bining Euclid's informal writings with his own extensive proofs in the timeless Disquistiones Arithmeticae.

2.2 Divisibility

When an integer is divided by a second integer($\neq 0$), the quotient may or may not be an integer. For instance, $36/6 = 6$ is an integer, while $18/7 = 2.5$ is not. This observation leads to the following definition.

Definition 2.2.1. *If a and b are integers, we say that b is divisible by $a(\neq 0)$ if there exists an integer c such that $b = ac$. Also, we say that a is a divisor or factor of b, denoted by $a|b$. If a does not divides b, then we write $a \nmid b$.*

Example 2.2.1. *10 is divisible by 5 because there exist an integer 2 such that $10 = 5 \times 2$. We say $5|10$.*

Proposition 2.2.1. *For any integers a, b, c, d the following statements are true:*

1. *$a|0, 1|a, a|a$.*
2. *$a|b \Rightarrow ca|cb, \forall c \in \mathbb{Z}$.*
3. *$a|b$ and $b|c \Rightarrow a|c$.*
4. *$a|b$ and $b|a \Rightarrow a = \pm b$.*
5. *$a|b$ and $a|c \Rightarrow a|(bx + cy)$ for arbitrary integers x and y.*

Proof. 1. Obvious.

2. Here,

$$\begin{aligned} a|b &\Rightarrow b = da \text{ for some integer } d, \\ &\Rightarrow cb = d(ca) \\ &\Rightarrow ca|cb. \end{aligned}$$

3. Here, $a|b \Rightarrow b = aq$ and $c|d \Rightarrow d = cp$ for some integers p and q. Therefore $c = a(pq)$. Hence $bd = ac(pq)$. Therefore $ac|bd$, as pq is an integer.

4. Here, $a|b \Rightarrow b = ap$ for some integer p. Also, $b|c \Rightarrow c = bq$ for some integer q. Therefore $c = bq = a(pq)$. Therefore $a|c$.

5. Here, $a|b \Rightarrow b = ap$ for some integer p. Therefore $b = bpq$. Also, $b|a \Rightarrow a = bq$ for some integer q implies $pq = 1$. As p, q are integers either, $p = q = 1$ or $p = q = -1$. Therefore $a = \pm b$.

6. Here, $a|b \Rightarrow b = ap$ for some integer p and Here, $a|c \Rightarrow b = aq$ for some integer q. Therefore $bx + cy = apx + aqy = a(px + qy)$. Now, $px + qy \in \mathbb{Z}$ as $p, q, x, y \in \mathbb{Z}$. Therefore $a|(bx + cy)$.

□

Theorem 2.2.1. *The Division Algorithm: Given any two integers a and b, with $b > 0$ there exists unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.*

Proof. Let a and b be two fixed integers with $b \neq 0$. Let $A = \{n \in \mathbb{N} | n = a - by, y \in \mathbb{Z}\}$. Our claim is $A \neq \phi$. For this there are two possibilities viz:

1. If $a \geq 0$, then $a - b(0) = a \geq 0$. So $a - by$ is non–negative for $y = 0 (a \geq 0)$.

2. If $a < 0$, then $-a > 0$. Since, b is a positive integer, we must have $b \geq 1$. Multiplying the inequality by a positive quantity gives, $(-a)b \geq (-a)$ implies $a - ab \geq 0$. So $a - by$ is non–negative for $y = a (< 0)$. Hence $A \neq \phi$.

Since, $A \subset \mathbb{N}$, by well ordering principle A has a least element say r. Since, $s \in A$, therefore, $r = a - by$ for some $y = q$. Thus we found integers r and q such that $r = a - bq$ or $a = r + bq$. Since, $r \in A$, therefore $r \geq 0$. Next our claim is $r < b$. On the contrary, if we assume $r \geq b$, then $0 \leq r - b = (a - bq) - b = a - b(q + 1) < r$, which leads to a contradiction as r is the least in A. Hence $r < b$. Thus we found two integers q and r such that $a = bq + r$ with $0 \leq r < b$.

The last part of the proof deals with the uniqueness of q and r with the above properties. If possible, let there be two pair of integers r_1, q_1 and r_2, q_2 satisfying

$$r_1 + bq_1 = a = r_2 + bq_2 \tag{2.2.1}$$

with

$$0 \leq r_1 \leq b \text{ and } 0 \leq r_2. \tag{2.2.2}$$

We need to prove $r_1 = r_2$ and $q_1 = q_2$.

If $r_1 \leq r_2$, then 2.2.1 shows

$$b(q_1 - q_2) = r_2 - r_1. \tag{2.2.3}$$

Since by hypothesis, $b > 0, r_2 \geq r_1$, therefore $q_1 - q_2$ must be a non negative integer. Hence $r_2 - r_1$ must be one of $0, b, 2b, 3b, \ldots$. But $0 \leq r_2 \leq r_1 \leq b$ implies $r_2 - r_1 = 0$. Hence by 2.2.3 and the preceeding equation together with the hypothesis $b > 0$, we have $q_1 = q_2$. Similarly, taking $r_1 \geq r_2$, proves the uniqueness of q and r. □

For another proof we give explicit formulae for the quotient and remainder in terms of the greatest integer function, which will be done in the consequent chapter of the book.

Remark 2.2.1. *1. When $b \nmid a, r$ satisfies strong inequality $0 < r < b$.*

2. Here q and r called quotient and remainder.

3. bq is largest multiple of b which does not exceed a.

Example 2.2.2. *Suppose we are dividing 51 by 5 then, $51 = 5 \times 10 + 1$. Comparing with the theorem we get, $a = 51, b = 5, q = 10, r = 1$.Here $q = 10$ is the quotient and $r = 1$ is remainder.*

Corollary 2.2.1. *If a, b be two integers with $b > 0$, then there exists integers Q and R such that $a = bQ \pm R,\ \ 0 \leq R < \dfrac{b}{2}$.*

Proof. From Division algorithm we have, for any two integers a and b with $b > 0$, there exists unique integers q and r such that

$$a = bq + r,\ 0 \leq r < b \tag{2.2.4}$$

We now consider three following cases: Case(i): Let $r < \frac{b}{2}$ and taking $q = Q$ and $r = R$ in equation (2.2.4), we have

$$a = bQ + R, 0 \leq R < \frac{b}{2}$$

Case(ii): Let $r > \frac{b}{2}$, then from equation(2.2.4)

$$\begin{aligned} a &= bq + r \\ &= b(q + 1) + (r - b) \\ &= b(q + 1) - (b - r). \end{aligned}$$

Taking $q+1 = Q$ and $b-r = R$, we have $a = bQ-R$ where $R = b-r < b-\frac{b}{2} = \frac{b}{2}$. Therefore $a = bQ - R,\ 0 \leq R < \frac{b}{2}$. Now combining case (i) and (ii) we have,

$$a = bQ \pm R,\ 0 \leq R < \frac{b}{2}$$

Case(iii): Let $r = \frac{b}{2}$, then from equation(2.2.4)

$$a = bQ + R, \text{ where } q = Q \text{ and } r = R = \frac{b}{2}$$

Again from the equation(2.2.4) we have,

$$a = bq + r = b(q + 1) - (b - r) = bQ + R$$

where $q + 1 = Q$ and $-(b - r) = R$ that is $R = -b + \frac{b}{2} = -\frac{b}{2}$. Which shows that Q and R is not unique in this case thus case(iii) is not possible. □

Remark 2.2.2. *(i) Here in the above proof Q and R are unique except when $R = \frac{b}{2}$. In this case that is for $R = \frac{b}{2}$, R is called minimal remainder or the absolutely least remainder of a with respect to b.*
(ii) When $r < \frac{b}{2}$, the minimal remainder is $R = r$.
(iii) When $r > \frac{b}{2}$, the minimal remainder is $R = r - b$.

Here we have done an illustration of the concept minimal remainder by an example. Let us choose $a = 51$ and $b = 6$ then $51 = 6 \times 8 + 3$(of the form $a = bQ + R,\ Q = 8,\ R = 3$). Also we can write $51 = 6 \times 9 - 3$(of the form $a = bQ - R,\ Q = 9,\ R = 3$). Thus Q and R are not unique as $R = \frac{b}{2} = 3$. Which is case (iii) of above corollary.
Now if we choose $a = 50$ and $b = 6$ then $50 = 6 \times 8 + 2$. Thus in this case $r = 2 < \frac{b}{2} = 3$ and the minimal remainder is $R = 2$. Which is case (i) of above corollary.
Now if we choose $a = 52$ and $b = 6$ then $52 = 6 \times 8 + 4$. Thus in this case $r = 4 > \frac{b}{2} = 3$ and the minimal remainder is $R = r - b = 4 - 6 = -2$. Which is case (ii) of above corollary.

