1.0 Introduction

Well Ordering Principle: Every nonempty set S of non-negative integers contains a least element; that is there is osme integer a in S such that $a \leq b$ for all b's belonging to S

Theorem 1.1: Archimedian property. If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.

Theorem 1.2 First Principle of Finite Induction. Let S be the set of positive integers.
(a) The integer 1 belongs to S
(b) Whenever the integer k is in S, the next integer $k+1$ must also be in S

Theorem 1.2 Second Principle of Finite Induction. Let S be the set of positive integers.
(a) The integer 1 belongs to S
(b') If k is a positive integer such that $1, 2, \cdots, k$ for $k \in S$, then $k+1$ must also be in S.

Thus S is the set of all positive integers.

Binomial Theorem

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Canceling either $k!$ or $(n-k)!$ yields

$\frac{n(n-1)\cdots(k+1)}{(n-k)!}$ or $\frac{n(n-1)\cdots(n-k+1)}{k!}$

If $k=0$ or $k=1$ then we have $\binom{n}{0} = \binom{n}{n} = 1$

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

Pascals Triangle

Rows of pascals triangle are built by $(a+b)^n$.
$(a+b)^1 = a+b$
$(a+b)^2 = a^2 + 2ab + b^2$
$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
$(a+b)^4 = a^4 + 5a^3b + 6a^2b^2 + 4ab^3 + b^4$
When $a=b=1$ the following triangle is built
1 1
1 2 1
1 3 3 1
1 4 6 4 1

The binomial expansion takes the form $(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} ab^{n-1} + \binom{n}{n} b^n$

or $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$

1.1 Chapter 2

Pythagoreans were pretty weird and attached tons of religious connotations to numbers.
The number 1 represents reason
The number 2 stood for man
The number 3 stood for woman
4 stood for justice since it is the first number that is the product of equals
5 was for marriage because it formed the union of 2 and 3 (man and woman)

All sums $1 + \cdots + n$ are actually triangular numbers.

Triangular Numbers
A number is triangular if it is of the form $\frac{n(n+1)}{2}$
n is triangular if $8n + 1$ is a perfect square.
The sum of any consecutive two triangular numbers is a perfect square. It is in fact the nth square. Take $1 + 1 + 2 = 4$ for example. Here 4 is the square of the second natural number and it is also the sum of the first two summations for $n = 1$ and $n = 2$ respecitively.
If n is triangular then so is $9n + 1$, $25n + 3$, and $49n + 6$

Let t_n denote the nth triangular number
$t_n = \binom{n+1}{2}$

$t_{n-1} + t_n = n^2$

$t_1 + t_2 + t_3 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}$ the sum of n consecutive triangular numbers is the same as the sum of n consecutive squares because we have previously shown that the sum of the two consecutive triangular numbers is the nth square.

$$\binom{2}{2} + \cdots \binom{n}{2} \binom{(n+1)}{3}$$
This formula is an extension of binomial expansion formula for summations

If t_n is a perfect square then $t_{4_n(n+1)}$ is also a perfect square.

The difference of two consecutive triangular numbers is a cube.

Pentagonal Numbers
let p_n = the nth pentagonal number

$p_n = \frac{n(3b-1)}{2}$

$p_n = t_{n-1} + n^2$

$p_n = 3t_{n-1} + n = 2t_{n-1} + t_n$

2.2 The Division Algorithm

Theorem 2.1: Division Algorithm. Given integers a and b with $b > 0$, there exists unique integers q and r such that
$a = qb + r \ 0 \leq r < b$
q is called the quotient and r the remainder in the division of a by b.

when $b = 2 \ r = 0$ or $r = 1$

when $a = 2q + 0$, a is called even

when $a = 2q + 1$, a is called odd

The previous 2 statements are imply that any integer is of the form $2n + 1$ or $2n + 0$ similary any square is of the form

$(2q)^2 = 4k$ or $(2q+1)^2 = 4(q^2+q)+1 = 4k+1$ this also implies that any square is has a remainder 0 or 1 when divided by 4

Greatest Common Divisor

An int a is said to be divisible by an integer $a \neq 0$, $a|b$ if there exists some integer c such that $b = ac$ we write $a \nmid b$ if a does not divide b.
$a|b$ means a divides b

Theorem 2.2

1. $a|0, 1|a, a|a$
2. $a|1$ iff $a = \pm 1$
3. If $a|b$ and $c|d$ then $ac|bd$
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 $a|(bx+cy)$ for arbitrary x, y

Definition 2.2: Let a and b be given integers, with at least one different from zero. The GCD of a and b, denoted by $gcd(a,b)$ is the positive integer d satisfying the following.

1. $d|a$ and $d|b$
2. If $c|a$ and $c|b$, then $c \leq d$

Theorem 2.3: Given integers a and b, not both of which are zero, there exists x and y such that $gcd(a,b) = ax + by$.

Definition 2.3: Two integers a and b, not both of which are zero, said to be relatively prime when $gcd(a,b) = 1$.

Theorem 2.4: Let a and b be integers, not both zero. Then a and b are relatively prime iff there exists integers x and y such that $1 = ax + by$.

