MATH 314 Spring 2018 - Class Notes

04/19/2018

Aabha Ghimire

Summary: In Today's Class we studied into further details about the Miller Rabin Primality Test, the Factoring Trick, Dixon's Factoring Algorithm, and the examples of how each of them are implemented.

Notes: What is the best way to factor a very large number n=pq?
The first attack with just pen and paper would be trail division. We have to divide n by numbers until we find a factor.
For example divide by 2,3,5,7,11,13 and might even have to go upto the square root. Which will take $O(\sqrt{n})$.

If n is an RSA modulus then,
$$n \approx 10^{240}$$
$$\sqrt{n} \approx 10^{120}$$

The second way is The Factoring Trick. If $x^2 \equiv y^2$ and $x \not\equiv \pm y$ then n is composite and $d = gcd(x-y, n)$always going to be a non-trivial factor of n.

First attempt at Factoring Trick:

- Pick a randomly with $\sqrt{n} < a < n$
- Lets Compare $c = a^2\%n$ (a^2)-is random
- If $C = x^2$ (already a square)for some integer x
- Then we have $a^2 \equiv x^2$
- We win!!!

Pick numbers/square/reducing mod n / end on a square//
How many steps do we expect this to take? a's are random so the $c = a^2\%n$ is essentially a residue mod n.
What is the probability that a random number less than n is a square?

numberofsquarelessthan(n)/n
$$= \sqrt{n}/n$$
This probability is $\sqrt{n}/n = 1/\sqrt{n}$

On average we have to do this $\sqrt{n}$ many times. So, this algorithm has running time $O(\sqrt{n})$

Dixon's Factoring Algorithm

Idea: Pick numbers a and computer $c = a^2\%n$, keep them if C does not have any big prime factors.

Fix a bound B, prime number are considered "big" if they are bigger than B.

We create a matrix F that has one column for every prime number, less than B.

- **Steps:**

1. Pick a random $a\sqrt{n} < a < n$
2. Compute $c = a^2\%n$
3. Trail division
4. If we have not completely factored C. We give up and go back to step 1.
5. If C is completely factored into primes up to B add a row to F where the entry in each column is the number of times that prime divides C.
6. Repeat steps 1-5 until F has more rows than columns.

Linear Algebra Fact: Any matrix that has more rows than columns has linear dependence.

We find a linear combination of rows that we can add together to get a row where all the entries are even. Suppose we add together the rows corresponding to a1,a2.. ak.

$$c1 = a1^2\%n, c2 = a2\%n$$

This means that the prime factors of y= c1c2...ck.(All the Cs multiplied together). All the prime numbers in Y appear to be an even power.

so, Y is a square 1. $Y = y^2$ $y = (a1^2)(a2^2)(ak^2)\%n$

Let $x = a1a2..ak$

Then $x^2 \equiv y^2 (modn)$