Number theory

Tanmay Joshi
Mentor: Shourya Pandey

Summer of Science 2021

Contents

Report overview

In this report I will be summarizing my readings in the first half of my summer of science- 2021 project on Number theory. The book I have referred to is *Elementary Number Theory - David M Burton*. We'll be going through some preliminaries and building up the required knowledge to understand some centuries old conjectures and also prove some historic theorems. Let us begin!

Chapter 1

Preliminaries

1.1 Constructing the integers

Definition 1.1.1. For a given set S and a given equivalence relation $\sim$ on S, the equivalence class of a, denoted by [a], is given by: $[a] = \{x \epsilon S | x \sim a\}$

Let the equivalence relation $\sim$ be defined on $\mathbb{N}X\mathbb{N}$ such that $(a,b) \sim (c,d)$ if and only if a+d = c+b , where (a,b) and (c,d) are ordered pairs of natural numbers. The integers can be constructed as equivalence classes of these ordered pairs.

Now let us define some operations on the integers using equivalent operations on the natural numbers. Thus

$$[(a,b)] + [(c,d)] := [(a+d, c+b)]$$
$$[(a,b)].[(c,d)] := [(ac+bd, ad+bc)]$$
$$-[(a,b)] = [(b,a)]$$

Now, every such equivalence class has at least one of the type of elements (a,0) and (0,a). The classes [(a,0)] denote the Natural numbers as a subset of the integers while [(0,a)] denote the remaining integers.

1.2 Mathematical induction

Let us first set up a few required tools and move on to the theorem of finite induction.

Well ordering Principle: Every non-empty set S of non-negative integers contains a least element. That is,

$$\exists\ a\ \epsilon\ S \text{ such that } \ \forall\ b\ \epsilon\ S, a \leq b$$

Theorem 1.2.1 (**Archimedean property**)**.** If a and b are any positive integers then there exists a positive integer n for which $na\ \geq\ b$

Proof. By contradiction: Let $na\ <\ b$ for every n, for some a and b. Thus the set S defined by
$S\ = \{b\ - na\ | n \epsilon \mathbb{N}\}$
will consist only positive integers. Therefore by the well ordering principle, it must have a least element of the form $a\ -\ bm$. But since $a\ -\ (m+1)b$ also lies in S and $(a\ -\ (m+1)b)\ <\ (a\ -\ bm)$, $a\ -\ bm$ cannot be the least element. Therefore our assumption does not hold. Hence,the Archimedean property is proved true. □

Theorem 1.2.2 (**Principle of finite induction**)**.** Let S be the set of positive integers with the properties:
(i) 1 belongs to S.
(ii) For each integer k belonging to S, k+1 belongs to S as well.
Then, S is the set of all positive integers.

Proof. By contradiction: Let there exist T, the set of all integers which do not belong to S. As T only has positive integers, by the well ordering principle, T must have some integer n which is the least element of T. Also as 1 belongs to S by the property (i), $0 < n - 1 < n$ as $n > 1$. Therefore as n is the smallest integer not belonging to S, n-1 must belong to S. But since n-1 belongs to S, n-1 + 1 = n must belong to S as well, by property (ii). Thus our assumption that T exists does not hold true. Therefore S is the set of all positive integers. □

Remark. Instead of having 1 as the least element of the set S, we could have a more general theorem on the principle of induction by having some positive integer n_0 as the least element.

1.3 Binomial theorem

Binomial Coefficients: For positive integers n and k such that $0\ \leq k\ \leq\ n$, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Some identities:
(i) $\binom{n}{0} = \binom{n}{n} = 1$
(ii) Pascal's rule: $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$. This can be used to construct Pascal's triangle.

