1.4 Division Algorithm and the Fundamental Theorem of Arithmetic

In the next few pages, we will try to study properties of integers that will be required later. We start with a lemma, commonly known as the "division algorithm". The proof again uses the technique "proof by contradiction".

Lemma 1.4.1 (Division Algorithm). *Let a and b be two integers with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$, where $0 \leq r < b$. The integer q is called the quotient and r, the remainder.*

Proof. Without loss of generality, assume that $a \geq 0$ and consider the set $S = \{a+bx : x \in \mathbb{Z}\} \cap \mathbb{N}$. Clearly, $a \in S$ and hence S is a non-empty subset of $\mathbb{N}$. Therefore, by Well-Ordering Principle, S contains its least element, say s_0. That is, there exists $x_0 \in \mathbb{Z}$, such that $s_0 = a + bx_0$. We claim that $0 \leq s_0 < b$.

As $s_0 \in S \subset \mathbb{N}$, one has $s_0 \geq 0$. So, let if possible assume that $s_0 \geq b$. This implies that $s_0 - b \geq 0$ and hence $s_0 - b = a + b(x_0 - 1) \in S$, a contradiction to the assumption that s_0 was the least element of S. Hence, we have shown the existence of integers q, r such that $a = qb + r$ with $0 \leq r < b$.

Uniqueness: Let if possible q_1, q_2, r_1 and r_2 be integers with $a = q_1 b + r_1 = q_2 b + r_2$, with $0 \leq r_1 \leq r_2 < b$. Therefore, $r_2 - r_2 \geq 0$ and thus, $0 \leq (q_1 - q_2)b = r_2 - r_1 < b$. Hence, we have obtained a multiple of b that is strictly less than b. But this can happen only if the multiple is 0. That is, $0 = (q_1 - q_2)b = r_2 - r_1$. Thus, one obtains $r_1 = r_2$ and $q_1 = q_2$ and the proof of uniqueness is complete.

This completes the proof of the lemma. ■

Definition 1.4.2 (Greatest Common Divisor).

1. *An integer a is said to* divide *an integer b, denoted $a|b$, if $b = ac$, for some integer c. Note that c can be a negative integer.*
2. Greatest Common Divisor: *Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then the greatest common divisor of a and b, denoted* $\gcd(a,b)$*, is the largest positive integer c such that*
   - *(a) c divides a and b, and*
   - *(b) if d is any positive integer dividing a and b, then d divides c as well.*
3. Relatively Prime/Coprime Integers: *Two integers a and b are said to be relatively prime if* $\gcd(a,b) = 1$.

Theorem 1.4.3 (Euclid's Algorithm). *Let a and b be two non-zero integers. Then there exists an integer d such that*

1. $d = \gcd(a,b)$*, and*

2. *there exist integers x_0, y_0 such that $d = ax_0 + by_0$.*

Proof. Consider the set $S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Then, either $a \in S$ or $-a \in S$, as exactly one of them is an element of $\mathbb{N}$ and both $a = a \cdot 1 + b \cdot 0$ and $-a = a \cdot (-1) + b \cdot 0$ are elements of the set $\{ax + by : x, y \in \mathbb{Z}\}$. Thus, S is non-empty subset of $\mathbb{N}$. So, by Well-Ordering Principle, S contains its least element, say d. As $d \in S$, there exist integers x_0, y_0 such that $d = ax_0 + by_0$.

We claim that d obtained as the least element of S also equals $\gcd(a, b)$. That is, we need to show that d satisfies both the conditions of Definition 1.4.2.2.

We first show that $d|a$. By division algorithm, there exist integers q and r such that $a = dq+r$, with $0 \le r < d$. Thus, we need to show that $r = 0$. On the contrary, assume that $r \neq 0$. That is, $0 < r < d$. Then by definition, $r \in \mathbb{N}$ and $r = a-dq = a-q\cdot(ax_0+by_0) = a\cdot(1-qx_0)+b\cdot(-qy_0) \in \{ax + by : x, y \in \mathbb{Z}\}$. Hence, $r \in S$ and by our assumption $r < d$. This contradicts the fact that d was the least element of S. Thus, our assumption that $r \neq 0$ is false and hence $a = dq$. This implies that $d|a$. In a similar way, it can be shown that $d|b$.

