The following notations will be followed in this report. These are basic notations, same as those done in high school or above, by most of the people.

Sets

A *set* is a collection of objects. The following sets (among others) will be used in this report:
$\mathbb{R}$: the set of real numbers.
$\mathbb{Z}$: the set of integers (positive, negative, or zero).
$\mathbb{Z}_n$: $\{0, 1, 2, \ldots, n-1\}$

The symbols $\varnothing$, $\in$, $\notin$, $\cup$, $\cap$, $\subseteq$ and $\supseteq$ have their usual meanings. If S and T are sets and, $S \cap T = \varnothing$, then S and T are said to be *disjoint*.
If S is a set and P a property (or a combination of properties), we can define a new set with the notation

$$\{x \in S \mid P(x)\}$$

which denotes 'set of all elements of S which have property P'.
The *order* or *cardinality* of a finite set S is the number of elements in S and is denoted by $|S|$. For example, $|\mathbb{Z}_n| = n$.
The *Cartesian Prooduct* of two sets S and T is given by

$$S \times T = \{(s,t) \mid s \in S,\ t \in T\}.$$

If S and T are finite sets, then $|S \times T| = |S| \cdot |T|$.
In general,

$$S_1 \times S_2 \times \cdots \times S_n = \{(s_1, s_2, \ldots, s_n) \mid s_i \in S_i,\ i = 1, 2, \ldots, n\},$$

is the *Cartesian Product* (a set of *ordered n-tuples*) of n sets $S_1, S_2, \ldots, S_n$.
In this report, an ordered n-tuple $(x_1, x_2, \ldots, x_n)$ will be denoted simply as $x_1 x_2 \cdots x_n$.

Combinatorics

Number of ways of choosing m distinct objects from n distinct objects
or
the coefficient of x^m in $(1+x)^n$
are both given by

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

where $p! = p(p-1)\cdots 3.2.1$ for $m > 0$ and $0! = 1$.
This bracket notation will be used throughout the report.

A *permutation* of a set $S = \{x_1, x_2, \ldots, x_n\}$ is a one-to-one mapping from set S to itself. It is denoted by

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \downarrow & \downarrow & & \downarrow \\ f(x_1) & f(x_2) & \ldots & f(x_n) \end{pmatrix}$$

Modular Arithmatic

Let m be a fixed positve integer. Two integers a and b are written as

$$a \equiv b \pmod{m}$$

if $a - b$ is divisible by m.
It can be noted that if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

(i) $a + b \equiv a' + b' \pmod{m}$
(ii) $ab \equiv a'b' \pmod{m}$

Fermat's Little Theorem: Let p be a prime, and a be any integer, then $a^p \equiv a \pmod{p}$