{l+1} \equiv a \mod p_1 p_2 \cdots p_k$$

Proof. Let $i \in \{1, 2, \cdots, k\}$. By Fermat's little theorem,

$$a^{p_i-1} \equiv 1 \mod p_i$$

$$a^l = a^{(p_i-1)\times\frac{l}{p_i-1}} \equiv 1 \mod p_i$$

$$a^{l+1} \equiv a \mod p_i$$

The above result is also true if $(a, p) \neq 1$ since then $p|a$, so $a^{l+1} \equiv a \equiv 0 \mod p_i$. The result now follows from Theorem 6.5. □

Exercise. Let p be a prime number with $p \geq 5$. Let $a \in \mathbb{Z}$. Prove that:

$$a^p \equiv a \mod 6p$$

Solution. $6p = 2 \cdot 3 \cdot p$. Then, $l = [2-1, 3-1, p-1] = p-1$, since p must be an odd integer. Hence, from Theorem 6.12,

$$a^p \equiv a \mod 6p$$

■

Fermat's Little Theorem can be generalized to create Euler's theorem. As a prerequisite, we need to know about **Euler's totient function**, $\phi(m)$. $\phi(m)$ is the number of integers less than or equal to m which are coprime to m. Some properties are:

- $\phi(p) = p - 1$ if and only if p is prime
- $\phi(p^k) = p^k - p^{k-1}$
- A closed form formula for $\phi(n)$ is:

  $$\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

  This formula allows us to compute all the values from 1 to n quickly using the Sieve of Eratosthenes.

Theorem 6.13 (Euler's Theorem)**.** If $\phi(m)$ is Euler's totient function, and a and m are coprime integers, then:

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

Proof. Consider the following lemma - let $r_1, \cdots, r_{\phi(m)}$ denote the positive integers less than m and coprime to m. Then the least residues of the integers:

$$ar_1, ar_2, \cdots, ar_{\phi(m)}$$

are a permutation of the integers $r_1, \cdots r_{\phi(m)}$. To prove this, it is enough to prove:

1. $(ar_i, m) = 1 \forall i \in \{1, \cdots, \phi(m)\}$
2. $ar_i \not\equiv ar_j \mod m$ if $i \neq j$, $i, j \in \{1, \cdots, \phi(m)\}$

(1) is simple to prove with Fundamental Theorem of Arithmetic. To prove (2), let us suppose that it is false. Then:

$$ar_i \equiv ar_j \mod m$$

$$r_i \equiv r_j \mod m$$

However, $|r_i - r_j| \leq m-1$, so that cannot be true. So, by contradiction, (2) is also true, and so is our lemma.

Using this lemma,

$$ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \mod m$$

$$a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi}(m) \mod m$$

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

□

In particular, if p is prime, then $\phi(p) = p-1$, and we have Fermat's Little Theorem. Just like with Fermat's Little Theorem, we find that the inverse of a is $a^{\phi(m)-1}$, and can solve congruences of the form $ax \equiv b \mod m$.

Lemma 6.14. Let $m \in \mathbb{N}$ and let a be an integer coprime to m. Let k, l be non negative integers with:

$$k \equiv l \mod \phi(m)$$

then:

$$a^k \equiv a^l \mod m$$

Proof. WLOG, suppose $k \leq l$. Then, $l - k = \phi(m)q, q \in \mathbb{Z}, q \geq 0$.

