Clearly, n is a divisor of each term in the right hand side of (iii). So, $n \mid 2S_n$ ... (iv)

Because n and $n+1$ are prime to each other, it follows from (ii) and (iv) that $n(n+1)$ is a divisor of $2S_n$

As $n(n+1)$ is divisible by 2, $\frac{n(n+1)}{2}$ is an integer and therefore $\frac{n(n+1)}{2}$ is a divisor of S_n.

That is, $1+2+\cdots+n$ is a divisor of $1^r+2^r+\cdots+n^r$ if r is an odd positive integer.

2.3.13 Euclidean Algorithm

Euclidean algorithm is an efficient method of finding the greatest common divisor of two given integers. The method involves repeated application of the division algorithm.

Let a and b two integers whose g.c.d is required.

Since $\gcd(a,b) = \gcd(|a|, |b|)$, it is enough to assume that a and b are positive integers. Without loss of generality, we assume $a > b > 0$

By division algorithm, $a = bq_1 + r_1$ where $0 \le r_1 < b$

If it happens that $r_1 = 0$ then $b \mid a$ and $\gcd(a,b) = b$

If $r_1 \neq 0$, then by division algorithm, $b = r_1 q_2 + r_2$ where $0 \le r_2 < r_1$.

If it happens that $r_2 = 0$, the process stops. If $r_2 \neq 0$, then by division algorithm, $r_1 = r_2 q_3 + r_3$ where $0 \le r_3 < r_2$

The process continues until some zero remainder appears. This must happen because the remainder $r_1, r_2, r_3, \ldots$, form a decreasing sequence of integers and since $r_1 < b$, the sequence contains at most b non-negative integers.

Let us assume that $r_{n+1} = 0$ and r_n is the last non-zero remainder.

We have the following relations

$$a = bq_1 + r_1 \qquad 0 \leq r_1 < b$$

$$b = r_1 q_2 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \qquad 0 < r_3 < r_2$$

$$\cdots \qquad \cdots \qquad \cdots \qquad \cdots$$

$$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + 0$$

We assert that $r_n = \gcd(a, b)$. First of all, we prove the Lemma — If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$

Proof: Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. This implies $d \mid a - bq$, i.e., $d \mid r$. This shows that d is a common divisor of b and r.

Let c be a common divisor of b and r. Then $c \mid bq + r$, i.e., $c \mid a$. This shows that c is a common divisor of a and b. Since $d = \gcd(a, b)$, it follows from the property of the gcd that $c \mid d$

and this gives $d = \gcd(b, r)$

We utilize this lemma to show that $r_n = \gcd(a, b)$

$$r_n = \gcd(0, r_n) = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(b, r_1) = \gcd(a, b)$$

Also, we have $r_n = r_{n-2} - r_{n-1} q_n$

$$= r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n$$

$$= (1 + q_{n-1} q_n) r_{n-2} + (-q_n) r_{n-3}$$

So, r_n is expressed as a linear combination of r_{n-2} and r_{n-3}.

Proceeding backwards we can express r_n as a linear combination of a and b

Worked Examples (continued)

10. Calculate $\gcd(567, 315)$ and express $\gcd(567, 315)$ as $567u + 315v$, where u and v are integers.

Solution: By division algorithm,

$$567 = 315 \times 1 + 252$$
$$315 = 252 \times 1 + 63$$
$$252 = 63 \times 4 + 0$$

The last non-zero remainder is 63. So, $\gcd(567, 315) = 63$

$$63 = 315 - 252 \times 1 = 315 - 1 \cdot (567 - 315) = 567(-1) + 315 \times 2$$

$$= 567u + 315v \quad \text{where } u = -1 \text{ and } v = 2$$

11. Find two integers u and v such that $63u + 55v = 1$

Solution: By division algorithm,

$$63 = 55 \times 1 + 8$$
$$55 = 8 \times 6 + 7$$
$$8 = 7 \times 1 + 1$$
$$7 = 7 \times 1 + 0$$

The last non-zero remainder is 1

So, gcd (63, 55) = 1

Now $1 = 8 - 7\times1 = 8 - (55 - 8\times6)\times1$

$= -55 + 8\times7$

$= -55 + (63 - 55\times1)\times7$

$= 55(-8) + 63\times7$

So, $63u + 55v = 1$ where $u = 7$ and $v = -8$

12. find two integers u and v satisfying $54u + 24v = 30$

Solution: Let us find gcd (54, 24)

By division algorithm, $54 = 24\times2 + 6$

$24 = 6\times4 + 0$

So, gcd (54, 24) = 6

Now $6 = 54 - 24\times2 = 54\times1 + 24(-2)$

Consequently, $30 = 54\times5 + 24(-10)$

So, $54u + 24v = 30$, where $u = 5$ and $u = -10$

2.4 Prime numbers

An integer $p > 1$ is said to be a prime number or simply a prime, if its only positive divisors are 1 and p. An integer > 1 which is not a prime is said to be a composite number.

The integers 2, 3, 5, 7, 11, ... are prime numbers, while the integers 4, 6, 8, 9, ... are composite numbers.

The integer 1 is regarded as neither prime nor composite