МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__» _____2016 г.

ДИСКРЕТНЫЕ ЛОГАРИФМЫ

Методические указания по выполнению практической работы
для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 511.172

Составители: М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Дискретные логарифмы: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 14 с., Библиогр.: с. 14.

Содержат основные сведения об индексах или дискретных логарифмах, и применении их для решения степенных сравнений. Указывается порядок выполнения работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ 4
2. ЗАДАНИЕ 4
3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ 4
4. СОДЕРЖАНИЕ ОТЧЕТА 4
5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ 5
5.1 Индексы (дискретные логарифмы) 5
5.2 Свойства индексов 5
6. ВЫПОЛНЕНИЕ РАБОТЫ 6
6.1 Пример выполнения задания 6
6.2 Варианты работ 9
7. КОНТРОЛЬНЫЕ ВОПРОСЫ 13
8. СПИСОК ИСПОЛЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 14

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - научиться составлять таблицу индексов и решать степенные сравнения методом дискретного логарифмирования.

2. ЗАДАНИЕ

Ознакомьтесь с теоретическим материалом. Составить таблицу индексов по заданному модулю. Решить степенное сравнение.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание в соответствии с вариантом.
2. Изучить теоретическую часть с примерами.
3. Составить таблицу индексов по заданному модулю.
4. Используя таблицу индексов, решить степенное сравнение.
5. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Составление таблицы индексов.
4. Решение степенного сравнения.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Индексы (дискретные логарифмы)

Индексы (дискретные логарифмы) по модулям $p^k, 2p^k, p$ - простое число, $k \in N$.

Обозначим через m модуль вида p^k или $2p^k$, а через q - первообразный корень по этому модулю. Положим $c = \phi(m)$.

Теорема.

Если число γ принимает последовательно значения 0,1,…,c-1, то q^γ пробегает приведённую систему вычетов по модулю m.

Определение.

Пусть $a \equiv q^\gamma (\mathrm{mod}\, m), \quad (a,m) = 1$. Число $\gamma \geq 0$ называется индексом (дискретным логарифмом) числа a по модулю m при основании q. Обозначения: $\gamma = inda, \quad или \quad \gamma = ind_q a$.

Замечание.

В силу теоремы Эйлера индекс определён по модулю c. Тем самым было бы правильнее говорить о классе вычетов по модулю c.

5.2 Свойства индексов

Свойства индексов.

1) $ind(ab) = inda + indb (\mathrm{mod}\, c)$.

2) $inda^n = n * inda (\mathrm{mod}\, c)$.

3) Для того, чтобы сравнение $x^n \equiv a (\mathrm{mod}\, m)$ было разрешимо, необходимо и достаточно, чтобы $d \mid inda, \quad d = (n,c)$.

В случае разрешимости имеется d решений.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Пример выполнения задания

Пример 1. Составить таблицу индексов по модулю 17.

Решение.

$m = 17$

$c = \varphi(17) = 16$

$(a,17) = 1 \Rightarrow a \in \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$

$\gamma \in [0,15],\ \gamma \in Z;$

$\mathrm{c} = 16 = 2^4$

$q_1 = 2;$

$a^{\frac{16}{2}-1} \equiv a(\mathrm{mod}16) \Rightarrow a^8 \equiv 1(\mathrm{mod}16)$

$\frac{2^8-1}{17} = 15 \in z$

$\frac{3^8-1}{17} = 385,88 \notin z$

$a = 3$

$a \equiv 3^{\gamma}(\mathrm{mod}17) \in [1,16]$

$3^0 \equiv 1(\mathrm{mod}17)$

$3^1 \equiv 3(\mathrm{mod}17)$

$3^2 \equiv 9(\mathrm{mod}17)$

$3^3 \equiv 10(\mathrm{mod}17)$

$3^4 \equiv 13(\mathrm{mod}17)$

$3^5 \equiv 5(\mathrm{mod}17)$

$3^6 \equiv 15(\mathrm{mod}17)$

$3^7 \equiv 11(\mathrm{mod}17)$

$3^8 \equiv 16(\mathrm{mod}17)$

$3^9 \equiv 14(\mathrm{mod}17)$

$3^{10} \equiv 8(\mathrm{mod}17)$

$3^{11} \equiv 7(\mathrm{mod}17)$

$3^{12} \equiv 4(\mathrm{mod}17)$

$3^{13} \equiv 12(\mathrm{mod}17)$

$3^{14} \equiv 2(\mathrm{mod}17)$

$3^{15} \equiv 6(\mathrm{mod}17)$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
inda	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Пример 2. Решить сравнение: $x^5 \equiv 17(\mathrm{mod}\,29)$.

Решение.