$$a^l \equiv a^{l-k}a^k \equiv a^{\phi(m)q}a^k \equiv a^k \mod m$$

□

Theorem 6.15 (Generalized Euler Theorem)**.** Let $m_1, \cdots, m_k \in \mathbb{N}$ and let a be an integer coprime to m_i for each i, then:

$$a^{[\phi(m_1), \cdots, \phi(m_k)]} \equiv 1 \mod [m_1, \cdots, m_k]$$

Proof. Let us fix i. Since $(a, m_i) = 1$, by Euler's theorem,

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

Hence, since $m_i | [\phi(m_1), \cdots, \phi(m_k)]$

$$a^{[\phi(m_1), \ldots, \phi(m_k)]} \equiv 1 \mod m_i$$

Since this is true for all m_i, we get the above result:

$$a^{[\phi(m_1),\cdots,\phi(m_k)]} \equiv 1 \mod [m_1, \cdots, m_k]$$

□

Chapter 7

Multiplicative Functions

7.1 Multiplicative Functions

Definition 16. A real or complex valued function defined on the set of positive integers is called an arithmetical function of number theoretic function.

Definition 17. An arithmetical function f is said to be multiplicative if $f(mn) = f(m) \cdot f(n)$ for all coprime positive integers m, n.

Examples of multiplicative functions are:

- $f(n) = 0 \forall n \in \mathbb{N}$
- $f(n) = 1 \forall n \in \mathbb{N}$
- $f(n) = n^k \forall n \in \mathbb{N}$

Exercise. Let f be a multiplicative function which is not identically zero. Prove that $f(1) = 1$.

Solution. From the definition of a multiplicative function,

$$f(mn) = f(m) \cdot f(n)$$

Let $m = 1$. Then,

$$f(n) = f(1) \cdot f(n)$$

From this, it is clear that $f(1) = 1$, the identity element. ■

Theorem 7.1. Let f be a multiplicative function and let $n \in \mathbb{N}$ with prime power factorization

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

Then

$$f(n) = f(p_1^{e_1}) \cdots f(p_k^{e_k})$$

The proof is straightforward from the factorization of an integer, so I have not included the proof here.

Remark. The value of a multiplicative function $f(x) \forall x \in [1, n]$ can be calculated in $O(n)$ time using a linear sieve.

Exercise. Prove that Euler's Totient Function is multiplicative.

Solution. We are trying to prove that if $(m, n) = 1, \phi(mn) = \phi(m)\phi(n)$. To prove this, we make a rectangular table of numbers from 1 to mn with m rows and n columns:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
m & 2m & 3m & \cdots & nm
\end{array}$$

The numbers in the r^{th} row of this table are of the form $km + r$ as k runs from 0 to $m - 1$.

Let $d = (r, m)$. If $d = 1$, then no number in the r^{th} row of the table is relatively prime to mn, since $d|(km + r)$ for all k. So to count the residues relatively prime to mn we need only to look at the rows indexed by values of r such that $(r, m) = 1$. There are $\phi(m)$ such rows.

Now we introduce an important lemma - if $r \in \mathbb{Z}$, then the n integers:

$$r, r + m, r + 2m, \cdots, r + (n-1)m$$

for a complete set of residues modulo n. Let us prove this. Suppose $r + im \equiv r + jm \mod n, i \neq j$. This means that $(i - j)m \equiv 0 \mod n$. So, $n|i - j$. However, $i - j < n$. So $i - j = 0$, i.e. $i = j$. This is a contradiction. Hence, no two numbers in the set are congruent. Since there are $n - 1$ numbers in the set, they form a complete set of residues modulo n.

From the above lemma, the numbers in a row, given by $km + r$ form a complete set of residues modulo n. Thus, exactly $\phi(n)$ of them will be coprime to n, and hence relatively prime to mn.

Hence, we have shown that there are $\phi(m)$ rows which contain $\phi(n)$ numbers coprime to mn, so there are in total $\phi(m)\phi(n)$ numbers in the table relatively prime to mn. ■

Theorem 7.2. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of n. Then,

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

Proof. Since ϕ is multiplicative,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k}) \\
&= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\
&= p_1^{e_1} \cdots p_k^{e_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

□

Exercise. Prove that $\phi(n)$ is even for $n > 2$.

