

# Математические основы криптологии

Автор курса: Применко Эдуард Андреевич  
Составитель: Смирнов Дмитрий Константинович

2022 г.

# Оглавление

<b>1</b>	<b>Домашние задания</b>	<b>1</b>
1.1	Элементы теории групп . . . . .	1
1.2	. . . . .	3
<b>2</b>	<b>Билеты</b>	<b>3</b>
2.1	Делимость в кольце целых чисел. НОД, алгоритм Евклида. Критерий взаимной простоты двух чисел. . . . .	3
2.2	Сравнения и их свойства. Китайская теорема об остатках. Кольцо вычетов. Функция Эйлера и её свойства. . . . .	3
2.3	Теоремы Эйлера и Ферма. Критерий обратимости, алгоритм вычисления обратного элемента. . . . .	3
2.4	Криптографическая теорема (обоснование криптосистемы RSA). . . . .	3
2.5	Теорема о цикличности мультипликативной группы по простому модулю. . . . .	3
2.6	Решение сравнений первой степени. . . . .	3
2.7	Сравнения второй степени. Символ Лежандра и его свойства. . . . .	3
2.8	Алгоритмы решения сравнений второй степени по простому модулю. . . . .	3
2.9	Символ Якоби и его свойства. Числа Блюма и их свойства. Эквивалентность задачи факторизации и решения сравнения второй степени. . . . .	3
2.10	Алгоритмы решения сравнений второй степени по простому и составному модулю. . . . .	3
2.11	Группа, порядок элемента. Теорема Лагранжа. . . . .	3
2.12	Нормальный делитель, фактор – группа, первая теорема о гомоморфизме. . . . .	4
2.13	Кольцо многочленов, идеал, теорема Безу, кольцо главных идеалов. . . . .	4
2.14	Конечное поле. Теорема о простом подполе конечного поля. Строение конечного поля. Теорема о примитивном элементе. . . . .	4

2.15 Построение конечных полей. Алгоритм вычисления обратного элемента. Арифметические операции в конечном поле.	4
2.16 Алгоритмы вычисления дискретного алгоритма. . . . .	4
2.17 Криптосистема Эль - Гамала. Протокол Диффи - Хеллмана.	4
2.18 Минимальный многочлен и его свойства. Теорема об изоморфизме конечных полей одной мощности. . . . .	4
2.19 Примитивный многочлен и его свойства. Теорема о разложении многочлена $f(x) = x^{p^n} - x$ на неприводимые многочлены. Критерий принадлежности элемента поля собственному подполю. . . . .	4
2.20 Теорема о группе автоморфизмов конечного поля. . . . .	4
2.21 Рекуррентные последовательности над конечным полем, линейные рекуррентные последовательности (ЛРП). Характеристический и минимальный многочлен ЛРП и их свойства. . . . .	4
2.22 Теорема об определении структуры ЛРП по её характеристическому многочлену. Теорема о ЛРП максимального периода. . . . .	4
2.23 Прямое произведение групп. Теорема о представлении группы в виде прямого произведения своих подгрупп. . . . .	4
2.24 Теорема о примарной абелевой группе. . . . .	4
2.25 Теорема о разложении конечной абелевой группы в произведение своих циклических подгрупп. . . . .	5
2.26 Нормализатор, централизатор, класс сопряженных элементов конечной группы. Теорема о числе множеств сопряженных с данным. Теорема о центре примарной группы. Теорема Коши. . . . .	5
2.27 Двойные смежные классы и их свойства. Теорема Силова (первая) . . . . .	5
2.28 Вторая и третья теоремы Силова. . . . .	5
2.29 Группы подстановок. Инвариантное множество, орбита. Теорема об индексе стабилизатора группы. Теорема о транзитивности нормализатора подгруппы транзитивной группы. (Ут . 13.4). . . . .	5
2.30 Лемма Бернсайда. . . . .	5
2.31 Регулярные и полурегулярные группы. Порядок полурегулярной группы. . . . .	5
2.32 Блоки и импримитивные группы. Критерий импримитивности. Теорема о импримитивности транзитивной группы с интранзитивным нормальным делителем. . . . .	5
2.33 Примитивные группы. Кратная транзитивность. Критерий кратной транзитивности. . . . .	5
2.34 Теорема о группе автоморфизмов конечной группы. . . . .	5

