MATH 314 Spring 2020 - Class Notes

2/12/2020

Scribe: Shania Foster

Summary: Today in class we covered Euclid's Algorithm, Modular Exponentiation, and Fermat's Theorem.l

Notes:

Theorem: If gcd(a,b) = d , then by using Euclids Algorithm backward, we can find two integers m and n so that am + bn = d

(a and b are a linear combination which gives us d)

This is called the extended euclidean algorithm

Example:
Take a=72, and b=26
find gcd(72,26) = d
then find m72 + n26 = d

Forward
gcd (72,26)
72 = 2(26) + 20
gcd (26,20) = 2
26 = 1(20) + 6
gcd (20,6) = 2
20 = 3(6) + 2
6 = 3(2) + 0

Work Backward
Solve each equation for the remainder
2 = 20 - 3(6)
6 = 26 - 1(20)
20 = 72 - 2(26)
2 = 20 - 3 (26-1(20))

- = 20 - 3(26) + 3(20)

  2 = 4(20) - 3(26)

- 20 = 72 - 2(26)

2 = 4(72 -2(26)) - 3(26)
2 = 4(72) - 11(26)

m = 4, amd n =-11

<u>Use this to find modular inverses</u>
If gcd(a,b) = 1
Find m and n
am + bn = 1 reduce $\pmod{b}$
    am + bn $\equiv$ 1 $\pmod{b}$
bn gets replaced by 0
am $\equiv$ 1 $\pmod{b}$

So m $\equiv a^{-1} \pmod{b}$

Use this to solve equations in $\pmod{n}$

Example:
Solve 27x + 3 $\equiv$ 10 $\pmod{50}$
Find$27^{-1} \pmod{50}$

Use Euclid's Algorithm

27x $\equiv$ 7 $\pmod{50}$
Multiple both sides by 13
13(27)x $\equiv$ 13(7) $\pmod{50}$
x $\equiv$ 91 $\equiv$ 41 $\pmod{50}$
x = 41

Example:
gcd(50,27)
50 = 1(27)+23
27 = 1(23)+4
23 = 5(4)+3
4 = 1(3)+1
3 = 1(3)+0

Work Backward
1 = 4-1(3)
3 = 23-5(4)
4 = 27-1(23)
23 = 50-1(27)

Fill in the numbers

1 = 4-1(23-5(4))
= -1(23)+6(4)
(the 4 was moved over making 6)
1 = -1(23)+6(27-1(23))
= 6(27)-7(23)
1 = 6(27)-7(50-1(27))
1 = -7(50)+13(27)
13 =$27^{-1} \pmod{50}$

Modular Exponentiation

Compute $a^m \pmod{n}$
a,m,n all big

Ex. Compute $3^{34} \pmod{11}$

(Trick: repeated squaring
Write the exponent in binary (sum of powers of 2))

34 base 10 = 10010 base 2
34 = 32 + 2

Repeated Squaring

$3^1 \equiv 3 \pmod{11}$
$3^2 \equiv 9 \pmod{11}$
$(3^2)^2 \equiv 3^4 \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$
$3^8 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$
$3^{16} \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$
$3^{32} \equiv 3^2 \equiv 9 \pmod{11}$
$3^{34} \equiv 3^{32+2}$
$\equiv (3^{32})(3^2) \pmod{11}$
$\equiv (9)(9) \pmod{11}$
$\equiv 4 \pmod{11}$

What are the last two digits of 11^{70}?

What is the $11^{70} \pmod{100}$
70 = 64 + 4 + 2

$= 2^6 + 2^2 + 2^1$
1000110 (Binary)

<u>Repeated Squaring</u>

$11^1 \equiv 11 \pmod{100}$
$11^2 \equiv 121 \equiv 21 \pmod{100}$
$11^4 \equiv 21^2 \equiv 41 \pmod{100}$
$11^8 \equiv 41^2 \equiv 81 \pmod{100}$
$11^{16} \equiv 81^2 \equiv (-19)^2 \pmod{100}$ (*Because 81 is 19 less than 100*)
$11^{32} \equiv 61^2 \equiv 21 \pmod{100}$
$11^{64} \equiv 21^2 \equiv 41 \pmod{100}$
$11^{70} \equiv 11^{64+4+2} \equiv (11^{64})(11^4)(11^{21})$
$\equiv (41)(41)(21)$
$\equiv (81)(21)$
$\equiv 01 \pmod{100}$

Even faster way if modulus is prime

<u>Fermat's Little Theorem</u>
If p is a prime number and p does not divide a then $a^{p-1} \equiv \pmod{p}$

Example: p=5
a = 1
$1^{5-1} \equiv 1^4 \equiv 1 \pmod{5}$
a = 2
$2^4 \equiv 16 \equiv 1 \pmod{5}$
a = 3
$3^4 \equiv 81 \equiv 1 \pmod{5}$
a = 4
$4^4 \equiv 256 \equiv 1 \pmod{5}$

Example: p=13
a = 2
$2^{13-1} \equiv 2^{12} \equiv 4096 \equiv 1 \pmod{13}$
Proof: Let p = (p-1)!
=(p-1)(p-2)....(2)(1)
a has an inverse $\pmod{p}$
gcd(a,p)=1
For each i , 1≤i≤(p-1)

If we compute (a)(i) $\pmod{p}$
We get another number between 1 and (p-1)
If we take all of the numbers between 1 and (p-1), multiply them all by the number a, we get all of the numbers between 1 and (p-1) one time.

So (1a)(2a)(3a)...((p-1)a) $\pmod{p}$
= (1)(2)....(p-1) $\pmod{p}$

p $\equiv$ 1(2)..(p-1)
$\equiv (a1)(a2)$..(a(p-1))
$\equiv (a^{p-1})$(1)(2)....(p-1)
$\equiv (a^{p-1})(p) \pmod{p}$
p $\equiv (a^{p-1})(p)^{p-1} \pmod{p}$ *You would then cancel on both sides with the inverse of* p^{-1}
$1 \equiv (a^{p-1}) \pmod{p}$