CSL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \ (mod \ m_1),$$
$$x \equiv a_2 \ (mod \ m_2),$$
$$\vdots$$
$$x \equiv a_n \ (mod \ m_n)$$

has a unique solution modulo $m = m_1 m_2 ... m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \ (mod \ m_1),$$
$$x \equiv a_2 \ (mod \ m_2),$$
$$\vdots$$
$$x \equiv a_n \ (mod \ m_n)$$

has a unique solution modulo $m = m_1 m_2 ... m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

- Proof of existence:
  - Let $M_k = m/m_k$ and let y_k denote the inverse of M_k modulo m_k (i.e., $M_k \cdot y_k \equiv 1 \ (mod \ m_k)$).
  - Claim: $x = \sum_i a_i \cdot M_i \cdot y_i$ is a solution modulo m.

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \ (mod \ m_1),$$
$$x \equiv a_2 \ (mod \ m_2),$$
$$\vdots$$
$$x \equiv a_n \ (mod \ m_n)$$

has a unique solution modulo $m = m_1 m_2 ... m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

- Proof of uniqueness:
  - Lemma: Let p, q be relatively prime positive integers. For any integers a, b, if $a \equiv b \ (mod \ p)$ and $a \equiv b \ (mod \ q)$, then $a \ \equiv b \ (mod \ pq)$.

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \ (mod \ m_1),$$
$$x \equiv a_2 \ (mod \ m_2),$$
$$\vdots$$
$$x \equiv a_n \ (mod \ m_n)$$

has a unique solution modulo $m = m_1 m_2 ... m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

- Let $m_1, ..., m_n$ be relatively prime and let $m = m_1 ... m_n$. Consider the following two sets:
  - $A = Z_m$
  - $B = \{(x_1, ..., x_n) | \forall i \ (x_i \in Z_{m_i})\}$.
- Claim: There is a bijection between A and B.

- Suppose we have to multiply the following two numbers:

$$x = 1682593 \quad \text{and} \quad y = 176234$$

- Let $m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19, m_5 = 23, m_6 = 29, m_7 = 31, m_8 = 37, m_9 = 41$. So, $m = m_1 ... m_9 = 1448810778701$.

r	$x \pmod r$	$y \pmod r$	$xy \pmod r$
11	0	3	?
13	3	6	?
17	1	12	?
19	10	9	?
23	5	8	?
29	13	1	?
31	6	30	?
37	18	3	?
41	35	16	?

- Suppose we have to multiply the following two numbers:

$$x = 1682593 \quad \text{and} \quad y = 176234$$

- Let $m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19, m_5 = 23, m_6 = 29, m_7 = 31, m_8 = 37, m_9 = 41$. So, $m = m_1 ... m_9 = 1448810778701$.

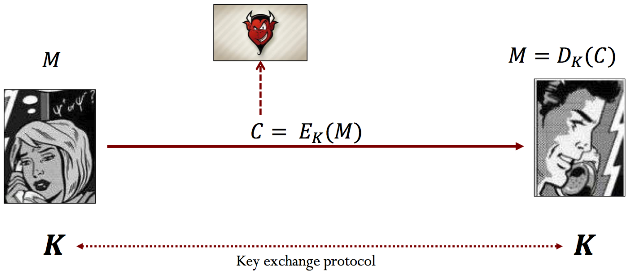
r	$x \pmod r$	$y \pmod r$	$xy \pmod r$
11	0	3	0
13	3	6	5
17	1	12	12
19	10	9	14
23	5	8	17
29	13	1	13
31	6	30	25
37	18	3	17
41	35	16	27

- Can we construct xy using the table above?

Read the chapter on application of congruences.

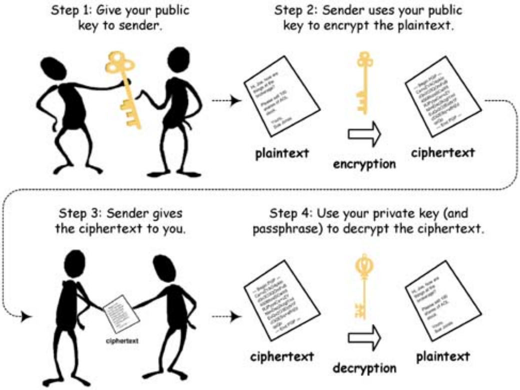
Number Theory and Cryptography

- One of the main tasks in Cryptography is *secure communication*.



