General Principle of Exponents ($\bmod p$)

- If an equation is $\bmod p$ where p is prime.
- Then we can treat all of the exponents $\bmod (p-1)$.
- Application of Fermat's Little Theorem.

Using this to speed up computation

- Use this to speed up computation (make exponent smaller).
- Use this to solve expressions involving exponents.

Example

$$\begin{aligned} \text{Solve} \quad x^5 &\equiv 7 \pmod{23} \\ \text{In calculus} \quad x^5 &\equiv 5^7 \pmod{23} \\ \text{5th root of } x^5 &\equiv \sqrt[5]{5^7} \\ x \cdot \sqrt[5]{7} &\equiv 7^{1/3} \end{aligned}$$

Imagine rasing both sides of the equation to an exponent e(TBD)

x$^5 \equiv 7 \cdot 5^e \pmod{23}$
$(x^5)^e \equiv 7^e \pmod{23}$
$x^{5e} \equiv 7^e \pmod{23}$
$5e \equiv 1 \pmod{22}$

We want
$5e \equiv 1 \pmod{22}$
$e \equiv 5^{-1} \pmod{22}$
$e \equiv 9 \pmod{22}$

Euclid's Algorithm

$$\begin{aligned}
22 &= 5(4) + 2 \\
5 &= 2(2) + 1 \\
1 &= 5 - 2(2) \\
2 &= 22 - 5(4) \\
1 &= 5 - 2(22 - 5(4))
\end{aligned}$$

Modular Arithmetic Calculations

$$\begin{aligned}
&7^2 \equiv 49 \equiv 3 \pmod{23} \\
&7^4 \equiv (7^2)^2 \equiv 3^2 \equiv 9 \pmod{23} \\
&7^8 \equiv (7^4)^2 \equiv 9^2 \equiv 81 \equiv 12 \pmod{23}
\end{aligned}$$

Encryption/Decryption Functions

We found that $F(x) = x^5 \pmod{23}$ and its inverse function $F^{-1}(x) = x^a \pmod{23}$. These functions can be thought of as encryption and decryption functions, respectively.

$$\begin{aligned}
E(x) &\equiv x^5 \pmod{23} \\
D(x) &\equiv x^9 \pmod{23}
\end{aligned}$$

Discrete Logarithm Problem

Given:

$$b^x \equiv y \pmod{p}$$

and you know b, y, p, solving for x is surprisingly hard.

However, in comparison:

$$bx \equiv y \pmod{p}$$

Solving for x is straightforward:

$$x \equiv b^{-1}y \pmod{p}$$

3-Pass Protocol

This is a method for Alice to send a message to Bob securely even when they have no shared secret key.

Physical World Version

1. Alice locks the box with her padlock and sends it to Bob.
2. Bob locks this again with his lock and sends it back to Alice.
3. Alice unlocks her padlock and sends the box to Bob.
4. Bob unlocks his lock and opens the box.

Math Version

- Alice and Bob pick a big prime p. (Example: $p \approx 10^{200}$)
- p isn't secret. Eve knows p.
- Alice and Bob both pick secret keys a, b where:

$$\begin{gathered} 2 \leq a \leq p-1 \\ 2 \leq b \leq p-1 \end{gathered}$$

  And:

$$\begin{gathered} \gcd(a, p-1) = 1 \\ \gcd(b, p-1) = 1 \end{gathered}$$

Encryption Functions

$$\begin{aligned} E_A(x) &= x^a \pmod{p} && \text{(Alice's encryption function)} \\ E_B(x) &= x^b \pmod{p} && \text{(Bob's encryption function)} \end{aligned}$$

Inverse Calculations

$$\begin{gathered} a \cdot a^{-1} \equiv 1 \pmod{p-1} \\ b \cdot b^{-1} \equiv 1 \pmod{p-1} \end{gathered}$$

Alice finds:

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

Bob finds:

$$b \equiv b^{-1} \pmod{p-1}$$

Decryption Functions

$$\begin{gathered} D_A(y) \equiv y^{a^1} \pmod{p} \\ D_B(y) \equiv y^{b^1} \pmod{p} \end{gathered}$$

Message Encryption and Decryption Process

- Alice wants to send a plaintext message m encoded as a number, where $0 \leq m < p$.
- Alice encrypts the message:

  $$C_1 = E_A(m) \equiv m^a \pmod{p}$$

  Alice sends C_1 to Bob.
- Bob encrypts again:

  $$C_2 = E_B(C_1) \equiv C_1^b \pmod{p}$$

  Bob sends C_2 to Alice.
- Alice decrypts C_2:

  $$C_3 = D_A(C_2) \equiv C_2^{a^1} \pmod{p}$$

  She then sends C_3 to Bob.
- Bob decrypts:

  $$\begin{aligned} C_4 &\equiv D_B(C_3) \equiv C_3^{b^1} \pmod{p} \\ &\equiv ((m^a)^b)^{a^1 b^1} \pmod{p} \\ &\equiv m^{ab(a^1 b^{-1})} \pmod{p} \\ &\equiv m^{ab} \pmod{p} \quad \text{since } ab(a^1 b^1) \equiv 1 \pmod{p-1} \\ &\equiv m \pmod{p} \end{aligned}$$

  Which is the original message.