MATH 314 Fall 2023 - Class Notes

11/7/2023

Scribe: Curtis Oliver

Factoring Trick:

If $a^2 \equiv b^2 (modn)$ but $a \neq b(modn)$ then n is compose and gcd(n,a-b) = d is a nontrivial factor of n

Factoring:

Brute Force

——Worse Case: $n = p * q$ and $p, q \approx \sqrt{n}$

——Try diving n by integers from 2 to $\sqrt{n}$ until we find a divisor: O($\sqrt{n}$)

————"Size" of n is the number of bits N= $\lceil \log_2(n) \rceil$ so O($2^{N/2}$)

So we want to use the factoring trick

——Naive Approach: Pick random values of a, $\sqrt{n}$ ¡ a ¡ n

————Compute: c=a^2 % n

————Check to see if b = $\sqrt{c}$ is an integer

————If it is we use the factoring trick

————$b^2 \equiv a^2$ (mod n) so gcd(n,a-b) is a factor

————How long do we expect this to take?

——————Each time we compute c we get a random number between 0 and n-1

——————n choices for c, $\sqrt{n}$ choices of them are perfect squares

——————Probability of success is $\sqrt{n}/n = 1/\sqrt{n}$

——————On average this takes $\sqrt{n}$ tries: O($\sqrt{n}$)

————Dixon's Factorization Algorithm

——————Pick a bound B, we only want to consider primes smaller than B

——————Pick random values of a, compute c = a^2 % n

——————If all prime factors of c are smaller than B we add it to our list (Divide c ———————— by all small primes up to B)

——————Keep a list of a's and corresponding c's

——————Need to get a list that has one more entry then there are primes up to B

——————Now we find a subset of c's that make a square

——————Let X be the product of all the a's we used while making the square and Y ———————— be the product of all the c's used to make the square and W^2 = Y

——————Now $W^2 \equiv X^2$ (mod n) so we can use the factoring trick to factor n