Домашнее задание №2

Математические основы криптографии группа 2.2

30 Ноября 2022

Преподаватель: Дакуо Жан-Мишель Никодэмович @jeandakuo

Дедлайн: Понедельник, 12 Декабря, 23:59 по МСК

Правила

- За домашнее задание вы должны набрать:
  - 15 баллов, если отправляете домашнее задание вовремя;
  - 20 баллов, если отправляете домашнее задание после дедлайна.
- Ответы без решения не принимаются (код - тоже решение).
- Если вы не можете решить, но думаете, что на правильном пути, отправьте свои мысли, они могут помочь получить некоторое количество баллов.
- Плагиат - это плохо :c
- Высылайте в любом удобном для прочтения формате (PDF файл). Если отправить домашнее до дедлайна, то можно получить фидбэк и возможность исправить выявленные недочеты, что позволит набрать дополнительные баллы. **Домашнее задание высылайте на почту:** **jeandakuo@mail.ru**

Задания

Шпаргалка

- $\mathbb{N} = \{1, 2, 3, 4, ...\}$ — множество натуральных чисел.
- $\mathbb{Z} = \{... -3, -2, -1, 0, 1, 2, 3, ...\}$ — множество целых чисел.
- $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ — фактор множество n.

- $\mathbb{Q} = \left\{ \frac{m}{n} \;\middle|\; m \in \mathbb{Z}, n \in \mathbb{N} \right\}$ — множество целых чисел.
- $\mathbb{R}$ — множество вещественных чисел.
- $\mathbb{R}_{>0}$ — множество положительных вещественных чисел.
- $\operatorname{ord}(a)$ — порядок элемента a.

Задание 1 Повторение - мать учения (2 балла, $\frac{1}{3}$ каждый).

Для каждого множества распиишете, как оно выглядит и (или) покажите его структуру

1. Множество всех цветов в флаге Сейшельских Островов.
2. Пусть $A = \{2, 4, 6, 8, 10, 12\}$, $B = \{3, 6, 9, 12\}$. Вычислите следующие множества:
   (a) $A \cup B$
   (b) $A \cap B$
   (c) $A \setminus B$
   (d) $B \setminus A$
   (e) $A \times B$
3. Найдите:
   (a) $\mathbb{Z}_7^* = \{x \in \mathbb{Z}_7 \mid \gcd(x, 7) = 1\}$
   (b) $\mathbb{Z}_8^* = \{x \in \mathbb{Z}_8 \mid \gcd(x, 8) = 1\}$
4. Пусть множество $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. Найдите:
   (a) $2\mathbb{Z}$
   (b) $3\mathbb{Z}$
   (c) $3\mathbb{Z} \cap 2\mathbb{Z}$

(d) $3\mathbb{Z} \setminus 2\mathbb{Z}$

5. Множество можно возводить в степень, что означает следующее:
$$A^n := \underbrace{A \times A \times ... \times A}_{n \text{ times}}$$
Найдите $\{0,1\}^3$.

6. Множество 2^A — это множество всех подмножеств заданного множества A:
$$2^A = \{B \mid B \subset A\}$$
Пусть $X = \{1,2,3\}$. Найдите 2^X.

Задание 2 Группа или не группа? (2 балла, $\frac{1}{4}$ за каждый).

2.a Докажите или опровергните, что следующее множество с заданной на ней операцией является группой.

1. $\langle \mathbb{N}, + \rangle$.

2. $\langle \mathbb{Z}, + \rangle$.

3. $\langle \mathbb{Q}, * \rangle$.

4. $\langle \mathbb{Z}_{12}^*, * \rangle$, где $\mathbb{Z}_{12}^* = \{x \in \mathbb{Z}_{12} \mid \gcd(x, 12) = 1\}$ и '$*$' — это умножение по модулю 12.

5. $\langle B_n, \vee \rangle$, где $B_n = \{0,1\}^n$ — множество всех бинарных строк длинны n и $\vee$ — побитовая операция ИЛИ.

6. $\langle B_n, \oplus \rangle$, где $B_n = \{0,1\}^n$ — множество всех бинарных строк длинны n и $\oplus$ — побитовая операция XOR.

7. $\langle \mathbb{F}, + \rangle$, где $\mathbb{F}$ — множество всех функций: $\mathbb{Z} \to \mathbb{Z}$ и $(f+g)(x) = f(x) + g(x)$.

