MATH 314 - Class Notes

09/14/2017

Scribe: Simranjeet Dulkoo

Summary: Insert a short summary of what today's class covered.

Notes:
Number Theory
How do we compute gcds?
Example

- Compute GCD(12,21) = 3
- Factor both of the numbers and take the factor they have in common

Euclids Algorithm
Think about the division with a remainder
Any number diving both a and b also divides r.
Euclids Observation:
gcd(a,b) = gcd(b,r), where r is the remainder when dividing a by b
Repeat this!
Eventually we won't have a remainder
Example
Compute GCD(12,21)

$$21 = 1 * 12 + 9$$
$$\text{gcd}(21,12) \rightarrow \text{gcd}(12,9)$$
$$12 = 1 * 9 + 3$$
$$\text{gcd}(12,9) \rightarrow \text{gcd}(9,3)$$
$$9 = 3 * 3 + 0$$

gcd(21,12)= 3

- Euclids Algorthims is super fast for huge numbers
- Factoring is "slow"

Theorem:

- If gcd(a,b) = d then there exists integer x,y such that
- ax + by = d
- Working backwards through Euclids Algorithm allows us to find x,y

Compute

$$\text{gcd}(21,12) \rightarrow 21{=}1{*}12{+}9$$
$$\text{gcd}\ (12,9) \rightarrow 12{=}1{*}9{+}3$$

Plug it in:
9 = 21 - (-12)
3 = 12 - 1(9)
3 = 12 -1(21 - 1(-12))
3 = -1(21) + 2(21)
3 = 2(21) - 1(12)

Example

Find the gcd(79,19) = d also find x, y

$$\underline{x}79 + \underline{y}19 = d$$

Step 1: Euclids algorithm Forward

gcd(79,19) $\rightarrow$ 79 = 4 * 19 +3
gcd(19, 3) $\rightarrow$ 19 = 6 * 3 + 1
gcd(3,1) $\rightarrow$ 3 = 3(1) + 0
gcd(79,19) = 1

Step 2: Work backwards

79 = 4 * 19 + 3 $\rightarrow$ 3 = 79 - 4(19)
19 = 6 * 3 + 1 $\rightarrow$ 1= 19 - 6(3)

Expand

1 = 19 - 6(3)
1 = 19 - 6(79 - 4 (19))
1 = -6 (79) + 25(19)
1 = 25(19) - 6(79) (mod 79)
gcd(79,19) x = -6 , y = 25 , d = 1

- If we want to find the inverse of a mod b we use Euclids Algorithm to find x, y such that ax+ by = d
- Then the inverse of a is x
- we can now do Arithmetic for any modulus m possible values are (0,1,..., m-1) call these numbers residue (mod m) do arthmetic on these residues
- We can add, subtract and multiply (usual rules of arthmetics apply) is called a <u>ring</u>