

# Математические основы криптологии

Автор курса: Применко Эдуард Андреевич  
Составитель: Смирнов Дмитрий Константинович

Версия от 13:58, 16 июня 2022 г.

# Оглавление

<b>1</b>	<b>Домашние задания</b>	<b>1</b>
1.1	Теоретико-числовые методы и алгоритмы . . . . .	2
1.2	Квадратичные вычеты, сравнения, символ Лежандра. . . .	5
1.3	Рекуррентные последовательности. . . . .	9
1.4	Шифр гаммирования . . . . .	11
1.5	Теория групп . . . . .	12

## Часть 1

# Домашние задания

## 1.1 Теоретико-числовые методы и алгоритмы

Задачи в этом разделе решаются со следующими параметрами:

<b>p</b>	<b>g</b>	<b>k</b>
23	-8	22

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

**Решение.**

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:

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

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

Делаем вывод, что  $g$  действительно является примитивным элементом  $\mathbb{Z}_p$ .

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

**Решение.**

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,

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

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

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

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

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

**Решение.**

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  $k$

**Решение.**

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  $a^x \equiv b \pmod{p}$

**Решение.**

p	a	b
701	2	163

### I. Алгоритм согласования

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  $\text{ord}(a) = 700$ .

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

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:  $x = 592$ .

### II. Алгоритм Полига-Хеллмана

Порядок поля  $\mathbb{Z}_{701}$  равен  $N = \phi(701) = 700 = 2^2 \cdot 5^2 \cdot 7$ . Количество простых множителей в разложении этого числа  $t = 3$ .

1. Вычисляем матрицу с элементами  $(i, j) = a^{j \frac{N}{p_i}}, i = \overline{1, t}, j = \overline{0, p_i - 1}$ :

$\begin{matrix} j \\ p_i \end{matrix}$	0	1	2	3	4	5	6
2	$2^{0 \cdot \frac{700}{2}}$	$2^{1 \cdot \frac{700}{2}}$	-	-	-	-	-
5	$2^{0 \cdot \frac{700}{5}}$	$2^{1 \cdot \frac{700}{5}}$	$2^{2 \cdot \frac{700}{5}}$	$2^{3 \cdot \frac{700}{5}}$	$2^{4 \cdot \frac{700}{5}}$	-	-
7	$2^{0 \cdot \frac{700}{7}}$	$2^{1 \cdot \frac{700}{7}}$	$2^{2 \cdot \frac{700}{7}}$	$2^{3 \cdot \frac{700}{7}}$	$2^{4 \cdot \frac{700}{7}}$	$2^{5 \cdot \frac{700}{7}}$	$2^{6 \cdot \frac{700}{7}}$

$\begin{matrix} j \\ p_i \end{matrix}$	0	1	2	3	4	5	6
2	1	700	-	-	-	-	-
5	1	210	638	89	464	-	-
7	1	19	361	550	636	167	369

2. Далее находим  $x_i = \log_a b \pmod{p_i^{k_i}} = \gamma_0 + \gamma_1 p_i + \dots + \gamma_{k_i-1} p_i^{k_i-1}, \gamma_j \in \mathbb{Z}_p$ .

Последовательно находим  $\gamma_j$  из  $M(p, \gamma_j) = b_j^{\frac{N}{p^{j+1}}}$ , где  $b_j = ba^{-\gamma_0 - \gamma_1 p - \dots - \gamma_{j-1} p^{j-1}}$ , а  $M$  – определённая выше матрица.

а)  $x_1 = \log_2 163 \pmod{2^2}$ ,  $p = 2$ ,  $k = 2$

$$M(p, \gamma_0) = b^{\frac{N}{p}} = 163^{\frac{700}{2}} = 1 \Rightarrow \gamma_0 = 0, \quad b_1 = ba^{-\gamma_0} = 163 \cdot 2^{-0} = 163$$

$$M(p, \gamma_1) = b_1^{\frac{N}{p^2}} = 163^{\frac{700}{4}} = 1 \Rightarrow \gamma_1 = 0$$

