PRELIMINARIES

The **counting numbers** or **natural numbers** are 1, 2, 3, 4, 5, 6. . . .
The **whole numbers** are the counting numbers with zero 0, 1, 2, 3, 4, 5, 6. . . .
The **integers** are the counting numbers and zero and negative numbers.

. . . -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6 . . .

The counting numbers are also called the *positive integers*. The whole numbers are also called the *non-negative integers*.

Meaning of addition

$a+b$ is the number of objects when combining a group of a objects with a group of b objects.

Meaning of multiplication

$a \cdot b$ is the number of objects in a groups with b objects in each group.

Definition: An *Arithmetic Sequence* is a sequence created by starting with a number. Each subsequent entry is obtained from the previous entry by adding the same fixed number. Alternately, an arithmetic sequence is a sequence in which there is a constant difference between successive terms.

Example: A +3 cricket that starts at 2, hops out an arithmetic sequence:

2, 5, 8, 11, 14, 17, . . .

A formula for the nth number in the sequence is given by $2+3 \cdot n$. When $n=0$ the cricket is on 2, when $n=1$ the cricket is on 5, etc.

Definition: An *Arithmetic Progression* is an arithmetic sequence in both directions.
Example: If consider where the +3 cricket was before she got to 2, we could still use the formula, $2+3 \cdot n$, but consider negative values of n. The entire progression may be written, in part by

. . . -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, . . .

(*n,m*) Combination Chart

A (*n,m*) *Combination Chart*, is created on a square grid by starting at 0 and adding n for each step in the positive x-direction and adding m for each step in the positive y-direction. Combination Charts can also be extended backwards to include negative combinations downwards and to the left.

Example: This shows part of a (3,5)-Combination Chart. That shaded part are positive combinations of positive. Going down from the shaded region, combinations have negative multiples of 5. Going left of the shaded region, combinations have negative multiples of 3.

10	13	16	19	22	25	28	31	34	37	40
5	8	11	14	17	20	23	26	29	32	35
0	3	6	9	12	15	18	21	24	27	30
-5	-2	1	4	7	10	13	16	19	22	25
-10	-7	-4	-1	2	5	8	11	14	17	20
-15	-12	-9	-6	-3	0	3	6	9	12	15
-20	-17	-14	-11	-8	-5	-2	1	4	7	10
-25	-22	-19	-16	-13	-10	-7	-4	-1	2	5
-30	-27	-24	-21	-18	-15	-12	-9	-6	-3	0
-35	-32	-29	-26	-23	-20	-17	-14	-11	-8	-5
-40	-37	-34	-31	-28	-25	-22	-19	-16	-13	-10

Notice: Each row going right and each column going up in a combination chart is an arithmetic sequence. The chart may be continued to include negative numbers. Then each row and each column is an arithmetic progression. The numbers on any diagonal also form an arithmetic progression. In fact any arrow combination, produces an arithmetic progression.

Example: Think of a cricket that hops →↑↑ on each hop. If this cricket starts on 3 on this (3,5) CC, it will hop out the sequence 3, 16, 29, 42, . . . If it starts on -6 it hops out the sequence -62, 15, 28, 41, . . .

Definitions and Basic Properties of Integers

	Addition	***Multiplication***
There is an unique **additive identity** named *0*	$a + 0 = a$	
There is an unique **multiplicative identity** named *1*		$a \cdot 1 = a$
Inverses: For any integer there is a unique additive inverse inverses,	$a + -a = 0$	1 and -1 are the only integers that have integer multiplicative they are called *units*
Associative Property:	$(a + b) + c = a + (b + c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Commutative Property:	$a + b = b + a$	$a \cdot b = b \cdot a$

The **Distributive** Property: $a \cdot (b + c) = a \cdot b + a \cdot c$

(Gives a relationship between addition and multiplication)

DIVISION

Meaning of division
$a \div d$ is *how many groups* can be made of *a* objects, if there are *d* objects in each group.
OR
it is *how many objects in each group* if *a* objects are grouped into *d* groups.

Division does not always have a whole number solution, but we can divide and keep track of the remainder:

Theorem 1 The Division Algorithm

Given two integers, m and $n > 0$, there exist *unique* integers q and r, with

$$m = q \cdot n + r, \text{ and } 0 \leq r < n$$

Proof: Repeatedly subtract n from m. Stop the last time you are able to subtract without going less than zero. q is the number of times you subtracted n and r is the amount left over.