Theorem 1.3.1 (The Binomial theorem)**.** For $n \epsilon \mathbb{N}$ and for a,b $\epsilon \mathbb{R}$ we have:
$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Proof. By Induction: For n=1, the formula gives:
$(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = a + b$
Which obviously holds.
Now, assuming that the formula works for m,
as $(a+b)^{m+1} = a(a+b)^m + b(a+b)^m$,
Now,
$a(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{k+1} b^{m-k} = a^{m+1} + \sum_{k=1}^{m} \binom{m}{k} a^k b^{m-k+1}$
$b(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k+1} = b^{m+1} + \sum_{k=1}^{m} \binom{m}{k-1} a^k b^{m-k+1}$

Thus adding the two equations and using Pascal's rule,
$(a+b)^{m+1} = a^{m+1} + \sum_{k=1}^{m} (\binom{m}{k-1} + \binom{m}{k}) a^k b^{m-k+1} + b^{m+1}$
$Thus,\ (a+b)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} a^k b^{m+1-k}$

□

Chapter 2

Divisibility theory

2.1 The Division Algorithm

Theorem 2.1.1 (The Division algorithm)**.** For any integers a and b, such than b $>$ 0, there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.

Proof. Let $S = \{a \ - bx$ |x is an integer and $a - bx \geq 0\}$
To use the well ordering principle, we must prove that S is a non-empty set, first.
Since b $\geq$ 1, we have $b|a| \geq |a|$.
Thus, for $x = -|a|$, we have $a \ - bx \ = a \ + b|a| \geq a + |a| \geq 0$.
Thus, S is non-empty. Now using the well-ordering principle on S, we must have some least element r in S, such that :
a - b q = r; where r $\geq$ 0.
If r $\geq$ b, a -(q+1)b = r-b $\geq$ 0 and a -(q+1)b which is less than a -qb would belong to S, violating the well ordering principle. Thus, $r < b$.
Uniqueness of q and r:
Let $a = bq + r = bq' + r'$
Thus, subtracting the two representations of a, we get:
$(r - r') = b(q - q')$
But, since $0 \leq r < b$ and $0 \leq r' < b$,
we have $-b < -r' \leq 0$
Therefore, $-b < r - r' < b$, i.e. $|r - r'| < b$
Plugging this in the previous equation,
$b \ |q - q'| < \ b$, so $|q - q'| < 1$
But since $|q - q'| \geq 0$, we have $|q - q'| = 0$. Thus $q = q'$ and $r = r'$. □

2.2 Greatest Common Divisor

Definition 2.2.1 (Divisibility)**.** An integer a is said to be divisible by an integer b is there exists an integer c such that a = bc.
This is denoted by $b|a$. If b does not divide a, $b \nmid a$.

Consequences of Definition 2.2.1 : Following are some easily provable consequences of the definition of divisibility:

1. $a|0$, $1|a$, $a|a$.
2. $a|1 \implies a = \pm 1$
3. If $a|b$ and $c|d$ then $ab|cd$.
4. If $a|b$ and $b|c$ then $a|c$.
5. $a|b$ and $b|a \iff a = \pm b$.
6. If $a|b$ and $b \neq 0$ then $|a| \leq |b|$.
7. If $a|b$ and $a|c$ then $a|(bx + cy)$ $\forall$ integers x,y.

Definition 2.2.2 (Greatest common divisor)**.** Let a and b be two integers, not both of them zero. The greatest common divisor of a and b, denoted by gcd(a,b) is an integer d which satisfies the following properties:

1. $d|a$ and $d|b$.
2. For each integer c satisfying $c|a$ and $c|b$, $d \geq c$.

Theorem 2.2.1. For any integers a and b, not both zero, there exist integers x and y such that:
$gcd(a, b) = ax + by$

Proof. Let $S = \{au + bv | au + bv > 0; u, v \text{ integers}\}$ As S isn't empty, we can apply the well ordering principle to get some integer d which is the least element of S.
Now by the division algorithm, for some q and r,
$a = qd + r$
$r = a - qd = a - (ax + by)q = a(1 - qx) + b(-qy)$
Thus, r would be a part of S too, if $r > 0$. Thus r=0. So, $d|a$. By a similar argument, $d|b$. But as $d = ax + by$, by the 7th consequence, any other divisor c would divide d. So as $c|d$, $c < d$. Thus d is the greatest common divisor of a and b. □

Corollary 2.2.1.1. If a,b are two integers not both zero, then the set $T = \{ax + by | x, y \text{integers}\}$ is precisely the set of all multiples of gcd(a,b) =d.

