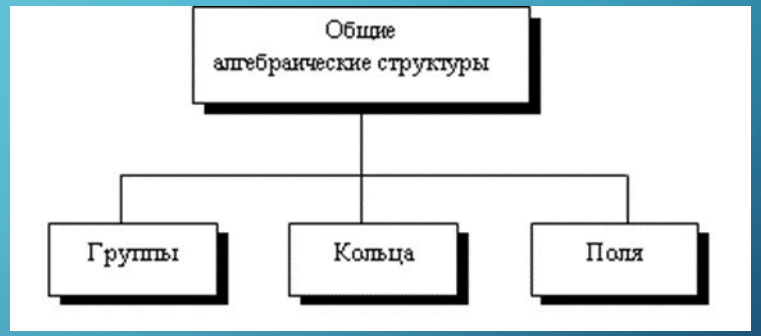
1.2. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ

ПОДГОТОВИЛ: ПРЕПОДАВАТЕЛЬ, К.Т.Н. РОЙ А.В.

МОСКВА, 2019

ВВЕДЕНИЕ

Ранее мы обсуждали некоторые множества чисел, таких как Z, Zn, Zn*, Zp^ и Zp*. Криптография требует, чтобы были заданы множества целых чисел, и операции, определенные для них. Комбинация множеств и операций, которые могут быть применены к элементам множества, называются алгебраической структурой. В этой лекции мы определим три общих алгебраических структуры: группы, кольца и поля



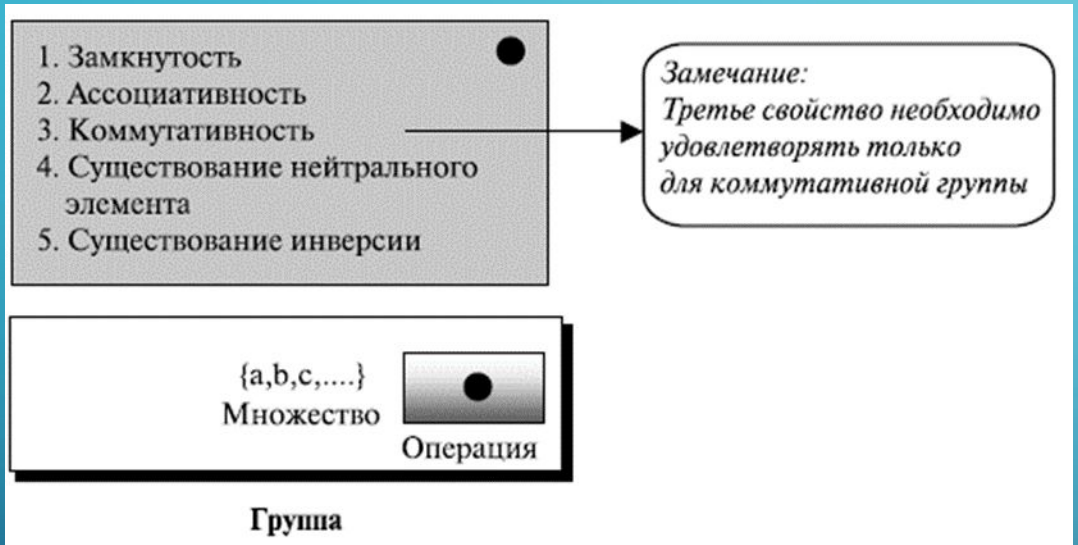
ГРУППЫ

Группа (G) — набор элементов с *бинарной операцией* "•" обладает четырьмя свойствами (или удовлетворяет *аксиомам*), которые будут перечислены ниже.

Коммутативная группа, также называемая **абелева**, — группа, в которой оператор обладает теми же четырьмя свойствами для групп плюс дополнительным — коммутативностью. Эти пять свойств определены ниже

- **Замкнутость**. Если a и b — элементы G, то c = a • b — также элемент G. Это означает, что результат применения операции с любыми двумя элементами множества есть элемент этого множества.
- **Ассоциативность**. Если a, b и c — элементы G, то верно (a• b) • c = a• (b •c) Другими словами, не имеет значения, в каком порядке мы применяем операцию более чем с двумя элементами.
- **Коммутативность**. Для всех a и b в G мы имеем a • b = b • a. Обратите внимание, что это свойство должно быть верно только для коммутативной группы.
- **Существование нейтрального элемента**. Для всех элементов в G существует элемент e, который называется нейтральным элементом, такой, что e • a = a • e = a.
- **Существование инверсии**. Для каждого a в G существует элемент a', называемый инверсией, такой, что a • a' = a' • a = e.