2.35	Утверждение об изоморфизме стабилизатора и специальной группы автоморфизмов регулярной подгруппы (Ут . 13.5). Утверждение о порядке регулярного нормального делителя кратно транзитивной группы. . . . .	5
2.36	Простая группа. Теорема о простоте знакопеременной группы. Теорема о нормальном делителе симметрической группы. . . . .	5

## Часть 1

# Домашние задания

### 1.1 Элементы теории групп

Задачи в этом разделе решаются со следующими параметрами:

p	g	k
23	-8	22

**Задача 1.1** Убедиться, что  $g \in \mathbb{Z}_p^*$  – примитивный элемент  $\mathbb{Z}_p$ .

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  $\mathbb{Z}_p$ .

**Задача 1.2** Найти образующий элемент  $h$  группы  $\mathbb{Z}_{p^2}^*$

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

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

Таким образом,

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

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

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

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

**Задача 1.3** Подсчитать число образующих группы  $\mathbb{Z}_{p^3}^*$

Число образующих группы  $\mathbb{Z}_{23^3}^*$  равно  $\phi(23^3) = (23-1)23^{3-1} = 11638$ .

**Задача 1.4** Найти элемент  $a$  группы  $\mathbb{Z}_{p^2}^*$  порядка  $k$

Так как  $\forall$  натурального  $k > 1$  и простого  $p \geq 3$  группа  $\mathbb{Z}_{p^k}^*$  является циклической, то  $\mathbb{Z}_{23^2}^*$  – циклическая группа. Элемент порядка  $k$  в циклической группе порядка  $N$  имеет вид  $h^r$ , где  $r = \frac{N}{k}$ . Таким образом,

$$a = h^{\frac{\phi(p^2)}{k}} = 15^{\frac{22 \cdot 23}{22}} = 15^{23} = 130$$

**Задача 1.5** Решить сравнение  $a^x \equiv b \pmod{p}$

p	a	b
701	2	163

1. Убедимся в том, что  $a = 2$  – примитивный элемент группы  $\mathbb{Z}_{701}$ .

$$\phi(701) = 700 = 2^2 \cdot 5^2 \cdot 7$$

$$g^{\frac{\phi(p)}{2}} = 2^{350} = 700 \not\equiv 1 \pmod{p},$$

$$g^{\frac{\phi(p)}{5}} = 2^{140} = 210 \not\equiv 1 \pmod{p},$$

$$g^{\frac{\phi(p)}{7}} = 2^{100} = 19 \not\equiv 1 \pmod{p},$$

$$g^{\phi(p)} = 2^{700} = 1 \equiv 1 \pmod{p},$$

Таким образом, порядок элемента  $a$  равен  $ord(a) = 700$ .

2. Выбираем минимальное  $m: m^2 \geq ord(a) \Rightarrow m = 27$ .

3. Вычисляем  $c = a^m = 2^{27} = 62$ .

4. Составляем два множества:

$i$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$c^i$	62	339	689	658	138	144	516	447	375	117	244	407	699	577

$i$	15	16	17	18	19	20	21	22	23	24	25	26	27
$c^i$	23	24	86	425	413	370	508	652	467	213	588	4	248

$j$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$ba^j$	163	326	652	603	505	309	618	535	369	37	74	148	296	592

$j$	14	15	16	17	18	19	20	21	22	23	24	25	26
$ba^j$	483	265	530	359	17	34	68	136	272	544	387	73	146

В таблицах совпадают элементы под номерами  $i = 22$  и  $j = 2$ .

5. Таким образом,  $x = mi - j = 27 \cdot 22 - 2 = 592$ .

Ответ:  $x = 592$ .

## 1.2

## Часть 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 RSA).
- 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 Блума 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 - Гамала. Протокол 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  $f(x) = x^{p^n} - x$  на неприводимые многочлены. Критерий принадлежности элемента поля собственному под полю.
- 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 транзитивности нормализатора подгруппы транзитивной 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 знако-