$$\Rightarrow x_1 = \gamma_0 + \gamma_1 p = 0 + 0 \cdot 2 = 0$$

б)  $x_2 = \log_2 163 \pmod{5^2}$ ,  $p = 5$ ,  $k = 2$

$$M(p, \gamma_0) = b^{\frac{N}{p}} = 163^{\frac{700}{5}} = 638 \Rightarrow \gamma_0 = 2, \quad b_1 = ba^{-\gamma_0} = 163 \cdot 2^{-2} = 216$$

$$M(p, \gamma_1) = b_1^{\frac{N}{p^2}} = 216^{\frac{700}{25}} = 89 \Rightarrow \gamma_1 = 3$$

$$\Rightarrow x_2 = \gamma_0 + \gamma_1 p = 2 + 3 \cdot 5 = 17$$

в)  $x_3 = \log_2 163 \pmod{7}$ ,  $p = 7$ ,  $k = 1$

$$M(p, \gamma_0) = b^{\frac{N}{p}} = 163^{\frac{700}{7}} = 636 \Rightarrow \gamma_0 = 4$$

$$\Rightarrow x_3 = \gamma_0 = 4$$

3. На основе вычисленных выше значений  $x_1, x_2, \dots, x_t$  и китайской теоремы об остатках находим искомым логарифм:

$$\begin{aligned} x &= \sum x_i \frac{N}{p_i^{k_i}} \left[ \left( \frac{N}{p_i^{k_i}} \right)^{-1} \pmod{p_i^{k_i}} \right] \pmod{N} = 0 \cdot \frac{700}{2^2} \left[ \left( \frac{700}{2^2} \right)^{-1} \pmod{2^2} \right] + \\ &+ 17 \cdot \frac{700}{5^2} \left[ \left( \frac{700}{5^2} \right)^{-1} \pmod{5^2} \right] + 4 \cdot \frac{700}{7} \left[ \left( \frac{700}{7} \right)^{-1} \pmod{7} \right] \pmod{700} = \\ &= 476 \cdot [28^{-1} \pmod{25}] + 400 \cdot [100^{-1} \pmod{7}] \pmod{700} = \\ &= 476 \cdot 17 + 400 \cdot 4 \pmod{700} = 592 \end{aligned}$$

Ответ:  $x = 592$ .

## 1.2 Квадратичные вычеты, сравнения, символ Лежандра.

Докажем вспомогательные леммы.

**Лемма 2.1** Если  $p = 2^m + 1$  – простое и  $\left(\frac{a}{p}\right) = -1$ , то  $\langle a \rangle = \mathbb{Z}_p^*$ .

■ По определению первообразного корня достаточно доказать два утверждения:  $a^{\phi(p)} = a^{2^m} \equiv 1 \pmod{p}$  и  $a^{\frac{\phi(p)}{2}} = a^{2^{m-1}} \not\equiv 1 \pmod{p}$ .

$$a^{2^{m-1}} = a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = -1 \not\equiv 1 \pmod{p},$$

$$a^{2^m} = (a^{2^{m-1}})^2 = (-1)^2 = 1 \equiv 1 \pmod{p}.$$

■

**Лемма 2.2** Если число  $p = 2^m + 1$  – простое,  $m > 1$ , то  $p \equiv 2 \pmod{3}$ .

■ По теореме о делении с остатком, число  $p$  представимо в виде:

$$p = 3k + t, 0 \leq t < 3.$$

Рассмотрим данное равенство при различных  $t$ .

а)  $t = 0 \Rightarrow p = 3k$ , то есть,  $p$  не является простым числом при  $k > 1$  (а значит, при  $m > 1$ ). Противоречие  $\Rightarrow t \neq 0$ .

б)  $t = 1 \Rightarrow 2^m = 3k$  – этого не может быть ни при каком целом  $k$  по лемме Евклида (по крайней мере один из сомножителей числа  $2^m$  должен делиться на 3). Следовательно,  $t \neq 1$ .

Тогда  $t = 2$  – единственный вариант,  $p = 3k + 2$ .

■

**Лемма 2.3** Если  $p = 2^{2^n} + 1$ ,  $n > 1$ , то  $p \equiv 2 \pmod{5}$ .

■ Докажем по индукции.

1) При  $n = 2$  утверждение верно:  $2^{2^2} + 1 = 17 \equiv 2 \pmod{5}$ .