8. $\langle \mathbb{F}, \circ \rangle$, где $\mathbb{F}$ — множество всех функций: $\mathbb{Z} \to \mathbb{Z}$ и $(f \circ g)(x) = f(g(x))$.

2.b Для каждой группы из (a):

1. Найдите порядок группы.
2. Выпишите таблицу Кэли (только для конечных групп).
3. Найдите нейтральный элемент.
4. Для каждого элемента a найдите порядок этого элемента: $\mathrm{ord}(a)$ (только для конечных групп)
5. Является ли группа цикличной? Если да, найдите генераторный элемент.
6. Является ли группа абелевой?

Задание 3 Уникальность обратного (1 балл).

Докажите, что в группе G для любого элемента $a \in G$ существует единственный обратный:

$$\forall a \in G : \exists! a^{-1} : aa^{-1} = a^{-1}a = e$$

Задание 4 Использование теории групп в теории чисел (2 балла).

Теорема: Если n — простое, и $a, b \in \{1, ..., n-1\}$, тогда уравнение $ax \equiv b \pmod{n}$ имеет единственное решение на множестве $\{1, ..., n-1\}$.

Докажите данную теорему, используя теорию групп.

Задание 5 Использование теории чисел в теории групп (2 балла).

Напоминание: Если a — это элемент группы G, тогда обозначение $\langle a \rangle$ означает все элементы сгенерированные a:

$$\langle a \rangle = \{..., a^{-2}, a^{-1}, e, a, a^{2}, ...\}$$

Пусть $\operatorname{ord}(a) = n$.

Tasks:

5.a ($\frac{2}{5}$ балла) Докажите, что $\langle a \rangle$ - это подгруппа группы G. Каков порядок данной подгруппы?

5.b ($\frac{2}{5}$ балла) Докажите, что $\langle a \rangle$ — это абелева группа.

5.c ($\frac{2}{5}$ балла) Докажите, что $a^{m} = e \iff m \,\vdots\, n$.

5.d ($\frac{2}{5}$ балла) Докажите, что $a^{k} = a^{l} \iff k \equiv l \pmod n$.

5.e ($\frac{2}{5}$ балла) Докажите, что $\operatorname{ord}(a^{k}) = \boxed{\frac{n}{\gcd(n,k)}}$.

Задание 6 Теорема Лагранжа (5 points).

Одним из следствий теоремы Лагранжа является:

Пусть G — группа с подгруппой $H \subset G$. Тогда, $|H|$ делит $|G|$.

Давайте это докажем! Для простоты скажем, что G абелева.

Для начала определим класс смежности. *Класс смежности* gH — это множество всех элементов из H умноженных на $g \in G$:

$$gH = \{gh \mid g \in G, h \in H\}$$

Заметим, что если $g \notin H$, тогда gH — не группа.

Задания:

6.a (1 балл) Докажите, что если $g \in H$, тогда $gH = H$

6.b (1 балл) Докажите, что любой элемент $g \in G$ принадлежит какому-либо классу смежности.

6.c (1 балл) Докажите, что для $g_1, g_2 \in G$ их классы смежности либо эквивалентны ($g_1H = g_2H$), либо непересекаются ($g_1H \cap g_2H = \varnothing$).

Таким образом, можно сказать, что любой элемент из G принадлежит ровно к одному классу смежности.

6.d (1 балл) Пусть есть 2 различных элемента $h_1, h_2 \in H$. Очевидно, что $gh_1, gh_2 \in gH$. Докажите, что $gh_1 \neq gh_2$.

Что это значит? Различные элементы $h_i \in H$ отображаются в различные элементы $gh_i \in gH$. Тогда, $|gH| = |H|$ для любого $g \in G$.

Таким образом, можно разбить группу G на части одинакового размера $|H|$ (рис. 1). Это доказывает, что $|G|$ делится на $|H|$. Теорема Лагранжа доказана. $\square$

Важное следствие:

6.e (1 балл) Докажите, что $\forall a \in G \;\; |G| \vdots \operatorname{ord}(a)$.