Theorem 2.2.2. *Prove that every integer is of the form,*

1. $3k$ *or* $3k \pm 1$.

2. $4k$ *or* $4k \pm 1$ *or* $4k \pm 2$.

3. $5k$ *or* $5k \pm 1$ *or* $5k \pm 2$.

4. $6k$ *or* $6k \pm 1$ *or* $6k \pm 2$ *or* $6k \pm 3$.

Proof. From the above corollary any integer a is of the form

$$a = bk \pm r \text{ where } b, k, r \in \mathbb{Z} \text{ and } 0 \leq |r| \leq \frac{b}{2}. \tag{2.2.5}$$

1. When $b = 3$, we get from 2.2.5 $a = 3k \pm r$ where $0 \leq |r| \leq \frac{3}{2} = 1.5$. Therefore $r = 0, \pm 1$.

2. When $b = 4$ we get from 2.2.5, $a = 4k \pm r, 0 \leq |r| \leq \frac{4}{2} = 2$, i.e. $r = 0, \pm 1, \pm 2$. Therefore $a = 4k, 4k \pm 1, 4k \pm 2$.

3. Rests treated as exercises.

□

2.3 Worked out Exercises

Problem 2.3.1. *For any two integers a and b with $b > 0$, there exists unique integers q_1 and r_1 such that $a = bq_1 + cr_1$ where $0 \leq r_1 < \frac{b}{2}, c = \pm 1$.*

Solution 2.3.1. *By division algorithm we have $a = bq + cr, 0 \leq r < b$.*

Case I *$r < \frac{b}{2}$, take $q_1 = q, c = 1, r_1 = r$. Therefore $a = bq_1 + cr_1, 0 \leq r_1 < \frac{b}{2}, c = \pm 1$.*

Case II *$r > \frac{b}{2}$, therefore $0 < b - r < \frac{b}{2}$ take $q_1 = q_0 + 1, r_1 = b - r$ and $c^2 = -1$, therefore, $a = bq_1 + cr_1$ where $0 \leq r_1 < \frac{b}{2}, c = -1$.*

Case III *$r = \frac{b}{2}$ then $q_1 = q, c = 1, r_1 = r$. Therefore $a = bq_1 + cr_1, r_1 = \frac{b}{2}, c = 1$ and if $q_1 = q + 1, r_1 = b - r$ and $c = -1$. Therefore $a = b(q + 1) - (b - r) = bq_1 + cr_1, \frac{b}{2} = r, c = -1$. In this case q_1 and r_1 is not unique, so $a = bq_1 + cr_1, 0 \leq r_1 < \frac{b}{2}, c = \pm 1$.*

Problem 2.3.2. *Show that every square integer is of the form $5k$ or $5k \pm 1$ for some $k \in \mathbb{Z}$.*

Solution 2.3.2. *Note that every integer is of the form $5p, 5p \pm 1, 5p \pm 2$ for some $p \in \mathbb{Z}$. Square of these numbers are of the form:*

$$
\begin{aligned}
(5p)^2 &= 5 \times 5p^2 = 5k, \text{ where } k = 5p^2 \text{ is a positive integer} \\
(5p \pm 1)^2 &= 25p^2 \pm 10p + 1 = 5(5p^2 \pm 2p) + 1 = 5k + 1, \text{ where } k = 5p^2 \pm 2p + 1 \in \mathbb{Z} \\
(5p \pm 2)^2 &= 25p^2 \pm 20p + 4 \\
&= 5(5p^2 \pm 4p + 1) - 1 \\
&= 5k - 1, \text{ where } k = 5p^2 \pm 4p + 1 \in \mathbb{Z}.
\end{aligned}
$$

Problem 2.3.3. *Show that cube of any integer is of the form $9p, 9p + 1, 9p + 8$ (or $9p, 9p \pm 1$).*

Solution 2.3.3. *Here,*

$$\begin{aligned}(3m)^3 &= 27m^3 = 9p, \text{ where } p = 3m^3 \in \mathbb{Z}\\ (3m+1)^3 &= 27m^3 + 27m^2 + 9m + 1\\ &= 9(3m^3 + 3m^2 + m) + 1\\ &= 9p + 1, \text{ where } p = 3m^3 + 3m^2 + m \in \mathbb{Z}\\ (3m-1)^3 &= 27m^3 - 27m^2 + 9m - 9 + 8\\ &= 9(3m^3 - 3m^2 + m - 1) + 8\\ &= 9p + 8, \text{ where } p = 3m^3 - 3m^2 + m - 1 \in \mathbb{Z}\\ \text{Also, } (3m-1)^3 &= 9(3m^3 - 3m^2 + m) - 1\\ &= 9p - 1, \text{ where } p = 3m^3 - 3m^2 + m \in \mathbb{Z}.\end{aligned}$$

Problem 2.3.4. *Prove that the expression* $\dfrac{a(a^2+2)}{3}$ *is an integer for* $a \geq 1$.

Solution 2.3.4. *Applying Division Algorithm, any integer* a *can be expressed in the form* $3q, 3q+1, 3q+2$. *Taking* $a = 3q$ *we obtain* $\frac{a(a^2+2)}{3} = q(9q^2+2)$, *an integer. Similarly putting* $a = 3q+1$ *and* $a = 3q+2$ *we obtain* $(3q+1)(3q^2+2q+1)$ *and* $(3q+2)(3q^2+4q+2)$ *respectively, both of which are integers. Hence the result is proved.*

Problem 2.3.5. *Show that one of every three consecutive integer is divisible by* 3.

Solution 2.3.5. *Let* $a, a+1, a+2$ *be any three consecutive integers, then* a *is of the form* $3p, 3p+1, 3p-1$ *where* $p \in \mathbb{Z}$. *If* $a = 3p$, *then* a *is divisible by* 3. *If* $a = 3p+1$, *then* $a+2 = 3p+3 = 3(p+1)$ *is divisible by* 3. *If* $a = 3p-1$, *then* $a+1 = 3p+1-1 = 3p$ *is divisible by* 3.

Problem 2.3.6. *Find the minimal remainder of* 416 *with respect to (i)* 37 *(ii)* 42.

Solution 2.3.6. **(i)** *Here* $a = 416, b = 37$. *Therefore* $416 = 37 \times 11 + 9$*(Why!). Therefore the minimal remainder is* $R = 9$.

(ii) *Left to the reader.*

Problem 2.3.7. *Show that* $a^{n+1} - (a-1)n - a$ *is divisible by* $(a-1)^2, a$ *being an integer.*

Solution 2.3.7. *Since $a \in \mathbb{Z}$, we have*

$$\begin{aligned} a^{n+1} - (a-1)n - a &= a(a^n - 1) - (a-1)n \\ &= a(a - 1\{a(a^{n-1} + \cdots + 1) - n\}) \\ &= (a-1)\{(a^n + a^{n-1} + \cdots + a) - n\} \\ &= (a-1)^2\{(a^{n-1} + a^{n-2} + \cdots + 1) + (a^{n-2} + \cdots + 1) + \cdots + 1\}. \end{aligned}$$

The given expression is divisible by $(a-1)^2$.

Problem 2.3.8. *If both a and b are odd positive integers then $a^4 + b^4 - 2$ is divisible by 8.*

Solution 2.3.8. *Let $a = 2n_1 + 1$ and $b = 2n_2 + 1$ be the odd positive integers, where n_1, n_2 are positive integers. Thus we have,*

$$\begin{aligned} &(2n_1 + 1)^4 + (2n_2 + 1)^4 - 2 \\ &= (2n_1)^4 + 4 \cdot (2n_1)^3 + 6 \cdot (2n_1)^2 + 4 \cdot (2n_1) + 1 + (2n_2)^4 + 4 \cdot (2n_2)^3 + 6 \cdot (2n_2)^2 \\ &+ 4 \cdot (2n_2) + 1 - 2 \\ &= 16(n_1^4 + n_2^4) + 16(n_1^3 + n_2^3) + 24(n_1^2 + n_2^2) + 8(n_1 + n_2) \\ &= 8[2(n_1^4 + n_2^4) + 2(n_1^3 + n_2^3) + 3(n_1^2 + n_2^2) + (n_1 + n_2)]. \end{aligned}$$

Problem 2.3.9. *Show that the product of two integers of the form $4n + 1$ is again of this form, while the product of two integers of the form $4n + 3$ is of the form $4k + 1$.*

Solution 2.3.9. *Product of two integers of the form $4n + 1$ gives us $(4n + 1)(4m + 1) = 4(4mn + m + n) + 1 = 4k + 1, k \in \mathbb{Z}$. Similarly $(4n + 3)(4m + 3) = 4(4mn + 3m + 3n + 2) + 1 = 4k + 1, k \in \mathbb{Z}$.*