2) Пусть для  $n = m$  верно, докажем для  $n = m + 1$ :

$$2^{2^{m+1}} + 1 = (2^{2^m} + 1 - 1)^2 + 1 = (2 - 1)^2 + 1 = 2 \equiv 2 \pmod{5}.$$

■

**Лемма 2.4** Если  $p = 2^{2^n} + 1$ ,  $n = 2k$ , то  $p \equiv 3 \pmod{7}$ .

■ Докажем по индукции.

- 1) При  $k = 0$  утверждение верно:  $2^{2^0} + 1 = 3 \equiv 3 \pmod{7}$ .
- 2) Пусть для  $k = m$  верно, докажем для  $k = m + 1$ :

$$2^{2^{2(m+1)}} + 1 = (2^{2^{2m}} + 1 - 1)^4 + 1 = (3 - 1)^4 + 1 = 17 \equiv 3 \pmod{7}$$

■

**Лемма 2.5** Если  $p = 2^{2^n} + 1$ ,  $n = 2k + 1$ , то  $p \equiv 5 \pmod{7}$ .

■ Докажем по индукции.

- 1) При  $k = 0$  утверждение верно:  $2^{2^1} + 1 = 5 \equiv 5 \pmod{7}$ .
- 2) Пусть для  $k = m$  верно, докажем для  $k = m + 1$ :

$$2^{2^{2(m+1)+1}} + 1 = (2^{2^{2m+1}} + 1 - 1)^4 + 1 = (5 - 1)^4 + 1 = 257 \equiv 5 \pmod{7}$$

■

**Задача 2.1** Доказать, что сравнение  $x^2 + 1 \equiv 0 \pmod{p}$  разрешимо тогда и только тогда, когда  $p \equiv 1 \pmod{4}$ .

**Решение.**

$$\begin{aligned} x^2 + 1 \equiv 0 \pmod{p} - \text{разрешимо} &\Leftrightarrow \left(\frac{-1}{p}\right) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow \frac{p-1}{2} = 2k \Leftrightarrow p = 4k + 1 \Leftrightarrow p \equiv 1 \pmod{4} \end{aligned}$$

**Задача 2.2** Доказать, что сравнение  $x^2 + 2 \equiv 0 \pmod{p}$  разрешимо тогда и только тогда, когда  $p \equiv 1, 3 \pmod{8}$ .

**Решение.**

$$\begin{aligned} x^2 + 2 \equiv 0 \pmod{p} - \text{разрешимо} &\Leftrightarrow \left(\frac{-2}{p}\right) = 1. \Leftrightarrow \left\{ \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \right\} \\ &= (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} \Leftrightarrow \frac{p-1}{2} + \frac{p^2-1}{8} = 2k \Leftrightarrow p^2 + 4p - 16k - 5 = 0. \end{aligned}$$

Представим  $p$ , используя теорему о делении с остатком, в следующем виде:  $p = 8m + t$ ,  $0 \leq t < 8$ . Решим полученную систему относительно  $t$ .

$$(8m + t)^2 + 4(8m + t) - 16k - 5 = 0$$

$$t^2 + (16k + 4)t + 64k^2 + 32k - 16m - 5 = 0$$

$$t_{1,2} = -8k - 2 \pm \sqrt{16m + 9} \pmod{8} = -2 \pm 3 \pmod{8} \Rightarrow t = 1, 3$$

Тогда  $p^2 + 4p - 16k - 5 = 0 \Leftrightarrow p \equiv 1, 3 \pmod{8}$ .

**Задача 2.3** Доказать, что сравнение  $x^2 + 3 \equiv 0 \pmod{p}$  разрешимо тогда и только тогда, когда  $p \equiv 1 \pmod{6}$ .