Proof. Notice that if k is coprime to n, then $n - k$ is also coprime to n. This can be proved since $(n, k) = (n - k, k)$. Hence, we can form pairs of coprime integers $k, n - k$, and thus $\phi(n)$ must be even. Notice also that the degenerate case where $n - k = k$ does not apply, since they could not be coprime for $n > 2$. □

7.2 The Möbius Transform

Definition 18. Let f be an arithmetical function. Define F to be

$$F(n) = \sum_{d|n} f(d)$$

Then F is called the Möbius Transform of f.

Theorem 7.3. If f is multiplicative, then it's Möbius transform F is also multiplicative.

Proof. Let $m, n \in \mathbb{N}$ with $(m, n) = 1$. Then:

$$\begin{aligned}
F(mn) &= \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|m} f(d_1 d_2) \\
&= \sum_{d_1|m, d_2|m} f(d_1) f(d_2) \\
&= \sum_{d_2|n} \left(\sum_{d_1|m} f(d_1) \right) f(d_2) \\
&= \sum_{d_2|n} F(m) f(d_2) \\
&= F(m) \sum_{d_2|n} f(d_2) \\
&= F(m) F(n)
\end{aligned}$$

□

Let us take a look at the τ function. If f is such that $f(n) = 1$, then:

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

counts the number of positive divisors of n. Next if p is prime and $e \in \mathbb{N}$, then:

$$\tau(p^e) = e + 1$$

From theorem 7.3, τ is multiplicative. So, if we express n as:

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

then

$$\tau(n) = \tau(p_1^{e_1}) \cdots \tau(p_k^{e_k}) = (e_1 + 1) \cdots (e_k + 1)$$

Exercise. Prove that $\tau(n)$ is odd if and only if n is a square.

Solution. To prove that if n is a square, $\tau(n)$ is odd, we see that $e_i \equiv 0 \mod 2$ for all prime factors of n. So, $e_i + 1 \equiv 1 \mod 2$. Then, $\tau(n)$ must be odd, since all the factors will be odd.

To prove the converse, we note that it $\tau(n)$ is odd, it must have no even factors. So, $e_i + 1 \equiv 1 \mod 2, \forall i$. Then, n must be a square. ■

The next important function is the σ function. Let f be $f(n) = n$. Then:

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

This is the sum of all positive divisors of n. If p is a prime and $e \in \mathbb{N}$,

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

Since σ will be multiplicative by Theorem 7.3, if

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

then

$$\sigma(n) = \sigma(p_1^{e_1}) \cdots \sigma(p_k^{e_k}) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}$$

Exercise. If n is a composite number, prove that $\sigma(n) > n + \sqrt{n}$.

Proof. Since n is composite, let $a, b \in \mathbb{N}, a \neq 1, n$ such that $ab = n$. Then,

$$\sigma(n) = 1 + n + a + b$$

We know that either $a \geq \sqrt{n}$ or $b \geq \sqrt{n}$. Hence,

$$\sigma(n) > 1 + n + \sqrt{n}$$

□

Lemma 7.4.

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

Proof. Define $F(n) = \sum_{d|n} \phi(d)$. From Theorem 7.3, F is multiplicative. It is simple to see that

$$\begin{aligned} F(p^k) &= \sum_{d|n} \phi(d) \\ &= \sum_{i=0}^{k} \phi(p^i) \\ &= \sum_{i=1}^{k} (p^i - p^{i-1}) + 1 \\ &= p^k \end{aligned}$$

Hence, if $n = \prod p_i^{e_i}$,

$$F(n) = \prod F(p_i^{e_i}) = \prod p_i^{e_i} = n$$

□

7.3 The Möbius Function

Definition 19. The Möbius function is $\mu(n)$ such that:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 | n \text{ for prime } p \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \end{cases}$$

This can also be expressed as another definition. $\mu(n)$ is:

- 1 if n is square free with an even number of prime factors
- -1 if n is square free with an odd number of prime factors
- 0 if n is not square free

Remark. This is an important function to remember. It can be found using a sieve, and is useful in many combinatoric problems involving numbers, especially for inclusion-exclusion.