Definition 2.2.3 (Relatively prime numbers)**.** Two integers a and b are said to be relatively prime in=f gcd(a,b) = 1.

Theorem 2.2.2. Two numbers a and b are relatively prime if and only if there exist integers x and y such that ax + by = 1.

Proof. Direct consequence of Theorem 2.2.1 and as Corollary 2.2.1.1 □

Corollary 2.2.2.1. If gcd(a,b)=d then gcd(a/d,b/d)=1.

Corollary 2.2.2.2. If $a|c$ and $b|c$ and gcd(a,b)=1 then $ab|c$

Theorem 2.2.3 (Euclid's Lemma)**.** If $a|bc$ and gcd(a,b) =1 then $a|c$

Proof. Since gcd(a,b)=1, for some integers x and y, we have:
1 = ax + by
Thus, c = ca x + cb y
Since $a|bc$, $a|(cax + bcy)$, and thus $a|c$ □

Lemma 2.2.4. If a = bq + r then gcd(a,b) = gcd(b,r)

Proof. If d=gcd(a,b) then $d|a$ and $d|b$. Thus, $d|(a - qb)$ or $d|r$. In other words, d is a common divisor of b and r.If c is another common divisor of b and r, $c|(bq + r)$ or $c|a$. Therefore by definition, $c \leq d$. Thus gcd(b,r) =d. □

Euclid's algorithm As a consequence of Lemma 2.2.4, we have:
$gcd(a, b) = gcd(b, r_1) = \cdots = gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$
Thus, the gcd of a and b can be found in finite steps.

Remark. The number of steps required to find the gcd by Euclid's algorithm is at most 5 times the number of digits of the smaller number.

Theorem 2.2.5. If $k > 0$ then gcd(ka,kb)=k*gcd(a,b)

Proof. Multiply each of the equations in Euclid's algorithm by k. □

Definition 2.2.4 (Least common multiple)**.** The least common multiple of two non-zero integers a and b is an integer c which satisfies the following properties:

1. $a|c$ and $b|c$

2. If $a|p$ and $b|p$ then $c \leq p$

Theorem 2.2.6. For two integers a, b we have gcd(a,b) lcm(a,b) =ab

Proof. Let d = gcd(a,b). So, a =dp and b=dq for some p and q.
Let m = ab/d = aq = bp.
As we know, d = ax + by.
Let c be a common multiple of a and b. So, c=au = bv.
Now, $\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{c}{b}$x + $\frac{c}{a}$y .
Thus, m—c, and by definition m is lcm(a,b). □

2.3 The Diophantine equation

Any equation with one or more variables to be solved in integers is called a Diophantine equation. A linear Diophantine equation in two variables x,y is :
ax + by = c.

Theorem 2.3.1. The linear Diophantine equation ax + by =c has a solution if and only if $d|c$ where d= gcd(a,b) and if x_0,y_0 is a particular solution then the general solution to the equation is given by :
x = x_0 +$\frac{bt}{d}$ and y = y_0 - $\frac{at}{d}$ for all integers t.

Proof. Since d = gcd(a,b), a = dr and b = ds for some r,s. Thus, if c = ax + by = d(sx + ry)
Therefore, $d|c$ for a solution to exist.
Now, let x_0,y_0 be a solution to the equation.
Thus, ax + by = c = ax_0 + by_0
Subtracting, a(x_0 -x)=b(y-y_0)
Thus as a = dr and b = ds, r(x_0 -x)=s(y-y_0) where gcd(r,s)=1
Now, since $r|s(y - y_0)$ and gcd(r,s)=1, $r|y - y_0$
Therefore $y - y_0 = rt$ for some t. So, $x_0 - x = rt$ Hence, proved. □

Corollary 2.3.1.1. If gcd(a,b) =1 and x_0, y_0 is a particular solution of the Diophantine equation ax + by = c, then all solutions are given by x = x_0 +bt, y = y_0 - at where t is any integer.

Chapter 3

Primes

3.1 The fundamental theorem of Arithmetic

Definition 3.1.1 (Prime numbers)**.** An integer p (> 1) is called a prime number if its only positive divisors are 1 and p itself. A number greater than 1 which is not prime is termed composite.

