MATH 314 Fall 2019 - Class Notes

9/18/2019

Scribe: Robert Connors

Summary: Class 9/18/19 consisted of using Euclid's algorithm to find GCD and working backwards to find the triple (GCD,x,y) as well as Repeated Squaring.

Notes:

- `Finding X,Y in 100x+83y=1`

1. `100 = 1(83) + 17`
2. `83 = 4(17)+15`
3. `17=1(15)+2`
4. `15=7(2)+1`

- `Now we work from the bottom up substituting as we can. The goal is to get the final equation in terms of 83 * some number pluse 17 * some number.`

1. `1 = 1(15) - 7(2)`
   `We can substitute in for 2 from our equations above:`
2. `1= 1(15) - 7(17-1(15))`

   `Now we simplify: Distributing the 7 gives us -(17) and 7(15). We already gave 1(15) so we combine to get 8(15).`
3. `1= -7(17)+8(15)`
4. `1 = (-7(17) + 8 (83-4(17))`
5. `1 = 8(83) - 39(17)`
6. `1 = 8(83) -39(100-(1(83))`
7. `1 = 47(83) - 39(100)`
   `Therefore x = -39, y = 47`

- `Steps to find` a^{-1} `(mod n)`

1. `Compute gcd(u,n) using Euclid's Algorithm. Note: if GCD != 1 then the inverse does not exist.`

2. Find x,y so that Ux+Ny = 1
3. reduce (mod n)
4. a^{-1} = x(mod n)

As an example take -39(100)+ 47(83) = 1 from the previous problem.
If you wanted to find 83^{-1} (mod 100), then -39(100) reduced (mod 100) would equal 0 leaving only 47(83) = 1. now solving the leftover equation you would get 83^{-1} = 47 (mod 100).

- **Repeated Squaring**

Solve for 5^{103} (mod 7): $(5^{64})(5^{32})(5^{4})(5^{2})(5^{1})$
5^{-1}= 5 (mod 7)
5^{2}= 25 = 4(mod 7)
$5^{2})^{2}$= $4^2 = 16 = 2(mod 7)$
5^{8} = $(5^{4})^{2} = 2^{2} = 4(mod 7)$
5^{16} = $(5^{8})^{2} = 2(mod 7)$
Notice that there is a pattern that will continue.
Following the pattern you get (2) (4) (2) (4) (5) for the corresponding powers which equals 5. So 5^{103} = 5 (mod 7).