**Решение.**

Пусть  $p = 3k + t, t < 3$ .

$$x^2 + 3 \equiv 0 \pmod{p} \Leftrightarrow \left(\frac{-3}{p}\right) = 1.$$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \left(\frac{p}{3}\right) = (-1)^{3k+t-1} \left(\frac{t}{3}\right)$$

$$\text{а) } t = 0 \Rightarrow \left(\frac{0}{3}\right) = 0, (-1)^{3k+t-1} \left(\frac{t}{3}\right) = 0 \neq 1$$

$$\text{б) } t = 1 \Rightarrow \left(\frac{1}{3}\right) = 1, (-1)^{3k+t-1} \left(\frac{t}{3}\right) = (-1)^{3k} \cdot 1 = (-1)^{3k}.$$

$$\text{в) } t = 2 \Rightarrow \left(\frac{2}{3}\right) = -1, (-1)^{3k+t-1} \left(\frac{t}{3}\right) = (-1)^{3k+1} \cdot (-1) = (-1)^{3k}$$

$$(-1)^{3k} = 1 \Leftrightarrow k = 2m \Leftrightarrow p = 6m + 1 \Leftrightarrow p \equiv 1 \pmod{6}$$

**Задача 2.4** Доказать, что если  $p = 2^n + 1$  – простое,  $n > 2$ , то  $\left(\frac{3}{p}\right) = -1$  и  $\langle 3 \rangle = \mathbb{Z}_p^*$ .

**Решение.**

$p = 3k + 2$  по лемме 2.2.

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{2^n+1-1}{2}} \left(\frac{p}{3}\right) = (-1)^{2^{n-1}} \left(\frac{2}{3}\right) = -1$$

Выполнены все условия леммы 2.1  $\Rightarrow \langle 3 \rangle = \mathbb{Z}_p^*$ .

**Задача 2.5** Доказать, что если  $p = 2^n + 1$  – простое и  $\left(\frac{a}{p}\right) = -1$ , то  $\langle a \rangle = \mathbb{Z}_p^*$ .

**Решение.**

Доказано в качестве леммы 2.1.

**Задача 2.6** Доказать, что если  $p = 4q + 1$ ,  $p$  и  $q$  – простые, то  $\langle 2 \rangle = \mathbb{Z}_p^*$ .

**Решение.**

По определению первообразного корня достаточно доказать три утверждения:

$$1) 2^{\phi(p)} = 2^{4q} \equiv 1 \pmod{p},$$

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

$$3) 2^{\frac{\phi(p)}{q}} = 2^4 \not\equiv 1 \pmod{p}.$$

Начнём с третьего. Представим  $2^4$  в следующем виде:  $2^4 = pk + t$ ,  $0 \leq t < p$ . Значит, нам нужно доказать, что  $t \neq 1$ . Предположим, что это не так, тогда  $pk = 2^4 - 1 = 15$ . Обратим внимание на условие: если  $p$  и  $q$  – простые числа, то  $p$  не может быть ни 3, ни 5. Значит, в левой части равенства содержится простой множитель, которого нет в правой части. Мы получили противоречие, а значит,  $t \neq 1 \Rightarrow 2^{\frac{\phi(p)}{q}} = 2^4 \not\equiv 1 \pmod{p}$ .

Рассмотрим теперь второе утверждение. Заметим, что:

$$\left(\frac{2}{4q+1}\right) = 2^{\frac{4q+1-1}{2}} = 2^{2q} \pmod{4q+1}.$$

Вычислим  $\left(\frac{2}{4q+1}\right) = (-1)^{\frac{(4q+1)^2-1}{8}} = (-1)^{2q^2+q} = \{q - \text{нечет}\} = -1$ .  
Тем самым мы доказали второе утверждение.

Поскольку  $2^{4q} = (2^{2q})^2 = (-1)^2 = 1 \pmod{4q+1}$ , то первое утверждение становится следствием второго.

**Задача 2.7** Доказать, что если  $p = 2^{2^n} + 1$  – простое и  $\left(\frac{a}{p}\right) = -1$ , то  $\langle a \rangle = \mathbb{Z}_p^*$ .

**Решение.**

Приняв  $m = 2^n$  в лемме 2.1, получим справедливость данного утверждения.

**Задача 2.8** Доказать, что если  $p = 2^{2^n} + 1$  – простое,  $n > 2$ , то  $\langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_p^*$ .

**Решение.**

Покажем  $\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = -1$ .

$2^{2^n} + 1 = 3k + 2$  по лемме 2.2.