Theorem 7.5. The Möbius function is multiplicative.

Proof. Let $m, n \in \mathbb{N}$ with $(m, n) = 1$. If $m = 1$ or $n = 1$ then $\mu(mn) = \mu(m)\mu(n)$. If m or n are not square free, then mn will not be square free, so $\mu(mn) = 0 = \mu(m)\mu(n)$. Finally, suppose both m and n are square free integers greater than 1. Let:

$$m = p_1 \cdots p_k$$

$$n = q_1 \cdots q_l$$

$p_i \neq q_j$ since the two numbers are coprime. $\mu(m) = (-1)^k, \mu(n) = (-1)^l$. mn will be a product of $k + l$ distinct primes, so $\mu(mn) = (-1)^{k+l}$. Hence, $\mu(mn) = \mu(m)\mu(n)$. Hence μ is a multiplicative function. □

Lemma 7.6.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

Proof. If $n = 1$, then the result is trivial. Since μ is multiplicative, then the Möbius transform F is also multiplicative. Now:

$$\begin{aligned} F(p^e) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) \\ &= 1 - 1 + 0 \\ &= 0 \end{aligned}$$

If $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime power factorization of n then since F is multiplicative,

$$F(n) = F(p_1^{e_1})F(p_2^{e_2}) \cdots F(p_k^{e_k}) = 0$$

□

Theorem 7.7 (Möbius Inversion Formula)**.** Let f be an arithmetical function and let F denote it's Möbius transform. Then:

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

and F is called the inverse Möbius transform of F.

Proof.

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') \\ &= \sum_{d|n} \sum_{d|\frac{n}{d}} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= \sum_{d'|n} f(d') \left[\frac{1}{n/d'}\right] \\ &= f(n) \end{aligned}$$

□

7.4 Dirichlet Convolution

This section is not in syllabus or taught in class, but is helpful when proving some identities. It is included in the notes for this purpose.

Definition 20. The Dirichlet Convolution of two arithmetic functions f and g are defined to be the function

$$h = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

where h is denoted by $f * g$.

Theorem 7.8. Let f and g be multiplicative. Then $h = f * g$ is multiplicative.

Proof. Let $(m,n) = 1$. If $d|mn$ and $(m,n) = 1$, then there exist unique $a|m$ and $b|n$ such that $d = ab$. Therefore

$$\begin{aligned} h(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\ &= \sum_{a|m}\sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right) \\ &= \sum_{a|m}\sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \left[\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right]\left[\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right] \\ &= h(m)h(n) \end{aligned}$$

Hence, h is also multiplicative □

Corollary 7.8.1. f is multiplicative if and only if F, it's Möbius transform, is also multiplicative

Proof. One direction of this statement has already been proved in Theorem 7.3. The other direction is clear from noticing that the Möbius inversion formula could alternatively be stated by $f = \mu F$. Since F and μ are multiplicative, f must be multiplicative. □

Theorem 7.8 allows us to solve lots of problems simply by stating that the convolution must be multiplicative. An example of a problem that uses Corollary 7.8.1 is given below.

Exercise. Let f be such that:

$$\mu(n) = \sum_{d|n} f(d)$$

Find $f(n)$

Solution. By the Möbius inversion formula,

$$f(n) = \sum_{d|n} \mu(n)\mu\left(\frac{n}{d}\right)$$

Hence $f = \mu * \mu$. This means that f must be multiplicative (or from Corollary 7.8.1). Let p be a prime. Then, from the formula:

- $f(p) = -2$
- $f(p^2) = 1$
- $f(p^a) = 0, \forall a > 2$

Hence, if n is divisible by p^3 for any prime p, $f(n) = 0$. Otherwise, $f(n) = (-2)^k$ where k is the number of primes such that $p|n$ but $p^2 \nmid n$. ■

Chapter 8

Primitive Roots

8.1 Order of numbers

Definition 21. (Order of an integer) Let m be an integer ≥ 2 and let a be an integer coprime to m. The order of a modulo m is the least positive integer k such that:

$$a^k \equiv 1 \mod m$$

This is denoted by $\operatorname{ord}_m a$

This is reminiscent of Euler's Theorem. As expected, $\phi(m)$ is not always the least integer satisfying the above equation. It is obvious that $\operatorname{ord}_m a \leq \phi(m)$.