Theorem 3.1.1. If p is a prime number and $p|ab$ then either $p|a$ or $p|b$.

Proof. If $p|a$, the statement is satisfied. So when $p \nmid a$, gcd(p,a)=1. Thus by Euclid's Lemma, as $p|ab$ and gcd(a,p)=1, $p|b$. □

Corollary 3.1.1.1. If p is a prime and $p|a_0a_1a_2 \dots a_n$, then $p|a_k$ for some $1 \leq k \leq n$

Corollary 3.1.1.2. If $p, q_0, q_1, q_2 \dots, q_n$ and $p|q_0q_1q_2 \dots q_n$ then $p = q_k$ for some k such that $1 \leq k \leq n$.

Theorem 3.1.2 (The fundamental theorem of Arithmetic)**.** Every positive integer n > 1 can be uniquely represented in an unordered product of primes.

Proof. If n is prime the statement holds true. If n is composite, it will have an integer d such that $d|n$ for some d, by definition. All such integers are positive and the set of these integers is non-empty. Thus by the well ordering principle, there exists a minimum divisor of n, p_1. As this doesn't have any further divisor and is minimum, it must be prime. We now use the same argument on $n_1 = n/p_1$, $n_2 = n_1/p_2$ and so on. Now since $n > n_1 > n_2 > \cdots > 1$, we must

have finite steps and the expression of $n = p_1 p_2 \dots p_k$ would hold. Uniqueness is a direct consequence of corollary 3.1.1.2. □

Corollary 3.1.2.1. Any positive integer $n > 1$ can be expressed in the form

$$n = p_1^k p_2^k p_3^k 3 \dots p_m^k m$$

Where for each i such that $1 \leq i \leq m$, k_i is a positive integer and p_i is a prime.

3.2 The sieve of Eratosthenes

For any composite number a >1 we have a=bc for some integers b and c by definition. Assuming $b \leq c$ WLOG, we have $b^2 \leq bc = a$. Thus $b \leq \sqrt{a}$. As b has at least one prime factor, (let p), $p \leq \sqrt{a}$. Eratosthenes devised an algorithm to find all primes from 1 to any number N. Arrange the numbers in increasing order, and start moving from 1 to N. Now whenever a prime, say p, is encountered, cross out all multiples of p till N. When you reach $x \geq \sqrt{N}$, you will have crossed out all composite numbers till N.

Theorem 3.2.1. There are an infinite number of primes

Euler's proof. Let $p_1, p_2, p_3 \dots p_n$ be all the primes, in ascending order. Now consider :

$$P = p_1 p_2 p_3 \dots p_n + 1$$

Since $P > 1$, we must have some prime q which divides P. But q must be one of $p_1, p_2, p_3 \dots, p_n$. Thus, $q|P$ and $q|p_1 p_2 p_3 \dots p_n$. Combining these two, we have $q|(P - p_1 p_2 p_3 \dots p_n)$, and thus $q|1$ which cannot be possible. □

Remark. $p_{n+1} \leq p_1 p_2 p_3 \dots p_n + 1 \leq p_n^n$

Alternate proof. Let $n_1 = 2$ and $n_i = n_1 n_2 n_3 \dots n_{i-1} + 1$ for all positive integers i. Since each $n_i > 0$, each of them is divisible by atleast one prime. Let d = gcd(n_i, n_j) where $i < j$. Thus, $d|n_i$ and $d|n_k$ or $d|(n_1 n_2 \dots n_i \dots n_k + 1)$. Thus $d|1$. Therefore d = 1. Thus all n_i are pairwise relatively prime and there exist as many primes ass n_i, that is, infinite. □

Theorem 3.2.2. If p_n is the n^{th} prime number, then $p_n \leq 2^{2^{n-1}}$

Proof. As the given assertion is true when n=1, let it be true for all integers upto n. Now,

$$p_{n+1} \leq p_1 p_2 p_3 \dots p_n + 1 \leq 2.2^2.2^3 \dots 2^n + 1$$

Now since $1 \leq 2^{2^n-1}$ we have

$$p_{n+1} \leq 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}$$

□

Corollary 3.2.2.1. There are at least n+1 prime less than 2^{2^n} for $n \geq 1$.