Problem 2.3.10. *Show that the square of every odd integer is of the form $8k+1$.*

Solution 2.3.10. *Let a be an odd integer. Then $n = 2s + 1$, s being an integer. Now, $a^2 = 4s(s + 1) + 1$. If s is even, then $s = 2m, m$ being an integer. Hence*

$$a^2 = 8m(2m + 1) + 1 = 8k + 1, k = 2m + 1 \in \mathbb{Z}.$$

If s is odd, then $s = 2m + 1$. It follows,

$$a^2 = 8(2m + 1)(m + 1) + 1 = 8k + 1, k = (2m + 1)(m + 1) \in \mathbb{Z}.$$

Problem 2.3.11. *Let m be a positive integer. We define*

$$T(m) = \begin{cases} \frac{m}{2}, & \text{if } m \text{ is even;} \\ \frac{3m+1}{2}, & \text{if } m \text{ is odd.} \end{cases}$$

We, then form the sequence obtained by iterating $T; m, T(m), T(T(m)), T(T(T(m))), \ldots$. *For instance, starting with* $m = 7$ *we have* $7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1, 2, 1, 2, 1, \ldots$. A *well-known conjecture, sometimes called the* ***Collatz conjecture****, asserts that the sequence obtained by iterating* T *always reaches the integer* 1 *no matter which positive integer* m *begins the sequence.*

Show that the sequence obtained by iterating T *starting with* $m = \dfrac{2^{k-1}}{3}$, *where* k *is an even positive integer,* $k > 1$, *always reaches the integer* 1.

Solution 2.3.11. *If* $3m$ *is odd, then so is* m. *So* $T(m) = \frac{3m+1}{2} = \frac{2^{2k}}{2} = 2^{2k-1}$. *Since* $T(m)$ *is a power of* 2, *the exponent will decrease down to* 1 *with repeated iterations of* T.

Problem 2.3.12. *Show that if* a *is an integer, then* 3 *divides* $a^3 - a$.

Solution 2.3.12. *Here* $a^3 - a = a(a-1)(a+1)$. *Applying division Algorithm we have* $a = 3k, a = 3k+1$ *or* $a = 3k+2$, k *being an integer. If* $a = 3k$ *and* $a = 3k+1$, *then* $3|a$ *and* $3|(a-1)$ *respectively. Finally, if* $a = 3k+2$ *i.e.* $a+1 = 3(k+1)$, *then* $3|(a+1)$. *Combining, it shows* $3|a(a-1)(a+1) = a^3 - a$.

2.4 Greatest Common Divisor

If c and d be two arbitrary integers, not simultaneously zero, then the set of common divisors of c and d is a finite set of integers, always containing the integers $+1$ and -1(hence, their set of common divisors is non-null). Now every integer divides zero, so that if $c = d = 0$, then every integer serves as a common divisor of c and d. In this case, the set of common divisors of c and d turns to be infinite. In this article, we are interested on the greatest integer among the common divisors of two integers.

Definition 2.4.1. *The greatest common divisor of two integers* c *and* d, *that are not both zero, is the greatest integer which divides both* c *and* d.

In other words, the above definition can be formulated as

Definition 2.4.2. *If* c *and* d *be two arbitrary integers, not simultaneously zero, the greatest common divisor of* c *and* d *is the common divisor* e *satisfying the following:*

1. $e|a$ *and* $e|b$.
2. *If* $f|a$ *and* $f|b$ *then* $e \geq f$.

The greatest common divisor of c and d is written as (c, d) or $\gcd(c, d)$.

Example 2.4.1. *The common divisors of* 20 *and* 80 *are* $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10 and \pm$ 20. *Hence* $\gcd(20, 80) = 20$. *Similarly, looking at sets of common divisors, we find that* $(12, 18) = 6, (50, 5) = 5, (19, 24) = 1, (0, 56) = 56, (-8, -16) = 8$, *and* $(-19, 361) = 19$.

We can also define the greatest common divisor of more than two integers.

Definition 2.4.3. *Let* $c_1, c_2, \ldots, c_n$ *be integers, that are not all zero. The greatest common divisor of these integers is the greatest integer which is a common divisor of all of the integers in the set. The greatest common divisor of* $c_1, c_2, \ldots, c_n$ *is denoted by* $(c_1, c_2, \ldots, c_n)$ *or* $\gcd(c_1, c_2, \ldots, c_n)$.

Example 2.4.2. *We see that* $(12, 18, 30) = 6$ *and* $(10, 15, 25) = 5$.

The following proposition can be used to find the greatest common divisor of a set of more than two integers.

Proposition 2.4.1. *If* $c_1, c_2, \ldots, c_n$ *are integers, not simultaneously zero, then*

$$\gcd(c_1, c_2, \ldots, c_n) = \gcd\big(c_1, c_2, \ldots, (c_{n-1}, c_n)\big).$$

Before proceeding for proof, let us explain the proposition with an example: To find the greatest common divisor of the three integers 105, 140, and 350, we see that $\gcd(105, 140, 350) = \gcd\big(105, (140, 350)\big) = \gcd(105, 70) = 35$.

Proof. In particular, a common divisor of the n integers $c_1, c_2, \ldots, c_n$ is a divisor of c_{n-1} and c_n and therefore, a divisor of (c_{n-1}, c_n). Also, any common divisor of the $n-2$ integers $c_1, c_2, \ldots, c_{n-2}$ and (c_{n-1}, c_n), must be a common divisor of all n integers, for if it divides (c_{n-1}, c_n), it must divide both c_{n-1} and c_n. Since the set of n integers and the set of the first $n-2$ integers together with the greatest common divisor of the last two integers have exactly the same divisors, their greatest common divisors are equal. □

Next we are particularly interested in pair of integers sharing no common divisors other than 1. Such pair of integers are said to be relatively prime or coprime.

Definition 2.4.4. *The integers* c *and* d, *not simultaneously zero, are said to be relatively prime(or coprime) if* c *and* d *have greatest common divisor* $(a, b) = 1$.

Example 2.4.3. *Since,* $\gcd(12, 13) = 1$ *therefore* $12, 13$ *are relatively prime.*

We can also define the relatively prime of more than two integers.

Definition 2.4.5. *We say that the integers $c_1, c_2, \ldots, c_n$ are mutually relatively prime(or coprime) if* $\gcd(c_1, c_2, \ldots, c_n) = 1$. *These integers are called pairwise relatively prime if for each pair of integers c_i, c_j from the set,* $\gcd(c_i, c_j) = 1$, *i.e., if each pair of integers from the set is relatively prime.*

If integers are pairwise relatively prime, they must be mutually relatively prime(Verify!). However, the converse fails is shown from the following example:

Example 2.4.4. *Consider the integers* $15, 21,$ *and* 35. *Since* $(35, 55, 77) = (35, (55, 77)) = (35, 11) = 1$, *we see that the three integers are mutually relatively prime. However, they are not pairwise relatively prime, because* $(35, 55) = 5, (35, 77) = 7$ *and* $(55, 77) = 11$.

Remark 2.4.1. *Since the divisors of $-a$ are the same as the divisors of a, it follows that* $\gcd(a, b) = (|a|, |b|)$ *(where $|a|$ denotes the absolute value of a which equals a if $a > 0$, equals $-a$ if $a < 0$) and equals 0 if $a = 0$. Hence we can restrict our attention to greatest common divisors of pairs of positive integers.*

We will show that the greatest common divisor of the integers c and d, not simultaneously zero, can be written as a sum of multiples of c and d. To phrase this more lucidly, we use the following definition:

Definition 2.4.6. *If c and d are integers, then a linear combination of c and d is a sum of the form $mc + nd$, where both m and n are integers.*

The following theorem relates definition 2.4.6 and greatest common divisors.

Theorem 2.4.1. *The greatest common divisor of the integers c and d, not simultaneously zero, is the least positive integer that is a linear combination of c and d.(In other words, given integers c and d, not both of which are zero, there exist integers m, n such that* $\gcd(c, d) = mc + nd$.*)*

Before proceeding for the proof, let us illustrate the theorem succinctly with an example:

Example 2.4.5. *Consider the case in which $c = 4$ and $d = 12$. Here, the set S becomes $S = \{4(-2) + 12 \cdot 1, 4(-1) + 12 \cdot 1, 4 \cdot 0 + 152 \cdot 1, \ldots\} = \{4, 8, 12, \ldots\}$. Here 4 is the smallest integer in S, whence* $4 = \gcd(4, 12)$.

