Математические основы криптографии

Вспомним какие бывают числа (:

Используемые в математике числовые множества включают в себя:

- Натуральные числа — числа, получаемые при естественном счёте:

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

- Целые числа — числа, получаемые объединением натуральных чисел с множеством чисел противоположных натуральным и нулём:

$$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$$

- Рациональные числа — числа, представимые в виде дроби m/n (n ≠ 0), где m — целое число, а n — натуральное число.

$$\mathbb{Q} = \{\dots -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \dots\}$$

- Действительные (вещественные) числа — множество чисел, представляющее собой расширение множества рациональных чисел, включающее иррациональные числа (те, которые нельзя представить в виде дроби с целыми числами, например $\sqrt[3]{2}$)
- Комплексные числа — расширение множества действительных чисел, включающее мнимую единицу $i = \sqrt{-1}$ ($\mathbb{C}$)

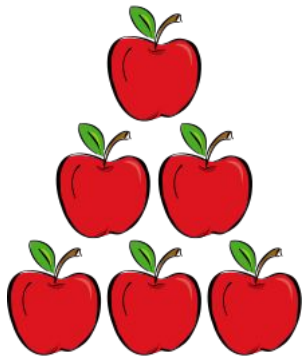
Link:
https://ru.wikipedia.org/wiki/Число

Что для нас важно?

Главным образом в криптографии используются НАТУРАЛЬНЫЕ числа.

Мы не работаем с дробными, иррациональными и комплексными числами.

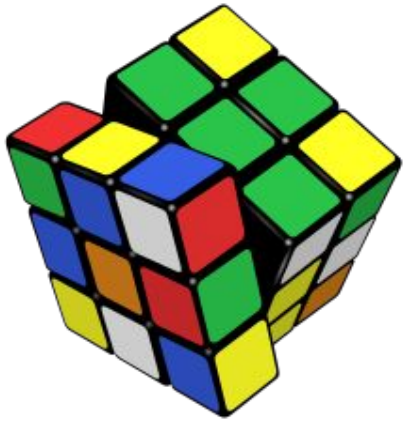
$$\mathbb{N}$$



Что еще для нас важно?

В криптографии как правило используется не бесконечное множество натуральных чисел, а вполне себе конечное.

О чем речь? Об алгебраических структурах.



Алгебраическая структура – некоторое множество элементов (не обязательно чисел) с определенных на ней операциях алгебры.

То есть их бывает много? Как правило 9.

Чтобы понять в чем их отличие нужно разобрать некоторые алгебраические свойства.

Алгебраические свойства

Давайте на время забудем про известные нам операции алгебры, такие как сложение, умножение, деление и т.д.

Вместо этого будем говорить, что у нас есть некоторая неопределенная операция « ∘ »

И пусть она будет бинарной, то есть, операцией над двумя элементами.

Какие алгебраические свойства у операции бывают?

- **Коммутативность** – свойство операции ∘ при которой a ∘ b = b ∘ a

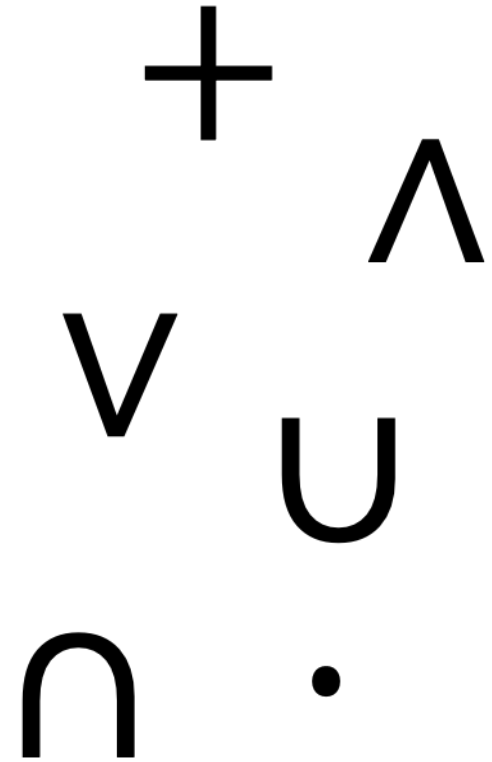
Сможете сказать какие известные вам операции являются коммутативными?

1) Конечно же + (известно со школы – от перестановки слагаемых сумма не меняется). 3+2 = 2+3. Еще?

2) Произведение. Еее, вы знали. 3*2 = 2*3. Может что-то из дискретной математики?

3) Молодец! Конъюнкция и дизъюнкция. А из теории множеств?

4) Объединение, пересечение и симметрическая разность. Супер!



Ок, это было просто, а какие тогда не коммутативны?

