MATH 314 - Class Notes

9/19/2017

Scribe: Christian Fortuna

Summary: Today's class covered the Chinese Remainder Theorem, Modular Exponentiation, and Fermat's little theorem.

Notes: Chinese Remainder Theorem
If m, n are two moduli and gcd(m,n) = 1
Then, for any a(mod m) and b(mod n)
There is exactly one residue c(mod mn) such that c $\equiv$ a (mod m) and c $\equiv$ b (mod n)
Example: m = 2 n = 13
a $\equiv$ 0 (mod 2) b $\equiv$ 5 (mod 13)
The unique solution to these equations modulo 26 is c $\equiv$ 18 (mod 26)
Example: Find x such that x $\equiv$ 3 (mod 7) and x $\equiv$ 11 (mod 13)
We need to find x (mod 91)
since x $\equiv$ 3 mod 7 x = 3+7k for some k
Plug this into the equation (mod 13)
3+7k $\equiv$ 11 (mod 13) 7k $\equiv$ 8 (mod 13) $7^{-1} \equiv$ 2 (mod 13) 2(7k) = 2(8) (mod 13) k $\equiv$ 3 (mod 13)
so, x = 3 + 7(3) = 24 (mod 91)
finding the 7^{-1} (mod 13) using Euclid's algo.
gcd(13,7) = 1
while x != 1 n = n+1 x = (7*n)
the inverse would be what n is equal to once x = 1

Modular Exponentiation

Compute 3^{521} (mod 19)
Write 521 in binary
512 = 1; 256 = 0; 128 = 0; 64 = 0; 32 = 0; 16 = 0; 8 = 1; 4 = 0; 2 = 0; 1 = 1;
1000001001
512 + 8 + 1 = 521
trick: repeated squaring
basically, 3^{521} can be rewritten as: $3^2 = 9 = (3^2)^2 = 81 = (3^4)^2 = 6561$ and so on... until you get to 512.
remember the binaries. 512 + 8 + 1 = 521 so, $3^{512} + 3^8 + 3^1 = what 3^{521}$ is going to be.

Fermat's little theorem

if p is a prime number and a is not a divisible by p then $a^{p-1} \equiv 1$ (mod p)

Example: P = 5 a = 2 check $2^{5-1} \equiv 16 \equiv 1$ (mod 5) check $3^{5-1} \equiv 81 \equiv 1$ (mod 5) check $2^{7-1} \equiv 64 \equiv 1$ (mod 7)

When computing exponents modulo a prime number p we can reduce the exponent (mod p-1)