School of Information Science and Technology
ShanghaiTech University

SI120 Discussion 4

Homework 4: CRT, Group and key exchange

SI120 TA

March 27, 2022

Set theory

Definition

- **Unordered** collection of elements.
- Finite set v.s. Infinite set
- Countable v.s. Uncountable
- Example: $\mathbb{Z}, (0, 1), \mathbb{R}$

Application

- Set operation: Union, intersection, complement, difference, symmetric difference, Cartesian product, power set.
- Generalized union and intersection
- Law of set operation.
- Cardinality of set.

Function

- Definition: map, domain, codomain, range, image, preimage
- Injective: $f(a) = f(b) \Rightarrow a = b$
- Surjective: $f(A) = B$
- bijective: Both injective and surjective.

Cardinality: Prove $|A| = |B|$

- By story telling.
- By constructing a bijection.
- By Schröder-Bernstein Theorem.
- Example: $|\mathbb{Z}| = |\mathbb{Z}^+| = |\mathbb{Q}| = |\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$
  $|(0,1)| = |[0,1)| = |[0,1]| = |\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$

Which of the following statement is not correct?

- The sets A, B have same cardinality if and only if there is an injection $f : A \to B$ and an injection $g : B \to A$.
- The set A is infinite if and only if A has a subset B such that $|B| = |\mathbb{Z}^+|$.
- The power set of a countable set is countable.
- The power set of an uncountable set is uncountable.

Counting and Permutation

Basic rules of Counting

- **The sum rule:** Finite set A has a partition $\{A_1, A_2, ..., A_k\}$. Then we have $|A| = \sum_{i=1}^{k} |A_k|$.
- **The product rule:** $|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \times |A_2| \times \cdots \times |A_k|$

Permutation

- **Without repetition:** $P(n, r) = \frac{n!}{(n-r)!}$
- **With repetition:** n^r

Multiset and its permutation

Definition

- **Multiset:** elements not necessarily different from each other.
- **r-permutation:** Permutation of a r-subset of multiset.
- **Permutation:** The number of permutations of a multiset is defined by $\frac{(n_1+n_2+\ldots+n_k)!}{n_1!n_2!\ldots n_k!}$

Application

- Grid shortest path: $\frac{(p+q)!}{p!q!}$
- T condition: Necessary and sufficient
- Number of T path: $\frac{(b-a)!}{\left(\frac{b-a}{2}+\frac{\beta-\alpha}{2}\right)!\left(\frac{b-a}{2}-\frac{\beta-\alpha}{2}\right)!}$

Exercise

Which of the following statement is not correct?

- The bijection rules says that if there is a bijection between two finite set A and B, then $|A| = |B|$.
- The sum rule says that if A is a finite set and $\{A_1, ..., A_k\}$ is a cover of A, then $|A| = |A_1| + .. + |A_k|$.
- The product rule says that if $A_1, ..., A_k$ are finite set (not necessarily disjoint), and $A = A_1 \times ... \times A_k$, then $|A| = |A_1| \cdot ... \cdot |A_k|$
- The number of 4-permutations of multiset $\{1 \cdot a, 2 \cdot b, 3 \cdot c\}$ is 38.

Exercise

Which of the following is not true?

A. The sets A, B have the same cardinality if and only if there is a bijection $f : A \to B$.

B. A set is uncountable if its power set is uncountable.

C. If A, B are countably infinite, then so is $A \cup B$.

D. If A, B are countably infinite, then so is $A \times B$.

Exercise

Which of the following is not true?

A. Let A be any set of sets. Then $\cup\mathcal{P}(A) = A$.

B. Let A be any set of sets. Then $\mathcal{P}(\cup A) = A$.

C. Let $A = \{1 \cdot a, 2 \cdot b, 3 \cdot c, 100 \cdot z\}$, $T = \{1 \cdot b, 98 \cdot z\}$. Then T is a 99-subset of A.

D. Let $A = \{1 \cdot a, 2 \cdot b, 3 \cdot c\}$. Then the 3-permutations of A is 19.

Exercise

Which of the following sets has different cardinality comparing to others?

