

Математические основы криптологии

Автор курса: Применко Эдуард Андреевич
Составитель: Смирнов Дмитрий Константинович

Версия от 01:41, 14 марта 2022 г.

Оглавление

1	Домашние задания	1
1.1	Элементы теории групп	1
1.2	Квадратичные вычеты, сравнения, символ Лежандра. . . .	4
2	Билеты	8
2.1	Делимость в кольце целых чисел. НОД, алгоритм Евклида. Критерий взаимной простоты двух чисел.	8
2.2	Сравнения и их свойства. Китайская теорема об остатках. Кольцо вычетов. Функция Эйлера и её свойства.	9
2.3	Теоремы Эйлера и Ферма. Критерий обратимости, алгоритм вычисления обратного элемента.	9
2.4	Криптографическая теорема (обоснование криптосистемы RSA).	9
2.5	Теорема о цикличности мультипликативной группы по простому модулю.	9
2.6	Решение сравнений первой степени.	9
2.7	Сравнения второй степени. Символ Лежандра и его свойства.	9
2.8	Алгоритмы решения сравнений второй степени по простому модулю.	9
2.9	Символ Якоби и его свойства. Числа Блюма и их свойства. Эквивалентность задачи факторизации и решения сравнения второй степени.	9
2.10	Алгоритмы решения сравнений второй степени по простому и составному модулю.	9
2.11	Группа, порядок элемента. Теорема Лагранжа.	9
2.12	Нормальный делитель, фактор – группа, первая теорема о гомоморфизме.	10
2.13	Кольцо многочленов, идеал, теорема Безу, кольцо главных идеалов.	10
2.14	Конечное поле. Теорема о простом подполе конечного поля. Строение конечного поля. Теорема о примитивном элементе.	10

2.15 Построение конечных полей. Алгоритм вычисления обратного элемента. Арифметические операции в конечном поле.	10
2.16 Алгоритмы вычисления дискретного алгоритма.	10
2.17 Криптосистема Эль - Гамала. Протокол Диффи - Хеллмана.	10
2.18 Минимальный многочлен и его свойства. Теорема об изоморфизме конечных полей одной мощности.	10
2.19 Прimitивный многочлен и его свойства. Теорема о разложении многочлена $f(x) = x^{p^n} - x$ на неприводимые многочлены. Критерий принадлежности элемента поля собственному подполю.	10
2.20 Теорема о группе автоморфизмов конечного поля.	10
2.21 Рекуррентные последовательности над конечным полем, линейные рекуррентные последовательности (ЛРП). Характеристический и минимальный многочлен ЛРП и их свойства.	10
2.22 Теорема об определении структуры ЛРП по её характеристическому многочлену. Теорема о ЛРП максимального периода.	10
2.23 Прямое произведение групп. Теорема о представлении группы в виде прямого произведения своих подгрупп.	10
2.24 Теорема о примарной абелевой группе.	10
2.25 Теорема о разложении конечной абелевой группы в произведение своих циклических подгрупп.	11
2.26 Нормализатор, централизатор, класс сопряженных элементов конечной группы. Теорема о числе множеств сопряженных с данным. Теорема о центре примарной группы. Теорема Коши.	11
2.27 Двойные смежные классы и их свойства. Теорема Силова (первая)	11
2.28 Вторая и третья теоремы Силова.	11
2.29 Группы подстановок. Инвариантное множество, орбита. Теорема об индексе стабилизатора группы. Теорема о транзитивности нормализатора подгруппы транзитивной группы. (Ут . 13.4).	11
2.30 Лемма Бернсайда.	11
2.31 Регулярные и полурегулярные группы. Порядок полурегулярной группы.	11
2.32 Блоки и импримитивные группы. Критерий импримитивности. Теорема о импримитивности транзитивной группы с интранзитивным нормальным делителем.	11
2.33 Примитивные группы. Кратная транзитивность. Критерий кратной транзитивности.	11
2.34 Теорема о группе автоморфизмов конечной группы.	11

2.35	Утверждение об изоморфизме стабилизатора и специальной группы автоморфизмов регулярной подгруппы (Ут . 13.5). Утверждение о порядке регулярного нормального делителя кратно транзитивной группы.	11
2.36	Простая группа. Теорема о простоте знакопеременной группы. Теорема о нормальном делителе симметрической группы.	11

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 .

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,

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

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

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

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 $ord(a) = 700$.

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: $x = 592$.

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

$j \backslash p_i$	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	$2^{0 \cdot \frac{700}{7}}$	$2^{1 \cdot \frac{700}{7}}$	$2^{2 \cdot \frac{700}{7}}$	$2^{3 \cdot \frac{700}{7}}$	$2^{4 \cdot \frac{700}{7}}$	$2^{5 \cdot \frac{700}{7}}$	$2^{6 \cdot \frac{700}{7}}$

$j \backslash p_i$	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 γ_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) $x_1 = \log_2 163 \pmod{2^2}, p = 2, k = 2$

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

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

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

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

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

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

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

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:

$$x = \sum x_i \frac{N}{p_i^{k_i}} \left[\left(\frac{N}{p_i^{k_i}} \right)^{-1} \pmod{p_i^{k_i}} \right] \pmod{N} = 0 \cdot \frac{700}{2^2} \left[\left(\frac{700}{2^2} \right)^{-1} \pmod{2^2} \right] +$$

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

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 $a^{\frac{\phi(p)}{2}} = a^{2^{m-1}} \not\equiv 1 \pmod{p}$.

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

■

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 $n > 1$). 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.

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

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

$$\begin{aligned}
(8m+t)^2 + 4(8m+t) - 16k - 5 &= 0 \\
t^2 + (16k+4)t + 64k^2 + 32k - 16m - 5 &= 0 \\
t_{1,2} = -8k - 2 \pm \sqrt{16m+9} \pmod{8} &= -2 \pm 3 \pmod{8} \Rightarrow t = 1, 3
\end{aligned}$$

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

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 $p = 3k + t, t < 3$.

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

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

$$\begin{aligned}
\text{а) } t = 0 &\Rightarrow \left(\frac{0}{3}\right) = 0, (-1)^{3k+t-1} \left(\frac{t}{3}\right) = 0 \neq 1 \\
\text{б) } t = 1 &\Rightarrow \left(\frac{1}{3}\right) = 1, (-1)^{3k+t-1} \left(\frac{t}{3}\right) = (-1)^{3k} \cdot 1 = (-1)^{3k} \\
\text{в) } t = 2 &\Rightarrow \left(\frac{2}{3}\right) = -1, (-1)^{3k+t-1} \left(\frac{t}{3}\right) = (-1)^{3k+1} \cdot (-1) = (-1)^{3k}
\end{aligned}$$

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

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 и 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.

Часть 2

Билеты

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

Теорема 1.1 (о делении с остатком) Пусть $a > 0$ и $b > 0$ – целые числа. Тогда a единственным образом представимо в виде

$$a = bq + r, \quad 0 \leq r < b.$$

Число q – неполное частное

- 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.
- 2.11 Группа, порядок элемента. Теорема Лагранжа.

- 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 $f(x) = x^p - x$ 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 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-