3.3 The Goldbach Conjecture

The Goldbach conjecture: Every even integer is the sum of two numbers that are either 1 or primes. In other words, every odd number n greater than 7 can be expressed as the sum of 3 primes, as n -3 is even.

Theorem 3.3.1. There is an infinite number of primes of the form 4n +3.

Proof. Let there be only finite primes of the form 4n +3, given by $q_1, q_2, \ldots q_n$. Let

$$N = 4q_1q_2q_3 \ldots q_n - 1 = 4(q_1q_2q_3 \ldots q_n - 1) + 3$$

Let $r_1, r_2, r_3, \ldots r_k$ be the prime factors of N. Since N is of the form 4n +3 too, 2 is not a factor of N. Thus each r_i is either of the form 4n +1 or 4n +3. But product of two numbers of the form 4n +1 is also of the form 4n +1. Therefore each prime factor of N is of the form 4n +3, and must belong to $q_1, q_2, \ldots q_n$. But that would mean $r_i|1$. Thus the assumption does not hold and there are infinite primes of the form 4n +3. □

Theorem 3.3.2. If a and b are relatively prime positive integers, then the arithmetic progression

$$a, a + b, a + 2b, a + 3b \ldots$$

has infinitely many primes.
But, there exists no infinite arithmetic progression consisting solely of primes.

Chapter 4

Congruences

4.1 Basic properties of congruence

Definition 4.1.1. Let n be a positive integer. Two integers a and b are said to be congruent modulo n if n divides the difference a - b, that is, a - b = kn for some integer k. This is denoted by:

$$a \equiv b(modn)$$

The set of integers 0,1,2,. . . ,n-1 is called the set of least positive residues modulo n.

Theorem 4.1.1. For arbitrary integers a and b, $a \equiv b(mod\ n)$ if anf only is a and b leaave the same remainder on dividing by n.

Proof. When $a \equiv b(mod\ n)$ we have a = b + kn. Now if b = qn +r for some q and r such that $0 \leq r < n$, we have a = qn +r + kn = (q+k)n +r. Thus a leaves the same remainder as b on dividing by n. Now, if $a = q_1 n\ +\ r$ and $b = q_2 n\ +\ r$, we have a-b = $(q_1 - q_2)$n, thus $a \equiv b$. □

Some properties Let a,b,c,d be arbitrary integers and n be an integer. Then:

1. $a \equiv a(mod\ n)$
2. $a \equiv b(mod\ n) \iff b \equiv a(mod\ n)$
3. $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n) \implies a \equiv c(mod\ n)$
4. If $a \equiv b(mod\, n)$ and $c \equiv d(mod\, n)$ then $a+c \equiv b+d(mod\, n)$ and $ac \equiv bd(mod\ n)$
5. If $a \equiv b(mod\ n)$ then $a+c \equiv b+c(mod\ n)$ and $ac \equiv bc(mod\ n)$
6. If $a \equiv b(mod\ n)$ then $a^k \equiv b^k(mod\ n)$ for any positive integer k.

Theorem 4.1.2. If $ca \equiv cb(mod\ n)$ then $a \equiv b(mod\ n/d)$ where d = gcd(n,c).

Proof. As ca - cb = c(a - b) = kn for some integer k, and d = gcd(c,n), we have c = dr and n = ds for some integers r and s. Thus, r(a - b) = s. As gcd(r,s) =1, we thus have that $s|(a-b)$ or in other words, $a \equiv b(mod\ s)$. □

Corollary 4.1.2.1. If $ca \equiv cb(mod\ n)$ and gcd(c,n) =1, we have $a \equiv b(mod\ n)$.