A. The set $\mathbb{R}^+$ of positive real numbers.

B. The set $\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 = 1\}$.

C. The set $\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 < 1\}$.

D. The set $\{S : S \subseteq \mathbb{Z}^+, |S| < \infty\}$.

Question 1

Let a_1, a_2, a_3, a_4 be arbitrary integers. Find ALL integer solutions of the following equation system.

$$\begin{cases} x \equiv a_1 \pmod{11} \\ x \equiv a_2 \pmod{13} \\ x \equiv a_3 \pmod{17} \\ x \equiv a_4 \pmod{19} \end{cases}$$

Solution: CRT

$$n = n_1 n_2 n_3 n_4 = 46189$$

$$N_1 = n_2 n_3 n_4 = 4199 \quad N_2 = n_1 n_3 n_4 = 3553$$

$$N_3 = n_1 n_2 n_4 = 2717 \quad N_4 = n_1 n_2 n_3 = 2431$$

By EEA, we could calculate that

$$1527n_1 - 4N_1 = 1; 820n_2 - 3N_2 = 1; 959n_3 - 6N_3 = 1; 128n_4 - N_4 = 1$$

$$s_1 = -4, s_2 = -3, s_3 = -6, s_4 = -1$$

$$\begin{aligned} b &= a_1(N_1 s_1) + a_2(N_2 s_2) + a_3(N_3 s_3) + a_4(N_4 s_4) \\ &= (4199 * (-4))a_1 + (3553 * (-3))a_2 \\ &\quad + (2717 * (-6))a_3 + (2431 * (-1))a_4 \\ &= -16796a_1 - 10659a_2 - 16302a_3 - 2431a_4 \\ x &\equiv b \bmod n \end{aligned}$$

Homework 1

Question 1

Let a_1, a_2, a_3, a_4 be arbitrary integers. Find ALL integer solutions of the following equation system.

$$\begin{cases} x \equiv a_1 \pmod{11} \\ x \equiv a_2 \pmod{13} \\ x \equiv a_3 \pmod{17} \\ x \equiv a_4 \pmod{19} \end{cases}$$

Solution: CRT

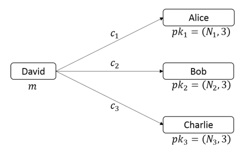
$$1527n_1 + 7N_1 = 1 \quad 820n_2 + 10N_2 = 1$$

$$959n_3 + 11N_3 = 1 \quad 128n_4 + 18N_4 = 1$$

$$\begin{aligned} s_1 &= 7, s_2 = 10, s_3 = 11, s_4 = 18 \\ b &= a_1(N_1 s_1) + a_2(N_2 s_2) + a_3(N_3 s_3) + a_4(N_4 s_4) \\ &= 29393a_1 + 35530a_2 + 29887a_3 + 43758a_4 \end{aligned}$$

Question 2

See the following figure. The RSA public keys of Alice, Bob and Charlie are $pk_1 = (N_1, 3)$, $pk_2 = (N_2, 3)$ and $pk_3 = (N_3, 3)$, respectively. David wants to send a private message m to Alice, Bob and Charlie, where m is an integer and $0 < m < N_i$ for $i = 1, 2, 3$. In order to keep m secret from an eavesdropper Eve, David encrypts m as $c_1 = m^3 \bmod N_1$, $c_2 = m^3 \bmod N_2$ and $c_3 = m^3 \bmod N_3$; and then sends c_1 to Alice, c_2 to Bob and c_3 to Charlie.



Suppose that N_1, N_2, N_3 are pairwise relatively prime. Show that with the knowledge of all public keys and all ciphertexts, Eve can decide the value of m.

Solution:

What does the eve know?

$$\begin{cases} m^3 \equiv c_1 \mod N_1 \\ m^3 \equiv c_2 \mod N_2 \\ m^3 \equiv c_3 \mod N_3 \end{cases}$$

Chinese Remainder Theorem:

Let $n_1, ..., n_k \in \mathbb{Z}^+$ be pairwise relatively prime, and $n = n_1 \cdots n_k$. Then for any $b_1, ..., b_k \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $b \equiv b_i \mod n_i$ for every $i \in [k]$. Furthermore if $x \equiv b_i \mod n_i$ for every $i \in [k]$, then $x \equiv b \mod n$.