Moreover, if $a \equiv b \mod m$, then $\operatorname{ord}_m a = \operatorname{ord}_m b$.

Lemma 8.1. Let $h \in \mathbb{N}$. Then $a^h \equiv 1 \mod m$ if and only if $\operatorname{ord}_m a | h$.

Proof. Let $k = \operatorname{ord}_m a$. Suppose $a^h \equiv 1 \mod m$. By division algorithm, there exists unique integers q, r such that:

$$h = kq + r, 0 \leq r < k$$

Suppose $r \neq 0$. Then

$$\begin{aligned} 1 \equiv a^h \equiv a^{kq+r} \equiv a^k q a^r \mod m \\ \equiv 1 \cdot a^r \mod m \end{aligned}$$

This is a contradiction since $r < k$, but k is the least positive integer such that $a^k \equiv 1 \mod m$. Hence, $r = 0$, so $k|h$. The converse is obvious. □

Corollary 8.1.1. $\operatorname{ord}_m a | \phi(m)$

This corollary allows us to prune the space of possible orders when trying to find the order of an integer. Instead of trying every single integer to check if it is the order, we only need to check divisors of $\phi(m)$.

Lemma 8.2. Let $a \in \mathbb{Z}$ with $(a, m) = 1$. Let $i, j \in \mathbb{N} \cup \{0\}$. Then $a^i \equiv a^j \mod m$ if and only if $i \equiv j \mod \operatorname{ord}_m a$.

Proof. The backwards direction is trivial to prove, by substitution. Let us prove the forward direction.

Let $k = \operatorname{ord}_m a$. WLOG, assume $i \geq j$. Then, let us assume that $i - j \not\equiv 0 \mod k$. Then we can express $i - j$ as:

$$i - j = kp + r, 0 < r < k$$

Substituting,

$$a^i \equiv a^j \mod m$$

$$a^{i-j} \equiv 1 \mod m$$

$$a^{kp+r} \equiv 1 \mod m$$

$$a^{kp} \cdot a^r \equiv 1 \mod m$$

$$a^r \equiv 1 \mod m$$

But, $r < k$, which is a contradiction since the order should be the least number satisfying the equation. Hence, the forward direction is proved. □

Corollary 8.2.1. If $k = \operatorname{ord}_m a$, then $a, a^2, \cdots, a^k$ are incongruent modulo m.

Lemma 8.3. Let $k = \operatorname{ord}_m a$ and let $h \in \mathbb{N}$. Then

$$\operatorname{ord}_m a^h = \frac{k}{(h, k)}$$

Proof. Let $l = \operatorname{ord}_m a^h$ and let $d = (h, k)$. Write

$$h = dh', k = dk'$$

We want to prove that $l = k'$. Since $a^h l \equiv 1 \mod m$, we get $k|hl$. Hence, $k'|h'l$. Since $(h', k') = 1$, we get $k'|l$. Now, it is enough to prove that $l|k'$. This will follow if we can prove that $(a^h)^{k'} \equiv 1 \mod m$. Now:

$$(a^h)^{k'} \equiv a^{h'dk/d} = (a^k)^{h'} \equiv 1 \mod m$$

□

8.2 Primitive Roots

Definition 22. Let m be an integer ≥ 2 and let a be an integer coprime to m. we say that a is a primitive root modulo m if $\operatorname{ord}_m a = \phi(m)$.