Proof. Let e be the least positive integer such that $e = ma + nb$ holds, m, n being integers.(Using the well-ordering property, there exist such least positive integer, also at least one of two linear combinations $1 \cdot c + 0 \cdot d$ and $(-1) \cdot c + 0 \cdot b$, where $c \neq 0$ is positive, do exist).

Claim(i) $e|c$ and $e|d$.

Claim(ii) $e = \gcd(c, d)$.

To fulfill Claim(i), applying Division Algorithm, we have $c = eq+r$ with $0 \leq r < e$. Now combining $e = ma + nb$ and $c = eq + r$, we obtain $r = (l - qm)c - qnd$. This shows that the integer r is a linear combination of c and d. Since $0 \leq r < e$, and e is the least positive linear combination of c and d, we conclude that $r = 0$, and hence $e|a$. In a similar manner, we can show that $e|d$.

For Claim(ii), all we need to show is that any common divisor f of c and d must divide e. Since $e = ma + nb$, if $f|c$ and $f|d$, proves $f|e$. This completes the proof. □

Remark 2.4.2. *The foregoing argument is just an "existence" proof and does not provide a practical method for finding the values of m and n.*

The following theorem illustrates the relation between relatively prime integers and linear combinations(of relatively prime integers).

Theorem 2.4.2. *Let c and d integers, not simultaneously zero. Then c and d are relatively prime if and only if there exist integers m and n such that $1 = mc+nd$.*

Proof. If c and d are relatively prime then $\gcd(c, d) = 1$. By virtue of Theorem 2.4.1, there exist integers m and n satisfying $1 = mc+nd$. In context of converse part, assume that $1 = mc+nd$ for some choice of m and n, and that $e = \gcd(c, d)$. Because $e|c$ and $e|d$, Proposition 2.2.1 yields $e|(mc + nd)$, or $e|1$ implies $e = 1$(Why!), and the desired conclusion follows. □

It is true, without adding an extra condition, that $a|c$ and $b|c$ together does not imply $ab|c$. For instance, $6|12$ and $3|12$, but $6 \cdot 3 \nmid 12$. Of course, if $\gcd(6, 3) = 1$, then this situation would not arise. This brings us to Corollary the following corollary:

Corollary 2.4.1. *If $c|e$ and $d|e$, with $\gcd(c, d) = 1$, then $cd|e$.*

Proof. As $c|e$ and $d|e$, there exist integers m and n satisfying $e = mc+nd$. Now the relation $\gcd(c, d) = 1$ implies $1 = ck + dl$ for some choice of integers k and l. Multiplying the last equation by e, we obtain $e = e \cdot 1 = e(ck + dl) = eck + edl$. The appropriate substitutions on the right-hand side allows $e = c(ds)k+d(cr)l = cd(sk + rl)$ implies $cd|e$. □

The following few propositions address some properties of greatest common divisors.

Proposition 2.4.2. *Let a, b and c be integers with $\gcd(a, b) = d$. Then*

1. $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
2. $\gcd(a + cb, b) = \gcd(a, b)$.
3. $\gcd(ma, mb) = md$ $(m > 0)$.

Proof. 1. Here a, b are integers with $\gcd(a, b) = d$. Our claim is $\frac{a}{d}, \frac{b}{d}$ have no common positive divisors other than 1. Assume that e is a positive integer such that $e|\frac{a}{d}$ and $e|\frac{b}{d}$. Then, there are integers k_1 and k_2 with $\frac{a}{d} = k_1 e$ and $\frac{b}{d} = k_2 e$, satisfying $a = dek_1$ and $b = dek_2$. Hence de is a common divisor of a and b. Hence $e = 1$(Why!). Consequently, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2. Here a, b and c be integers with $\gcd(a, b) = d$. Its suffices to show that the common divisors of a, b are exactly the same as the common divisors of $a + cb, b \Rightarrow \gcd(a + cb, b) = \gcd(a, b)$. Let e be a common divisor of a, b. Then $e|(a + cb)$(Why!), such that e is a common divisor of $a + cb, b$. If f is a common divisor of $a + cb, b$ we see that $f|\big((a + cb) - cb\big) = a$(Why!), showing f is a common divisor of a, b. Hence $\gcd(a + cb, b) = \gcd(a, b)$.

3. Since $d = \gcd(a, b)$ then $\exists$ integers x and y such that $d = xa + yb$(by Theorem 2.4.1). Then we have,

$$\begin{aligned} & m(xa + yb) = md \\ \Rightarrow\ & x(ma) + y(mb) = md \end{aligned}$$

As $m > 0$ then from the above equation we can assert that $\gcd(ma, mb) = m \gcd(a, b) = md$.

□

Proposition 2.4.3. *Prove that $\gcd(a, c) = 1$ if and only if $\gcd(c - a, c)$.*

Proof. Every common divisor d of a and c is also a common divisor of $c - a$ and a. Conversely, every common divisor d of $c - a$ and a is also a common divisor of $c - a + a = c$ and a. Therefore the greatest common divisor of a and c is the same as the greatest common divisor of $c - a$ and a. So in general, $\gcd(a, c) = \gcd(c - a, c) = 1$. □

Proposition 2.4.4. *Let a, b and c be integers with $\gcd(a, b) = 1$. Then*

1. *If $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.*

2. *If* $\gcd(a,b)=1$, *and* $c|a$, *then* $\gcd(b,c)=1$.

3. *If* $c\big|(a+b)$, *then* $\gcd(a,c)=\gcd(b,c)=1$.

4. *If* $d|ac$, *and* $d|bc$, *then* $d|c$.

Proof. 1. Since $\gcd(a,b)=1$, and $\gcd(a,c)=1$, therefore $\exists\ x,y,u,v\in\mathbb{Z}$ such that $1=ax+by=au+cv$.

$$\begin{aligned}\therefore\ 1&=(ax+by)(au+cv),\\&=a(axy+byu+axu)+bcyu,\\&=ak_1+bck_2,\ k_1=axy+byu+axu,\ k_2=yu.\end{aligned}$$

Hence $\gcd(a,bc)=1$.

2. left to the reader.

3. Since $\gcd(a,b)=1,\exists\ u,v\in\mathbb{Z}$ such that $au+bv=1$. Also, $c\big|(a+b)\Rightarrow\exists\ m$ such that $cn=a+b\Rightarrow cn-b=a$.

$$\begin{aligned}\therefore\ (cn-b)u+bv&=1,\\cnu-bu+bv&=1,\\cnu-b(u-v)&=1\Rightarrow\gcd(c,b)=1.\end{aligned}$$

Similarly, $\gcd(c,a)=1$.

4. left to the reader.

□

Our next theorem seems simple, but is of fundamental importance.

Theorem 2.4.3. *Euclid's Lemma: If* $a|bc$, *with* $\gcd(a,b)=1$, *then* $a|c$.

Proof. By virtue of Theorem 2.4.2, writing $1=am+bn$, where m and n are integers. Multiplication of this equation by c produces $c=1\cdot c=(am+bn)c=acm+bcn$. Because $a|ac$ and $a|bc$, it follows that $a|(acm+bcn)$, which can be recast as $a|c$. □

Remark 2.4.3. *The condition* $\gcd(a,b)=1$ *is necessary is evident from the following example:* $12|9\cdot 8$, *but* $12\nmid 9$ *and* $12\nmid 8$.

Theorem 2.4.4. *Let* c,d *be integers, not both zero. For a positive integer* e, $e=\gcd(c,d)$ *if and only if*

1. $e|c$ *and* $e|d$.

2. Whenever $f|c$ and $f|d$, then $f|e$.

Proof. Hint: Use Theorem 2.4.1. □

Simple application of the last theorem leads to the following proposition.

Proposition 2.4.5. *Let a, b and c be integers with* $\gcd(a, b) = 1$*, then* $\gcd(ac, b) = gcd(c, b)$.

Proof. Let $\gcd(c, b) = d$. Its suffices to show that $d|ab$ and secondly if $k|ac$ and $k|b$ then $k|d$. Since $d|c$, $\exists\ n$ such that $dn = c$ so $(dn)a = ca \Rightarrow d|ca$.

Next, $\exists\ u, v \in \mathbb{Z}$ such that $d = au + cv$. Since $k|b$, then $\exists\ n$ such that $kn = b$. Hence $d = cu + knv$. Since $\gcd(a, b) = 1\ \exists\ p, q$ such that $ap + bq = 1 \Rightarrow apc + bqc = c$.

$$\begin{aligned} \therefore\ d &= (apc + bqc)x + kny, \\ &= axpc + bqcx + kny. \end{aligned}$$

But, $k|ac \Rightarrow \exists\ r$ such that $kr = ac$.

$$\begin{aligned} \therefore\ d &= krpx + knqcx + kny, \\ &= k(rpx + nqcx + ny) \Rightarrow k|d. \end{aligned}$$

Hence using Theorem 2.4.4 we obtain the desired result. □

Remark 2.4.4. *The Theorem 2.4.4 sometimes serves as a definition of* $\gcd(c, d)$. *The advantage of using it as a definition is that order relationship is not involved. Thus, it may be used in algebraic systems having no order relation.*

Euclid's Algorithm

While finding the gcd of two integers (not both 0), we can of course list all the common divisors and pick the greatest one amongst those. However, if a and b are very large integers, the process is very much time consuming. However, there is a far more efficient way of obtaining the gcd. That is known as the Euclid's algorithm. This method essentially follows from the division algorithm for integers.

