1 Things Past

1.1 Some Number Theory

Definition. *The set of **natural numbers** $\mathbb{N}$ is defined by*

$$\mathbb{N} = \{integers\ n : n \geq 0\}$$

Least Integer Axiom[1]**.** *There is a smallest number n in every non-empty subset C of $\mathbb{N}$.*

Definition. *A natural number is **prime** if $p \geq 2$ and there is no factorization $p = ab$ where $a < p$ and $b < p$ are natural numbers.*

Proposition 1.1. *Every integer $n \geq 2$ is either a prime or a product of primes.*

Proof. Let C be the subset of $\mathbb{N}$ consisting of all those $n \geq 2$ for which the proposition is false. If C is non-empty, then there exists a smallest number k in C. Since k is not a prime, then there are natural numbers a and b such that $k = ab$, where $a < k$ and $b < k$. But a and b are not in C since k is the smallest in C, then a and b are primes or product of primes. Therefore, the smallest number k in C is a product of primes, contradicting the proposition. □

Theorem 1.2 (Mathematical Induction). *Let $S(n)$ be a family of statements, one for each integer $n \geq m$, where m is some fixed number. If*

(i) $S(m)$ is true, and

(ii) if $S(n)$ is true implies $S(n+1)$ is ture,

then $S(n)$ is true for all integers $n \geq m$.

Proof. Let C be the set of all integers $n \geq m$ for which $S(n)$ is false. If C is not empty, there is a smallest integer k in C such that $S(k)$ is false. By (i) we have $k > m$, then there exists an integer $k-1 \notin C$ such that $S(k-1)$ is true. By (ii), we have $S((k-1)+1) = S(k)$, where $(k-1)+1 = k \notin C$ is also true. This contradicts the assumption that C is non-empty, thus C is empty. Therefore, the proposition is true. □

Theorem 1.3 (Second Form of Induction). *Let $S(n)$ be a family of statements, one for each integer $n \geq m$, where m is some fiexed integer. If*

1. *$S(m)$ is true, and*
2. *if $S(k)$ is true for all k with $m \leq k < n$, then $S(n)$ is itself true,*

then $S(n)$ is true for all integers $n \geq m$.

Proof. Let C be the set of all integers $n \geq m$ for which $S(n)$ is false. If C is not empty, there is a smallest integer k in C such that $S(k)$ is false. By (i) we have $k > m$, then there exists an integer $k-1 \notin C$ such that $S(k-1)$ is true. Then by (ii), since $S(i)$ is true for all i with $m \leq i < k$, then $S(k)$ is itself true, contradicting the assumption that $S(k)$ is false. □

Theorem 1.4 (Division Theorem). *Given integers a and b with $a \neq 0$, there exist unique integers q and r with*

$$b = qa + r \quad and \quad 0 \leq r < |a|$$

[1] This property is usually called the *well-ordering principle*

Proof. Suppose there exist another pair of integers q' and r' with $b = q'a + r'$ where $0 \leq r' < |a|$. Then $qa+r = q'a+r' \implies |(q-q')a| = |r'-r|$. Since $0 \leq |r'-r| < |r'| < |a| \implies 0 \leq |(q-q')a| < |a|$, if $a > 0$, then $0 \leq |q - q'| < 1$, recall that q and q' are both integers, then $q = q'$; if $a < 0$, then $-1 < |q - q'| \leq 0 \implies q = q'$. Both cases implies $r = r'$ as well. This contradicts the assumption, therefore, the integers are unique. $\square$

Definition. *If a and b are integers with $a \neq 0$, then the integers q and r occurring in the division algorithm are called* ***quotient*** *and* ***remainder*** *after dividing b by a.*

Corollary 1.5. *There are infinitely many primes.*

Proof. (***Euclid***) Suppose there are k finite primes $p_1, p_2, \cdots, p_k$. Then define $M = \prod_{i=1}^{k} p_i + 1$, by Proposition 1.1, it is either a prime or a product of primes. Since our assumption indicates M is not a prime, then it must be a product of primes. But the fact that $\frac{M}{\prod_{i=1}^{k} p_k}$ gives remainder not 0 but 1 shows M cannot be divided by the existing product of primes, by definition, M is a prime, which contradicting the assumption. So there must be infinite number of primes. $\square$

Definition. *If a and b are integers, then a is a* ***divisor*** *of b if there is an integer d with $b = ad$. We also say that a* ***divides*** *b or that b is a* ***multiple*** *of a, and we denote this by $a \mid b$*

Definition. *A* ***common divisor*** *of integers a and b is an integer c with $c \mid a$ and $c \mid b$. The* ***greatest common divisor*** *or* ***gcd*** *of a and b, denoted by (a, b), is defined by*

$$(a, b) = \begin{cases} 0 \ if \ a = 0 = b \\ the \ largest \ common \ divisor \ of \ a \ and \ b \ otherwise \end{cases}$$

Proposition 1.6. *If p is a prime and b any given integer, then*

$$(p, b) = \begin{cases} p \ if \ p \mid b \\ 1 \ otherwise \end{cases}$$