Exercise. Prove that 2 is not a primitive root modulo any Fermat prime f_n, $n \geq 2$.

Solution.

$$2^{2^n} \equiv -1 \mod f_n$$

$$2^{2^{n+1}} \equiv 1 \mod f_n$$

$$\phi(f_n) = f_n - 1$$

since f_n is prime. $2^{n+1} < f_n - 1$ for $n \geq 2$. Hence, 2 cannot be a primitive root since $\operatorname{ord}_{f_n} 2 < \phi(f_n)$. ■

Theorem 8.4. Let $a_1, \cdots, a_{\phi(m)}$ denote all positive integers $\leq m$ that are coprime to m. If a is a primitive root modulo m, then

$$a, a^2, \cdots, a^{\phi(m)}$$

are congruent modulo m to $a_1, \cdots, a_{\phi(m)}$ in some order

Proof. TODO □

Corollary 8.4.1. If m has a primitive root, then the number of primitive roots modulo m is $\phi(\phi(m))$.

Proof. Suppose a is a primitive root modulo m. Since any other primitive root is coprime to m, it is congruent modulo m to one of

$$a, a^2, \cdots, a^{\phi(m)}$$

Since $\operatorname{ord}_m a^h = \frac{\phi(m)}{(h,\phi(m))}$, a^h is a primitive root modulo m if and only if $(h, \phi(m)) = 1$. Hence the number of primitive roots modulo m equals the number of positive integers $\leq \phi(m)$ coprime to $\phi(m)$ and hence $\phi(\phi(m))$ □

Exercise. Let $m \geq 3$ and let a be a primitive root modulo m. Prove that:

$$a^{\phi(m)/2} \equiv -1 \mod m$$

Solution. Since $(m-1, m) = 1$, there exists i in $[1, \phi(m))$, such that $a^i \equiv m - 1 \equiv -1 \mod m$. Then $a^{2i} \equiv 1 \mod m$. If $i < \phi(m)/2$, then $2i < \phi(m)$ and we get a contradiction as a is a primitive root modulo m. If $i > \phi(m)/2$, then $0 < i - \phi(m)/2 < \phi(m)/2$. $(a^{i-\phi(m)/2})^2 \equiv 1 \mod m$. Since $2(i - \phi(m)/2) < \phi(m)$, this is again a contradiction as a is a primitive root modulo m. Hence $i = \phi(m)/2$. ■

Theorem 8.5. Let $n \in \mathbb{Z}$. If p is an odd prime dividing $n^2 + 1$, then $p \equiv 1 \mod 4$.

Proof. TODO □

Exercise. Let $\operatorname{ord}_m a = h$, $\operatorname{ord}_m b = k$. Then:

1. $(\operatorname{ord}_m ab)|hk$
2. If h and k are coprime, then $\operatorname{ord}_m ab = hk$.

Solution. Let $l = \operatorname{ord}_m ab$. Since $a^h \equiv 1 \mod m$ and $b^k \equiv 1 \mod m$, we get:

$$(ab)^{hk} = a^{hk} b^{hk} \equiv 1 \mod m$$

Hence $\operatorname{ord}_m ab|hk$.

To prove 2, we must show that $hk|l$. Since h and k are coprime, we can just show that $h|l$ and $k|l$. Let us prove that $h|l$. To do this, we prove that $a^l \equiv 1 \mod m$. Now $a^{lh} \equiv 1 \mod m$. Next,

$$(a^l)^k \equiv a^{lk} b^{lk} \equiv (ab)^{lk} \equiv 1 \mod m$$

Since $(h, k) = 1$, there exist integers such that $hx + ky = 1$. Now

$$a^l \equiv (a^{lh})^x (a^{lk})^y \equiv 1 \mod m$$

(polish, late for class) ■

Theorem 8.6 (Lucas' Theorem)**.** Let $m \geq 3$. Suppose that there exists $x \in \mathbb{N}$ such that $x^{m-1} \equiv 1 \mod m$ and $x^{(m-1)/q} \not\equiv 1 \mod m$ for all prime factors q of $m-1$. Then m is prime.

