**PRIMITIVE ROOT**

**Definition:**  is a primitive root modulo if and only if for any integer such that , there exists an integer such that:

**Definition**: Let and . The order of modulo is the smallest positive integer such that

**Theorem:** Primitive root modulo exists if and only if

**How to find the primitive root:**

If is primitive root modulo , then and is of order

Hence, to know if a number is a primitive root modulo , we must check that there is no such a that

Additionally, if this exists, it has to be a divisor of

Hence, we just have to check all the divisors of the form because other divisor d satisfy :

**DISCRETE ROOT**

Eq : , is prime

Corner case: if

Suppose we know , primitive root of , then by definition there exists a that :

Then :

We find by discreteLog and then the answer is