Now, assume that there is an integer c such that c divides both a and b. We need to show that $c|d$. Observe that as c divides both a and b, c also divides both ax_0 and by_0 and hence c also divides $ax_0 + by_0 = d$. Thus, we have shown that d satisfies both the conditions of Definition 1.4.2.2 and therefore, the proof of the theorem is complete. ■

The above theorem is often stated as "the $\gcd(a, b)$ is a linear combination of the numbers a and b".

Example 1.4.4. 1. *Consider two integers, say 155 and -275. Then, by division algorithm, one obtains*

$$\begin{aligned} -275 &= (-2)\cdot 155 + 35 & \qquad 155 &= 4 \cdot 35 + 15 \\ 35 &= 2 \cdot 15 + 5 & 15 &= 3 \cdot 5. \end{aligned}$$

Hence, $5 = \gcd(155, -275)$ *and* $5 = 9 \cdot (-275) + 16 \cdot 155$, *as*

$$5 = 35-2\cdot15 = 35-2(155-4\cdot35) = 9\cdot35-2\cdot155 = 9(-275+2\cdot155)-2\cdot155 = 9\cdot(-275)+16\cdot155.$$

Also, note that $275 = 5\cdot55$ *and* $155 = 5\cdot31$ *and thus,* $5 = (9+31x)\cdot(-275)+(16+55x)\cdot155$, *for all* $x \in \mathbb{Z}$. *Therefore, we see that there are infinite number of choices for the pair* $(x, y) \in \mathbb{Z}^2$, *for which* $d = ax + by$.

2. *In general, given two non-zero integers a and b, we can use the division algorithm to get* $\gcd(a, b)$. *This algorithm is also attributed to Euclid. Without loss of generality, assume that both a and b are positive and $a > b$. Then the algorithm proceeds as follows:*

$$\begin{aligned} a &= bq_0 + r_0 \;\; \textit{with } 0 \le r_0 < b, & \qquad b &= r_0q_1 + r_1 \;\; \textit{with } 0 \le r_1 < r_0, \\ r_0 &= r_1q_2 + r_2 \;\; \textit{with } 0 \le r_2 < r_1, & r_1 &= r_2q_3 + r_3 \;\; \textit{with } 0 \le r_3 < r_2, \\ \vdots &= \vdots & & \\ r_{\ell-1} &= r_\ell q_{\ell+1} + r_{\ell+1} \;\; \textit{with } 0 \le r_{\ell+1} < r_\ell, & r_\ell &= r_{\ell+1}q_{\ell+2}. \end{aligned}$$

The process will take at most $b-1$ steps as $0 \le r_0 < b$. Also, note that $\gcd(a,b) = r_{\ell+1}$ *and it can be recursively obtained, using backtracking. That is,*

$$r_{\ell+1} = r_{\ell-1} - r_\ell q_{\ell+1} = r_{\ell-1} - q_{\ell+1}\left(r_{\ell-2} - r_{\ell-1}q_\ell\right) = r_{\ell-1}\left(1 + q_{\ell+1}q_\ell\right) - q_{\ell+1}r_{\ell-2} = \cdots .$$

To proceed further, we need the following definitions.

Definition 1.4.5 (Prime/Composite Numbers). *1. The positive integer* 1 *is called the unity or the unit element of* $\mathbb{Z}$*.*

2. A positive integer p is said to be a prime, if p has exactly two factors, namely, 1 *and p itself.*

3. An integer r is called composite if $r \neq 1, -1$ and is not a prime.

We are now ready to prove an important result that helps us in proving the fundamental theorem of arithmetic.