ГРУППЫ



Хотя группа включает единственный оператор, свойства, присущие каждой операции, позволяют использование пары операций, если они — инверсии друг друга. Например, если определенный выше оператор — сложение, то группа поддерживает и сложение, и вычитание, ибо вычитание и сложение — аддитивно инверсные операции. Это также верно для умножения и деления. Однако группа может поддержать только сложение/вычитание или умножение/деление, но не оба сочетания операторов одновременно

ПРИМЕР ГРУППЫ № 1

Множество целых чисел, входящих в вычет с оператором сложения, $G = \langle Z_n, + \rangle$, является коммутативной группой. Мы можем выполнить сложение и вычитание на элементах этого множества, не выходя за его пределы.

Проверим эти свойства.

1. Замкнутость удовлетворяется. Результат сложения двух целых чисел в Z_n — другое целое число в Z_n.
2. Ассоциативность удовлетворяется. Результат $4 + (3 + 2)$ тот же самый, что в случае $(4 + 3) + 2$.
3. Коммутативность удовлетворяется. Мы имеем $3 + 5 = 5 + 3$.
4. Нейтральный элемент — 0. Мы имеем $3 + 0 = 0 + 3 = 3$.
5. Каждый элемент имеет аддитивную инверсию. Инверсия элемента — его дополнение. Например, инверсия 3 — это -3 ($n - 3$ в Z_n), и инверсия -3 — это 3. Инверсия позволяет нам выполнять вычитание на множестве.

ПРИМЕР ГРУППЫ № 2

Множество Z_{n*} с оператором умножения $G = <Z_{n*}, >$, является также абелевой группой. Мы можем выполнить умножение и деление на элементах этого множества, не выходя за его пределы. Это облегчает проверку первых трех свойств. Нейтральный элемент равен 1. Каждый элемент имеет *инверсию*, которая может быть найдена согласно расширенному *алгоритму Евклида*.

ПРИМЕР ГРУППЫ № 3

- Хотя мы обычно представляем группу как множество чисел с обычными операторами, такими, как сложение или вычитание, определения группы позволяют нам определять любое множество объектов и операций, которые удовлетворяют вышеупомянутым свойствам. Определим множество G = <{a, b, c, d,}, •> и операцию, показанную с помощью таблицы.