Proof. Let $k = \operatorname{ord}_m x$. Since $x^{m-1} \equiv 1 \mod m$, we get that $k|m-1$. Write $m-1 = kt, t \in \mathbb{N}$. Suppose $t > 1$. Then we can find a prime q dividing t. Now

$$x^{(m-1)/q} \equiv (x^k)^{t/q} \equiv 1 \mod m$$

which is a contradiction. Hence $t = 1$, or $k = m-1$. Thus $m - 1 = \phi(m)$. Hence m is prime. □

This gives us a primality test for integers. This is in fact faster than brute force checking in $O(\sqrt{n})$ since the number of prime factors of a number grows very slowly - see highly composite numbers. (or perhaps finding the necessary x is slow?)

Corollary 8.6.1. Let $m \geq 3$. Suppose that there exists $x \in \mathbb{N}$ such that $x^{(m-1)/2} \equiv -1 \mod m$ and $x^{(m-1)/q} \equiv 1 \mod m$ for all odd prime factors q of $m-1$. Then m is prime.

8.3 Polynomial Congruences

Definition 23. Let $f(x) \in Z[x]$. We say that $\alpha \in \mathbb{Z}$ is a solution of

$$f(x) \equiv 1 \mod m$$

if $f(\alpha) \equiv 0 \mod m$.

Theorem 8.7 (Lagrange's Theorem)**.** Let p be a prime and let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial of degree n with integer coefficients, where $p \nmid a_n$. The congruence has $f(x) \equiv 0 \mod p$ has at most n incongruent solutions modulo p.

Proof. We prove the theorem by induction on n. If $n = 0$, then $f(x) = a_0$ with $p \nmid a_0$. Hence, the number of solutions will be 0, which is $\leq n$.

Assume that the theorem is true for polynomials of degree $< k$. Consider a polynomial of degree k $f(x)$.

If $f(x) \equiv 0 \mod p$ has no solutions, we are done. Otherwise if it has a solution $\alpha, 0 \leq \alpha < p$. No:

$$\begin{aligned} f(x) &\equiv f(x) - 0 \mod p \\ &\equiv f(x) - f(\alpha) \mod p \\ &\equiv a_k(x^k - \alpha^k) + a_{k-1}(x^{k-1} - \alpha^{k-1}) + \cdots + a_1(x - \alpha) \mod p \end{aligned}$$

Since $x - \alpha$ divides each of the summands, we get that $x - \alpha$ divides $f(x)$. Write

$$f(x) \equiv (x - \alpha)q(x) \mod p$$

where $q(x)$ is a polynomial of degree $k - 1$.

If β is any other incongruent solution of $f(x) \equiv 0 \mod p$, then $q(\beta) \equiv 0 \mod p$. By induction hypothesis, $q(x)$ has at most $k-1$ solutions. Hence, $f(x)$ has at most k solutions. Hence, by PSI, Lagrange's theorem holds true. □

Corollary 8.7.1. Let p be a prime and let d be a positive divisor of $p - 1$. Then the congruence $x^{d-1} \equiv 0 \mod p$ has exactly d solutions

Proof. Let $f(x) = x^{p-1} - 1$. By Fermat's little theorem,

$$f(x) \equiv 0 \mod p$$

has exactly $p - 1$ solutions. Since $d | p - 1$, we have that $x^d - 1$ divides $x^{p-1} - 1$. So,

$$f(x) = (x^d - 1)q(x)$$

where

$$q(x) = x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1$$

By Lagrange's theorem, the congruence

$$x^d - 1 \equiv 0 \mod p$$

has $\leq d$ solutions and

$$q(x) \equiv 0 \mod p$$

has $\leq p - 1 - d$ solutions. Since $f(x) \equiv 0 \mod p$ has $p - 1$ solutions and $q(x) \equiv 0$ has $\leq p - 1 - d$ solutions, we get that

$$x^d - 1 \equiv 0 \mod p$$

must have $\geq (p - 1) - (p - 1 - d) = d$ solutions. Hence it has exactly d solutions. □

Theorem 8.8. Let p be a prime and let d be a positive divisor of $p-1$. Then there are exactly $\phi(d)$ incongruent integers of order d modulo p.

