MATH 314 Spring 2018 - Class Notes

4/18/2018

Scribe: Alex Jackson

Summary: This day we talked about different methods to find the factors of a number

- Factoring Trick
- Dixon's Factoring Algorithm

Notes: How can we factor large numbers?

1. First method is trail division try division by 2,3,5,7,..., $\sqrt(n)$ has time of $O(\sqrt(n))$
2. The Second is `Factoring Trick`

Theorem: If $x^2 \equiv y^2 \pmod(n)$ and $x \equiv \pm y \pmod n$

- then "n" is a *composite number* and the of $gdc(n, x-y) = d$, the "d" is *non-trivial* factor of "n"
- non-trivial means it is not 1 or itself

First attempt to use Factoring Trick

1. Pick random values of "a" and compute $a^2 \pmod(n)$
2. If $a^2\%n = y^2$ for some "y" then we factor "n"

- This takes between 1 to n tries before getting the right "y"
- The probability of "a" is a square factor is

$$\frac{1}{\sqrt(n)}$$

- Has a time of $O(\sqrt(n))$

Def: Dixon's Factoring Algorithm

- The idea is to factor some "n"
- The Goal is to find number "a" where $a^2\%(n)$ doesn't have any Prime factors
- With a fixed bound "B" that is the limit of how Big the Prime factor we'll consider for our $a^2\%n$

- With those "a" create a Matrix F
- Having a column for every prime numbers less than "B"

<u>Steps to Dixon's Factoring Algorithm</u>

1. Pick "a" randomly where $\sqrt(n) < a < n-1$
2. Compute $C = a^2\%n$ Do trail division on "C" with Prime numbers up to "B"
3. If we haven't completely factored "C", go back to step 1
4. If "C" is fully factored into primes less than "B"
   - Add "a" row to Matrix F
   - Where the entries in each column are the number of times that each primes divided "C"
5. Repeat Steps 1-4 until F has more rows than columns

   <u>Recall:</u> Any Matrix with more rows than columns has "linear dependence" among the rows linear dependence- has some way to add/subtract Rows to get a all 0 matrix

   <u>Note:</u> We find "linear dependence" among Rows of $F \mod (2)$ (working with $\mathbb{F}_2$)
6. Suppose that the Rows corresponding to $a_1, a_2, \ldots, a_k$ are involved in this linear dependence $a_1^2\%n = C_1, a_2^2\%n = C_2, a_3^2\%n = C_3$
7. Now multiplying $C_1, C_2, \ldots, C_k = Y$ gives a number where all prime factors appear to an even power, so $Y = y^2 (Y = \sqrt(y))$
8. let $x = a_1, a_2, \ldots, a_k$
9. Find out if $x^2 \equiv (y^2 \mod (n))$ but $x \not\equiv y \pmod n$ if it does then
10. now you can find the factors by getting the gcd of $(X - Y, N)$

<u>EX:</u> use Dixon's to factor n=629 with a bound of 12, try different a's then factor them

$$
\begin{array}{r}
\\ a = 73 \\ a = 59 \\ a = 62 \\ a = 80 \\ a = 87 \\ a = 94
\end{array}
\begin{array}{c}
\begin{array}{ccccc} 2 & 3 & 5 & 7 & 11 \end{array} \\
\begin{pmatrix}
0 & 3 & 0 & 0 & 1 \\
4 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0
\end{pmatrix}
\end{array}
$$

- So in order to find the square we need to add rows together to get a square

- If you add rows $73, 80, 94$ you get $\begin{array}{lc} & \begin{array}{ccccc} 2 & 3 & 5 & 7 & 11 \end{array} \\ \begin{array}{l} a = 73 \\ a = 80 \\ a = 94 \\ AddingRows \end{array} & \begin{pmatrix} 0 & 3 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 2 & 4 & 2 & 0 & 2 \end{pmatrix} \end{array}$
- With this you can get the factors of 629 by find y,Y,x,X
- $Y = 73^2\%629 * 80^2\%629 * 94^2\%629 = 118 \pmod{629}$
- $y = \sqrt{Y} = \lceil y \rceil = 11$
- $x = (73 * 80 * 94)\%(629) = 472$
- $X = x^2 \equiv 118 \pmod{629}$
- as you can see $x \neq y$ but $X \equiv Y \pmod{629}$ so we can get one of the factors of 629 by the $gcd(x - y, n) = gcd(472 - 11, 629) = 1$