To prove the Euclidean algorithm, the following lemma will be helpful.

Lemma 2.4.1. *If $a = qb + r$ then the* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d = \gcd(a, b)$ and $d_1 = \gcd(b, r)$. Then, $d|a, d|b$ implies $d|(a - qb)$ i.e, $d|r$. Thus d is a common divisor of b and r, hence $d|d_1$. Similarly, $d_1|b, d_1|r$ implies $d_1|(bq + r)$ i.e., d_1 divides both a and b. Then, $d_1|d$. Thus, $d = d_1$, as both d and d_1 are positive by our definition of gcd. □

Theorem 2.4.5. *Euclid's Algorithm: Let a and b $(a > b)$ be any two integers . If r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on. Thus $r_{n+1} = 0$, then the last non zero remainder r_n is the* $\gcd(a, b)$.

Proof. Euclid's algorithm is an efficient way of computing the gcd of two integers by repeated application of the above lemma. At each step the size of the integers concerned gets reduced. Suppose we want to find the gcd of two integers a and b, neither of them being 0. As $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$, we may assume $a > b > 0$. By performing division algorithm repeatedly, we obtain

$$\begin{aligned}
a &= bq_1 + r_1, & 0 \le r_1 \le b.\\
b &= r_1q_2 + r_2, & 0 \le r_2 \le r_1.\\
r_1 &= r_2q_2 + r_3, & 0 \le r_3 \le r_3.\\
&\vdots = \vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 \le r_n \le r_{n-1}.\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, & 0 \le r_{n+1} \le r_n.
\end{aligned}$$

As we have a decreasing sequence of non-negative integers $b > r_1 > r_2 > \ldots > r_n > r_{n+1}$ we must have $r_{n+1} = 0$ for some n. Then, by applying the previous lemma repeatedly, we find that $\gcd(a, b) = \gcd(r_1, b) = \gcd(r_2, r_1) = \ldots = \gcd(r_{n-1}, r_{n-2}) = \gcd(r_n, r_{n-1}) = r_n$. Thus, the last non-zero remainder r_n in the above process gives us the $\gcd(a, b)$. □

Theorem 2.4.6. *If $k > 0$, then* $\gcd(ka, kb) = k \gcd(a, b)$.

Let us illustrate the statement of the above theorem with an example: $\gcd(12, 30) = \gcd(3 \cdot 4, 3 \cdot 10) = 3\gcd(4, 10) = 3\gcd(2 \cdot 2, 2 \cdot 5) = 3 \cdot 2\gcd(2, 5) = 6$.

Proof. If each of the equations appearing in the Euclidean Algorithm for a and b is multiplied by k, we obtain

$$\begin{aligned}
ak &= (bk)q_1 + r_1k, & 0 \le r_1k \le bk.\\
bk &= (r_1k)q_2 + r_2k, & 0 \le r_2k \le r_1k.\\
r_1k &= (r_2k)q_2 + r_3k, & 0 \le r_3k \le r_3k.\\
&\vdots = \vdots\\
r_{n-2}k &= (r_{n-1}k)q_n + r_nk, & 0 \le r_nk \le r_{n-1}k.\\
r_{n-1}k &= (r_nk)q_{n+1} + 0.
\end{aligned}$$

But here the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder $r_n k$; that is, $\gcd(ka, kb) = r_n k = k \gcd(a, b)$. □

Based on the above theorem, let us state and prove the following corollary:

Corollary 2.4.2. *Its suffices to consider the case $k < 0$. Then $-k = |k| > 0$ and*

$$\begin{aligned}\gcd(ka, kb) &= \gcd(-ka, -kb)\\ &= \gcd(|k|a, |k|b)\\ &= |k| \gcd(a, b).\end{aligned}$$

2.5 Least Common Multiple

There is a concept parallel to that of the greatest common divisor of two integers, known as their least common multiple. Prime factorizations can also be used to find the smallest integer that is a multiple of two positive integers(treated in later chapters). The problem of finding this integer arises when fractions are added.

Definition 2.5.1. *The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by a and b, denoted by $lcm(a, b)$ or $[a, b]$.*

The above definition can also be formulated as follows:

Definition 2.5.2. *The least common multiple of two nonzero integers a and b is the positive integer l satisfying the following:*

1. *$a|l$ and $b|l$.*
2. *If $a|c$ and $b|c$, with $c > 0$, then $l \leq c$.*

Example 2.5.1. *We have the following least common multiple: $lcm(16, 20) = 80, lcm(24, 36) = 72, lcm(4, 20) = 20$, and $lcm(5, 13) = 65$.*

Remark 2.5.1. *Given nonzero integers a and b, $lcm(a, b)$ always exists and $lcm(a, b) < |ab|$ (Verify!).*

Proposition 2.5.1. *For nonzero integers a and b, the following statements are equivalent(TFAE):*

1. $\gcd(a, b) = |a|$.

2. $a \big| b$.

3. $lcm(a, b) = |b|$.

Proof. (1)⇒(2): Let (1) holds. Then $\exists\ n \in \mathbb{Z}$ such that $b = \big|a\big|n$. Now $a > 0 \Rightarrow b = an \Rightarrow a|b$. Again, $a < 0 \Rightarrow |a| = -1 \Rightarrow b = (-a)n \Rightarrow b = a(-n) \Rightarrow a|b$. $a|b$. Hence (2) holds.

(2)⇒(3): Let (2) holds. Then $a\big||b|$ and clearly $b\big||b|$. Let c be another common multiple. Then $a\big|c$ and $b\big|c$ with $c > 0$. Now $b\big|c$ implies $\exists\ n \in \mathbb{Z}$ such that $c = bn$ and $\big|n\big| \geq 1$. Thus, $|c| = |b||n| \geq b$ which further gives $|c| \geq |b|$ and by definition $|b| = lcm(a, b)$.

(3)⇒(1): Let (3) holds. Therefore $a\big||b| \Rightarrow |a|\big||b|$. Let c be another common multiple. Then $\exists\ n \in \mathbb{Z}$ such that $a = cn \Rightarrow |a| = |c||n|$. But $|n| \geq 1 \Rightarrow |c||n| \geq |c| \Rightarrow |a| \geq |c|$.Therefore $\gcd(a, b) = |a|$. □

The following theorem filled the gap between greatest common divisor and least common multiple.

Theorem 2.5.1. *If a and b are positive integers, then $[a, b] = \dfrac{ab}{(a, b)}$, where $[a, b]$ and (a, b) are the least common multiple and greatest common divisor of a and b, respectively.*

Proof. Let us begin with taking $c = (a, b)$ and write $a = cr, b = cs$ for integers r and s. If $l = \dfrac{ab}{c}$, then $l = as = rb$, making l a (positive) common multiple of a and b.

Now let d be any positive integer that is a common multiple of a and b, implies $d = au = bv$. As we know, there exist integers k and l such that $c = ak + bl$. As a result of which,

$$\frac{d}{l} = \frac{dc}{ab} = \frac{d(ak + bl)}{ab} = \frac{d}{b}k + \frac{d}{a}l = vk + ul \Rightarrow l|c \Rightarrow l \leq c.$$

Hence $l = lcm(a, b)$ and $[a, b] = \dfrac{ab}{(a, b)}$. □

Remark 2.5.2. *The alternate proof of the above theorem can be done using the prime factorizations of integers a and b (for further details refer to chapter Prime Numbers).*

Corollary 2.5.1. *For any choice of positive integers a and b, $[a, b] = ab$ if and only if $(a, b) = 1$.*

Proof. Obvious. □

We conclude this section with a simple but interesting proposition.

Proposition 2.5.2. *For a and b be two non zero integers. Then*

1. $\gcd(a,b) = lcm(a,b)$ *if and only if* $a = \pm b$.
2. *If* $k > 0$, *then* $lcm(ka, kb) = k\ lcm(a,b)$.
3. *If m is any common multiple of a and b, then* $lcm(a,b) \big| m$.