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{2^{2^n}+1-1}{2}} \left(\frac{p}{3}\right) = (-1)^{2^{2^n-1}} \left(\frac{3k+2}{3}\right) = \left(\frac{2}{3}\right) = 2^{\frac{3-1}{2}} \pmod{3} = -1$$

$2^{2^n} + 1 = 5k + 2$  по лемме 2.3.

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{2^{2^n}+1-1}{2}} \left(\frac{p}{5}\right) = (-1)^{2^{2^n}} \left(\frac{5k+2}{5}\right) = \left(\frac{2}{5}\right) = 2^{\frac{5-1}{2}} \pmod{5} = -1$$

$2^{2^n} + 1 = 7k + 3$ ,  $n = 2t$  по лемме 2.4.

$$\left(\frac{7}{p}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{2^{2^n}+1-1}{2}} \left(\frac{p}{7}\right) = (-1)^{2^{2^n}} \left(\frac{7k+3}{7}\right) = \left(\frac{3}{7}\right) = 3^{\frac{7-1}{2}} \pmod{7} = -1$$

$2^{2^n} + 1 = 7k + 5$ ,  $n = 2t + 1$  по лемме 2.5.

$$\left(\frac{7}{p}\right) = \left(\frac{5}{7}\right) = 5^{\frac{7-1}{2}} \pmod{7} = -1.$$

Осталось применить лемму 2.1, и исходное утверждение будет доказано.

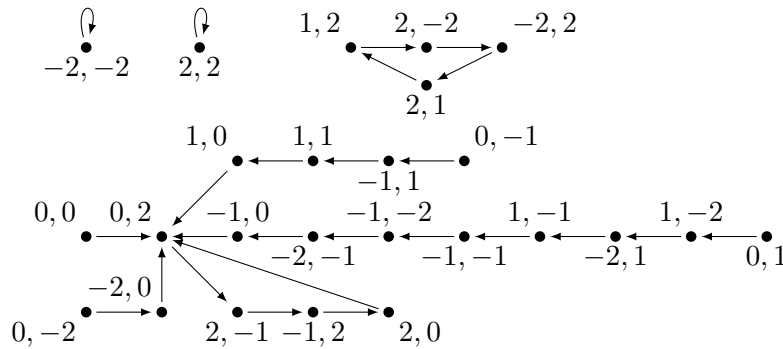
### 1.3 Рекуррентные последовательности.

**Задача 3.1**  $F = GF(5)$ . Построить граф отображения и найти период РП, заданной характеристической функцией:

$$x_i = x_{i-1} + 2x_{i-2}x_{i-1} + 2.$$

Начальное заполнение:  $12 = \gamma_1 + 5\gamma_2$  ( $\gamma = (2, 2)$ ).

**Решение.**



В случае  $\gamma = (2, 2)$  последовательность оказывается полностью состоящей из двоек, поэтому период такой последовательности будет равен единице.

**Задача 3.2** Над полем  $GF(2)$  построить ЛРП периода  $T$  и ранга  $n$  и указать начальное заполнение.

$$T = 84, n = 8.$$

**Решение.**

Разложим  $T$  на множители:  $T = 84 = 4 \cdot 3 \cdot 7$ .

ЛРП<sub>1</sub> с периодом 4 соответствует минимальный многочлен

$$f_1(x) = x^3 + x^2 + x + 1, \quad x_i = x_{i-1} + x_{i-2} + x_{i-3}.$$

ЛРП<sub>2</sub> с периодом 3 соответствует минимальный многочлен

$$f_2(x) = x^2 + x + 1, \quad x_i = x_{i-1} + x_{i-2}.$$

ЛРП<sub>3</sub> с периодом 7 соответствует минимальный многочлен

$$f_3(x) = x^3 + x + 1, \quad x_i = x_{i-2} + x_{i-3}$$

Искомый характеристический многочлен

$$f(x) = (x^3 + x^2 + x + 1)(x^2 + x + 1)(x^3 + x + 1) = x^8 + x^4 + x^3 + x^2 + x + 1.$$