Examples:

If $m = 100$, $n = 23$, then q=4 and r=8. $100 = 4 \cdot 23 + 8$
If $m = 124$, $n = 4$, then q=41 and r=0. $124 = 41 \cdot 4 + 0$
If $m = 60$, $n = 7$, then q=8 and r=4. $60 = 8 \cdot 7 + 4$

Examples with negative numbers:
If $m = -60$, $n = 7$, then q=-9 and r=3. $-60 = -9 \cdot 7 + 3$
NOT $-60 = -8 \cdot 7 - 1$ because r must be positive.
If $m = 60$, $n = -7$, then q=-8 and r=4. $60 = -8 \cdot -7 + 4$
If $m = -60$, $n = -7$, then q=9 and r=3. , $-60 = 9 \cdot -7 + 3$

The special case when $r = 0$ is worth special terminology and notation:

DIVISIBILITY

Definition: For d, a integers, we say that "***d* divides *a***" – and we write, ***d* | *a*** -- if there is an unique integer, q, such that $a=q\cdot d$.
In this case, we may also write

$$\frac{a}{d}=q \qquad \text{or} \qquad a \div d = q \qquad \text{or} \qquad d\overline{)a}\,.$$

In more familiar language, we also say that d is a factor of a or that a is a multiple of d.

Theorem 1.1: If $d \mid a$, then $0 < |d| \leq |a|$. In particular, d cannot be zero, that is we cannot divide by zero. Even 0 cannot be divided by 0.

Theorem 1.2

a) $d \mid a$ if and only if $d \mid -a$

b) $d \mid a$ if and only if $-d \mid a$

c) $\pm 1 \mid a$, for every integer a.

d) If $d \mid \pm 1$, then $d = \pm 1$.

e) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

Theorem 1.3

a) If $a \mid b$ and $b \mid c$, then $a \mid c$

b) If $d \mid a$ and $d \mid b$, then $d \mid a+b$

c) If $d \mid a$, then $d \mid c\cdot a$ for every integer c.

d) If $d \mid a$ and $d \mid b$, then $d \mid x\cdot a+y\cdot b$ for arbitrary integers x and y.

GREATEST COMMON DIVISOR

Definition: The *greatest common divisor* of two or more non-zero numbers is the greatest positive integer that divides all of the numbers. The greatest common divisor of two non-zero integers A and B is abbreviate: gcd(A, B). Sometimes in elementary school it is called the *greatest common factor*.

Euclidian Algorithm: The Euclidean Algorithm uses repeated subtraction to find the gcd(A,B). The following theorem is the major step we need to justify finding the gcd(A, B) using the Euclidean Algorithm.

Theorem 1.4 If $A - q \cdot B = r$, then gcd(A,B)=gcd(B,r)

This theorem shows how the Euclidean Algorithm can be use to find the gcd of two numbers, A and B. The Euclidean algorithm, like long division, has many steps. First we use the division algorithm to write

$A - q_1 \cdot B = r_1$ Now our problem (by Thm 1.4) has been reduced to finding gcd (B, r) since, by Theorem 1.6, gcd(A,B)=gcd(B,r), so B is our new A and r is our new B.

$B - q_2 \cdot r = r_2$ Notice that gcd(A,B)=gcd(B,r)=gcd(r, r_2)

$r - q_3 \cdot r_2 = r_3$ and we can continue for as many steps as needed until we see what the gcd must be. Now gcd(A,B)=gcd(B,r)=gcd(r, r_2)= gcd(r_2, r_3).

$r_{n-1} - q_{n-1} \cdot r_n = r_{last}$ It is important to notice that the algorithm will eventually stop because the r's are getting smaller and smaller. Eventually some last r will be 0,

$r_n - q_n \cdot r_{last} = 0$ and so gcd(A,B)=gcd(B,r)=gcd(r, r_2)= gcd(r_2, r_3) . . . gcd(r_{last},0). But the least common divisor of any number and zero has to be that number itself so r_{last} is the least common divisor of A and B as well.

Theorem 2 The Extended Euclidean Algorithm The equation A·N + B·M = C has a solution N and M, integers, if and only if gcd (A, B) | C.

(Note: this is equivalent to saying that C must be on the (A, B) - Combination Chart.)

A – (B * Q) = R	N	M
	R = A*N + B*M	
	A	1	0
	B	0	1
	Q=int(A/B)	R=A-Q*B	N2-Q*N1	M2-Q*M1
A	B				

IMPORTANT CONSEQUENCES OF THE EUCLIDEAN ALGORITHM

Theorem 2.1 If $m \mid a \cdot b$ and if $\gcd(a,m) = 1$, then $m \mid b$. In particular, if $p \mid a \cdot b$ where p is a prime number, then $p \mid a$ or $p \mid b$.

Proof: Find N and M such that $a \cdot N + m \cdot M = 1$. Multiply both sides by b to get $a \cdot b \cdot N + m \cdot b \cdot M = b$. m divides both terms on the left hand side, so m divides b as well.

The following theorem is too important to have a number. It is just known by it's name:

Fundamental Theorem of Arithmetic Every positive integer can be factored uniquely as a product of prime numbers.

MODULAR ARITHMETIC

Definition: $a \equiv b \pmod{m}$ means that $m \mid (a - b)$ or equivalently that $a - b$ is a multiple of m or that m is a factor of $a - b$.

Theorem 3.0 $a \equiv b \pmod{m}$ if and only if a and b both have the same remainder when divided by m.

