Practical Number 4

Aim: To find all the primitive roots of the group G = <Zp*, *>

Theory: In the group G=<Z_n*, x>, when the order of an element is the same as Φ(n) i.e. the order of the group, that element is called the primitive root of the group.

The order of a group, |G| is the number of elements in the group.

The order of an element *a* in a group, ord(a), is the smallest integer n such that a^n = e. i.e. the order of an element is the order of the cyclic group it generates.

If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic group. The term power means repeatedly applying the group operation to the element. Thus, a^n a • a • . . . . • a (n times) where *a* is an element of the group and • is the operation defined for the group. The set made from this process, discarding the duplicate elements, is referred to as <a>. Also, a^0 = *e* where *e* is the identity element of the group.

Example: Consider the group **G = <Z_7*, x>**

The order of the group i.e. Φ (7) = 6. Z_7* = {1, 2, 3, 4, 5, 6} and the identity element *e* = 1

We now find the cyclic group generated by each of the element of this group

	i = 1	**i = 2**	**i = 3**	**i = 4**	**i = 5**	**i = 6**
a = 1	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
a = 2	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
a = 3	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
a = 4	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
a = 5	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
a = 6	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

Since ord(3) = ord(5) = 6 which is the order of the group, 3 and 6 are the primitive roots of the given group.

It has been proved that the group G=<Z_n*, x> has a primitive root only if n=2, 4, p^t, or $2p^t$, where p is an odd prime and *t* is an integer.

If the group has G=<Z_n*, x> has any primitive root, the number of primitive roots is Φ (Φ (n)).

The concept of primitive roots is used in many cryptographic algorithms including ElGamal cryptosystem and Diffie-Hellman key exchange algorithm.

Conclusion: The concepts of primitive roots have been understood and the algorithm to find primitive roots has been implemented.