Lemma 1.4.6 (Euclid's Lemma). *Let p be a prime and let $a, b \in \mathbb{Z}$. If $p|ab$ then either $p|a$ or $p|b$.*

Proof. If $p|a$, then we are done. So, let us assume that p does not divide a. But p is a prime and hence $\gcd(p,a) = 1$. Thus, by Euclid's algorithm, there exist integers x, y such that $1 = ax + py$. Therefore,

$$b = b \cdot 1 = b \cdot (ax + py) = ab \cdot x + p \cdot by.$$

Now, the condition $p|ab$ implies that p divides $ab \cdot x + p \cdot by = b$. Thus, we have shown that if $p|ab$ then either $p|a$ or $p|b$. ■

Now, we are ready to prove the fundamental theorem of arithmetic that states that "every positive integer greater than 1 is either a prime or is a product of primes. This product is unique, except for the order in which the prime factors appear".

Theorem 1.4.7 (Fundamental Theorem of Arithmetic). *Let $n \in \mathbb{N}$ with $n \ge 2$. Then there exist prime numbers $p_1 > p_2 > \cdots > p_k$ and positive integers $s_1, s_2, \ldots, s_k$ such that $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, for some $k \ge 1$. Moreover, if n also equals $q_1^{t_1} q_2^{t_2} \cdots q_\ell^{t_\ell}$, for distinct primes $q_1, q_2, \ldots, q_\ell$ and positive integers $t_1, t_2, \ldots, t_\ell$ then $k = \ell$ and for each i, $1 \le i \le k$, there exists j, $1 \le j \le k$ such that $p_i = q_j$ and $s_i = t_j$.*

Proof. We prove the result using the strong form of the principle of mathematical induction. If n equals a prime, say p then clearly $n = p^1$ and hence the first step of the induction holds true. Hence, let us assume that the result holds for all positive integers that are less than n. We need to prove the result for the positive integer n.

If n itself is a prime then we are done. Else, there exists positive integers a and b such that $n = ab$ and $1 \le a, b < n$. Thus, by the strong form of the induction hypothesis, there exist primes p_i's, q_j's and positive integers s_i and t_j's such that $a = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, for some $k \geq 1$ and $b = q_1^{t_1} q_2^{t_2} \cdots q_\ell^{t_\ell}$, for some ℓ. Hence,

$$n = ab = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} q_1^{t_1} q_2^{t_2} \cdots q_\ell^{t_\ell}.$$

Now, if some of the p_i's and q_j's are equal, they can be multiplied together to obtain n as a product of distinct prime powers.

Thus, using the strong form of the principle of mathematical induction, the result is true for all positive integer n. As far as the uniqueness is concerned, it follows by a repeated application of Lemma 1.4.6.

To see this, observe that p_1 divides $n = q_1^{t_1} q_2^{t_2} \cdots q_\ell^{t_\ell}$ implies that p_1 divides exactly one of them (the primes are distinct), say q_1. Also, it is clear that in this case $s_1 = t_1$. For otherwise, either p_1 will divide $q_2^{t_2} \cdots q_\ell^{t_\ell}$, or $q_1 = p_1$ will divide $p_2^{s_2} \cdots p_k^{s_k}$. This process can be continued a finite number of times to get the required result. ■

As an application of the fundamental theorem of arithmetic, one has the following well known result. This is the first instance where we have used the contrapositive argument technique to prove the result.

Corollary 1.4.8. *Let $n \in \mathbb{N}$ with $n \geq 2$. Suppose that for any prime $p \leq \sqrt{n}$, p does not divide n then n is prime.*

Proof. Suppose n is not a prime. Then there exists positive integers a and b such that $n = ab$ and $2 \leq a, b \leq n$. Also, note that at least one of them, say $a \leq \sqrt{n}$. For if, both $a, b > \sqrt{n}$ then $n = ab > n$, giving us a contradiction.

Since $a \leq \sqrt{n}$, by Theorem 1.4.7, one of its prime factors, say p will satisfy $p \leq a \leq \sqrt{n}$. Thus, if n has no prime divisor less than or equal to $\sqrt{n}$ then n must be itself be a prime. ■