Proof. For every positive divisor d of $p-1$, let:

$$S_d = \{a : 1 \leq a \leq p-1, \operatorname{ord}_p a = d\}$$

Let $\psi(d) = |S_d|$. Since

$$\{1, 2, 3, \cdots, p-1\} = \bigcup_{d|p-1} S_d$$

we get

$$p-1 = \sum_{d|p-1} \psi(d)$$

We know that:

$$\sum_{d|p-1} \phi(d) = p-1 = \sum_{d|p-1} \psi(d)$$

We want to prove that $\psi(d) = \phi(d) \forall d$. It is enough to prove that $\psi(d) \leq \phi(d)$.

Suppose d is a divisor of $p-1$ with $\psi(d) \neq 0$. Let a be an integer with $\operatorname{ord}_p a = d$. We know that

$$a, a^2, \cdots, a^d$$

are mutually incongruent, modulo p. Moreover,

$$(a^i)^d - 1 \equiv (a^d)^i - 1 \equiv 1 - 1 \equiv 0$$

Hence, $a, a^2, \cdots, a^d$ are the d solutions of $x^d - 1 \equiv 0 \mod p$. This implies that $S_d \subseteq \{a, a^2, \cdots, a^d\}$.

We know that

$$\operatorname{ord}_p a^i = \frac{d}{(i, d)}$$

Thus $\operatorname{ord}_p a^i = d$ if and only if i and d are coprime. There are $\phi(d)$ such i. Hence, $|S_d| = \psi(d) = \phi(d)$. □

Corollary 8.8.1. Let p be a prime. There are $\phi(p-1)$ incongruent primitive roots modulo p.

Proof. Note that this also follows from Corollary 8.4.1. To show that this follows from Theorem 8.8, we see that if a number is a primitive root, it's order is $d = p-1$. So, there must be $\phi(p-1)$ incongruent primitive roots. □

Chapter 9

Quadratic Residues

9.1 Quadratic Congruences

Definition 24. A quadratic congruence is an equation of the form:

$$ax^2 + bx + c \equiv 0 \mod m$$

where $a \neq 0$ and $m \geq 2$.

When $m = 2$, we can easily reduce it to a linear congruence since $x^2 \equiv x \mod 2$ for all x. Hence

$$ax^2 + bx + c \equiv (a + b)x + c \mod 2$$

We already know how to solve this. Hence, we will assume that $m \geq 3$ from now on.

Theorem 9.1. Let p be an odd prime and let $a, b, c \in \mathbb{Z}$ where $(a, p) = 1$. The quadratic congruence

$$ax^2 + bx + c \equiv 0 \mod p$$

has a solution x if and only if the quadratic congruence

$$y^2 \equiv b^2 - 4ac \mod p$$

has a solution y. Further, $y \equiv 2ax + b \mod p$.

Proof. The solution x will exist if and only if:

$$4a(ax^2 + bx + c) \equiv 0 \mod p$$

$$(2ax)^2 + 2 \cdot (2ax) \cdot b + 4ac \equiv 0 \mod p$$

$$(2ax)^2 + 2 \cdot (2ax) \cdot b + 4ac + b^2 - b^2 \equiv 0 \mod p$$

$$(2ax + b)^2 \equiv b^2 - 4ac \mod p$$

$$y^2 \equiv b^2 - 4ac \mod p$$

□

Theorem 9.1 gives us a method to transform a quadratic congruence to a smaller, more easily solvable form.