Proof. 1. Let us consider $\gcd(a,b) = lcm(a,b) = d$. Now by Theorem 2.5.1 we get $d = ab$. Since $d \big| a$ then $\exists x \in \mathbb{Z}$ such that $dx = a$. This implies $d^2 = dxb \Rightarrow d = xb \Rightarrow b \big| d$. Thus we have $d \big| b$ and $d \big| b$ which together implies $d = \pm b$(by Proposition 2.2.1). By similar arguments we also have $d = \pm a$. Therefore $|d| = |a| = |b|$ implying $a = \pm b$.

Conversely let $d = \pm a$ holds. Then again by Proposition 2.2.1 we can assert that $a \big| b$ and $b \big| a$. This claims that $\gcd(a,b) = lcm(a,b)$.

2. To prove this we are to start with $\gcd(ka, kb) \cdot lcm(ka, kb) = k^2|ab|$. Then,

$$\begin{aligned} k \gcd(a,b) \cdot lcm(ka,kb) &= k^2|ab| \text{ [by Proposition 2.4.2]} \\ \Rightarrow \gcd(a,b) \cdot lcm(ka,kb) &= k|ab| \\ \Rightarrow \gcd(a,b) \cdot lcm(ka,kb) &= k \gcd(a,b) \cdot lcm(a,b) \\ \Rightarrow lcm(ka,kb) &= k\ lcm(a,b). \end{aligned}$$

3. Let us consider $l = lcm(a,b)$ and by division algorithm $\exists$ integers q and r such that $m = lq + r,\ 0 \le r < l$.

If $r = 0$ then obviously $l \big| m$.

If $0 < r < l$ then we can write $r = m - lq$. Since m and l are multiples of a and b then $\exists$ integers x, y, u, v such that $r = ax - ayq = a(x - yq)$ and also $r = bu - bvq = b(u - vq)$. This shows that r is a multiple of $a,\ b$ and this contradicts the fact $l = lcm(a,b)$. So $r < l$ is not possible. This proves our assertion.

□

2.6 Worked out Exercises

Problem 2.6.1. *If a, b, c are integers, then* $\gcd(a, bc) = 1$ *if and only if* $\gcd(a,b) = \gcd(a,c) = 1$.

Solution 2.6.1. *Let* $\gcd(a,b) = \gcd(a,c) = 1$ *holds. Then there exists integers* m_1, n_1, m_2 *and* n_2 *satisfying*

$$am_1 + bn_1 = 1 = am_2 + cn_2.$$

Therefore

$$\begin{aligned} am_1cn_2 + bn_1cn_2 = cn_2 &= 1 - am_2, \\ \Rightarrow a(m_2 + cm_1n_2) + bc(n_1n_2) &= 1. \end{aligned}$$

As $m_2 + cm_1n_2$ *and* n_1n_2 *are integers, therefore* $\gcd(a,bc) = 1$.

Conversely, let $\gcd(a,bc) = 1$ *holds. We are to show* $\gcd(a,b) = \gcd(a,c) = 1$. *Let* $\gcd(a,b) \neq 1$. *Then* $\gcd(a,b) = d$ *implies there exists* m, n *such that*

$$\begin{aligned} am + bn &= d \\ \Rightarrow acm + bcn &= cd \\ \Rightarrow a(cm) + b(cn) &= cd. \end{aligned}$$

Therefore $\gcd(a,bc) = cd(\neq 1)$, *a contradiction. Thus both* a, b *and* a, c *are coprime.*

Problem 2.6.2. *Prove or disprove: If* $a|(b+c)$, *then either* $a|b$ *or* $a|c$.

Solution 2.6.2. *Hint: Take* $a = 3, b = 2, c = 7$.

Problem 2.6.3. *If* $a|bc$, *show that* $a|\gcd(a,b)\gcd(a,c)$.

Solution 2.6.3. *Let* $\gcd(a,b) = d_1$ *and* $\gcd(a,c) = d_2$. *Then* $\exists\ x, y, u, v \in \mathbb{Z}$ *such that*

$$d_1 = ax + by,\ \&\ d_2 = au + cv.$$

Also, $\exists\ n \in \mathbb{Z}$ *satisfying* $an = bc$. *Now,*

$$\begin{aligned} d_1d_2 &= (ax + by)(au + cv), \\ &= a^2xu + acxv + abuy + bcyv, \\ &= a(axu + cxv + buy) + anyv, \\ &= a(axu + cxv + buy + nyv). \end{aligned}$$

$\therefore\ a|\gcd(a,b)\gcd(a,c)$.

Problem 2.6.4. *Prove that if* $d|n$, *then* $(2^d - 1)|(2^n - 1)$.

Solution 2.6.4. *We know that*

$$\begin{aligned} a^n - 1 &= (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1), \\ \therefore\ 2^n - 1 &= (2-1)(2^{n-1} + 2^{n-2} + \ldots + 2 + 1), \\ \therefore\ 2^d - 1 &= (2-1)(2^{d-1} + 2^{d-2} + \ldots + 2 + 1). \end{aligned}$$

Since $d|n$, $\exists\ x \in \mathbb{Z}$ *such that* $dx = n$. *Therefore*

$$\begin{aligned} 2^n - 1 = 2^{dx} - 1 &= (2^d)^x - 1, \\ &= (2^d - 1)(2^{d(x-1)} + 2^{d(x-2)} + \ldots + 2^d + 1). \\ \therefore\ (2^d - 1)\big|(2^n - 1). & \end{aligned}$$

Problem 2.6.5. *Prove that the product of any three consecutive integers is divisible by* 6.

Solution 2.6.5. *Here we need to show* $6|a(a+1)(a+2)$, *for any arbitrary* $a \in \mathbb{Z}$.

Let $S = a(a+1)(a+2)$. *Here* $6 = 3 \cdot 2$ *and* $\gcd(2,3) = 1$. *If* a *is even, then* $2|a \Rightarrow 2|S$. *And if odd, then* $2\big|(a+1) \Rightarrow 2|S$. *Let* $a = 3q + r,\ q, r \in \mathbb{Z}$. *Now* $r = 0, 1, 2$. *For all the values of* r, $3|S$*(verify!). Hence* $2|S, 3|S$ *together implies* $6|S$.

Problem 2.6.6. *If* a *is an odd integer, then* $24|a(a^2 - 1)$.

Solution 2.6.6. *Let us first prove,* a *is of the form* $8k + 1$. *Let* $a = 4q + r$. *Therefore* $r = 0$ *or* 3*(Why!). Therefore*

$$\begin{aligned} a^2 &= 16q^2 + 8q + 1 = 8k + 1, \text{ for } r = 0 \\ a^2 &= 16q^2 + 24q + 9 = 8k' + 1, \text{ for } r = 3. \end{aligned}$$

So $a(a^2 - 1) = a(8k)$, *for some* k. *Hence* $8\big|a(a^2 - 1)$. *Therefore* $6\big|a(a^2 - 1) \Rightarrow 3|a(a^2 - 1)$. *As* $\gcd(3, 8) = 1$, *hence* $24|a(a^2 - 1)$*(Why!).*

Problem 2.6.7. *If* a *is an integer not divisible by* 2 *or* 3, *then* $24|(a^2 + 23)$.

Solution 2.6.7. *Let* $a = 12q + r,\ q, r \in \mathbb{Z}$ *with* $0 \leq r < 12$. *But here,* $r = 1, 5, 7, 11$*(Why!). Now*

$$\begin{aligned} a^2 + 23 &= (12q + r)^2 + 23, \\ &= 144q^2 + 24qr + r^2 + 23, \\ &= 24(6q^2 + qr) + r^2 + 23. \end{aligned}$$

$$\begin{aligned} \textit{Now, } r = 1 \textit{ gives } r^2 + 23 &= 24 \\ r = 5 \textit{ gives } r^2 + 23 &= 48 = 24 \cdot 2 \\ r = 7 \textit{ gives } r^2 + 23 &= 72 = 24 \cdot 3 \\ r = 11 \textit{ gives } r^2 + 23 &= 144 = 24 \cdot 6 \\ \therefore\ a^2 + 23 &= 24(6q^2 + qr) + 24 \cdot k, \textit{ for some } k. \end{aligned}$$

Hence $24|(a^2 + 23)$.

Problem 2.6.8. *For* $n \geq 1$, *and positive integers* a, b, *prove that* $\gcd(a^n, b^n) = 1$ *where* $\gcd(a, b) = 1$.

Solution 2.6.8. *For* $n = 1$, *the statement is obvious. Let us assume the statement be true for* $n(> 1) = k$ *i.e.* $\gcd(a^k, b^k) = 1$. *Now* $\gcd(a^k, b^{k+1}) = \gcd(a^k, b^k) = 1$*[refer to the properties of GCD]. Since* $\gcd(a, b) = \gcd(b, a) = 1$, *then* $\gcd(a^k, b^{k+1}) = 1 = \gcd(a^{k+1}, b^{k+1})$.

