КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 5

Математические основы криптографии: исследование колец классов вычетов

Данный материал демонстрирует разбор задания, посвященного исследованию колец классов вычетов.

Кольца классов вычетов представляют собой класс колец, нашедший широкое применение в криптографии. Данное понятие тесно связано с так называемой арифметикой остатков, когда задается некоторое натуральное число n, и все целые числа рассматриваются как их остатки от деления на n. При этом разные числа, имеющие одинаковый остаток r от деления на n, объединяются в одно множество, называемое классом вычетов r. Говорят еще, что такие числа сравнимы друг с другом по модулю n. Множество классов вычетов $\mathbb{Z}_n$ образует кольцо, в котором операции сложения и умножения классов вычетов реализуются через сложение и умножение их представителей с приведением результата по модулю n.

Исследование кольца классов вычетов $\mathbb{Z}_n$ сводится к исследованию группы обратимых элементов $\mathbb{Z}_n^*$ данного кольца. Поэтому, в первую очередь, необходимо найти все обратимые элементы кольца $\mathbb{Z}_n$, пользуясь теоремой–критерием обратимости элементов $\mathbb{Z}_n$, и составить из них группу $\mathbb{Z}_n^*$. Чтобы исследовать группу $\mathbb{Z}_n^*$, необходимо выполнить следующее:

- найти порядок всех элементов группы $\mathbb{Z}_n^*$;
- установить, является ли группа $\mathbb{Z}_n^*$ циклической, и при положительном исходе найти все ее образующие элементы;
- найти все циклические подгруппы группы $\mathbb{Z}_n^*$;
- составить диаграмму, описывающую внутреннее устройство группы $\mathbb{Z}_n^*$.

При выполнении данного задания необходимо опираться на свойства абстрактных циклических групп и навыки, приобретенные при исследовании подобных групп.

Пример.

Исследовать кольцо классов вычетов $\mathbb{Z}_{15}$.

Решение.

Данное кольцо классов вычетов состоит из 15 элементов и может быть записано следующим образом: $\mathbb{Z}_{15} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}\}$.

Составим группу обратимых элементов данного кольца классов вычетов и исследуем ее.

В соответствии с критерием обратимости элементов кольца классов вычетов, ненулевой элемент $\bar{s}$ кольца $\mathbb{Z}_n$ является обратимым тогда и только тогда, когда НОД$(s, n) = 1$.

Последовательно проверим ненулевые элементы кольца $\mathbb{Z}_{15}$, отличные от $\bar{1}$, на взаимную простоту их наименьших представителей с числом 15. Для $\bar{1}$ такая проверка является избыточной, поскольку 1 представляет собой число, взаимно простое с любым другим числом.

НОД$(2,15) = 1$, следовательно $\overline{2} \in \mathbb{Z}_{15}^*$.

НОД$(3,15) = 3$, следовательно $\overline{3} \notin \mathbb{Z}_{15}^*$.

НОД$(4,15) = 1$, следовательно $\overline{4} \in \mathbb{Z}_{15}^*$.

НОД$(5,15) = 5$, следовательно $\overline{5} \notin \mathbb{Z}_{15}^*$.

НОД$(6,15) = 3$, следовательно $\overline{6} \notin \mathbb{Z}_{15}^*$.

НОД$(7,15) = 1$, следовательно $\overline{7} \in \mathbb{Z}_{15}^*$.

НОД$(8,15) = 1$, следовательно $\overline{8} \in \mathbb{Z}_{15}^*$.

НОД$(9,15) = 3$, следовательно $\overline{9} \notin \mathbb{Z}_{15}^*$.

НОД$(10,15) = 5$, следовательно $\overline{10} \notin \mathbb{Z}_{15}^*$.

НОД$(11,15) = 1$, следовательно $\overline{11} \in \mathbb{Z}_{15}^*$.

НОД$(12,15) = 3$, следовательно $\overline{12} \notin \mathbb{Z}_{15}^*$.

НОД$(13,15) = 1$, следовательно $\overline{13} \in \mathbb{Z}_{15}^*$.

НОД$(14,15) = 1$, следовательно $\overline{14} \in \mathbb{Z}_{15}^*$.

Таким образом, группа обратимых элементов кольца классов вычетов по модулю 15 имеет следующий вид: $\mathbb{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$.

Определим порядок всех элементов построенной группы $\mathbb{Z}_{15}^*$. Для единицы группы $\overline{1}$ порядок очевидно равен 1, поскольку 1 — это наименьшая натуральная степень, при возведении в которую единица группы обращается в единицу группы: $O(\overline{1}) = 1$.

Для всех прочих элементов необходимо выполнить последовательное возведение в различные степени до получения единицы группы.

Начнем с $\overline{2}$.