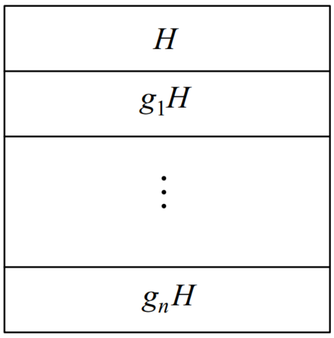

Рис. 1: Разбиение G на классы смежности

Задание 7 Изоморфизм (2 балла).

Изоморфизм — это биективное отображение из группы $\langle G, \oplus \rangle$ в группу $\langle H, \otimes \rangle$

$$f : G \to H$$

где для любых $a, b \in G$:

$$c = a \oplus b$$

$$f(c) = f(a) \otimes f(b)$$

Биективность отображения f означает, что для любого $g \in G$ существует единственный $h \in H : f(g) = h$ и для любого $h \in H$ существует единственный $g \in G : h = f(g)$. Тогда, для отображения f можно найти обратное f^{-1} такое, что: $g = f^{-1}(h)$.

Такие группы G и H называются *изоморфными* и обозначаются $G \cong H$. В терии групп изоморфные группы могут рассмариватся как одинаковые группы обладающие одинаковыми свойствами.

Задание: Даны 2 группы:

- $\langle \mathbb{R}, + \rangle$ — все действительные числа по сложению.
- $\langle \mathbb{R}_{>0}, \cdot \rangle$ — положительные действительные числа по умножению.

Найдите изоморфизм f между ними и его обратный f^{-1}.

Задание 8 Гомоморфное шифрование (2 балла).

Гомоморфизм — это отображение из группы $\langle G, \oplus \rangle$ в группу $\langle H, \otimes \rangle$

$$f : G \to H$$

, где для любых $a, b \in G$:

$$c = a \oplus b$$

$$f(c) = f(a) \otimes f(b)$$

В криптографии, существуют алгоритмы *гомоморфного шифрования*. Пусть дано пространство сообщений $\mathcal{M}$ и пространство шифротекстов $\mathcal{C}$. Для заданного ключа k, функция гомоморфного шифрования $E_k : \mathcal{M} \to \mathcal{C}$, удовлетворяет свойству:

$$E_k(m_1) \otimes E_k(m_2) = E_k(m_1 \oplus m_2)$$

для $m_1, m_2 \in \mathcal{M}$, где $\otimes$ — это действие над сообщениями и $\oplus$ — действие над шифротекстами.

Задание: Докажите, что RSA является алгоритмом гомоморфного шифрования. В каких случаях это может быть полезно?

Задание 9 Рубашка и пиджак (2 балла).

G — группа. Пусть a, b — 2 элемента из G. Также, $a_1, a_2, ..., a_k \in G$.

9.a Докажите, что $(ab)^{-1} = b^{-1}a^{-1}$.

9.b На основании (a) найдите $(a_1 \cdot a_2 \cdot ... \cdot a_k)^{-1}$. Докажите вашу правоту, используя метод математической индукции.

Задание 10 Генератор подгруппы (5 балла).

Пусть q — простое число, такое, что:

$$q = 2 \cdot p_1 \cdot p_2 \cdot ... \cdot p_n + 1$$

, где $p_1, ..., p_n$ — это n различных нечетных простых чисел.

Такое q задает группу $\mathbb{Z}_q^*$ по умножению по модулю q.

Приведите эффективный (с полимиальной сложностью по времени) алгоритм, который принимает $q, p_1, ..., p_n$ в качестве входных значений и для любого $i \in \{1, ..., n\}$ возвращает элемент $a_i \in \mathbb{Z}_q^*$, такой, что $\mathrm{ord}(a_i) = p_i$.

Материалы

Книги

1. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone *Handbook of Applied Cryptography*
   - ch. 2.5.1 Groups
   - ch. 12.6.1 Diffie-Hellman key agreement
2. R. Lidl, H. Niederreiter *Finite Fields*
3. N. C. Carter *Visual Group Theory*
4. Ch. Paar, J. Pelzl *Understanding Cryptography. A Textbook for Students and Practitioners*
5. (RUS) V. B. Alekseev *Abel's Theorem in Problems and Solutions*

Видео

1. Playlist: Abstract Algebra by Socratica
2. Playlist: Group Theory by Daniil Rudenko
3. Set Theory All-in-One Video by Dr. Will Wood