Scribe: Cryptography and Network Security (Class.10.4.A)

Ankit Saurabh

6-Nov-2020

1 Introduction

In earlier lecture, we learnt about about Chinese Remainder theorem and Solovay Strassen Algorithm for its primality test. Chinese remainder theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime.

2 Langrange's Theorem

Langrange Theorem says order of subgroup divides order of the group. This was shown using an example of cyclic group.

3 Solvay Strassen Algorithm continuation

The Solovay–Strassen algorithm is a probabilistic test to determine if a number is composite or probably prime.
In the algorithm, it is used that-
For any odd composite n, n is an Euler pseudo prime to the base a for at most half of the integers

$$a\epsilon\ Z_{n*}$$

.

3.1 Error Probability of this algorithm

Let G be a group such that,

$$G(n) = a, a\epsilon Z_{n*}, (\frac{a}{n}) \equiv a^(n - 1/2)(modn)$$

3.1.1 Proof of G(n) is subgroup of Zn*

By Langrange's algorithm if G(n) $\neq Z_{n*}, then |G(n)| \leq |Z(n)|/2 \leq (n-1)/2.$
$Suppose, a, bareelementofG,$
$(\frac{a}{n}) \equiv a^(n-1/2)(modn)$
$(\frac{b}{n}) \equiv b^(n-1/2)(modn)$

Since cardinality of G(n) divides Zn* wich is less than equal to (n-1/2).

$$(\frac{ab}{n}) \equiv a^(n-1/2)(modn) * b^(n-1/2)(modn)$$

So,

$$(\frac{ab}{n}) \equiv ab^(n-1/2)(modn)$$

Therefore ab is also an element of G(n). Since, G(n) is a subset of multiplicative finite group and also closed under multiplication, then it must be a subgroup. So, next we need to show there exit atleast one element in Zn* which does not belong to G(n).

3.1.2 show there exist at least one element in Zn* which does not belong to G(n)

(Lets take n =

$$p^k * q$$

, where p and q are odd and p is prime. k $\geq 2. Clearly, pandqarecoprime. Leta = 1 + p^(k-1) * q$
$Wehave(\frac{a}{n}) = (\frac{a}{p})^k * (\frac{a}{q}) = 1.$
$As(\frac{a}{n}) \equiv a^(n-1/2)(modn)$
$So, (\frac{a}{n}) \equiv a(modn)^(n-1/2)$
$Therefore, (\frac{a}{n}) = 1.)$

Using Binomial theorem,
$\equiv a^(n-1/2) = 1 + \frac{n-1}{2} p^(k-1) * q(modn).$
$(Asothertermsofbinomialexpansionwillhaveafactorofp^(k * q.$
$p^(k-1) * qraisedtoanypower \geq 2willcontainthatterm. So, theywillbe0)$

Therefore,

(a$\frac{}{n) \equiv a^(n-1/2)(modn) \equiv 0(modn) therefore n divides (\frac{a}{n}) i.e, p^(k*q | \frac{n-1}{2} p^(k-1)*qp | \frac{n-1}{2} n \equiv 1(modp) But, this contradicts n \equiv 0(modp). Ther}$

4 Discrete Logarithm

In a finite mathematical group (G, .), an element a

$$\epsilon G$$

let ¡a¿ = a raised to the power i : 0$\leq i \leq n-1$

Discrete Logarithm Problem is finding such unique integer i between 0 and n-1(both inclusive), such that:

$$\alpha^i = \beta(modp).$$

$$i = \log_\alpha \beta(mod(p-1)).$$

5 Conclusion

So, we have seen the proof of error probability of Solovay Strassay algorithm using Jacobian. This algorithm is essential in Chinese Algorithm.