1) Хм. Это ты сам догадался или мне послышалось?
Возведение в степень, да. $2^3 \neq 3^2$

2) Матрицы, матрицы... Ага. Перемножение матриц!

$$\begin{pmatrix} 5 & 4 \\ 8 & 0 \end{pmatrix} \begin{pmatrix} 2 & 9 \\ 6 & 1 \end{pmatrix} = \begin{pmatrix} 34 & 49 \\ 16 & 72 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 9 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 8 & 0 \end{pmatrix} = \begin{pmatrix} 82 & 8 \\ 38 & 24 \end{pmatrix}$$

Какие они бывают?

- **Ассоциативность** – свойство операции ∘ при которой (a ∘ b) ∘ c = a ∘ (b ∘ c). Тут и без примеров поймете (:

Дистрибутивность – определяется как проявление двух бинарных операций (бинарные – операции над двумя элементами) (возьмем ∘ и ∴) для которых (a ∘ b) ∴ c = a ∴ c ∘ b ∴ c.

Сложно? Да бросьте!

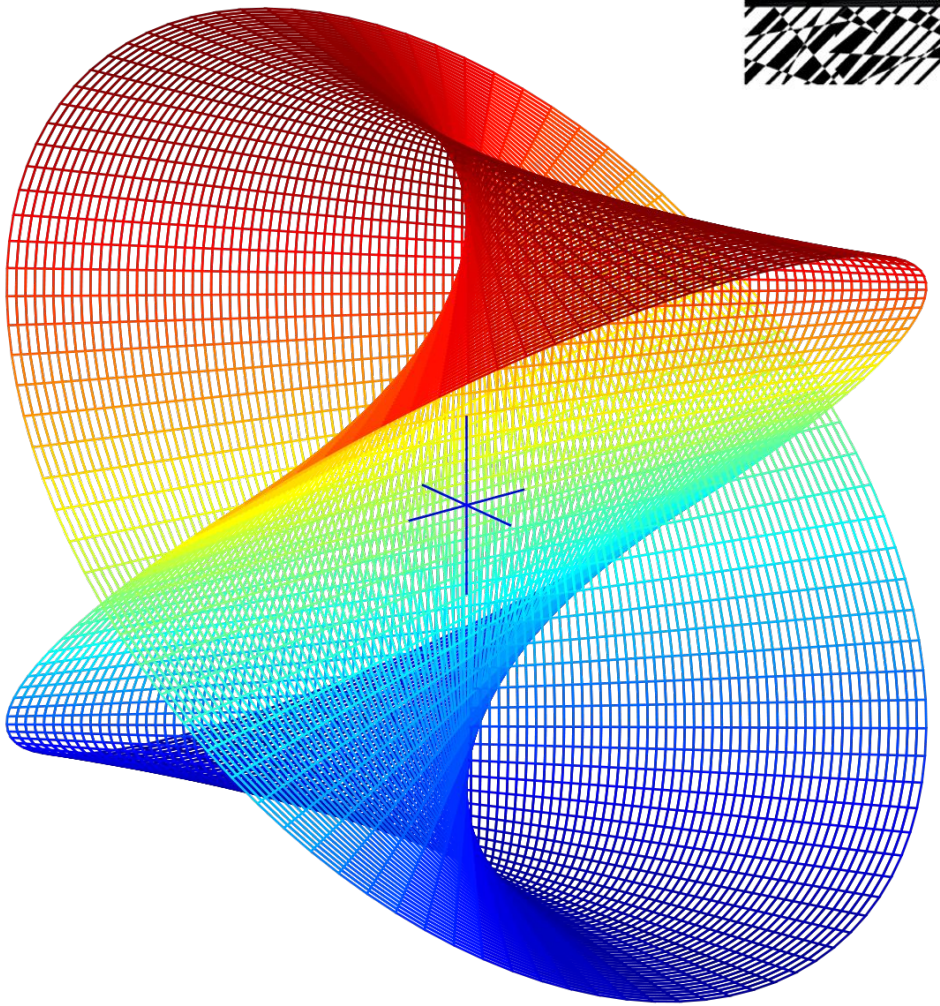
Например, для операций (+, *): (a+b)*c = a*c + b*c

Идемпотентность – когда повторная операция уже не меняет значения. Например, $|-5| = 5$; $||-5||$ = 5 и тд. Сколько бы не брали модуль от модуля ничего уже не изменится ☹ Даже обидно.

Вроде разобрались. У нас есть некоторые операции и свойства этих операций. А еще мы будем работать с натуральными числами.

Все супер, переходим к алгебраическим структурам.

Алгебраические структуры



К основным алгебраическим структурам относятся:

Алгебраические структуры с одной бинарной операцией

- Группоид
- Полугруппа
- Моноид
- Группа

Алгебраические структуры с двумя бинарными операциями

- Кольцо
- Кольцо с единицей
- Коммутативное кольцо
- Тело
- Поле

Группоид (он же «магма»)

- Множество элементов с одной бинарной операцией « · », *которую будем называть «Умножение»*

$$G \times G \to G$$

Эта запись означает, что результатом операции « · » над двумя элементами множества G будет элемент множества G.

