MATH 314 - Class Notes

5/2/2017

Scribe: Ma. Bettina Bienvenida

Summary: This class we discussed factoring large primes using the factoring theorem and Dixon's Factoring Algorithm

Notes:

Recall: Using trial division to factor a large prime $n \approx 10^{100}$ will take around $\sqrt{n} \approx 10^{50}$ steps. This is still way to many...

Theorem: (aka the 'factoring trick')

$$\text{If } x \not\equiv \pm y \text{ (mod n) and } x^2 \equiv y^2$$
$$\text{then n is composite and } d = gcd(x-y, n),\ d \neq 1, n, \text{ is a non trivial factor of n.}$$

Naive way of using our factoring trick:

- pick x (mod n) randomly
- square it x^2 and reduce mod n
- if this is already a square, we win!

What is the probability of this happening? In other words, what is the probability that x^2 (mod n) is a square?

- about $\sqrt{n}$ numbers are square...
- therefore the probability is $\frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}}$

On average, we would have to try $\sqrt{n}$ times before we find one (this is not any faster than trial division...)

Example: Factor n = 77

- $9^2 \equiv 81 \equiv 4$ (mod 77)
- $9^2 \equiv 2^2$ (mod 77)
- Then d = gcd(9 - 2, 77) = 7
- 7 is a factor of 7.

Dixon's Factoring Algorithm

General idea:

- pick x randomly
- compute x^2 (mod n)
- try and factor x^2 (mod n) into small prime factors (2, 3, 5, ...)
- only keep x^2 (mod n) if all prime factors are small (less than $B \approx e^{\sqrt{hn}}$)
- repeat this several times until we have lots of x_i^2 all have small prime factors
- piece them together to make a square.

Steps to factor(n):

1. pick $x_i \in (\sqrt{n}, n-1)$ randomly
2. compute $y_i = x_i^2$ % n
3. use *trial division* to factor y_i into primes of size at most B.
4. If it only has factors at most B, write down the powers of the primes dividing y_i, into a table (matrix) where each column n corresponds to a prime less than B.
    - put the number of times p divides into y_i into the entry in column p.
5. Repeat this until the matrix has more rows than columns.
6. By *linear algebra*, there is some combination of rows that we can add together so that the sum has all even entries
    - Lets suppose these rows correspond to $y_{i_1}, y_{i_2}, y_{i_3} ... y_{i_k}$ then $y_{i_1} \times y_{i_2} \times y_{i_3} \times ... \times y_{i_k}$ is only divisible by primes to an even power.
    - So $y_{i_1} \times y_{i_2} \times y_{i_3} \times ... \times y_{i_k} = s^2$
    - but $y_{i_1} \neq x_{i_1}$ and $y_{i_2}^2 \equiv x_{i_2}^2$

Example: Factor n = 629, B = 12 (bound)

- Pick x_i put $y_i = x_i^2$ % n in table
- x = changes, y = x_i^2 % 629
- factor(y)

x_i	2	3	5	7	11
59	4	1	0	1	0
73	0	3	0	0	5
80	1	0	1	0	1
87	0	1	0	1	0
94	1	1	1	0	0
113	1	0	1	0	1

- We want an even number summations each column

x	2	3	5	7	11
73, 80, 94	2	4	2	0	2

- $73^2 \equiv 3^3 \times 11 \pmod{n}$
- $80^2 \equiv 2 \times 5 \times 11 \pmod{n}$
- $94^2 \equiv 2 \times 3 \times 5 \pmod{n}$
- $(70 \times 80 \times 94)^2 = 2^2 \times 3^4 \times 5^2 \times 11^2 = (2 \times 3^2 \times 5 \times 11)^2 \pmod{n}$

Check using sage:

- $x = 70 \times 80 \times 94$ and $y = 2 \times 3^2 \times 5 \times 11$
- $x \pmod{629} = 472$ and $y \pmod{629} = 361$
- $x^2 \pmod{629} = 118$ and $y^2 \pmod{629} = 118$ (yay!!!)
- $\gcd(x - y, 629) = 37$
- $629/37 = 17$ and $37 \times 17 = 629$
- we successfully factored 629!!