- The above picture shows a *symmetric* scheme.
- How do you construct such a scheme?

- The main issue with symmetric schemes is *key distribution*.
- The picture below shows an alternate mechanism known as *Public key encryption*.



- How do we construct a public key encryption scheme?
- The description of a public key encryption scheme involves defining three procedures.
  - *Gen*: This generates the public-key, secret-key pair (pk, sk).
  - $Encrypt_{pk}(M)$: This takes as input a message and then uses just the public key to generate a cipher text.
  - $Decrypt_{sk}(C)$: This takes as input a cipher text and uses the secret key to generate the message.
- The correctness property that should hold for the above procedures is:

$$Decrypt_{sk}(Encrypt_{pk}(M)) = M.$$

- Consider the following scheme:
  - *Gen*: Find large n-bit primes p, q (n is usually 1024). Let $N = pq$ and $\phi(N) = (p-1)(q-1)$. Find integers e, d such that $ed \equiv 1 \ (mod\ \phi(N))$. Output (pk, sk), where

$$pk = (N, e) \quad \text{and} \quad sk = (N, d)$$

  - $Encrypt_{pk}(M)$: Output $M^e \ (mod\ N)$.
  - $Decrypt_{sk}(C)$: Output $C^d \ (mod\ N)$.
- This is popularly called the RSA scheme. This is named after its inventors Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman.
- Does the correctness property hold for the above scheme?

Definition (Group)

A group is a set G along with a binary operator $\cdot$ for which the following conditions hold:

1. Closure: For all $g, h \in G$, $g \cdot h \in G$.
2. Identity: There exists an identity $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. Inverse: For all $g \in G$, there exists an $h \in G$ such that $g \cdot h = e = h \cdot g$. Such h is called an *inverse* of g.
4. Associativity: For all $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

Definition (Finite Group)

When a group G has finite number of elements, then we say that it is a finite group of *order* $|G|$.

Definition (Abelian Group)

$G$is called an *abelian* group if it is a group and also satisfies the following condition:

- Commutativity: For all $g, h \in G$, $g \cdot h = h \cdot g$.

- Exercise 1: Identity element in any group is unique.
- Exercise 2: Every element in any group has a unique inverse.
- Exercise 3: Let G be a group and $a, b, c \in G$.If $a \cdot c = b \cdot c$, then $a = b$. In particular, is $a \cdot c = c$, then a is the identity element.

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

- Let m be prime and a be an integer such that $1 \leq a < m$. What is the value of a^{m-1}?

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

Theorem (Fermat's little theorem)

If p is a prime number, then for any integer a we have: $a^p \equiv a \ (mod \ p)$.

- Let p, q be primes, let $N = pq$, let $\phi(N) = (p-1)(q-1)$, and let e, d be such $ed \equiv 1 \ (mod \ \phi(N))$. Then for any $M \in Z_N^*$, what is the value of $M^{ed} \ (mod \ N)$?

Theorem

Let G be a finite abelian group with $m = |G|$. Then for any element $g \in G, g^m = 1$. (Here g^m denotes $g \cdot g \cdot ... \cdot g$ (m operations).)

Theorem (Fermat's little theorem)

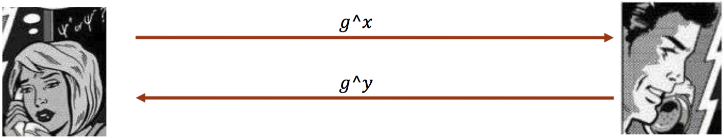
If p is a prime number, then for any integer a we have: $a^p \equiv a \pmod{p}$.

Theorem

Let p, q be primes, let $N = pq$, let $\phi(N) = (p-1)(q-1)$, and let e, d be such $ed \equiv 1 \pmod{\phi(N)}$. Then for any $M \in Z_N$, $M^{ed} \pmod{N} = M$

- The above theorem proves the correctness of the RSA algorithm.
- Question 1: Can we *break* RSA if we can factor N?
- Question 2: Can we factor N if we can *break* RSA?

- Suppose we talk about symmetric schemes. How do two parties exchange secret key?
- Diffie-Hellman Key Exchange.



Both parties share g^{xy} which is the secret key for the session.

- The assumption used here is that there are groups in which computing g^{xy} given just g^x and g^y is difficult.

Number Theory and Cryptography
Diffie-Hellman key exchange

- Authentication is an issue in the this key exchange protocol.
- Diffie-Hellman Key Exchange: *Man-in-the-middle attack*

End