Таблица 5.1. Таблица операции для примера 5.3

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

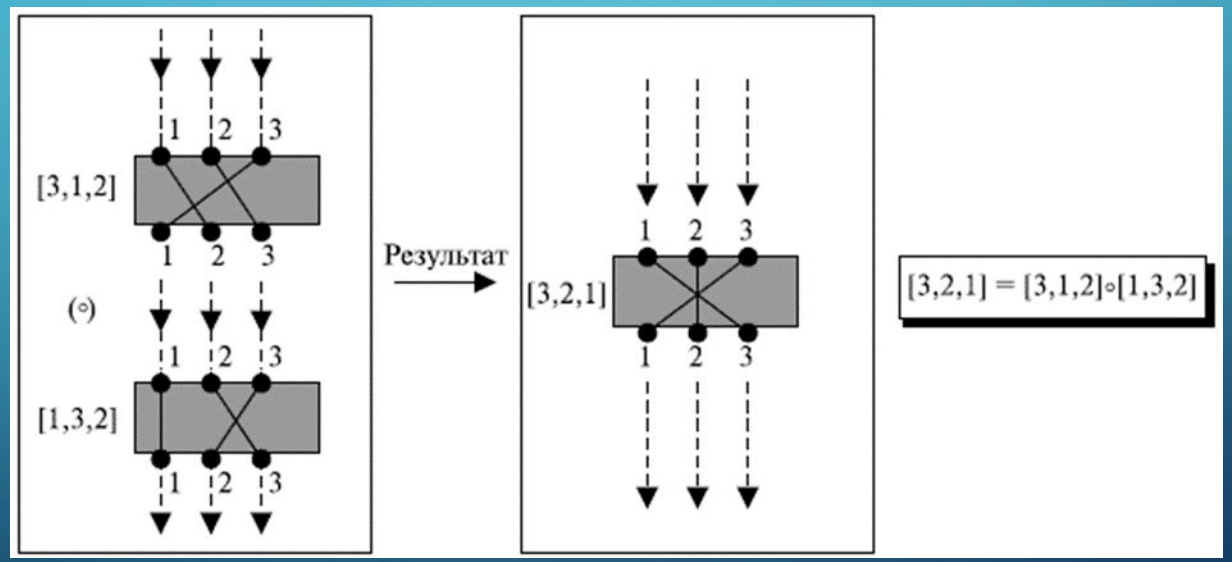
ПРИМЕР ГРУППЫ № 3

Это — абелева группа. Все пять свойств удовлетворены.

1. Замкнутость удовлетворена. Применение оператора на любой паре элементов дает в результате другой элемент этого множества.
2. Ассоциативность также удовлетворена. Чтобы доказать это, мы должны проверить свойство для любой комбинации из трех элементов. Например, (a+ b) + c = a+ (b + c) = d.
3. Операция *коммутативна*. Мы имеем a + b = b + a.
4. Группа имеет нейтральный элемент, которым является a.
5. Каждый элемент имеет *инверсию*. Обратные пары могут быть найдены. В таблице они указаны теневыми элементами в каждой строке. Пары — (a, a), (b, d), (c, c).

ПРИМЕР ГРУППЫ № 4

В группе элементы в множестве не обязательно должны быть числами или объектами; они могут быть правилами, отображениями, функциями или действиями. Очень интересная группа — **группа подстановок**. Множество всех перестановок и оператор является композицией: применения одной перестановки за другой. Рисунок показывает композиции двух перестановок, которые перемещают три входных сигнала, чтобы создать три выходных сигнала.



ПРИМЕР ГРУППЫ № 4

Таблица 5.2. Таблица операции для группы перестановок						
	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

В этом случае удовлетворены только четыре свойства; поэтому группа — не абелева.

1. Замкнутость удовлетворена.
2. Ассоциативность также удовлетворена. Чтобы доказать это, мы должны проверить свойство для любой комбинации из трех элементов.
3. Свойство коммутативности не удовлетворено. Это может быть легко проверено, но мы оставим это для упражнения.
4. Множество имеет нейтральный элемент [1 2 3] (перестановка отсутствует). Эти элементы показаны другим цветом.
5. Каждый элемент имеет инверсию. Обратные пары могут быть найдены, если использовать нейтральные элементы.

ПОДГРУППЫ

Подмножество H группы G — **подгруппа** G, если само H — группа относительно операции на G. Другими словами, если G = <S, •> — группа, то H = <T, •> — группа для той же самой операции, и T — непустое подмножество S, то H — *подгруппа* G. Вышеупомянутое определение подразумевает, что:

1. если a и b — члены обеих групп, то c = a • b — также элемент обеих групп;
2. для группы и подгруппы имеется один и тот же нейтральный элемент;
3. если этот элемент принадлежит обеим группам, *инверсия* a — также элемент обеих групп;
4. группа, полученная с помощью нейтрального элемента G, H = <{e}, •>, является *подгруппой* G ;
5. каждая группа — *подгруппа* самой себя.

ЦИКЛИЧЕСКИЕ ПОДГРУППЫ

Если *подгруппа* группы может быть сгенерирована, используя возведение в степень элемента, то такая *подгруппа* называется **циклической подгруппой**. Термин *возведение в степень* здесь означает многократное применение к элементу групповой операции:

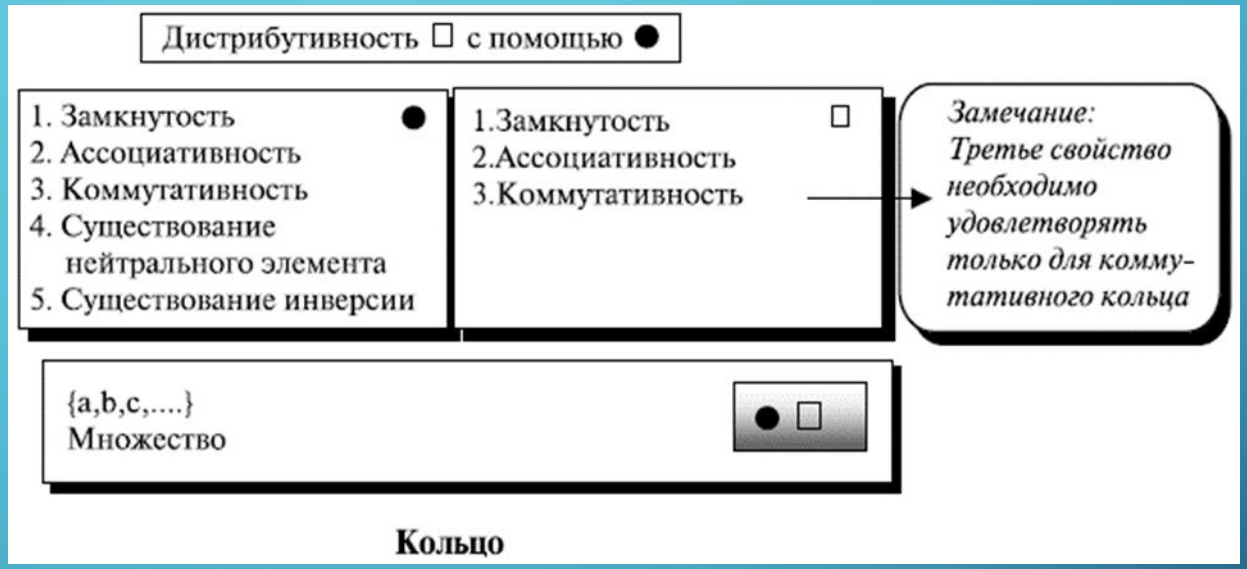
$a^n = a \cdot a \cdot a \cdot \ldots \cdot a$ (n раз)

Множество, полученное в результате этого процесса, обозначается в тексте как <a>. Обратите внимание также, что $a^0 = e$.

ЦИКЛИЧЕСКИЕ ГРУППЫ

Циклическая группа — группа, которая является собственной циклической *подгруппой*. В примере *5.7* группа G имеет циклическую подгруппу $H_5 = G$. Это означает, что группа G — циклическая группа. В этом случае элемент, который генерирует циклическую подгруппу, может также генерировать саму группу. Этот элемент далее именуется "генератор". Если g — генератор, элементы в конечной циклической группе могут быть записаны как $\{e,g,g^2,\ldots\ldots, g^{n-1}\}$, где $g^n = e$.

КОЛЬЦО



Кольцо, обозначенное как R = {…}, •,⊥ - является алгебраической структурой с двумя операциями. Первая операция должна удовлетворять всем пяти свойствам, требуемым для абелевой группы. Вторая операция должна удовлетворять только первым двум свойствам абелевой группы. Кроме того, вторая операция должна быть распределена с помощью первой. Дистрибутивность означает, что для всех a, b и c элементов из R мы имеем a ⊥ (c • b) = (a ⊥ c) • (a ⊥ b) и (a • b) ⊥ c = (a ⊥ c) • (b ⊥ c).

ПОЛЕ

Поле, обозначенное как F = {…}, •,⊥ - это коммутативное кольцо, в котором вторая операция удовлетворяет всем пяти свойствам, определенным для первой операции, за исключением того, что нейтральный элемент первой операции (иногда называемый нулевой элемент) не имеет инверсии. Поле — структура, которая поддерживает две пары операций, используемые в математике: сложение/вычитание и умножение/деление. Есть одно исключение: не разрешено деление на нуль.