Chinese Remainder Theorem:

Let $n_1, ..., n_k \in \mathbb{Z}^+$ be pairwise relatively prime, and $n = n_1 \cdots n_k$. Then for any $b_1, ..., b_k \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $b \equiv b_i \mod n_i$ for every $i \in [k]$. Furthermore if $x \equiv b_i \mod n_i$ for every $i \in [k]$, then $x \equiv b \mod n$.

Solution:

- By CRT, we could calculate a x such that $m^3 \equiv x \bmod N$ where $N = N_1 N_2 N_3$.
- As $m < N_i$, $m^3 < N$, so $m = \sqrt[3]{x}$.

RSA vulnerabilities: Hastad's broadcast attack

Suppose Bob wishes to send an encrypted message M to a number of parties $P_1, P_2, \cdots, P_k$. Each party has its own RSA key (N_i, e_i). We assume m is less than all the N_i. Idealistically, to send m, Bob encrypts it using each of the public keys and sends out of the i-th ciphertext to P_i. An attacker Eve can eavesdrop on the connection out of Bob's sight and collect the k transmitted ciphetexts.

- Proposed by Hastad in 1985.
- If all public exponents are equal to e, Eve can recover m as soon as $k > e$.
- The attack is feasible only when a small e is used.

RSA vulnerabilities: Hastad's broadcast attack

- Proposed by Hastad in 1985.
- If all public exponents are equal to e, Eve can recover m as soon as $k > e$.
- The attack is feasible only when a small e is used.

Note:

- You need to explicitly mention that $m^3 < N$, otherwise, it is far more difficult to learn m.
- Generally, it is hard to learn m from $m^e \bmod N$ when given e is large, otherwise, RSA is not secure anymore.
- Again, it is difficult to calculate $phi(N)$ given N, factoring integer is hard.

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Review: what is Abelian group?

A **Abelian group** is a set G, together with an binary operation $*$ such that the following hold:

- **Closure:** $\forall a, b \in G, a * b \in G$.
- **Associativity:** $\forall a, b, c \in G, (a * b) * c = a * (b * c)$.
- **Identity:** $\exists e \in G, \forall a \in G$ such that $a * e = e * a = a$.
- **Inverses:** $\forall a \in G, \exists b \in G$ such that $a * b = b * a = e$.
- **Commutative:** $\forall a, b \in G, a * b = b * a$.

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Closure:

By definition:

- $x * y = xy - x - y + 2 = (x - 1)(y - 1) + 1$
- $\forall x, y > 1, x * y > 1, x * y \in \mathbb{R}$
- $x * y \in G$

By calculus, suppose $f(x, y) = xy - x - y + 2$:

- $\frac{\partial f(x,y)}{\partial x} = y - 1 > 0$, $\frac{\partial f(x,y)}{\partial y} = x - 1 > 0$.
- $f(x, y) > f(1, 1) = 1$

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Associativity

For $x, y, z \in G$:

- $(x * y) * z = xyz - xy - yz - zx + x + y + z$
- $x * (y * z) = xyz - xy - yz - zx + x + y + z$
- $(x * y) * z = x * (y * z)$

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Identity:

For $\forall x \in G$, suppose $\exists e \in G$ such that:

- $x * e = xe - x - e + 2$, $e * x = ex - e - x + 2$
- $x * e = e * x$ is obviously satisfied.
- If $x * e = x$, then $xe - x - e + 2 = x$
- $e = \frac{2x-2}{x-1} = 2 \in G$

So, $\forall x \in G, \exists 2 \in G, x * e = e * x = 2x - x - 2 + 2 = x$.