Problem 2.6.9. *For* $n \geq 1$, *and positive integers* a, b, *prove that the relation* $a^n|b^n$ *implies* $a|b$.

Solution 2.6.9. *The relation is obvious for* $n = 1$. *If possible, let us assume the relation is true for* $n = k$. *Then* $a^n|b^n$ *implies* $a|b$, *which further implies* $\exists\ x, y$ *such that*

$$b^k = xa^k \ \&\ b = ay.$$

$$\therefore\ xa^{k+1} = ab^k = \left(\frac{b}{y}\right) b^k = \frac{b^{k+1}}{y}.$$

$$\therefore\ xya^{k+1} = b^{k+1} \Rightarrow a^{k+1}|b^{k+1}.$$

Problem 2.6.10. *Prove that if* $\gcd(a, b) = 1$, *then* $\gcd(a + b, ab) = 1$.

Solution 2.6.10. *Let* c *be the common divisor of* $a+b$ *and* ab. *Then* $\gcd(a, c) = \gcd(b, c) = 1$. *Since* $c\big|ab$ *and* $\gcd(c, a) = 1$, *then by Euclid's Lemma we have* $c\big|b$. *By similar reasoning,* $c\big|a$. *As* $c \leq \gcd(a, b) = 1 \Rightarrow c = 1 \Rightarrow \gcd(a + b, ab) = 1$.

Problem 2.6.11. *Prove that the greatest common divisor of two positive integers divides their least common multiple.*

Solution 2.6.11. *Let* $a, b > 0$. *We are to prove* $\gcd(a, b)\big|lcm(a, b)$. *We know that* $\gcd(a, b)lcm(a, b) = ab$. *Let* $d = \gcd(a, b)$. *Then* $\exists,\ m, n$ *such that* $a = dn, b = dm$.

$$d \cdot lcm(a, b) = (dn)(dm).$$

$$\therefore\ lcm(a, b) = d(nm) \Rightarrow d\big|lcm(a, b) \Rightarrow \gcd(a, b)\big|lcm(a, b).$$

Problem 2.6.12. *If a and b are prime to each other then prove that* $\gcd(a+b, a^2+b^2) = 1$ *or* 2.

Solution 2.6.12. *Let* $\gcd(a+b, a^2+b^2) = d$. *Then* $d\big|(a^2+b^2) \iff d\big|(a+b)(a-b)+2b^2$. *Since* $d\big|(a+b)$, $\exists\ x$ *such that* $dx = a+b$. *Let* $m \in \mathbb{Z}$ *be such that*

$$dm = (a+b)(a-b)+2b^2 \Rightarrow dm = dx(a-b)+2b^2 \Rightarrow d[m-x(a-b)] = 2b^2 \Rightarrow d\big|2b^2.$$

Now combining the facts $d\big|(a+b)$ *and* $\gcd(a,b) = 1$, *we find* $\gcd(b,d) = 1$*(Why!). Thus we get* $d \nmid b$, *which implies* $d|2$. *Therefore* $d \leq 2$ *implies* $d = 1$ *or* 2.

Problem 2.6.13. *Let* a, b, c *be integers, no two of which are zero, and* $d = \gcd(a,b,c)$. *Show that* $d = \gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b)$.

Solution 2.6.13. *Firstly, we will show* $d = \gcd(\gcd(a,b),c)$. *Let* $f = \gcd(a,b)$ *and* $g = \gcd(f,c)$. *Now* $g|f \Rightarrow g|a, g|b$. *Here* $g|c \Rightarrow g \leq d$. *Our next task is to show* $d|f$. *Here for some* $x, y \in \mathbb{Z}$, $f = ax+by$*[refer to Theorem 2.4.1]. Now* $a = du, b = dv$ *for some* $u, v \in \mathbb{Z}$. *Hence* $f = dux+dvy \Rightarrow d|f$. *Now* $d|c \Rightarrow d|g \Rightarrow d \leq g$. *Hence combining,* $d = g$ *holds i.e.* $d = \gcd(\gcd(a,b),c)$. *Proceeding as above, we can show that* $d = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b)$. *Thus* $d = \gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b)$.

2.7 Linear Diophantine Equations

Before delving deep into the topic, let us start with the following problem:

A person wishes to buy ice cream bar for a get-together at home. After going to the ice cream parlour he came across with some flavours: one is chocolate bar costing Rs.126 and another is strawberry bar costing Rs.99. He decided to buy both combinations with a budget of Rs.2000. Now the problem is; whether there exist any such combinations of these two flavours? To answer this, let k denote the number of chocolate bars and l denote the number of strawberry bars, the person can purchase. Then we must have $126k + 99l = 2000$, where both k and l are nonnegative integers.

Now the need for Diophantine equation get along to find the solutions of a particular equation, which follow from the set of integers. Diophantine equations get their name from the ancient Greek mathematician Diophantus, who wrote extensively on such equations. The type of diophantine equation $ak + bl = c$, where a, b and c are integers is called a linear diophantine equations in two variables. We now develop the theory for solving such equations. The following

theorem illustrates that when such an equation has solutions, and when there are solutions, explicitly describes them.

Theorem 2.7.1. *Let a, b be positive integers with $d = \gcd(a, b)$. If $d \nmid c$, the equation $ax + by = c$ has no solutions(in integers). There are infinitely many solutions(integers) if $d|c$. Moveover in particular, if $x = x_0, y = y_0$ is a solution of the equation, then all solutions are given by*

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n, \ n \text{ being an integer.}$$

Before proceeding for the proof, first we demonstrate the above theorem for finding all the integral solutions of the two diophantine equations described at the beginning of this section. We first consider the equation $126x + 99y = 2000$. The greatest common divisor of 126 and 99 is $\gcd(99, 126) = 9$. Since $9 \nmid 2000$, we can say no integral solutions exist. Hence no combination of 126 and 99 rupees he can purchase.

Proof. Assume that x and y are integers satisfying $ax+by = c$. Together $d|a$ and $d|b$ implies $d|c$(Why!). Hence if $d \nmid c$ there does not exists any integral solutions. So we assume that $d|c$. Then from theorem (2.4.1), for some integers s, t

$$d = as + bt. \tag{2.7.1}$$

Since, $d|c$ there exist some integer e such that $de = c$ holds. Multiplying (2.7.1), we obtain

$$c = a(se) + b(te).$$

Hence one particular solution of the equation is given by $x = x_0 = se, y = y_0 = te$.

Now, to prove the remaining part of the theorem suppose $x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n$, n being an integer. Since,

$$ax + bl = a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) = ax_0 + bl_0 = c,$$

we see that (x, y) is a solution.

Next our claim is to show every solution of the equation $ax + bl = c$ must be of the form described in the theorem. since,

$$ax_0 + bl_0 = c,$$

on subtraction we obtain

$$a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = b(-y + y_0). \tag{2.7.2}$$

Dividing both sides by d, we see that

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(-y + y_0).$$

By virtue of Proposition 2.4.2, we know $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Also, using Euclid's Lemma it follows $\frac{a}{d}|(y_0 - y)$. Hence there exists an integer n with $\frac{a}{d}n = y_0 - y$ means $y = y_0 - \frac{a}{d}n$. Now putting this value of y into the (2.7.2), we find $a(x - x_0) = b\left(\frac{a}{d}\right)n$ implies $x = x_0 + \left(\frac{b}{d}\right)n$. □

Example 2.7.1. *A man wishes to purchase Rs* 510 *of travelers checks. The checks are available only in denominations of Rs* 20 *and Rs* 50. *How many of each denomination should he buy?*

Answer 2.7.1. *Consider the equation* $20k + 50l = 510$. *The greatest common divisor of* 20 *and* 50 *is* $(20, 50) = 10$, *and since* $10|510$, *there are infinitely many integral solutions. Using the Euclidean algorithm, we find that* $20(-2) + 50 = 10$. *Multiplying both sides by* 51, *we obtain* $20(-102) + 50(51) = 510$. *Hence a particular solution is given by* $k_0 = -102$ *and* $l_0 = 51$. *Theorem 2.7.1 tells us that all integral solutions are of the form* $k = -102 + 5n$ *and* $l = 51 - 2n$. *Since we want both* k *and* l *to be nonnegative, we must have* $-102 + 5n > 0$ *and* $51 - 2n > 0$; *thus,* $n > \frac{102}{5}$ *and* $n < \frac{51}{2}$. *Since* n *is an integer, it follows that* $n = 21, 22, 23, 24, 25$. *Hence we have the following* 5 *solutions:* $(k, l) = (3, 9), (8, 7), (13, 5), (18, 3), (23, 1)$.

