Математические основы криптологии

Автор курса: Применко Эдуард Андреевич
Составитель: Смирнов Дмитрий Константинович

2022 г.

Оглавление

Глава 1

Домашние задания

1.1 Элементы теории групп

Задачи в этом разделе решаются со следующими параметрами:

p	g	k
23	-8	22

Убедиться, что $g \in Z_p^*$ – примитивный элемент Z_p.

Так как $p = 23$ – простое число, то $\phi(p) = p - 1 = 22$. Разложим это число на простые множители: $\phi(p) = 2 \cdot 11$. Тогда достаточно проверить следующие 2 неравенства:

$$g^{\frac{\phi(p)}{2}} = (-8)^{11} = 15 \cdot 15^{10} = 15 \cdot 18^5 = 17 \cdot 2^2 = 22 \not\equiv 1 \pmod{p},$$

$$g^{\frac{\phi(p)}{11}} = (-8)^2 = 18 \not\equiv 1 \pmod{p},$$

и одно равенство:

$$g^{\phi(p)} = (-8)^{22} = 18^{11} = 18 \cdot 2^5 = 18 \cdot 9 \equiv 1 \pmod{p}.$$

Делаем вывод, что g действительно является примитивным элементом Z_p.

Найти образующий элемент h группы $Z_{p^2}^*$

Образующий элемент группы $Z_{p^n}^*, n \geq 2$ имеет вид:

$$h = g + t_0 p,\ t_0 \not\equiv g\nu \pmod{p};\ \nu = \left(\frac{g^{\frac{p-1}{2}} + 1}{p}\right) \cdot (-2)^{-1}$$

Таким образом,

$$\nu = \left(\frac{(-8)^{\frac{23-1}{2}} + 1}{23}\right) \cdot (-2)^{-1} = (1 \cdot (-2)^{-1}) = 21$$

$$t_0 \not\equiv (-8) \cdot 21 \pmod{23} = 16 \pmod{23}$$

$$t_1 = 1 \Rightarrow h = (-8) + 1 * 23 = 15$$

Следовательно, $h = 15$ – образующий элемент группы $Z^*_{23^2}$

Подсчитать число образующих группы $Z^*_{p^3}$

Найти элемент a группы $Z^*_{p^2}$ порядка k

Глава 2

Билеты

2.1 **Делимость в кольце целых чисел. НОД, алгоритм Евклида. Критерий взаимной простоты двух чисел.**

2.2 **Сравнения и их свойства. Китайская теорема об остатках. Кольцо вычетов. Функция Эйлера и её свойства.**

2.3 **Теоремы Эйлера и Ферма. Критерий обратимости, алгоритм вычисления обратного элемента.**

2.4 **Криптографическая теорема (обоснование криптосистемы RCA).**

2.5 **Теорема о цикличности мультипликативной группы по примарному модулю.**

2.6 **Решение сравнений первой степени.**

2.7 **Сравнения второй степени. Символ Лежандра и его свойства.**

2.8 **Алгоритмы решения сравнений второй степени по простому модулю.**

2.9 **Символ Якоби и его свойства. Числа Блюма и их свойства. Эквивалентность задачи факторизации и решения сравнения второй степени.**

2.10 **Алгоритмы решения сравнений второй степени по примарному и составному модулю.**

2.12 Нормальный делитель, фактор – группа, первая теорема о гомоморфизме.

2.13 Кольцо многочленов, идеал, теорема Безу, кольцо главных идеалов.

2.14 Конечное поле. Теорема о простом подполе конечного поля. Строение конечного поля. Теорема о примитивном элементе.

2.15 Построение конечных полей. Алгоритм вычисления обратного элемента. Арифметические операции в конечном поле.

2.16 Алгоритмы вычисления дискретного алгоритма.

2.17 Криптосистема Эль - Гамаля. Протокл Диффи - Хеллмана.

2.18 Минимальный многочлен и его свойства. Теорема об изоморфизме конечных полей одной мощности.

2.19 Примитивный многочлен и его свойства. Теорема о разложении многочлена $f(x) = xp^{n\smile}x$ на неприводимые многочлены. Критерий принадлежности элемента поля собственному подполю.

2.20 Теорема о группе автоморфизмов конечного поля.

2.21 Рекуррентные последовательности над конечным полем, линейные рекуррентные последовательности (ЛРП). Характеристический и минимальный многочлен ЛРП и их свойства.

2.22 Теорема об определении структуры ЛРП по её характеристическому многочлену. Теорема о ЛРП максимального периода.

2.23 Прямое произведение групп. Теорема о пред-

2.25 **Теорема о разложении конечной абелевой группы в произведение своих циклических подгрупп.**

2.26 **Нормализатор, централизатор, класс сопряженных элементов конечной группы. Теорема о числе множеств сопряженных с данным. Теорема о центре примарной группы. Теорема Коши.**

2.27 **Двойные смежные классы и их свойства. Теорема Силова (первая)**

2.28 **Вторая и третья теоремы Силова.**

2.29 **Группы подстановок. Инвариантное множество, орбита. Теорема об индексе стабилизатора группы. Теорема о транзитвности нормализатора подгруппы транзитвной группы. (Ут . 13.4).**

2.30 **Лемма Бернсайда.**

2.31 **Регулярные и полурегулярные группы. Порядок полурегулярной группы.**

2.32 **Блоки и импримитивные группы. Критерий импримитивности. Теорема о импримитивности транзитивной группы с интранзитивным нормальным делителем.**

2.33 **Примитивные группы. Кратная транзитивность. Критерий кратной транзитивности.**

2.34 **Теорема о группе автоморфизмов конечной группы.**

2.35 **Утверждение об изоморфизме стабилизатора и специальной группы автоморфизмов регулярной подгруппы (Ут . 13.5). Утверждение о порядке регулярного нормального делителя кратно транзитивной группы.**

2.36 **Простая группа. Теорема о простоте знакопеременной группы. Теорема о нормальном**