Properties of the Integers

Let \( a, b \in \mathbb{Z} \) then

1. if \( c = a + b \) then \( c \in \mathbb{Z} \)
2. if \( c = a - b \) then \( c \in \mathbb{Z} \)
3. if \( c = (a)(b) \) then \( c \in \mathbb{Z} \)
4. if \( c = a/b \) then \( c \in \mathbb{Q} \)

If \( a \) & \( b \) are integers the quotient \( a/b \) may not be an integer. For example if \( c = 1/2 \), then \( c \) is not an integer. On the other hand with \( c = 6/3 \) then \( c \) is an integer.

We can say that \textit{there exists} integers \( a,b \) such that \( c = a/b \) is not an integer.

We can also say that \textit{for all} integers \( a,b \) we have \( c = a/b \) is a rational number.
Divisibility

Let $a, b \in \mathbb{Z}$, $a \neq 0$.
If $c = \frac{b}{a}$ is an integer,
or alternately if $c \in \mathbb{Z}$ such that $b = ca$
then we say that $a$ divides $b$ or equivalently,
b is divisible by $a$, and this is written

\[ a \mid b \]

NOTE: Recall long division:

```
  Quotient  015
  Divisor   32  487
  Dividend  48 32 167 160
  Remainder 7
```
Referring to the long division example, $a = 32$, is the divisor $b = 487$ is the dividend. The quotient $q = 15$ and the remainder $r = 7$.
In this case $a$ does not divide $b$ or equivalently $b$ is not divisible by $a$.

This can be notated as:

$$a \nmid b$$

and we can write $a = bq + r$ or, $487 = (32) (15) + 7$

**Division Algorithm Theorem**

Let $a, b \in \mathbb{Z}, b \neq 0$ there exists $q, r \in \mathbb{Z}$, such that:

$$a = bq + r, \quad 0 \leq r \leq |b|$$
NOTE: The remainder in the Division Algorithm Theorem is always positive. Therefore for values 

\[ a = 22, \ b = 7, \text{ and } a = -22, \ b = -7 \text{ we get} \]

\[ 22 = (7)(3) + 1 \]

but

\[ -22 = (-7)(4) + 6. \]
Divisibility

Suppose on the other hand that we have \( a = 217 \) and \( b = 7 \). We have \( 217 = (31)(7) + 0 \) so we conclude that \( b \mid a \).

\[
\begin{array}{c}
31 \\
7 \mid 217 \\
21 \\
07 \\
7 \\
0
\end{array}
\]
Divisibility Theorems.

Let \( a, b, c \in \mathbb{Z} \). If \( a \mid b \) and \( b \mid c \) then \( a \mid c \).

Suppose \( a \mid b \) then there exists an integer \( j \) such that

\[(1) \ b = aj\]

Similarly if \( b \mid c \) then there exists an integer \( k \) such that

\[(2) \ c = bk\]

Replace \( b \) in equation (2) with \( aj \) to get

\[(3) \ c = ajk\]

And thus we have proved that if \( a \mid b \) and \( b \mid c \) then \( a \mid c \).
**Divisibility Theorems.**

Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ then $a \mid bc$.

Since $a \mid b$ there exists an integer $j$ such that $b = aj$, and $bc = ajc$ for all (any) $c \in \mathbb{Z}$.

It should be obvious that $a \mid ajc$ ($\frac{ajc}{a} = jc$ is an integer)

so $a \mid bc$. 
Divisibility Theorems.

Let $a,b,c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$. Then $a \mid (b + c)$ and $a \mid (b - c)$.

Since $a \mid b$ there exist $a j \in \mathbb{Z}$ such that $b = aj$.

Since $a \mid c$ there exist $a k \in \mathbb{Z}$ such that $c = ak$.

Therefore $b + c = (aj + ak) = a(j + k)$.

Obviously $a \mid a(j + k)$ so $a \mid (b + c)$.

Similarly $a \mid a(j - k)$ so $a \mid (b - c)$.
Notation

The absolute value of a denoted by $|a|$ is defined as:

- $|a| = a$ if $a \geq 0$
- and $|a| = -a$ if $a < 0$.

Divisibility Theorems.

If $a | b$ then $|a| \leq |b|$.

If $a | b$ and $b | a$ then $|a| = |b|$.

If $a | 1$ then $|a| = 1$. 
Prime Numbers
A positive integer $p > 1$ is called a prime number if its only divisors are 1, -1, and $p$, -p.

The first 10 prime numbers are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

If an integer $c > 2$ is not prime, then it is composite. Every composite number c can be written as a product of two numbers a, b such that $a, b \not\in \{1, -1, c, -c\}$. 
Determining whether a number, \( n \), is prime or composite is a difficult computationally. A simple method (which is in essence of the same computational difficulty as more sophisticated methods) checks all integers \( k, \ 2 \leq k \leq \sqrt{n} \) to determine divisibility.

**Example:** Let \( n = 143 \)

- 2 does not divide 143
- 3 does not divide 143
- 4 does not divide 143
- 5 does not divide 143
- 6 does not divide 143
- 7 does not divide 143
- 8 does not divide 143
- 9 does not divide 143
- 10 does not divide 143
- 11 divides 143, \( 11 \times 13 = 143 \)
**Theorem:** Every integer \( n > 1 \) is either prime or can be written as a product of primes.

**For example:**

\[
12 = 2 \times 2 \times 3.
\]

17 is prime.

\[
90 = 2 \times 5 \times 3 \times 3.
\]

143 = 11 \times 13.

147 = 3 \times 7 \times 7.

330 = 2 \times 5 \times 3 \times 11.

Note: If factors are repeated we can use exponents.

\[
48 = 2^4 \times 3.
\]