$\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^4 = \overline{16} = \overline{1}$, следовательно, $O(\overline{2}) = 4$. Более того, из проделанных вычислений следует, что $\overline{2}$ порождает четыре различных элемента группы $\mathbb{Z}_{15}^*$ и, значит, является образующим элементом циклической подгруппы порядка 4, составленной из этих элементов.

Запишем эту группу:

$H_1 = \langle \overline{2} \rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$, $H_1 \leq \mathbb{Z}_{15}^*$.

Имея циклическую группу данного порядка и зная, какой степени образующего соответствует каждый элемент группы, можно легко определить порядок всех ее элементов. Таким образом, нет необходимости выполнять возведение элементов $\overline{4}$ и $\overline{8}$ в различные степени до получения $\overline{1}$, поскольку можно легко определить порядок каждого из этих элементов, пользуясь свойствами циклических групп.

$O(\overline{4}) = 2$, так как $O(\overline{2}) = 4$ и $\overline{4} = \overline{2}^2$. При этом $\overline{4}$ является образующим элементом циклической подгруппы порядка 2:

$H_2 = \langle \overline{4} \rangle = \{\overline{1}, \overline{4}\}$, $H_2 \leq H_1 \leq \mathbb{Z}_{15}^*$.

$O(\overline{8}) = 4$, так как $O(\overline{2}) = 4$, $\overline{8} = \overline{2}^3$ и НОД$(3,4) = 1$. Это означает, что $\overline{8}$, как и $\overline{2}$, является образующим циклической подгруппы H_1:

$H_1 = \langle \overline{2} \rangle = \langle \overline{8} \rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$, $H_1 \leq \mathbb{Z}_{15}^*$.

Следующим элементом, порядок которого еще неизвестен, является $\overline{7}$.

$\overline{7}^2 = \overline{49} = \overline{4}$, $\quad \overline{7}^3 = \overline{7}^2 \cdot \overline{7} = \overline{4} \cdot \overline{7} = \overline{28} = \overline{13}$, $\quad \overline{7}^4 = (\overline{7}^2)^2 = \overline{4}^2 = \overline{16} = \overline{1}$, из чего следует, что $O(\overline{7}) = 4$. Отметим, что при расчете $\overline{7}^3$ и $\overline{7}^4$ был использован стандартный для арифметики остатков прием: в последующих вычислениях используется результат предыдущих вычислений, приведенный по модулю. Это позволяет вычисления, особенно при работе с достаточно большими числами.

Итак, $O(\overline{7}) = 4$, значит, $\overline{7}$ является образующим элементом циклической группы порядка 4. Кроме того, из проделанных вычислений следует, что $O(\overline{4}) = 2$ и $O(\overline{13}) = 4$. Первое значение согласуется с выводами, сделанными при исследовании $\overline{2}$. Второе значение говорит о том, что $\overline{13}$ является образующим той же циклической группы, что и $\overline{7}$. Запишем эту группу:

$H_3 = \langle\overline{7}\rangle = \langle\overline{13}\rangle = \{\overline{1}, \overline{4}, \overline{7}, \overline{13}\}$, $H_3 \le \mathbb{Z}_{15}^*$, причем $H_2 = \langle\overline{4}\rangle = \{\overline{1}, \overline{4}\} \le H_3$.

На данном этапе исследования можно сделать вывод, что группа $\mathbb{Z}_{15}^*$ не является циклической, поскольку циклическая группа не может содержать двух различных циклических подгрупп одного порядка. Это следует из теоремы, обратной к теореме Лагранжа. В рассматриваемом же примере $H_1 \le \mathbb{Z}_{15}^*$ и $H_3 \le \mathbb{Z}_{15}^*$, причем $|H_1| = |H_3|$, но $H_1 \ne H_3$.

Осталось установить порядок двух элементов.

$\overline{11}^2 = \overline{121} = \overline{1}$, следовательно $O(\overline{11}) = 2$ и $H_4 = \langle\overline{11}\rangle = \{\overline{1}, \overline{11}\}$, $H_4 \le \mathbb{Z}_{15}^*$.

$\overline{14}^2 = (-\overline{1})^2 = \overline{1}$, следовательно $O(\overline{14}) = 2$ и $H_5 = \langle\overline{14}\rangle = \{\overline{1}, \overline{14}\}$, $H_5 \le \mathbb{Z}_{15}^*$.

При расчете $\overline{14}^2$ был использован еще один стандартный для арифметики остатков прием: замена положительного вычета отрицательным вычетом, меньшим по абсолютному значению.

Таким образом, в группа $\mathbb{Z}_{15}^*$ нет элемента, который бы ее порождал, поэтому данная группа не является циклической. При этом группа $\mathbb{Z}_{15}^*$ содержит пять нетривиальных циклических подгрупп: три подгруппы порядка 2 и две подгруппы порядка 4.