4.2 Special Divisibility tests

Place value notation of numbers Given an integer b > 1, any integer N can be written as a unique combinations of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} \dots a_1 b + a_0$$

Or in other form,

$$N = (a_m a_{m-1} \dots a_1 a_0)_b$$

Proof. The division algorithm yields $N = q_0 b + r$ where $0 \leq r < b$. Now similarly it will yield $q_0 = q_1 b + r$ and so on. As $N > q_0 > q_1 \cdots > 0$, it is a decreasing sequence of integers and must terminate. Thus, let the last of q_i be q_m. Now substituting all of q_i's in
N = q_0b + r, we get the required form. For uniqueness, let a_i and

c_i be the two distinct sets of coefficients of b^i for all i from 0 to m, then subtracting the representations of N, we get

$$0 = (a_m - c_m)b^m + \cdots + (a_0 - c_0)$$

Let $d_i = a_i - c_i$ and d_k be the non-zero d_i for the smallest subscript k. Now,

$$0 = d_m b^m + \ldots d_k b^k$$

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1})$$

Thus $b|d_k$. But, $|d_k| < b$ as $|a_k - c_k| < b$. Thus, we have reached contradiction. □

Theorem 4.2.1. Let P(x) = $\sum_{m=0}^{k} c_l x^k$ be a polynomial in x, and if $a \equiv b(mod\ n)$ then $P(a) \equiv P(b)(mod\ n)$

Proof. Direct consequence of properties discussed earlier. □

Corollary 4.2.1.1. If a is a solution of $P(x) \equiv 0(mod\ n)$ and $a \equiv b(mod\ n)$ then b is also a solution.

Theorem 4.2.2. Let N = $\sum_{k=0}^{m} a_k 10^k$ and S = $\sum_{k=0}^{m} a_k$ then we have $9|N$ only if and only if $9|S$.

Proof. We can prove this by simply using the previous theorem and the fact that $10 \equiv 1(mod\ 9)$ □

Theorem 4.2.3. Let N = $\sum_{k=0}^{m} a_k 10^k$ and T = $\sum_{k=0}^{m} a_k(-1)^k$ then we have $11|N$ only if and only if $11|T$.

Proof. We can similarly prove this theorem by using a similar argument as the previous, and the fact that
$10 \equiv (-1)(mod\ 11)$. □

4.3 Linear Congruences

An equation of the form ax ≡ b (mod n) is called a linear congruence. A solution of this equation is an integer x_0 for which ax_0 ≡ b (mod n). This, by definition, means $ax_0 - b = ny_0$ for some y_0. This reduces to the diophantine equation $ax_0 - ny_0 = b$.

Theorem 4.3.1. The linear congruence x ≡ b (mod n) has a solution if and only if $d|b$ where d = gcd(a,n). In this case, it has d mutually congruent sets of solutions.

Proof. Recall results of Diophantine equation's solution analysis from chapter 2. □

Remark. Here the d mutually incongruent solutions are:

$$x_0, x_0 + n/d, x_0 + 2(n/d) \ldots, x_0 + (d-1)n/d$$

Corollary 4.3.1.1. If gcd(a,n) =1 then the linear congruence ax ≡ b (mod n) has a unique solution modulo n.

Theorem 4.3.2 (The Chinese remainder theorem)**.** Let $n_1, n_2, n_3 \ldots n_r$ be positive integers such that gcd(n_i, n_j) =1 $\forall\ i \neq j$. Then the system of linear congruences :

$$x \equiv a_1 (mod n_1)$$

$$x \equiv a_2 (mod n_2)$$

$$x \equiv a_3 (mod n_3)$$

.

.

$$x \equiv a_r (mod n_r)$$

has a simultaneous solution which is unique modulo $(n_1 n_2 n_3 \ldots n_r)$.

Proof. Let n = $n_1 n_2 n_3 \ldots n_r$
Now, for each i such that $1 \leq i \leq r$, let $N_i = n/n_i$. By hypothesis, gcd(N_i, n_i) =1. Thus a solution for the linear congruence $N_i x \equiv 1$ (mod n_i) exists, let that be x_i.
Let $\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r$.
As $N_i \equiv 0$(mod n_k) for k *neq* i. Thus, $\bar{x} \equiv a_k N_k x_k (mod\ n_k)$. But since $N_k x_k \equiv 1 (mod\ n_k)$ we have
$\bar{x} \equiv a_k.1 (mod\ n_k)$ for all k
Thus a simultaneous solution exists.
If there is another solution x' satisfying the given system of linear congruences, then $n_k | (\bar{x} - x')$ for each k.
Thus $n_1 n_2 n_3 \ldots n_r | (\bar{x} - x')$.
Therefore $\bar{x} \equiv x' (mod\ n)$. □

