Example 6: If a, b are positive integers such that $\gcd(a,b)=1$, then show that $\gcd(a+b, a-b) = 1$ or 2

Solution: Let $\gcd(a+b, a-b) = d$. Then d divides $a+b$ and d divides $a-b$. Hence d divides $(a+b)+(a-b) = 2a$ and d divides $(a+b)-(a-b) = 2b$. So, we find that d is a common divisor of $2a$ and $2b$. But $\gcd(2a, 2b) = 2\gcd(a,b) = 2\cdot 1 = 2$

This implies $d = 1$ or 2

Exercises: 1. Prove that $7^n - 1$ is divisible by 6 for any positive integer n.

2. Prove that 19 divides $7^{n+2} + 8^{2n+1}$ for any integer $n \in \mathbb{N}$

3. If a, b are positive integers, then prove that $\gcd(ka, kb) = k.\gcd(a,b)$ for any positive integer k.

4. If a, b, c are positive integers such that $\gcd(a, bc) = 1$, then prove that $\gcd(a,b) = 1 = \gcd(a,c)$

5. Find the gcd of 315 and 4235 and find integers s and t such that $\gcd(315, 4235) = 315s + 4235t$

Representation of Positive integers: In our natural number system (including 0), number ten plays an important role. If we consider the number 353, we mean

$$3\times 10^2 + 5\times 10 + 3$$

and the 4595 means

$$4.10^3 + 5.10^2 + 9.10 + 5$$

So, we see that any non-negative integer can be expressed as $a_k 10^k + a_{k-1}10^{k-1} + \dots + a_1.10 + a_0$ where each a_i is an integer such that $0 \le a_i \le 9$, for $i = 0, 1, 2, \dots, k$. This is called a decimal ~~representation~~ representation of the non-negative integers or is called a representation in the base 10 of the non-negative integers. If we add sign only we can represent the whole set of integers. Now-a-days we find a computing machines use numbers in the base two or three or some different base other than 10 in its mathematical calculations. Here we see how to represent a number uniquely in an arbitrary base k, where k is an integer and $k > 1$.

Theorem 8 Let k be an integer greater than 1. Then any positive integer n can be expressed uniquely in the form

$$n = a_r k^r + a_{r-1} k^{r-1} + \cdots + a_1 k + a_0,$$

where r is a non-negative integer, $a_r \neq 0$ and each a_i is an integer such that $0 \le a_i \le k-1$ for $i = 0, 1, 2, \ldots, r$

Proof: By division algorithm, there exist integers q_0 and a_0 such that

$n = q_0 k + a_0$ with $0 \le a_0 \le k-1$

If $q_0 \neq 0$, then applying the division algorithm, we obtain

$q_0 = q_1 k + a_1, \quad 0 \le a_1 \le k-1$

If $q_1 \neq 0$, we apply division algorithm again for the integers q_1 and k to obtain q_2 and a_2 such that

$q_1 = q_2 k + a_2, \quad 0 \le a_2 \le k-1$

If $q_2 \neq 0$, we repeat the process. Thus we obtain

$$q_2 = q_3 k + a_3 \qquad 0 \le a_3 \le k-1$$
$$q_3 = q_4 k + a_4 \qquad 0 \le a_4 \le k-1$$
$$\vdots$$

Since $n > q_0 > q_1 > q_2 > q_3 > q_4 \cdots > 0$ and the number of positive integers small than n is $n-1$, we must, in a finite number of steps, find integers $q_{r-1}, q_r, q_{r-1}, a_r$ such that

$$q_{r-2} = q_{r-1} k + a_{r-1} \qquad 0 \le a_{r-1} \le k-1, \quad q_{r-1} \neq 0$$
$$q_{r-1} = q_r k + a_r \qquad 0 \le a_r \le k-1, \quad q_r = 0$$

Then, $n = q_0 k + a_0 = (q_1 k + a_1)k + a_0$

$= q_1 k^2 + a_1 k + a_0$

$= (q_2 k + a_2)k^2 + a_1 k + a_0$

$= q_3 k^3 + a_2 k^2 + a_1 k + a_0$

$= \cdots$

$= a_r k^r + a_{r-1} k^{r-1} + \cdots + a_2 k^2 + a_1 k + a_0$

Since $q_{r-1} \neq 0$, the equality $q_{r-1} = 0.k + a_r$ implies $a_r \neq 0$.
So, we find that n can be expressed as

$$n = a_r k^r + a_{r-1} k^{r-1} + \cdots + a_2 k^2 + a_1 k + a_0 \quad \text{where } r \text{ is} \quad \cdots (1)$$

a non-negative integer and $0 \leq a_i \leq k-1$

The representation of n by (1) is called a representation of n in the base k. We can show that this representation is unique.

