2.4.2. Relatively Prime Integers

Two integers a and b, not both zero, are said to prime to each other or relatively prime or coprime if $gcd(a, b) = 1$.

Scanned by CamScanner

Thus 8 and 9 are relatively prime as $gcd(8, 9) = 1$.

Theorem 2.14. If a and b be integers, not both zero, then a and b are prime to each other if and only if there exist integers u and v such that $au + bv = 1$. In other words,

$gcd(a, b) = 1 \Leftrightarrow au + bv = 1$ for some integers u, v.

Proof. Let a and b are prime to each other. Then $gcd(a, b) = 1$. Hence by Theorem 2.9, there exist integers u and v such that $1 = au + bv$.

Now, let $\exists\, u, v \in \mathbb{Z}$ such that $au + bv = 1$.

Let $d = gcd(a,b)$. Then $d \mid a$ and $d \mid b \Rightarrow \exists\, x, y \in \mathbb{Z}$ such that

$d \mid (ax + by)$ [by Theorem 2.2 (vi)]

Thus $d \mid 1$. This implies that $d = 1$, since $d > 0$.

Thus $gcd(a, b) = 1$. Hence the theorem.

Theorem 2.15. If $d = gcd(a, b)$, then $\dfrac{a}{d}$ and $\dfrac{b}{d}$ are integers prime to each other.

Proof. We have $gcd(a, b) = d \Rightarrow d \mid a$ and $d \mid b$. Also $d > 0$.

$$\therefore \exists\, m, n \in \mathbb{Z} \text{ such that } a = md \text{ and } b = nd.$$

Since $\dfrac{a}{d} = m$ and $\dfrac{b}{d} = n$, therefore, $\dfrac{a}{d}$ and $\dfrac{b}{d}$ are integers.

Since $gcd(a, b) = d$, $\exists\, u, v \in \mathbb{Z}$ such that $d = au + bv$.

[by Theorem 2.9]

$$\Rightarrow 1 = \left(\frac{a}{d}\right)u + \left(\frac{b}{d}\right)v \quad [\because d > 0]$$

This form of representation implies that $\dfrac{a}{d}$ and $\dfrac{b}{d}$ are prime to each other (Theoren 2.14]). Hence proved.

Scanned by CamScanner

2.5. Prime Numbers, Composite Numbers

An integer $p > 1$ is said to be a ***prime number*** or a ***prime*** if its only positive divisors are 1 and p.

An integer $c > 1$ which is not a prime is called ***composite number.***

The integers 2, 3, 5, 7, 11, 13,........are primes whereas 4, 6, 8, 9, 10, 12, 14 ..... are composite numbers.

The integer 1 is neither a prime nor a composite number.

2 is the only even prme number. All other prime numbers are odd.

Twin Primes

Successive odd integers p and $p+2$ which are primes are called twin primes.
For example, (3, 5), (5, 7), (11, 13) etc. are twin primes.

Lemma 1. A positive integer n is prime if $gcd(n, p) = 1$ where p is a prime number such that $p \le \sqrt{n}$.
Equivalently, a positive integer n is a composite number if it is divisible by at least one prime $p \le \sqrt{n}$.

Proof. If a positive integer n be composite, then $n = bc$ for some integers b and c satisfying
$1 < b < n,\ 1 < c < n$.

Let $b \le c$. Then $b^2 \le bc = n \Rightarrow b \le \sqrt{n}$.

Since $b > 1$, b has at least one prime divisor p and $p \le b \le \sqrt{n}$.
Hence proved.

Remark. Lemma 1 is used to test whether a given integer n is prime.

Theorem 2.15. If p be a prime and $p|ab$, then either $p|a$ or $p|b$.

Scanned by CamScanner

Proof. If $p|a$, then the theorem is proved. Let p be not a divisor of a. Since p is a prime, it has only divisors 1 and p.

It follows that $gcd(a, p) = 1$.

Hence $\exists u, v \in \mathbb{Z}$ such that $au + pv = 1 \Rightarrow abu + pbv = b$ ...... (1)

Now, $p|ab$ and $p|pb$

$\Rightarrow p|\{(ab)u + (pb)v\}$ [by Theorem 2.2 (vi)]

$\Rightarrow p|b$ [by (1)]

Hence the theorem.

Theorem 2.16. If p be a prime number and a is an integer such that $1 \le a < p$, then p is prime to a.

Proof. Let $gcd(a, p) = d$. Then $d | a$ and $d | p$.

Again p is prime $\therefore d|p \Rightarrow$ either $d=1$ or $d=p$.

But $a<p$ and $d|a$ $\therefore d \neq p$. Hence $d=1$.

Thus $gcd(a, p) = 1$ implying that a and p are prime to each other *(Proved)*

Theorem 2.17. A composite number has at least on prime divisor.

Proof. Let c be a composite number. Then c has positive divisors besides 1 and c.

Let $S = \{x \in \mathbb{Z}^+ : x \text{ is a positive divisor of } c \text{ other than } 1 \text{ and } c\}$.

Then S is a non-empty subset of the set $\mathbb{N}$ of natural numbers.

Hence by the Well-ordering property of $\mathbb{N}$, S has a least element, say, d.

Then $1 < d < c$.

We assert that d is a prime number. If d is not a prime then d has a divisor d_1 other than 1 and d and $1 < d_1 < d < c$.

Scanned by CamScanner

But $d_1 | d$ and $d | n \Rightarrow d_1 | c \Rightarrow d_1 \in S$, which contradicts that d is the least element of S. It follows immediately that d is a prime. Since $d \in S$, the theorem follows. *(Proved)*

Theorem 2.18. (Fundamental Theorem of Arithmetic) Any positive integer is either 1, or a prime or it can be expressed uniquely as a product of primes (irrespective of the order of the factors in the product).

Canonical Form of an Integer

Any integer $n>1$ can be expressed in the following form, known ***canonical form of n*** :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots. p_n^{\alpha_n}$$

where p_i, $i = 1(1)n$ are distinct primes such that

$p_1 < p_2 < \ldots. < p_n$ and α_i, $i = 1(1)n$ are positive integers.

The above canonical form is the application of the Fundamental theorem and is the best representation of a composite number.

For example, consider the composite numbers 3528 and 81675.

Their canonical forms are $3528 = 2^3 \times 3^2 \times 7^2$ and

$81675 = 3^3 \times 5^2 \times 11^2$.

Theorem 2.19. Let $n(>1)$ be a positive integer whose camonical form is $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots. p_n^{\alpha_n}$ where p_i, $i = 1(1)n$ are distinct primes with $p_1 < p_2 < \ldots. < p_n$ and $\alpha_i \in \mathbb{Z}^+$, $i = 1(1)n$. Then the total number of positive divisors of n is

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots..(\alpha_n + 1).$$

Scanned by CamScanner