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Inverse:

For $\forall x \in G$, suppose $\exists y \in G$ such that:

- $x * y = y * x$ is obviously satisfied.
- If $x * y = e$, then $xy - x - y + 2 = 2$
- $(x-1)(y-1) = 1 \Rightarrow y = \frac{1}{x-1} + 1 > 1$

So, $\forall x \in G, \exists y = \frac{1}{x-1} + 1 \in G, x * y = y * x = 2.$

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Commutative:

For $\forall x, y \in G$:

- $x * y = xy - x - y + 2$, $y * x = yx - y - x + 2$.
- $x * y = y * x$.

Question 3

Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

Note:

- Five properties, and 4 points for each one.
- In proof of inverse, state that $y = \frac{x}{x-1} \in G$.
- You need to explicitly calculated the value of e thus prove the existence.

Question 4

Let $(G,)$ be a multiplicative (Abelian) group of order m. Show that $o(a)|m$ for any $a \in G$, i.e., the order of any group element must be a divisor of the group's order.

Idea: Division algorithm

Apply division algorithm to m and $o(a)$:

- $\exists q \in \mathbb{Z}^+$ such that $m = o(a) \cdot q + r$ where $0 \leq r < o(a)$.
- By theorem, we have $a^m = 1$. By definition, we have $a^{o(a)} = 1$.
- $a^m = a^{o(a) \cdot q} \cdot a^r \Rightarrow a^r = 1 \Rightarrow r = 0$
- $m = o(a) \cdot q \Rightarrow o(a)|m$

Extension: Lagrange Theorem

Let $(G,)$ be a finite group and $H \subset G$ a subgroup. Then $|H|$ divides $|G|$.

Proof

Could be proved by properties of equivalence class and coset. Beyond the range of this course.

Solution: by Lagrange Theorem **Not Recommended**

- Suppose $H \subset G$ is a cyclic subgroup generated by a, then it is clear that $o(a) = |H|$.
- By Lagrange Theorem, $o(a) = |H| \mid m$.

Question 5

Let $G = \langle g \rangle$ be a subgroup of $\mathbb{Z}_p^*$ of order q, where p is a large prime and $q = (p-1)/2$ and $g = 3$. Suppose that in a Diffie-Hellman key exchange protocol Alice and Bob exchanged the following information $(q, G, g; A, B)$, where A, B are given and $\log_g A, \log_g B < 10^4$. Find the output of Alice and Bob.

Review: Diffie-Hellman key exchange

- Alice: $a \leftarrow \mathbb{Z}_q$, $A = g^a$, send (q, G, g, A) to Bob.
- Bob: $b \leftarrow \mathbb{Z}_q$, $B = g^b$, send B to Alice, output $k = A^b$.
- Alice: Output $k = B^a$

Question 5

Let $G = \langle g \rangle$ be a subgroup of $\mathbb{Z}_p^*$ of order q, where p is a large prime and $q = (p-1)/2$ and $g = 3$. Suppose that in a Diffie-Hellman key exchange protocol Alice and Bob exchanged the following information $(q, G, g; A, B)$, where A, B are given and $\log_g A, \log_g B < 10^4$. Find the output of Alice and Bob.

Solution: Brute force for a or b

- For $i = 1, \cdots, 10^4$
- If $3^i = A$, then $a \leftarrow i$.
- Output B^a.

Question 5

Let $G = \langle g \rangle$ be a subgroup of $\mathbb{Z}_p^*$ of order q, where p is a large prime and $q = (p-1)/2$ and $g = 3$. Suppose that in a Diffie-Hellman key exchange protocol Alice and Bob exchanged the following information $(q, G, g; A, B)$, where A, B are given and $\log_g A, \log_g B < 10^4$. Find the output of Alice and Bob.

Discussion: Why feasible?

- Here, p is a large prime, $p \approx 10^{309} \approx 2^{1024}$, i.e. 1024-bit prime.
- If we pick a number uniformly random from subgroup G of $\mathbb{Z}_p^*$, on average we need $q/2$ multiplication to get the discrete log, and that is 2^{1022} multiplications.
- In this question, performing 10^4 requires 0.2 second, then 2^{1022} multiplications requires 10^{302} second, that is 10^{294} years.

In this question, it is $\log_g A, \log_g B < 10^4$ that it is feasible.

That’s all today.
Have a nice weekend.