ОТЛИЧИЯ АЛГЕБРАИЧЕСКИХ СТРУКТУР

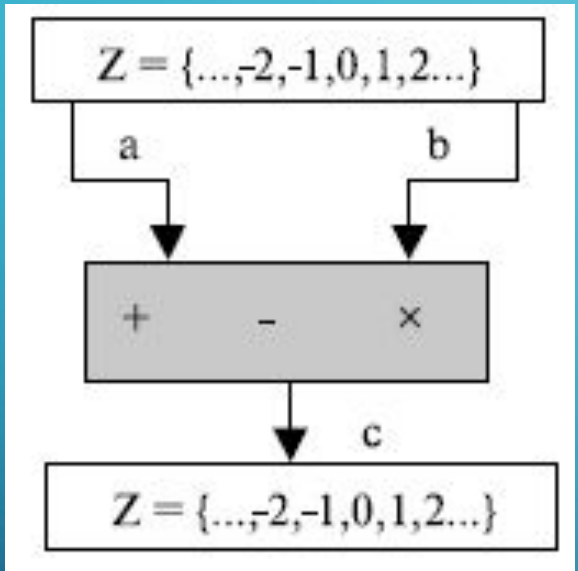
Таблица 5.3. Итоги определения алгебраических структур		
Алгебраическая структура	Используемые операции	Используемые наборы целых чисел
Группа	(+ -) или (x /)	Z_n или Z_n^*
Кольцо	(+ -) и (x)	Z
Поле	(+ -) и (x /)	Z_p

Изучение трех алгебраических структур позволяет нам использовать множества, в которых могут применяться операции, подобные сложению/вычитанию и умножению/делению. Мы должны различать эти три структуры. Первая структура — группа, поддерживает одну пару связанных операций. Вторая структура — кольцо, поддерживает одну пару связанных операций и одну одиночную операцию. Третья структура — поле, поддерживает две пары операций

МНОЖЕСТВО ЦЕЛЫХ ЧИСЕЛ. БИНАРНЫЕ ОПЕРАЦИИ

- Множество целых чисел, обозначенных Z, содержит все числа (без дробей) от минус бесконечности до плюс бесконечности.
- В криптографии нас интересует три бинарных операции в приложении к множеству целых чисел. Бинарные операции имеют два входа и один выход. Для целых чисел определены три общих бинарных операции — сложение, вычитание и умножение. Каждая из этих операций имеет два входа (a и b) и выход (c), как это показано на следующем слайде. Два входа принимают числа из множества целых чисел; выход выводит результат операции — число из множества целых чисел.

ТРИ БИНАРНЫХ ОПЕРАЦИИ ДЛЯ МНОЖЕСТВА ЦЕЛЫХ ЧИСЕЛ



Следующие примеры показывают результаты трех бинарных операций на множестве двух целых чисел. Поскольку каждый вход может быть или положителен или отрицателен, мы имеем четыре случая для каждой операции.

Сложение	5+9=14	(-5)+9=4	5+(-9)=-4	(-5)+(-9)=-14
Вычитание	5-9=-4	(-5)-9=-14	5 - (-9)=14	(-5)- (-9)=+4
Умножение	5 x 9=45	(-5) x 9=-45	5 x (-9)=-45	(-5) x (-9)=45

ДЕЛЕНИЕ ЦЕЛЫХ ЧИСЕЛ

В арифметике целых чисел, если мы a делим на n, мы можем получить q и r. Отношения между этими четырьмя целыми числами можно показать как

$$a = q \cdot n + r$$

В этом равенстве a называется делимое ; q — частное ; n — делитель и r — остаток. Обратите внимание, что это — не операция, поскольку результат деления a на n — это два целых числа, q и r. Мы будем называть это уравнением деления.

ДЕЛЕНИЕ ЦЕЛЫХ ЧИСЕЛ

- Когда мы используем вышеупомянутое уравнение деления в криптографии, мы налагаем два ограничения. Первое требование: чтобы делитель был положительным целым числом ($n > 0$). Второе требование: чтобы остаток был неотрицательным целым числом ($r >= 0$).
- Как можно сделать, чтобы выполнялось ограничение, что число r должно быть положительным? Решение простое: мы уменьшаем значение q на 1 и добавляем значение n к r, чтобы r стало положительным:
- $-255 = (-23 \cdot 11) + (-2)$ $-255 = (-24 \cdot 11) + 9$

ТЕОРИЯ ДЕЛИМОСТИ

- Если a не равно нулю, а r = 0, в равенстве деления мы имеем
  - $a = q \times n$
- Мы тогда говорим, что a делится на n (или n — делитель a). Мы можем также сказать, что a делится без остатка на n. Когда мы не интересуемся значением q, мы можем записать вышеупомянутые отношения как $n \mid a$. Если остаток не является нулевым, то n не делит, и мы можем записать отношения как $n \nmid a$.

