Math 314 - Spring 2020
Class Notes - 2/17/2020
Scribe: Cody Price

General Principle of Modular Exponents Mod a Prime Number

General Principle: Anytime we are working with exponents (mod P), we can reduce the exponent (mod P-1).

Example: Find a value of x so that $(a^3)^x \equiv a \pmod{11}$:
In calculus we'd do $(a^3)^x \quad x = 1/3 \quad \sqrt[3]{a^3} = a$ but, (mod 11) forces x to be an integer.
Since 11 is prime, we instead use the General Principle to reduce the exponent to (mod 10).
In the exponent, we want $3x \equiv 1 \pmod{10}$, so we need to find $3^{-1} \pmod{10}$.
To do this, we use Euclid's algorithm $10 = (3)(3) + 1 \quad 1 = 1(10) - 3(3) \quad 3^{-1} \equiv 7 \pmod{10}$.
Therefore $(a^3)^7 \equiv a \pmod{11}$.

---

3 Pass Protocol

This protocol creates a secure message that is sent without the sender and recipient first agreeing on a key.
To better understand the concept, this will be explain in both physical and mathematical terms.

Physical Terms: Imagine Alice has a safe that she locked with her padlock, and she wants to mail it to Bob.
The problem is, Bob doesn't have Alice's padlock key and the key may be stolen if mailed.
To solve this, first Alice mails the safe to Bob with her padlock on it.
Second, Bob puts his own padlock on the safe (double locked), and mails it back to Alice.
Third, Alice unlocks her padlock (leaving only Bob's), and mails it back to Bob again.
Finally, Bob unlocks his padlock, and now he can open the safe.

Mathematical Terms:
1) Alice picks a very big prime number (to be secure, $P > 10^{120}$)
2) Alice tells everyone what P is (does not need to be a secret).
3) Alice picks a secret number a $(2 < a < P - 1)$ where a = Alice's key.
4) Bob picks a secret number b $(2 < b < P - 1)$ where b = Bob's key.
5) Both Alice and Bob use Euclid's algorithm to compute their decryption keys.
$A = a^{-1}$ (mod P-1) and $B = b^{-1}$ (mod P-1)
6) Alice encrypts using $C1 = E(m) \equiv m^a$ (mod P) and sends C1 to Bob.
7) Bob encrypts using $C2 = E(C1) \equiv C1^b$ (mod P) and sends C2 back to Alice.
8) Alice decrypts using $C3 = D(C2) \equiv C2^A$ (mod P) and sends C3 back to Bob.
Since $(m^{a*b})^A \equiv m^b$ (mod P) only Bob's encryption remains.
8) Bob decrypts using $C4 = D(C3) \equiv C3^B$ (mod P).
Since $(m^b)^B \equiv m$ (mod P) now Bob has the message.

Example: Message = 'BE' $\rightarrow$ 1,4 $\rightarrow$ 14 $\quad P = 103 \quad a = 95 \quad b = 23$

Forwards: $gcd(102, 95) \quad 102 = 1(95) + 7 \quad gcd(95, 7) \quad 95 = 13(7) + 4 \quad gcd(7, 4)$
$7 = 1(4) + 3 \quad gcd(4, 3) \quad 4 = 1(3) + 1 \quad gcd(3, 1) \quad 3 = 3(1) + 0$

Backwards: $1 = 4 - 1(3), \quad 3 = 7 - 1(4), \quad 4 = 95 - 13(7), \quad 7 = 102 - 1(95)$
$1 = 4 - 1(7 - 1(4)) \quad = -1(7) + 2(4) \quad = -1(7) + 2(95 - 13(7)) \quad = 2(95) - 27(7)$
$= 2(95) - 27(102 - 1(95)) \quad = -27(102) + 29(95) \qquad \underline{A \equiv 29 \pmod{102}}$

Forwards: $gcd(102, 23) \quad 102 = 4(23) + 10 \quad gcd(23, 10) \quad 23 = 2(10) + 3$
$gcd(10, 3) \quad 10 = 3(3) + 1 \quad gcd(3, 1) \quad 3 = 3(1) + 0$

Backwards: $1 = 10 - 3(3), \quad 3 = 23 - 2(10), \quad 10 = 102 - 4(23),$
$1 = 10 - 3(23 - 2(10)) \quad = -3(23) + 7(10) \quad = -3(23) + 7(102 - 4(23))$
$= 7(102) - 31(23) \qquad \underline{B \equiv -31 \pmod{102} \equiv 71 \pmod{102}}$

Alice encrypts: $14^{95} \equiv 13 \pmod{103}$
Bob encrypts: $13^{23} \equiv 23 \pmod{103}$
Alice decrypts: $23^{29} \equiv 30 \pmod{103}$
Bob decrypts: $30^{71} \equiv 14 \pmod{103} \rightarrow$ 'BE' = the original message.

Chinese Remainder Theorem (CRT)

If $gcd(a,b) = 1$, $x \equiv m \pmod{a}$, and $x \equiv n \pmod{b}$ then there exists a unique $y \pmod{a * b}$ such that $y \equiv x \equiv m \pmod{a}$ and $y \equiv x \equiv n \pmod{b}$.

Example: $a = 2, b = 13, m = 1, n = 4$ Find $x \equiv 1 \pmod{2}$ and $x \equiv 4 \pmod{13}$.

Forwards: $gcd(13, 2)$ $13 = 6(2) + 1$ $gcd(2, 1)$ $2 = 2(1) + 0$
Backwards: $1 = 1(13) - 6(2)$
CRT: $y = n * 1(13) - m * 6(2)$ $= 1 * 1(13) - 4 * 6(2)$ $= -35 \equiv 17 \pmod{2 * 13}$
Test: $17 \equiv 1 \pmod{2}$ and $17 \equiv 4 \pmod{13}$.

Rings

A collection of things we can add, subtract, and multiply (but not necessarily divide) and still stay inside the collection (when regular rules of math apply).

Examples:

- Integers
- Real Numbers
- Complex Numbers
- Rational Numbers
- Modulus
- Matrices
- Polynomials