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

Theorem 2.5 Euclid's Lemma: If $a|bc$, and $gcd(a, b) = 1$, then $a|c$

Theorem 2.6: Let a, b be integers, not both zero. For a positive integer d, $d = gcd(a, d)$ iff

1. $d|a$ and $d|b$
2. Whenever $c|a$ and $c|b$, then $c|d$

2.4 The Euclidian Algorithm

The Euclidian Algorithm is a process for finding the gcd of two numbers. The equations that describe it are as follows.

Given intergers a and b where $a \geq b > 0$

$a = q_1 b + r_1$
$b = q_2 r_1 + r_2$
$r_1 = q_3 r_2 + r_3$
$\vdots$
$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n-1} = q_{n+1} r_n + 0$

r_n the last non-zero remainder that appears is equal to $gcd(a, b)$.

Theorem 2.7: If $k > 0$, then $gcd(ka, kb) = kgcd(a, b)$.

For all $k \neq 0$, $gcd(ka, kb) = |k|gcd(a, b)$.

Definition 2.4: The least common multiple of two non-zero integers a and b, denoted $lcm(a, b)$, is the positive integer m satisfying

1. $a|m$ and $b|m$
2. If $a|c$ and $b|c$, with $c > 0$, then $m \leq c$.

$gcd(a, b) * lcm(a, b) = ab$.

The ideas of the gcd() can be extended to more than two integers a, b, c. $gcd(a, b, c)$ is defined as the psoitive integer d haveing the following properties

1. d is a divisor of each a, b, c.
2. If e divides the integers a, b, c, then $e \leq d$.

For any choice of positive integers a and b, $lcm(a, b) = ab$ iff $gcd(a, b) = 1$.

2.3 Diophantine Equations

Theorem 2.9: The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$, where $d = gcd(a, b)$. If x_0, y_0 is any particular solution of this equation then all other solutions are given by $x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$. Where t is an arbitrary integer.

Relatively prime form of theorem 2.9: $r(x' - x_0) = s(y_0 - y')$ where $a = dr$ and $b = ds$.

Corallary: If $gcd(a, b) = 1$ and if x_0, y_0 is a particular solution of the linear Diophantine equation $ax + by = c$, then all solutions are given by
$x = x_0 + bt$ and $y = y_0 - at$.

3.0 Chapter 3 Primes And Their Distributions

Definition 3.1: An integer $p > 1$ is called a prime number if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed composite.

Theorem 3.1: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Corollary: If p is a prime and $p|a_1a_2 \cdots a_n$, then $p|a_k$ for some k, where $1 \leq k \leq n$.

Corollary: If $p, q_1, q_2, \cdots, q_n$ are all primes and $p|q_1q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.

theorem 3.2 The fundamental Theorem of Arithmetic: Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Corollary: Any positive integer $n > 1$ can be written uniquely in a canonical form $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.
this theorem just states that primes can be repeated in a numbers representation. Just think of $18 = 2 * 2 * 3$ it prime factorization has 2 2's.

Theorem 3.3 The Famous Pythagororas Result: The number $\sqrt{2}$ is irrational (he almost got stoned for this).

3.1 Sieve of Eratosthenes

If a is a composite and $a > 1$ then $a = bc$, where $1 < b < a$ and $1 < c < a$. In other words it has two non-zero factors. Assuming $b \leq c$ implies $b^2 \leq bc = a$ and $b \leq \sqrt{a}$; and becuase theorem 3.2 ensures will will have at least one prime factor p, it follows that $p|b \wedge b|a$, therefor $p|a$. Thus a composite number a will always possess a prime divisor p satisfiying $p \leq \sqrt{a}$.

This result means that in testing the primality of a you need only test disvision by all primes $p < \sqrt{a}$. Similarly to find the prime factorization of a you need only test divisability of by all primes less than $\sqrt{a}$. A simple algorithm to determine prime factorization then would be.
for $a \in \mathbb{Z}$ and prime p where $p < \sqrt{a}$. If $p|a$ add p to the list of prime factors and divide a by p. Repeat process with all prime factors $q < \sqrt{\frac{a}{p}}$ until $a = 1$ and all factors are exhausted.

Theorem 3.4 Euclid: There is an infinite number of primes.

There are a couple ways to estimate the size of the nth prime.

$p_n^2 < p_1 p_2 \cdots p_{n-1} n \geq 5$.

Theorem 3.5: If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.

Corollary: For $n \geq 1$ there are at least $n+1$ primes less than 2^{2^n}.

The proof is omitted but, there is a proven theorem stating that between $n \geq 2$ and $2n$ there is at least one prime. Base on this result it can be shown that $p_n < 2^n$ where $n \geq 2$.
Consequently $p_{n+1} < 2p_n$ for $n \geq 2$.

3.2 Goldbachs Conjecture

The product of two or more integers of the form $4n + 1$ is of the same form.

Theorem 3.6: There are infinite number of primes of the form $4n + 3$.

Theorem 3.7 Dirichlet: If a and b are relatively prime positive integers, then the arithmetic progression $a, a + b, a + 2b, 2 + 3b, \cdots$ contains infinitely many primes.

Theorem 3.8: If all the $n > 2$ terms of the arithmetic progression $p, p + d, p + 2d, \cdots, p + (n - 1)d$ are prime
then the common difference d is divisible by every prime $a < n$.

Interesting Fact: Any prime above 5 must end in a 1, 3, 7, or a 9. This sounds kind of obvious since anything ending in 5 is divisble by 5 but still interesting to note.