MATH 314 Spring 2018 - Class Notes

9/19/2018

Scribe: Kyle Clabough

Summary: Today we learned about Fermat's Little Theorem, and start on the first modern cipher: 3-Pass Protocol

Notes:

Fermat's Little Theorem:

- Suppose p is a prime number
- and a is not divisible by p
- then: $a^{p-1} = 1 \mod p$

Try this:

Ex1:

$$p = 3 \quad \text{and} \quad a = 4$$
$$4^{3-1} \equiv 16 \equiv 1 \mod 3$$

Ex2:

$$p = 5 \quad \text{and} \quad a = 2$$
$$2^{5-1} \equiv 16 \equiv 1 \mod 5$$

Ex3:

$$p = 5 \quad \text{and} \quad a = 3$$
$$3^{5-1} \equiv 3^4 \equiv 81 \equiv 1 \mod 5$$

NOTE: if m is not prime, this does not work

Try:

$$m = 6 \quad \textit{and} \quad a = 2$$

$$2^{6-1} \equiv 2^5 \equiv 32 \equiv 2 \quad \textit{not} \quad \equiv 1 \mod 6$$

Last class, we determined:

$$5^{273} \mod 11 = 5^{270} * 5^3 \mod 11$$
$$= (5^{10})^{27} * 5^3 \mod 11$$

using the FLT:

$$(5^{10}) \equiv 1 \mod 11$$

so

$$(5^{10})^{27} * 5^3 \mod 11 \equiv 1^{27} * 5^3 \mod 11$$
$$\equiv 5^3 \mod 11$$
$$\equiv 125 \mod 11$$
$$\equiv 4 \mod 11$$

General Principle of Exponents Modulo a Prime Number:

When computing $a^b \mod p$, we can first reduce $b \mod p-1$
When working $\mod p$ you work $\mod p-1$ in the exponent.

First Modern Cipher: 3-Pass Protocol:

Real World Example:

Alice wants to send Bob an object securely in a box. She wants to put a lock on the box to keep it secure, but she and Bob do not have any of the same keys.

1. Alice puts a lock on the box using her key, and mails the box to Bob.
2. Bob locks the box again with his key.
3. Bob sends the box, with both locks, back to Alice
4. Alice unlocks her lock
5. Alice sends the box back to Bob
6. Bob unlocks his lock and opens the box

Math version of 3-Pass Protocol:
Alice picks a big prime number p (p is about 100 digits long)
Alice's key is a secret number a where $1 < a < (p-1)$ and $gcd(a, p-1) = 1$

Encryption Function:

$$E(x) \equiv x^a \mod p$$

NOTE: x must be smaller than p

What is the Decryption Function?

We need to get a 1 in the exponent.
It is okay (because of Fermat's Little Theorem) if the exponent is congruent to 1 $\mod p-1$
Alice computes the inverse of $a \mod p-1$

$$a^{-1} \equiv a^{-1} \mod p-1$$

So Alice's Decryption Function is:

$$D(y) \equiv y^{a^{-1}} \mod p$$

Suppose $y = E_a(x) = x^a \mod p$
Alice decrypts:

$$D(y) = y^{a^{-1}} \mod p = (x^a)^{a^{-1}} \mod p$$
$$D(y) = x^{a*a^{-1}} \mod p \equiv x^1 \mod p$$

Bob also picks a number b where $1 < b < p-1$ and $gcd(b, p-1) = 1$

$$E_b(x) \equiv x^b \mod p$$

He finds $b^{-1} \equiv b^{-1} \mod p-1$ His decryption function is:

$$D_b(y) \equiv y^{b^{-1}} \mod p$$

Alice picks her secret a wants to send the number m to Bob.
Alice computes $C_1 = E_a(m)$ which she sends to Bob.
Bob computes $C_2 = E_b(C_1)$. He sends this back to Alice.
Alice computes $C_3 = D_a(C_2)$ and sends this back to Bob.
Finally, Bob computes $D_b(C_3) = C_3^{b^{-1}} \mod p$

$$D_b(C_3) = ((C_2)^{a^{-1}})^{b^{-1}} \mod p$$
$$D_b(C_3) = (((C_1)^b)^{a^{-1}})^{b^{-1}} \mod p$$
$$D_b(C_3) = ((((m)^a)^b)^{a^{-1}})^{b^{-1}} \mod p$$
$$D_b(C_3) = m^{aba^{-1}b^{-1}} \mod p$$
$$D_b(C_3) = m^{1 \mod p-1} \mod p$$
$$D_b(C_3) = m \mod p$$