$G \times G$ – декартово произведение множества G на себя. Допустим, G – множество из трех элементов $G = \{1,2,3\}$.
Тогда $G \times G$= $\{(1,1), (1,2), (1,3), (2,1), (2,2), (3,1), (3,2), (3,3)\}$ - множество всех возможных пар элементов G.

$G \times G \to G$ означает, что каждой паре элементов G (то бишь, двух элементов, над которыми производится операция « · ») соответствует один элемент множества G (результат операции)

Таким образом, группоид (G, ·) можно представить как отдельную алгебру, где вместо чисел – элементы множества G, а вместо сложения, умножения и прочего – всего одна операция « · ».

Полугруппа

- группоид, в котором «умножение» ассоциативно

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Моноид

- полугруппа с нейтральным элементом.

Группа

- моноид, в котором для каждого элемента a группы можно определить обратный элемент a^{-1}

Коммутативная (Абелева) группа

- Группа, в которой «умножение» коммутативно

$$a \cdot b = b \cdot a$$

Так так так стоп! Ничего не понятно, что за нейтральный элемент, что за обратный элемент и нужны же примеры!

Ок, справедливо. Давайте разберёмся.

Нейтральный элемент

- Нейтральным элементом e называется такой элемент, что для любого x

$$x \cdot e = e \cdot x = x$$

Ничего сложного, правда? Да и вы и сами сможете назвать нейтральный элемент множества натуральных чисел по сложению и умножению.

Итак, по умножению?

«1», ну конечно! $x \cdot 1 = 1 \cdot x = x$

А по сложению?

«0», да. $x + 0 = 0 + x = x$

Обратный элемент

Обратным элементом a^{-1} для некоторого a называется такой элемент, что:

$$a^{-1} \cdot a = e$$

Где e – нейтральный элемент

Что будет обратным элементом для 4 по сложению для множества рациональных чисел (те, что с дробями) -4; $4+(-4) = e = 0$

Что будет обратным элементов для 4 по умножению для множества рациональных чисел (те, что с дробями) $\frac{1}{4}$; $4 * \frac{1}{4} = e = 1$

Кольцо

- Множество с двумя операциями (сложение и умножение), обладающими свойством ассоциативности

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),\ (a+b)+c=a+(b+c)$$

- При этом сложение коммутативно

$$a + b = b + a$$

- Имеется нейтральный элемент по сложению

$$a + 0 = 0 + a = a$$

- Имеется обратный элемент по сложению

$$a + (-a) = (-a) + a = 0$$

- Выполняется дистрибутивность этих двух операций

$$\begin{cases} (a + b) \cdot c = (a \cdot c) + (b \cdot c) \\ c \cdot (a + b) = (c \cdot a) + (c \cdot b) \end{cases}$$

Кольцо с единицей

- Кольцо с нейтральным элементом по умножению

$$a \cdot 1 = 1 \cdot a = a$$

Коммутативное кольцо

- Кольцо с коммутативным умножением

$$a \cdot b = b \cdot a$$

Тело

- Кольцо с единицей, в котором для каждого не нелевого элемента a группы можно определить обратный элемент a^{-1}

Поле

- Группа с четырьмя операциями, имеющие свойства, близкие к свойствам четырех основных операций с числами (сложения, умножения, вычитания, деления)

- Выполняются коммутативность, ассоциативность и дистрибутивность для сложения и умножения

- Имеется нейтральный и обратный элемент по сложению и по умножению

Поле Галуа (конечное поле)

- Поле, количество элементов в котором не бесконечно.

Математические операции

Для работы с криптографическими алгоритмами нам потребуются математические операции, свойства которых важны для криптографии. Начнем с простого.

Простое число

-Число, имеющее два натуральных делителя – себя и единицу. Обозначается p

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61….

Факторизация числа

-Представление числа в виде произведения простых сомножителей

$$a = \sum_{i=1}^{n} p_i^k = p_1^k + p_2^k + \cdots + p_n^k$$

Функция Эйлера

Для работы с криптографическими алгоритмами нам потребуются математические операции, свойства которых важны для криптографии. Начнем с простого.

Простое число

-Функция от натурального n, равная количеству чисел от 1 до n и не имеющих с ним общих делителей, кроме единицы. Обозначается $\varphi(n)$

$$\varphi(1) = 1$$
$$\varphi(2) = 1$$
$$\varphi(3) = 2$$
$$\varphi(4) = 2$$
$$\varphi(5) = 4$$

Свойства

-Если число - простое, $\varphi(p) = p - 1$

-Если число – простое в степени натурального числа, $\varphi(p^a) = p^a - p^{a-1}$

-Если число – произведение двух чисел, не имеющих общих делителей, $\varphi(ab) = \varphi(a) * \varphi(b)$

-Для разложения числа на простые множители

$$a = \sum_{i=1}^{n} p_i^k = p_1^k + p_2^k + \cdots + p_n^k \qquad \varphi(a) = \prod \varphi\left(p_i^k\right) = \prod \left(p^a - p^{a-1}\right)$$

Спасибо за внимание!