Характеристическое уравнение будет иметь вид:

$$x_i = x_{i-4} + x_{i-5} + x_{i-6} + x_{i-7} + x_{i-8}.$$

Выберем начальные заполнения для ЛРП<sub>1-3</sub>, отличные от нуля, и получим первые начальные отрезки ЛРП длины  $n = 8$ :

$$\tilde{\alpha}_1 = 001 \Rightarrow \tilde{\beta}_1 = 00110011$$

$$\tilde{\alpha}_2 = 01 \Rightarrow \tilde{\beta}_2 = 01101101$$

$$\tilde{\alpha}_3 = 001 \Rightarrow \tilde{\beta}_3 = 00101110$$

Искомое начальное заполнение:

$$\tilde{\beta} = \tilde{\beta}_1 \oplus \tilde{\beta}_2 \oplus \tilde{\beta}_3 = 01110000.$$

Ответ:  $f(x) = x^8 + x^4 + x^3 + x^2 + x + 1$ ,  $\tilde{\beta} = 01110000$ .

## 1.4 Шифр гаммирования

**Задача 4.1** Зашифровать свою фамилию, используя шифр гаммирования с ЛРП из задачи 3.2.

**Решение.**

Кодирование алфавита приведено в следующей таблице:

А	00000	И	01000	Р	10000	Ш	11000
Б	00001	Й	01001	С	10001	Щ	11001
В	00010	К	01010	Т	10010	Ъ	11010
Г	00011	Л	01011	У	10011	Ы	11011
Д	00100	М	01100	Ф	10100	Ь	11100
Е	00101	Н	01101	Х	10101	Э	11101
Ж	00110	О	01110	Ц	10110	Ю	11110
З	00111	П	01111	Ч	10111	Я	11111

ЛРП задана многочленом  $f(x) = x^8 + x^4 + x^3 + x^2 + x + 1$ ,  $\tilde{k} = 01110000$ ,  $M = \text{СМИРНОВ}$ . Согласно кодовой таблице получим:

$$\tilde{M} = 10001 \ 01100 \ 01000 \ 10000 \ 01101 \ 01110 \ 00010$$

Получаем гамму:

$$\tilde{\Gamma} = 01110 \ 00011 \ 01100 \ 10101 \ 00010 \ 01011 \ 00011$$

Получим шифротекст:

$$\tilde{T} = 11111 \ 01111 \ 00100 \ 00101 \ 01111 \ 00101 \ 00001$$

Представим его в буквенном виде.

Ответ:  $T = \text{ЯПДЕПЕБ}$ .

## 1.5 Теория групп

**Задача 5.1** Определить структуру группы  $\mathbb{Z}_n^*$ , разложить её в прямое произведение циклических подгрупп и подсчитать число элементов различного порядка,  $n = 84$ .

**Решение.**

$$|G| = \phi(84) = \phi(2^2) \cdot \phi(3) \cdot \phi(7) = (4-2)(3-1)(7-1) = 24 = 2^3 \cdot 3.$$

Следовательно,  $G \cong S_1(8) \times S_2(3)$ .

1. Определим структуру примарной группы  $S_1(8)$ . Для этого нужно решить сравнение:

$$x^2 \equiv 1 \pmod{84}.$$

По КТО это равносильно следующей системе:

$$\begin{cases} x^2 \equiv 1 \pmod{3} \\ x^2 \equiv 1 \pmod{4} \\ x^2 \equiv 1 \pmod{7} \end{cases}$$

$$p = 3 = 4 \cdot 0 + 3 \Rightarrow \left(\frac{1}{3}\right) = 1 - \text{два решения: } x_1 \equiv \pm 1^{0+1} \pmod{3}.$$

$$p = 4 = 2^2, a = 1 \Rightarrow \text{два решения: } x_2 \equiv \pm 1 \pmod{4}.$$

$$p = 7 = 4 \cdot 1 + 3 \Rightarrow \left(\frac{1}{7}\right) = 1 - \text{два решения: } x_3 \equiv \pm 1^{1+1} \pmod{7}.$$

Общее решение системы по КТО будет равно:

$$X = x_1(4 \cdot 7)[(4 \cdot 7)^{-1} \pmod{3}] + x_2(3 \cdot 7)[(3 \cdot 7)^{-1} \pmod{4}] + x_3(3 \cdot 4)[(3 \cdot 4)^{-1} \pmod{7}] \pmod{84} = 28x_1 + 21x_2 + 36x_3 \pmod{84}$$

Таким образом, множество элементов второго порядка группы  $G$  это:

$$M_2 = \{13, 43, 55, 29, 41, 71, 83\}.$$

Обозначим за  $A_i = \langle M_{2,i} \rangle$ , где  $M_{2,i}$  —  $i$ -тый элемент множества  $M_2$ . Тогда  $S_1(8) \cong A_i \times A_j \times A_k$ ,  $i, j, k = \overline{1, 7}$ .

