RSA

Modular Congruence

- In modular arithmetic, we choose a positive integer m and view all other integers as being equivalent to their unique representatives between 0 and $m-1$.
- Two integers are *congruent modulo m* if they both have the same remainder when divided by m.
- This is the same as saying that two integers a and b are congruent modulo m if and only if $a-b$ is divisible by m.
- We write $a \equiv b \bmod m$ to express a and b being congruent modulo m.
- In math notation, $a \equiv b \bmod m \iff m|(a-b)$.

Modular Congruence

- In modular arithmetic, we choose a positive integer m and view all other integers as being equivalent to their unique representatives between 0 and $m - 1$.
- Two integers are *congruent modulo m* if they both have the same remainder when divided by m.
- This is the same as saying that two integers a and b are congruent modulo m if and only if $a - b$ is divisible by m.
- We write $a \equiv b \bmod m$ to express a and b being congruent modulo m.
- In math notation, $a \equiv b \bmod m \iff m|(a - b)$.
- Write examples on the board, please.

Modular Arithmetic

- If $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$, then $(a_1 + a_2) \equiv (b_1 + b_2) \bmod m$ and $a_1 a_2 \equiv b_1 b_2 \bmod m$.
- This allows us to compute exponents that could otherwise be too big. Look at the nice example on the board.

Inverses

- Given a and m, there exists an integer b such that $ab \equiv 1 \bmod m$ if and only if $\gcd(a, m) = 1$.
- If $ab \equiv 1 \bmod m$, then we say that a and b are *multiplicative inverses* of each other mod m. (or just inverses).
- We can also say that a is invertible, or that a is a unit, if a has an inverse mod m.
- Examples

Inverses

- Given a and m, there exists an integer b such that $ab \equiv 1 \mod m$ if and only if $\gcd(a, m) = 1$.
- If $ab \equiv 1 \mod m$, then we say that a and b are *multiplicative inverses* of each other mod m. (or just inverses).
- We can also say that a is invertible, or that a is a unit, if a has an inverse mod m.
- Examples
- $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$.
- $$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\star &= \{a \in \mathbb{Z}/m\mathbb{Z} \mid a \text{ has an inverse}\} \\ &= \{a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}\end{aligned}$$

Euler's Function

- Two integers a and b are relatively prime if and only if $\gcd(a, b) = 1$.
- The Euler Phi Function (or the Euler Totient Function) is defined as the number of positive integers less than m that are relatively prime to m. So this is the size of the set of units in $\mathbb{Z}/m\mathbb{Z}$. In math notation,

$$\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\star|$$

- Examples

Euler's Function

- Two integers a and b are relatively prime if and only if $\gcd(a, b) = 1$.
- The Euler Phi Function (or the Euler Totient Function) is defined as the number of positive integers less than m that are relatively prime to m. So this is the size of the set of units in $\mathbb{Z}/m\mathbb{Z}$. In math notation,

$$\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\star|$$

- Examples
- If p is prime, then $\phi(p) = p - 1$.
- If $N = pq$ where both p and q are prime, then $\phi(N) = (p-1)(q-1)$.

Euclid

You can use the Euclidean algorithm (google it or look in a textbook if you need) to find $\gcd(a, m)$ for two positive integers a and m. You can also use the extended Euclidean algorithm to obtain a linear combination: $as + mt = \gcd(a, m)$ for some integers s and t.

Now suppose that $\gcd(a, m) = 1$. Then we can find s and t such that $as + mt = 1$. Then $as = 1 - mt$. So $as \equiv 1 \bmod m$, and s is the inverse of a mod m.

To summarize: we can use the Euclidean algorithm to quickly find the gcd of a and m. If that gcd is 1, then we can use the extended Euclidean algorithm to quickly find the multiplicative inverse of a mod m.

Euler's Theorem

If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.

Public Key Cryptography

- Ask if they know what public key cryptography is.

Public Key Cryptography

- Ask if they know what public key cryptography is.
- Do a demonstration of public key cryptography.

RSA

- Suppose Bob wants to send a message to Alice. For simplicity, suppose the message is in the form of a positive integer m.
- Alice chooses two large prime numbers, p and q. She multiplies them to get $N = p \times q$ and she publishes N for Bob to see.
- Alice chooses a positive integer e that is relatively prime to $\phi(N)$ and also publishes it. The pair (e, N) is called Alice's *public key*.

RSA (continued)

- Alice finds the multiplicative inverse, d, of e modulo $\phi(N)$. This is called Alice's *private key*.
- Bob computes $c \equiv m^e \bmod N$. This value c is the ciphertext he sends to Alice.
- Alice computes $c^d \bmod N$. This is the original message m.

Proof that RSA Works

When Alice receives Bob's message, she computes

$$\begin{aligned} c^d \bmod N &\equiv (m^e)^d \bmod N \\ &\equiv m^{ed} \bmod N \\ &\equiv m^{1+k\phi(N)} \bmod N \\ &\equiv (m)(m^{\phi(N)})^k \bmod N \\ &\equiv m * 1^k \bmod N \\ &= m. \end{aligned}$$

The Security of RSA

- If Eve can find d, then she can decrypt any message Bob sends. Only e and N are published by Alice, so Eve has to try to recover d with just those two values.
- Knowing p and q would reveal d (since $e \times d \equiv 1 \bmod (p-1)(q-1)$).
- So Eve just needs to factor N into $p \times q$.

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be a set of pairwise relatively prime positive integers (so $\gcd(m_i, m_j) = 1$ for all $i \neq j$). Then the set of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \text{ mod } m_1 \\ x &\equiv a_2 \text{ mod } m_2 \\ &\ldots \\ x &\equiv a_k \text{ mod } m_k \end{aligned}$$

has a unique solution mod $m_1 m_2 \ldots m_k$.