We write $n = (a_r a_{r-1} \cdots a_1 a_0)_k$ to represent

$$a_r k^r + a_{r-1} k^{r-1} + \cdots + a_1 k + a_0$$

Here $a_r a_{r-1} \cdots a_1 a_0$ is not the product of integers. It is just a symbolic notation. For example $(102011)_3$ represents the integer $1.3^5 + 0.3^4 + 2.3^3 + 0.3^2 + 1.3 + 1$

If the base k is less than or equal to 10, then the a_i's are chosen from $0, 1, 2, \ldots, k-1$. For example, If $k = 10$ then the a_i's are chosen from $0, 1, 2, \ldots, 9$. If the base is 2 i.e., $k=2$ then a_i's are chosen from 0, 1

Consider the integer 75 which is in base 10. To represent 75 in the base 2, we first divide 75 by 2. We obtain the quotient 37 and the remainder 1, i.e., we can write $75 = 37.2 + 1$. Then we divide 37 by 2. We find $37 = 18.2 + 1$. We perform the division algorithm successive, replacing the divident each time with the quotient until the quotient is zero.

$75 = 37.2+1$

$37 = 18.2+1$

$18 = 9.2+0$

$9 = 4.2+1$

$4 = 2.2+0$

$2 = 1.2+0$

$1 = 0.2+1$

Hence
$$\begin{aligned}75 &= 37.2+1\\ &= (18.2+1).2+1\\ &= 18.2^2+1.2+1\\ &= (9.2+0).2^2+1.2+1\\ &= 9.2^3+0.2^2+1.2+1\\ &= (4.2+1).2^3+0.2^2+1.2+1\\ &= 4.2^4+1.2^3+0.2^2+1.2+1\\ &= (2.2+0).2^4+1.2^3+0.2^2+1.2+1\\ &= 2.2^5+0.2^4+1.2^3+0.2^2+1.2+1\\ &= (1.2+0).2^5+0.2^4+1.2^3+0.2^2+1.2+1\\ &= 1.2^6+0.2^5+0.2^4+1.2^3+0.2^2+1.2+1\end{aligned}$$

So, we find $(75)_{10} = (1001011)_2$

Note: From the above, we find that to get the binary representation of $(75)_{10}$ we simply write the remainders of the above divisions. The first remainder in the unit place, the second remainder in the second place and so on, i.e., starting from right to left.

Definition Let n be a positive integer and k is an integer and $k>1$. Then (i) the representation of n in the base $k=10$ is called the decimal representation of n, (ii) the representation of n in the base $k=2$ is called the binary representation of n and in the base $k=3$ is called the ternary representation of n (iii) the representation of n in the base $k=8$ is called the octal ~~represent~~ representation of n, (iv) the representation of n in the base $k=16$ is called the hexadecimal representation of n.

The binary system is most convenient for use in modern electronic computing machines. We have seen that binary numbers are expressed by strings of zeroes and ones; 0 and 1 can be expressed in a machine by a switch or similar electronic device being either off or on.

Now to represent a number in the base k, where k is a positive integer greater than 1, we need k symbols. For example, when $k \leq 10$, we take the symbols $1, 2, \ldots, k-1$. For example, if $k = 7$, then we take the symbol $1, 2, \ldots, 6$. But if $k > 10$, we take different symbols. For example, for hexadecimal system, i.e., for $k = 16$, we the following 16 symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Here A, B, C, D, E, F are used to represent the digits that correspond to 10, 11, 12, 13, 14 and 15 respectively.

Let us consider the number $(A10CA3)_{16}$. The number is in base 16. If we want to know the number, i.e., if we want to express it in the base 10, we proceed in the following way:

$$(A10CA3)_{16} = A \cdot 16^5 + 1 \cdot 16^4 + 0 \cdot 16^3 + C \cdot 16^2 + A \cdot 16 + 3$$
$$= 10 \cdot 16^5 + 1 \cdot 16^4 + 0 \cdot 16^3 + 12 \cdot 16^2 + 10 \cdot 16 + 3$$
$$= (10554531)_{10}$$

Some worked out exercises:

1. Convert $(79)_{10}$ from decimal to binary system

Solution:

$$79 = 2 \cdot 39 + 1$$
$$39 = 2 \cdot 19 + 1$$
$$19 = 2 \cdot 9 + 1$$
$$9 = 2 \cdot 4 + 1$$
$$4 = 2 \cdot 2 + 0$$
$$2 = 2 \cdot 1 + 0$$
$$1 = 2 \cdot 0 + 1$$

Hence $(79)_{10} = (1001111)_2$