Chapter 5

Fermat's theorem

5.1 Fermat's factorization method

For any odd integer n, finding factors n = ab is equivalent to solving for x and y in n = $x^2 - y^2$, where $x = (a + b)/2$ and $y = (a - b)/2$. For even integers, powers of 2 can be separated into factors and thus odd integers are our concern.
Now for $x^2 - n = y^2$, we need to determine the smallest integer k such that $k^2 \geq n$. Now the numbers

$$k^2 - n, (k + 1)^2 - n, \ldots$$

are to be searched for perfect squares, until the trivial solution of n=n.1, or

$$((n + 1)/2)^2 - n = ((n - 1)/2)^2$$

is reached.

5.2 Fermat's Little Theorem

Theorem 5.2.1. If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1(\text{mod p})$.

Proof. Consider the set of integers a, 2a, 3a, ... (p-1)a. None of these is congruent modulo p to any other, or 0. Also, this set of integers is congruent modulo p to 1, 2, 3, ... ,p-1 in some order. Multiplying these congruences, we get:

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

But as gcd(p,(p-1)!) =1, we can cancel (p-1)! on both sides and reach our result. □

Corollary 5.2.1.1. If p is prime, $a^p \equiv a(\text{mod p})$ for any integer a.

Lemma 5.2.2. If p and q are distinct primes, $a^{pq} \equiv a(\text{mod pq})$.

Proof. Use a^q in the above corollary to obtain
$a^{pq} \equiv a(\text{mod p})$. Similarly, $a^{pq} \equiv a(\text{mod q})$. Therefore $a^{pq} \equiv a(\text{mod pq})$. □

5.3 Wilson's theorem

Theorem 5.3.1. If p is prime, then (p-1)! ≡ (-1) (mod p).

Proof. As p=2 and p=3 are obvious cases, let us take $p > 3$. Now consider the integers 1,2,3,4 . . . ,p-1. Let us consider the linear congruence ax ≡ 1(mod p). But gcd(a,p) =1. Thus a solution a' exists such that
$1 \leq a' \leq p-1$. Since p is prime, a = a' only is a =1 or a = p -1, since the congruence $a^2 \equiv 1(mod\ p)$ is nothing but $(a^2 - 1) \equiv 0(mod\ p)$ or either $a - 1 \equiv 0(mod\ p)$ where a =1 or $a + 1 \equiv 0(mod\ p)$ where a =p -1. Thus grouping the remaining numbers from the earlier list into (p-3)/2 pairs, and multiplying the congruences, we get:

$$2.3.4 \ldots (p-2) \equiv 1(modp)$$

Thus multiplying by p -1.

$$(p-1)! \equiv (p-1)(mod\ p) \equiv (-1)(mod\ p)$$

□

Theorem 5.3.2. The quadratic congruence $x^2 + 1 \equiv 0(mod\ p)$ where p is an odd prime, has a solution only if $p \equiv 1(mod\ 4)$

Proof. Let a be a solution of the quadratic congruence, so that $a^2 + 1 \equiv 0(mod\ p)$
Therefore, $a^2 \equiv (-1)(mod\ p)$
But since $p \nmid a$, by Fermat's theorem we have

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

As $1 \equiv -1(mod\ p)$ is false, p cannot be of the form
4n + 3. Thus, p is of the form 4n + 1. □

Chapter 6

Number theoretic functions

6.1 The functions τ and σ

Any function whose domain of definition is the set of positive integers is called as a number theoretic function.

Definition 6.1.1. For any positive integer n, τ(n) denotes the number of divisors of n and σ(n) denotes the su of all divisors of n. Here,

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

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

Theorem 6.1.1. If n $= p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}$ is the prime factorization of an integer n > 1, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$ for all $1 \leq i \leq r$.