СВОЙСТВА ДЕЛИМОСТИ

- **Свойство 1**: если $a \mid 1$, то $a = \pm 1$.
- **Свойство 2**: если $a \mid b$ и $b \mid a$, то $a = \pm b$
- **Свойство 3**: если $a \mid b$ и $b \mid c$, то $a \mid c$
- **Свойство 4**: если $a \mid b$ и $a \mid c$, то $a \mid (m \times b + n \times c)$, где m и n — произвольные целые числа.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

- Одно целое число, часто необходимое в криптографии, — наибольший общий делитель двух положительных целых чисел. Два положительных целых числа могут иметь много общих делителей, но только один наибольший общий делитель. Например, общие делители чисел 12 и 140 есть 1, 2 и 4. Однако наибольший общий делитель.
- Наибольший общий делитель двух положительных целых чисел — наибольшее целое число, которое делит оба целых числа.

ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

- Каждое натуральное число, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется **простым**, а если у числа есть еще делители, то **составным**. Единица же не считается ни простым числом, ни составным. Например, числа 7, 29 — простые; числа 9, 15 — составные (9 делится на 3, 15 делится на 3 и на 5).
- Интересный факт: если два простых числа отличаются на 2, то их называют числами-"близнецами". Чисел-"близнецов" не очень много. Например, "близнецами" являются 5 и 7, 29 и 31, 149 и 151, а также $242\,206\,083 * 2^{38\,880} \pm 1$ (наибольшая найденная на момент написания учебного пособия пара "близнецов").

ФАКТОРИЗАЦИЯ ПРОСТЫХ ЧИСЕЛ

- Поиск больших простых чисел имеет важное значение для математики и не только. Например, в криптографии большие простые числа используются в алгоритмах шифрования с открытым ключом. Для обеспечения надежности шифрования там используются простые числа длиной до 1024 бит.
- Перемножить два числа сравнительно нетрудно, особенно если у нас есть калькулятор, а числа не слишком велики. Существует и обратная задача – *задача факторизации* – нахождение двух или более чисел, дающих при перемножении заданное число. Эта задача гораздо труднее, чем перемножение чисел, и любому, кто пытался ее решить, об этом известно. Сложность задачи факторизации используется в

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

- В математике рассматривается так называемая основная теорема арифметики, которая утверждает, что любое натуральное число (n>1) либо само является простым, либо может быть разложено на произведение простых делителей, причем единственным способом (если не обращать внимания на порядок следования сомножителей). Воспользовавшись обозначением степени, разложение числа 2009 на простые множители можно записать так: 2009 = 72 * 41
- Разложение на множители называется каноническим, если все множители являются простыми и записаны в порядке возрастания. Например, запишем каноническое разложение числа 150 на

ВЗАИМНО ПРОСТЫЕ ЧИСЛА

- Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы. Например, числа 11 и 12 взаимно просты (у них нет общих делителей кроме единицы), числа 30 и 35 — нет (у них есть общий делитель 5).
- Исследованием закономерностей, связанных с целыми числами, долго занимался швейцарский математик Леонард Эйлер. Одним из вопросов, которым он интересовался, был следующий: сколько существует натуральных чисел, не превосходящих n и взаимно простых с n? Ответ на этот вопрос был получен Эйлером в 1763 году и этот ответ связан с каноническим разложением числа n на простые множители.

ФУНКЦИЯ ЭЙЛЕРА

- Если $n = p1^{a1} \cdot p2^{a2} \cdot p3^{a3} \cdot \ldots \cdot p_n^{a\,n}$, где p1, p2, p3… - простые множители, то число ϕ натуральных чисел , не превосходящих n и взаимно простых с n можно точно определить по формуле: $\phi(n) = n \cdot 1/(1-p1) \cdot 1/(1-p2) \cdot 1/(1-p3) \cdot \ldots \cdot 1/(1-p_n)$, которая называется функцией Эйлера. Формулу Эйлера удобно использовать для больших n, если известно разложение числа n на простые множители. Для криптографии формула Эйлера важна тем, что она позволяет легко получить число $\phi(n)$ для простых и некоторых других чисел. Это гораздо удобнее, чем рассматривать все числа из довольно большого диапазона и