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. $\square$

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. $\square$

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. $\square$

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*

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

Proof. Since p is a prime, i.e., $p = p \cdot 1$ then $(p, p) = p$. If $p \mid b$, then we have $p \mid p$ and $p \mid b$ thus $(p, b) = p$; otherwise, if $p \nmid b$, then we have $1 \mid p$ and $1 \mid b$ thus $(p, b) = 1$. $\square$

Theorem 1.7. *If a and b are integers, then $(a, b) = d$ is a linear combination of a and b; that is, there are integers s and t with $d = sa + tb$.*

Proof. Since $(a, b) = d$, by division algorithm, we have $a = dq_a$ and $b = dq_b$ where $q_a,\ q_b \in \mathbb{Z}$. If $q_a = 0 = q_b$, the statement is obviously true. Then, $\forall q_a,\ q_b \in \mathbb{Z},\ \exists s,\ t \in \mathbb{Z}$ such that $sq_a = 1 - tq_b$. Thus

$$d = \frac{a}{q_a} = \frac{b}{q_b}$$

$$aq_b = bq_a \implies saq_b = sbq_a = (1 - tq_b)b$$

$$saq_b + tq_b b = b \implies sa + tb = \frac{b}{q_b} = d$$

$\square$

Proposition 1.8. *Let a and b be integers. A nonnegative common divisor d is their* gcd *if and only if $c \mid d$ for every common divisor c.*

Proof. Suppose c is a common divisor of both a and b, and C a set of all common divisors of a and b. By definition of gcd we have $d = \max S$, $\forall c \in S$, thus $c \mid d$. Conversely, if $c \mid d$ for every common divisor c, then $d = \max S$. $\square$

Corollary 1.9. *Let I be a subset of $\mathbb{Z}$ such that*

1. $0 \in I$;

2. *if $a,\ b \in I$, then $a - b \in I$;*

3. *if $a \in I$ and $q \in \mathbb{Z}$, then $qa \in I$.*

Then there is a natural number $d \in I$ consisting precisely of all the multiples of d.

Proof. Suppose there is no such a natural number $d \in I$. Then $\exists q' \in \mathbb{Z}$ such that $q'd \notin I$. This contradicts the third fact, thus the statement is true. $\square$

Theorem 1.10 (Euclid's Lemma). *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p devides a product $\prod_{i=1}^{n} a_i$, then it must divide at least one of the factors a_i.*

Proof. If $p \nmid a$, then $(p, a) = 1$ and $1 = sp + ta$. Then $b = spb + tab$ is a multiple of p. Thus the first statement is true.
As for the second statement, we prove by induction:

1. $n = 1$, p divides a_1 is obviously true;

2. Suppose $n = k$ is true, i.e., a prime p dividing a product $(a_1 \cdots a_k)$ implies p must divide at least one of the factors a_i is true. Then, when $n = k + 1$, it is still true as the factor (factors) still exists in the new product $(a_1 \cdots a_k a_{k+1})$, thus $n = k + 1$ is true.

Since $n = 1$ is true and $n = k$ true implies $n = k+1$ also true, therefore, by induction the statement is true for all $n \in \mathbb{Z}$. $\square$

Definition. *Call integers a and b are* ***relatively prime*** *is* $\gcd(a, b) = 1$.

Corollary 1.11. *Let a, b, and c be integers. If c and a are relaively prime and if $c \mid ab$, then $c \mid b$.*

Proof. Because $c \mid ab$, by Euclid's Theorem, $c \mid a$ or $c \mid b$. Since c and a are relatively prime, $c \nmid a$. Thus $c \mid b$. $\square$

Proposition 1.12. *If p is a prime, then $p \mid \binom{p}{j}$ for $0 < j < p$.*

Proof. By definition, the binomial coefficient $\binom{p}{j} = \frac{p!}{j!(p-j)!}$, such that $p! = \binom{p}{j} j!(p-j)!$, as $p \mid p!$, then $p \mid \binom{p}{j} j!(p-j)!$. By Corollary 1.11, since $p \nmid j!(p-j)!$, $p \mid \binom{p}{j}$. $\square$

Proposition 1.13.

1. *If a and b are integers, then a and b are relatively prime if and only if there are integers s and t with $1 = sa + tb$.*

2. *If $d = (a, b)$, where a and b are not both 0, then $(a/d, b/d)$=1.*

Proof. 1. Since $(a, b) = 1$, by Theorem 1.7, $1 = sa + tb$; conversely, suppose there is a common divisor $d = (a, b) \neq 1$, Then $d = s'a + t'b$, and $(s' - sd)a + (t' - td)b = 0$. This implies that 0 is also a common dividor, which is false. 2. Since $d = (a, b)$, then $d = sa + tb$ where s and t are integers. Thus $1 = s(\frac{a}{d}) + t(\frac{b}{d})$. $\square$

Theorem 1.14 (Euclidean Algorithm). *Let a and b be positive integers. There is an algorithm that finds the gcd, $d = (a, b)$, and there is an algorithm that finds a pair of integers s and t with $d = sa + tb$.*

Proof. ☐

Algorithm 1 My algorithm

procedure MyProcedure
    $stringlen \leftarrow$ length of $string$
    $i \leftarrow patlen$
top:
    if $i > stringlen$ **then return** false
    $j \leftarrow patlen$
$loop$:
    if $string(i) = path(j)$ **then**
        $j \leftarrow j - 1.$
        $i \leftarrow i - 1.$
        goto *loop*.
        close;
    $i \leftarrow i + \max(delta_1(string(i)), delta_2(j)).$
    goto *top*.