2. Определим структуру примарной группы  $S_2(3)$ . Для этого нужно решить сравнение:

$$x^3 \equiv 1 \pmod{84}.$$

По КТО это равносильно следующей системе:

$$\begin{cases} x^3 \equiv 1 \pmod{3} \\ x^3 \equiv 1 \pmod{4} \\ x^3 \equiv 1 \pmod{7} \end{cases}$$

Первые два сравнения, очевидно, имеют единственные решения  $x_1 = 1$ ,  $x_2 = 1$ . Последнее сравнение имеет 3 решения:  $x_3 = \{1, 2, 4\}$ . Общее решение исходного сравнения будет равно:

$$X = 28x_1 + 21x_2 + 36x_3 \pmod{84} = 49 + 36x_3 \pmod{84}$$

Множество элементов третьего порядка группы  $G$  это:

$$M_3 = \{25, 37\}$$

Таким образом,  $S_2(3) = \langle 25 \rangle = \langle 37 \rangle$ .

Ответ:  $G \cong A_i \times A_j \times A_k \times \langle 25 \rangle = A_i \times A_j \times A_k \times \langle 37 \rangle$ ,  $i, j, k = \overline{1, 7}$ .

**Задача 5.2** Доказать, что  $y = x^3$  – подстановка над  $\mathbb{Z}_p$ , если  $p \equiv 2 \pmod{3}$ , то есть,

$$x_1^3 \equiv x_2^3 \pmod{p} \Rightarrow x_1 \equiv x_2 \pmod{p}.$$

**Решение.**

Поле  $\mathbb{Z}_p$  имеет порядок  $\phi(p) = p - 1$ . Из  $x_1^3 \equiv x_2^3 \pmod{p}$  получим, что  $(x_1 x_2^{-1})^3 \equiv 1 \pmod{p}$ . Тогда порядок  $x_1 x_2^{-1}$  является делителем 3. Существует два варианта:

1.  $\text{Ord}(x_1 x_2^{-1}) = 1$ . Это означает, что  $x_1 \equiv x_2 \pmod{p}$ .

2.  $\text{Ord}(x_1 x_2^{-1}) = 3$ . Так как  $p = 3m + 2$ , то  $\phi(p) = 3m + 1$ . То есть, порядок элемента не является делителем порядка группы, что противоречит теореме Лагранжа.

Следовательно,  $x_1 \equiv x_2 \pmod{p}$ . А значит,  $y = x^3$  – подстановка над  $\mathbb{Z}_p$ .

**Задача 5.3** Найти порядок и цикловое представление подстановки  $y = x^3$ ,  $p = 11$ .

**Решение.**

$x$	0	1	2	3	4	5	6	7	8	9	10
$y$	0	1	8	5	9	4	7	2	6	3	10

Получим 5 циклов:  $(0)$ ,  $(1)$ ,  $(2, 8, 6, 7)$ ,  $(3, 5, 4, 9)$ ,  $(10)$ . Порядок подстановки равен НОК длины циклов:  $\text{НОК}(1, 1, 4, 4, 1) = 4$ .

Ответ: Порядок подстановки  $(0)(1)(2, 8, 6, 7)(3, 5, 4, 9)(10)$  равен 4.

**Задача 5.4** Найти порядок подстановки  $y = 5x + 3 \pmod{12}$

**Решение.**

$x$	0	1	2	3	4	5	6	7	8	9	10	11
$y$	3	8	1	6	11	4	9	2	7	0	5	10

Получим 3 цикла:  $(0, 3, 6, 9)$ ,  $(1, 8, 7, 2)$ ,  $(4, 11, 10, 5)$ . Порядок подстановки равен НОК длины циклов:  $\text{НОК}(4, 4, 4) = 4$ .

Ответ: Порядок подстановки равен 4.