2.8 Worked out Exercises

Problem 2.8.1. *Examine the nature of the following Diophantine equations:*

1. $14x + 35y = 93$.

2. $33x + 14y = 115$.

Solution 2.8.1. 1. *Here* $\gcd(14, 35) = 7$ *and* $7 \nmid 93$, *hence not solvable.*

2. *Here* $\gcd(33, 14) = 1$ *and* $1|115$, *hence solvable.*

Problem 2.8.2. *Determine all solutions, in positive integers, of the following Diophantine equations:*

1. $158x - 57y = 7$.

2. $54x + 21y = 906$.

Solution 2.8.2. *1. To find the solution of this equation we need to find the* gcd *of* $158, 57$. *Now applying Euclid's Algorithm, we obtain*

$$\begin{aligned} 158 &= 3 \cdot 57 - 13 \quad \textit{Again } 1 = 3 - 2 = 3 - (5 - 3) \\ 57 &= 4 \cdot 13 + 5 \qquad\qquad = 2 \cdot 3 - 5 = 2(13 - 2 \cdot 5) - 5 \\ 13 &= 2 \cdot 5 + 3 \qquad\qquad = 2 \cdot 13 - 5 \cdot 5 \\ 5 &= 3 \cdot 1 + 2 \qquad\qquad = 2 \cdot 13 - 5(57 - 4 \cdot 13) \\ 3 &= 2 \cdot 1 + 1 \qquad\qquad = 22 \cdot 13 - 5 \cdot 57 \\ &\qquad\qquad\qquad = 22(3 \cdot 57 - 158) - 5 \cdot 57 \\ &\qquad\qquad\qquad = 61(57) + (-22) \cdot 158. \end{aligned}$$

Thus, $\gcd(158, 57) = 1$. $\quad \therefore 7 = (61 \cdot 7)57 + (-22 \cdot 7)158.$

Since $\gcd(158, 57) | 7 = 7$ *therefore, an integral solution do exist for the given equation. Hence* $(x_0, y_0) = (-154, -427)$ *is an integral solution. Hence all integral solutions of the given equation is of the form,*

$$x = -154 + \frac{-57}{1}n = -154 - 57n > 0 \qquad \Rightarrow n < -2.7 \Rightarrow n \leq -3$$

$$y = -1510 + \frac{-158}{1}n = -1510 - 158n > 0 \quad \Rightarrow n < -2.7 \Rightarrow n \leq -3.$$

2. To find the solution of this equation we need to find the gcd *of* $54, 21$. *Now applying Euclid's Algorithm, we obtain,*

$$\begin{aligned} 54 &= 2 \cdot 21 + 12 \quad \textit{Again, } 3 = 12 - 9 = 12 - (21 - 12) \\ 21 &= 12 \cdot 1 + 9 \qquad\qquad = 2 \cdot 12 - 21 \\ 12 &= 9 \cdot 1 + 3 \qquad\qquad = 2(54 - 2 \cdot 21) - 21 \\ 9 &= 3 \cdot 3 + 0 \qquad\qquad = 2 \cdot 54 + (-5) \cdot 21. \end{aligned}$$

Thus, $\gcd(54, 21) = 3$ & $3 \big| 906$. $\quad \therefore 906 = (302 \cdot 2)54 + (302 \cdot (-5))21.$

Since $\gcd(54, 21) | 906 = 302$ *therefore, an integral solution do exist for the given equation. Hence* $(x_0, y_0) = (604, -1510)$ *is an integral solution. Hence all integral solutions of the given equation is of the form,*

$$x = 604 + \frac{21}{3}n = 604 + 7n > 0 \qquad \Rightarrow n > -86.3$$

$$y = -1510 + \frac{-54}{3}n = -1510 - 18n > 0 \qquad \Rightarrow n < -83.9.$$

Thus, $n = -84, -85, -86$, *which gives* $(x, y) = (16, 2), (9, 20), (2, 38)$.

Problem 2.8.3. *Determine all solutions of the Diophantine equation* $24x + 138y = 18$.

Solution 2.8.3. *First we need to calculate the gcd of* 24 *and* 138 *. Here,*

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \qquad && \textit{Again, } 6 = 24 - 18 \\ 24 &= 18 + 9 && = 24 - (138 - 5 \cdot 24) \\ 18 &= 3 \cdot 6 + 0 && = 6 \cdot 24 - 138 \\ \textit{Thus, } \gcd(24, 138) &= 6 \ \& \ 6 \big| 18. && \therefore 18 = (18)54 + (-3)138. \end{aligned}$$

So the integral solution is $x_0 = 18,\ y_0 = -3$. *Thus the solution of this equation is,*

$$x = 18 + \left(\frac{138}{6}\right) n = 18 + 23n$$
$$y = -3 - \left(\frac{24}{6}\right) n = -3 - 4n \ [n \in \mathbb{Z}].$$

Problem 2.8.4. *A farmer purchased* 100 *heads of livestock for a total cost of Rs.*4000. *Prices were as follow: sheep, Rs.*120 *each; hen, Rs.*25 *each; duck, Rs.*50 *each. If the farmer obtained at least one animal of each type how many had he bought?*

Solution 2.8.4. *Let us consider the variables* x, y *and* z *for sheep, hen and duck respectively. Then from given hypothesis we have,* $x + y + z = 100$ *and* $120x + 25y + 50z = 4000$, *where* $x, y, z \geq 1$. *Then* $24x + 5y + 10z = 800$ *and* $24x + 10z + 5(100 - x - z) = 800$ *holds. Combining last two equations yield* $19x + 5z = 300$. *Hence the solutions are* $x = 0,\ z = 60$. *Therefore*

$$x = 5k,\ z = 60 - 19k,$$
$$y = 40 + 14k,\ k \in \mathbb{Z}.$$

Consequently,

$$5k \geq 1 \Rightarrow k \geq 1$$
$$60 - 19k \geq 1 \Rightarrow k \leq 3$$
$$40 + 14k \geq 1 \Rightarrow k \geq -2.$$

Considering last three inequalities, we get $1 \leq k \leq 3 \Rightarrow k = 1, 2, 3$. *Therefore the possibilities are* 5 *sheep,* 54 *hens and* 41 *ducks or* 10 *sheep,* 68 *hens and* 22 *ducks or* 15 *sheep,* 82 *hens and* 3 *ducks.*

2.9 Exercises:

1. Let a, b and c be integers with $\gcd(a, b) = 1$. Then $\gcd(a^2, b^2) = 1$.

2. Verify that $3a^2 - 1$ is never a perfect square.

3. For $n \geq 1$, establish that the integer $n(7n^2 + 5)$ is of the form $6k$.

4. For an odd integer n, show that $n^4 + 4n^2 + 11$ is of the form $16k$.

5. Verify that if an integer is simultaneously a square and a cube (as is the case with $64 = 8^2 = 4^3$), then it must be either of the form $7k$ or $7k + 1$.

6. If $a \big| bc$, show that $a \big| \gcd(a, b) \gcd(a, c)$.

7. Verify the followings:
   (a)the product of any four consecutive integers is divisible by 24;
   (b)the product of any five consecutive integers is divisible by 120.

8. Prove that the expression $\frac{(3n)!}{(3!)^n}$ is an integer for all $n \geq 0$.

9. Establish each of the statements below:
   (a)If a and b are odd integers, then $8 \big| (a^2 - b^2)$.
   (b)If a is an arbitrary integer, then $6 \big| a(a^2 + 11)$.

10. Assuming that $\gcd(a, b) = 1$, prove that $\gcd(2a + b, a + 2b) = 1$ or 3.

11. Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

12. Find integers x, y, z satisfying $\gcd(198, 288, 512) = 198x + 288y + 512z$.

13. Use the Euclidean Algorithm to obtain integers x and y satisfying $\gcd(1769, 2378) = 1769x + 2378y$.

14. Examine the nature of the Diophantine equation $14x + 35y = 93$.

15. Determine all solutions in the positive integers of $158x - 57y = 7$.

16. Determine all solutions in the integers of $221x + 35y = 11$.

17. Mr.Sen had gone to a medical shop to buy two medicines: medicine A and medicine B. By mistake, the chemist had given him the number of medicine A in place of medicine B and vice versa.Unaware of the fact, Mr.Sen received an extra amount Rs.68 from the shop keeper. Considering the price of each medicine A and medicine B to be Rs.10 and Rs.15 respectively, find the least number of medicine A, Mr. Sen wanted to purchase.

18. One hundred packets of dry food are distributed among 100 persons in such a way that every man, woman and child receives 3 packets, 2 packets, and half a packet respectively. Find the total number of persons over there?