MATH 314 Fall 2019 - Class Notes

9/23/2019

Scribe: Katya Doersam

Summary: Today's class covered the basic principle, 3 pass protocol, the Euler ϕ function and Euler's theorem.

Notes:

The Basic Principle: for exponents $\pmod p$

When working $\mod p$, the exponents can be resolved $\pmod{p-1}$

Solve $x^3 \equiv 7 \pmod{11}$:

- $x^3 - 7 \pmod{11}$ should be equivalent to $0 \pmod{11}$
- Need to find a number cube that gives you $x^3 \equiv 7 \pmod{11}$

What exponent could we raise both sides to to get $1 \pmod{p-1}$ as the exponent on x?

$(x^3)^a \equiv 7^a \pmod{11}$

Find a so that $3a \equiv 1 \pmod{10}$:

Compute $3^{-1} \pmod{10}$:

$\gcd 10, 3$

$$10 = 3(3) + 1$$
$$3 = 3(1) + 0$$

$\gcd 10, 3$ must be 1 in order for there to be an inverse for $3 \pmod{10}$

$$1 \equiv 10 - 3(3) \pmod{10}$$
$$1 \equiv (-3)(3) \pmod{10}$$
$$1 \equiv (7)(3) \pmod{10}$$

$3^{-1} \equiv 7 \pmod{10}$

$\gcd 10, 3$ must be 1 in order for there to be an inverse for 3.

Now find x:

$$3^{-1} \equiv 7 \pmod{10}$$
$$(x^3)^a \equiv 7^a \pmod{11}$$
$$(x^3)^7 \equiv 7^7 \pmod{11}$$
$$x^{21} \equiv 7^7 \pmod{11}$$
$$(x^{10})^2(x^1) \equiv 7^7 \pmod{11}$$
$$x \equiv 7^7 \pmod{11}$$

$(x^{10})^2 \equiv 1 \pmod{11}$ according to Fermat's Little Theorem.

Use Modular Exponentiation to Find x:
$7^7 = 7^4 * 7^2 * 7^1$
$7^2 \equiv 49 \pmod{11} \equiv 5 \pmod{11}$
$(7^2)^2 \equiv 25 \pmod{11} \equiv 3 \pmod{11}$

$7^7 = 7^4 * 7^2 * 7^1 \equiv (3)(5)(7) \equiv 6 \pmod{11}$

$x \equiv 7^7 \pmod{11}$
$x \equiv 6 \pmod{11}$

3 Pass Protocol:

Physical version:

Alice takes a box and locks it using her padlock. Bob takes the box he receives from Alice with his lock. He sends the box back to Alice. Alice takes off her lock and sends the box back to Bob. Bob takes off his lock and reads the message inside the box.

Math Version:

Protocol set up:

1. Alice picks a big prime p (200 digits or more typically)
2. She picks a secret exponent, a, $\gcd a, p-1 = 1$
3. She keeps a secret but can tell anyone p.
4. Bob also picks a secret exponent b, where $\gcd b, p-1 = 1$
5. Both Alice and Bob compute their decryption exponents using Euclid's algorithm

Alice Decryption: $a^{-1} \pmod{p-1}$

Bob Decryption: $b^{-1} \pmod{p-1}$

Sending the message:

1. Alice wants to send Bob a message. She encodes her message as a number m, $0 \leq m < p$
2. Alice computes $c_1 \equiv m^a \pmod{p}$, where m is the plaintext written as a number.
3. Alice sends c_1 to Bob.
4. Bob computes $c_2 \equiv c_1^b \pmod{p}$ and sends it back to Alice
5. Alice computes $c_3 \equiv c_2^{-a} \pmod{p}$ and sends it back to Bob
6. Bob computes $c_4 \equiv c_3^{-b} \pmod{p} \equiv m \pmod{p}$
7. $c_4 \equiv (((m^a)^b)^{-a})^{-b} \equiv m^1 \pmod{p}$

There is not a good way to attack this system. Brute force is most likely the only way to attack the system.

Big Drawback of 3 Pass Protocol:

- Messages have to be sent 3 times. Vulnerable to man-in-the-middle attacks.
- Example of man in the middle: UPS takes a package from Alice and encrypts it with the USPS encryption key. Alice unlocks the package with her key, then sends it back to UPS. UPS can now unlock the box using its own decryption key.

Euler ϕ function

$\phi(n)$: how many numbers in (1, n-1) have a $\gcd a, n = 1$
$\phi(12) = 4$
$\phi(26) = 12$
$\phi(11) = 10$

Euler's ϕ Function:
This function is used when the modulus is not prime. Fermat's is used for prime modulo.

1. In general, for any prime p, $\phi(p) = p - 1$
2. $\phi(p^k) = p^{k-1}(p-1), p^k$ does not have to be prime.
3. If $\gcd a, b = 1$, then $\phi(a * b) = \phi(a) * \phi(b)$

Examples:

1. $\phi(27) = \phi(3^3) = 3^2(3-1) = 9(2) = 18$. *Note that 3 is a prime, p*
2. $\phi(75) = \phi(5^2 * 3) = \phi(5^2) * \phi(3) = (5^1 * 4) * 2 = 20 * 2 = 40$ *Note: $\gcd 5^2, 3 = 1$
3. $\phi(900) = \phi(3^2 * 10^2) = \phi(3^2 * 5^2 * 2^2) = \phi(3^2) * \phi(5^2) * \phi(2^2) = (3^1 * 2) * (5^1 * 4) * (2^1 * 1) = 240$ *Note: need to reduce 10 further because 10 is not a prime.

Euler's Theorem:

If $\gcd a, n = 1$ then $a^{\phi(n)} = 1 \pmod{n}$
If n is prime, then $\phi(n) = n - 1$, then Euler's Theorem becomes Fermat's Little Theorem

New General Principle: when working $\pmod{n}$ we work $\pmod{\phi(n)}$ in the exponent