Proof. Let d $= q_1 q_2 \dots q_s$ and $d' = t_1 t_2 \dots t_x$ be the divisors of n, where q_i and t_i are prime, such that n $= dd'$. Thus,

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_r^{k_r} = q_1 q_2 \dots q_s t_1 t_2 \dots t_x$$

Now by uniqueness of the prime factor representation, Each q_i must be one of p_k. Thus, d $= p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_r^{a_r}$. Now, $d' = n/d$. The exponents of primes being positive in d' gives the condition that $a_i < k_i$. □

Theorem 6.1.2. If n $= p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}$ is the prime facrorization of an integer $n > 1$ then:

$$1.\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1)$$

$$2.\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Remark. The product of all divisors of n is $n^{\frac{\tau(n)}{2}}$.

Definition 6.1.2. A number theoretic function f is said to be multiplicative if

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

where gcd(m,n) = 1.

Remark. The funtions τ and σ are multiplicative.

Lemma 6.1.3. If gcd(m,n) =1, then the set of positive divisors of mn consist of all the numbers $d_1 d_2$ such that $d_1 | m$ and $d_2 | n$ and gcd$(d_1, d_2\ )$ =1. Also, all these products are distinct.

Proof. Trivial using prime factorization and theorem 6.1.1. □

Theorem 6.1.4. If f is a multiplicative function and F is a funtion defined by

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

then F is also multiplicative.

Proof. Let m, n be two positive integers. Therefore,

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2)$$

By the previous Lemma and multiplicativity of f, we have:

$$F(mn) = \sum_{d_1|m, d_2|n} f(d_1)f(d_2) = (\sum_{d_1|m} f(d_1))(\sum_{d_2|n} f(d_2)) = F(m)F(n)$$

□

6.2 The Mobius inversion formula

Definition 6.2.1 (The Mobius function μ)**.** For any integer n, define
$\mu(n) = 1$ if $n = 1$;
$\mu(n) = 0$ if $p^2|n$ for some prime p ;
$\mu(n) = (-1)^r$ if $n = p_1p_2p_3 \dots p_r$ where p_i are primes.

Remark. μ is a multiplicative function.

Theorem 6.2.1. For any integer n ≥ 1, we have :
$\sum_{d|n} \mu(d) = 1$ if n =1
$\sum_{d|n} \mu(d) = 0$ is $n > 1$

Theorem 6.2.2 (Mobius inversion formula)**.** Let f and F be two number theoretic functions related by the formula :

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

Then,

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

Proof.

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

As $d|n$ and $c|(n/d)$, we have $c|n$ and $d|(n/c)$. Thus,

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

But, by theorem 6.2.1, $\sum_{d|(n/c)} \mu(d)$ is non-zero only when n/c =1, i.e. n=c. Thus,

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

□

Remark.

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

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

6.3 The greatest integer function

Definition 6.3.1. For any real number x, define [x] to be the largest integer less than or equal to x. In other words, [x] is the unique integer satisfying $x - 1 < [x] < x$.

Theorem 6.3.1. If n is a positive integer and p is a prime, then the exponent of p in the prime factorization of n! is

$$\sum_{k=1}^{\infty} [n/p^k]$$

Theorem 6.3.2. Let f and F be number theoretic functions such that

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

Then, for any integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)[N/k]$$

Proof.

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d)$$

For a fixed integer k $\leq$ N, we have $[N/k]$ multiples of k occuring from 1 to N, and thus the function f will be evaluated $[N/k]$ times. Summing over, we get the desired result. □

Corollary 6.3.2.1. If N is a positive integer,

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} [N/n]$$

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n[N/n]$$

Revised plan of action

Following is my revised Plan of action:

1. Week 5- Chapter 7: Euler's generalization of Fermat's theorem.
2. Week 6- Chapter 8: Primitive roots and indices.
3. Week 7- Chapter 9: The quadratic reciprocity law ,Chapter 10: Perfect numbers.
4. Week 8- Chapter 11: The Fermat conjecture ,Chapter 12: Representation of integers as sum of squares.
5. Extra- Chapter 13: Fibonacci numbers and continued fractions.