Definition: The *least residues* mod m are the positive integers from *0* to *m-1*.

Theorem 3.1 $a \equiv a \pmod{m}$

Theorem 3.2 If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

Theorem 3.3 If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

Theorem 3.4 If $a \equiv b \pmod{m}$, then $a+c \equiv b+c \pmod{m}$

Theorem 3.5 If $a \equiv b \pmod{m}$, then $a \cdot c \equiv b \cdot c \pmod{m}$

Theorem 3.6 If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \cdot c \equiv b \cdot d \pmod{m}$

Theorem 3.7 If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$

Theorem 3.8 If If $a \equiv b \pmod{m}$ and k is any natural number, then $a^k \equiv b^k \pmod{m}$

Definition: We say that two positive integers, *a* and *b*, are *relatively prime* when gcd(*a,b*)=1.

Cipher fact: An integer, *k*, makes a "good" multiplicative key if and only if *k* and *26* are relatively prime [gcd(*k,* 26)=1].

Reason: Multiplicative key *k* is a "good" key if there is a multiplicative inverse for *k,* that is, there is a number, *N,* such that $k \cdot N \equiv 1 \,(mod\, 26)$. Which means that $k \cdot N - 1$ is a multiple of 26. That is, $k \cdot N - 1 = 26 \cdot M$ OR $k \cdot N - 26M = 1$. We know from the Extended Euclidean Algorithm that this Diophantine equation has solutions if and only if gcd(*k,* 26)=1.

In general,

Definition: Given integers *a* and *b*, we say that *b* is the inverse of *a* mod *m* if and only if $a \cdot b \equiv 1 \pmod{m}$

Theorem 2.9: For any integers *a* and *m*, *a* has an inverse (mod *m*) if and only if gcd(*a, m*)=1.

Proof: We can find the inverse by using the extended Euclidean Algorithm to solve $a \cdot N - m \cdot M = 1$

Theorem 2.10: The congruence equation $ax \equiv b \pmod{m}$ has solutions if and only if $(a,m) \mid b$

EXAMPLE: Compare congruence equation $ax \equiv b \pmod{m}$ to linear Diophantine equation $ax + my = b$.

Definition: Least residue (mod *m*) means numbers from 0 to *m*-1.

Theorem 2.11: If $(a,m) = 1$ then $ax \equiv b \pmod{m}$ has exactly one least residue solution.

Proof: Because *a* is relatively prime to *m*, *a* has an inverse mod *m.* Multiply both sides of the congruence by the inverse of *a*, so *x* = (inverse of *a*) ·*b*.

Theorem 2.12: If $(a,m) = d$ and $d \mid b$ then $ax \equiv b \pmod{m}$ has exactly d least residue solutions. If *d* does not divide *b,* there are no solutions.

Here are two theorems we've know for some time:

Theorem 3.1 If $a \mid b \cdot m$ and if gcd$(a,m) = 1$ then $a \mid b$

Theorem 3.2 If $a \cdot c \equiv b \cdot c \pmod{m}$ and if gcd$(c,m) = 1$, then $a \equiv b \pmod{m}$

Theorem 4.1: If gcd $(a,m)=1$, then the least residues of the numbers $a, 2a, 3a, 4a, \ldots, (m-1)\cdot a$ are the numbers 1, 2, 3, 4, …, $(m-1)$.

Fermat's Theorem 4.2: If p is prime and if gcd $(a,p)=1$, than $a^{p-1} \equiv 1 \bmod p$.

Definition: We call the set of all positive numbers that are relatively prime to m and less than m the **reduced residue system mod *m***.

Theorem 5.1 If gcd$(a,m)=1$, then the set of all products $a \cdot x$, where x is relatively is in the reduced residue is the reduced residue system.

Definition: The number of integers in the reduced residue system mod m is called $\phi(m)$.

Theorem 5.2 $\phi(p)=p-1$ if p is a prime number.

Theorem 5.3 $\phi(p \cdot q)=(p-1)\cdot(q-1)$ if p and q are prime numbers.

Theorem 5.4 If gcd(a,n)=1, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Theorem 5.5 If gcd$(m,n)=1$, then $m^{\varphi(n)\cdot k+1} \equiv m \bmod n$.

Theorem 5.6 If $n=p \cdot q$, then $m^{\varphi(n)\cdot k+1} \equiv m \pmod{n}$, for all integers, m.

This is the theorem that tells us that RSA encryption works. That is, if we make a public key, (N, e), base on two prime numbers, p and q, and encode messages by raising to the e^{th} power, then raising the encrypted numbers to the d^{th} power will undo the encryption.

Theorem 5.7 If $N= p \cdot q$, where p and q are prime numbers and
if e is relatively prime to $\phi(N)=(p-1)\cdot(q-1)$ and
if d is the inverse of e mod $\phi(N)=(p-1)\cdot(q-1)$ and
if $C \equiv m^e \pmod{N}$
then
$m \equiv C^d \pmod{N}$.