$\varphi(29) = 28; \quad (5,28) = 1.$

$ind17 = 21$

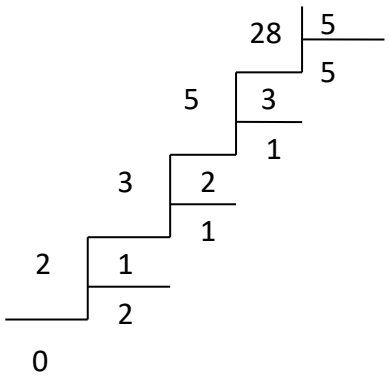
(см. например, И.М.Виноградов “Элементы высшей математики” М., “Высшая школа”, 1999, с.497).

$1|21$, следовательно, сравнение имеет только одно решение.

$x^5 \equiv 17(\mathrm{mod}\,29) \quad \Leftrightarrow \quad 5indx \equiv ind17(\mathrm{mod}\,28).$

$5indx \equiv 21(\mathrm{mod}\,28).$

Решаем сравнение $5indx \equiv 21(\mathrm{mod}\,28)$ с помощью расширенного алгоритма Евклида.



Находим мультипликативно обратный элемент к 5 по модулю 28.

i	Остатки	Частные	x_i	y_i
-1	28	-	1	1
0	5	-	0	0
1	3	5	1-0*5=1	0-1*5=-5
2	2	1	0-1*1=-1	1-(-5)*1=6
3	1= d	1	1-(-1)*1=2	-5-6*1=11
4	0	2	-	-

$U = -11(\mathrm{mod}\,28) = 17$ (т.к.. -11=28*(-1)+17).

$indx \equiv 21*17(\mathrm{mod}\,28) = 357(\mathrm{mod}\,28) = 21(28).$

В таблице индексов по модулю 29 находим решение $x \equiv 17(\mathrm{mod}\,29)$ исходного сравнения.

6.2 Варианты работ

Вариант 1.

1. Составить таблицу индексов по модулю 71.
2. Решить сравнение: $X^{55} = 17(\mathrm{mod}\,97)$.

Вариант 2.

1. Составить таблицу индексов по модулю 68.
2. Решить сравнение: $X^{35} = 17(\mathrm{mod}\,67)$.

Вариант 3.

1. Составить таблицу индексов по модулю 67.
2. Решить сравнение: $x^5 \equiv 37(\mathrm{mod}\,43)$.

Вариант 4.

1. Составить таблицу индексов по модулю 62.
2. Решить сравнение: $x^8 \equiv 27(\mathrm{mod}\,37)$.

Вариант 5.

1. Составить таблицу индексов по модулю 61.
2. Решить сравнение: $x^{10} \equiv 33(\mathrm{mod}\,37)$

Вариант 6.

1. Составить таблицу индексов по модулю 59.
2. Решить сравнение: $x^{12} \equiv 27(\mathrm{mod}\,83)$.

Вариант 7.

1. Составить таблицу индексов по модулю 58.
2. Решить сравнение: $x^2 \equiv 239(\mathrm{mod}\,661)$.

Вариант 8.

1. Составить таблицу индексов по модулю 53.
2. Решить сравнение: $x^{27} \equiv 7(\mathrm{mod}\,10)$.

Вариант 9.

1. Составить таблицу индексов по модулю 47.
2. Решить сравнение: $x^{10} \equiv 9(\mathrm{mod}17)$.

Вариант 10.

1. Составить таблицу индексов по модулю 46.
2. Решить сравнение: $x^{27} \equiv 1(\mathrm{mod}\,29)$.

Вариант 11.

1. Составить таблицу индексов по модулю 43.
2. Решить сравнение: $x^{15} \equiv 6(\mathrm{mod}\,21)$.

Вариант 12.

1. Составить таблицу индексов по модулю 41.
2. Решить сравнение: $x^{7} \equiv 10(\mathrm{mod}\,65)$.

Вариант 13.

1. Составить таблицу индексов по модулю 38.
2. Решить сравнение: $x^{6} \equiv 10(\mathrm{mod}\,37)$

Вариант 14.

1. Составить таблицу индексов по модулю 37.
2. Решить сравнение: $x^{19} \equiv 31(\mathrm{mod}\,41)$.

Вариант 15.

3. Составить таблицу индексов по модулю 34.
4. Решить сравнение: $x^{18} \equiv 4(\mathrm{mod}\,20)$.

Вариант 16.

1. Составить таблицу индексов по модулю 31.
2. Решить сравнение: $x^{11} \equiv 18(\mathrm{mod}\,71)$.

Вариант 17.

1. Составить таблицу индексов по модулю 29.
2. Решить сравнение: $x^{14} \equiv 31(\mathrm{mod}\,33)$.

Вариант 18.

1. Составить таблицу индексов по модулю 23.
2. Решить сравнение: $x^{22} \equiv 37(\mathrm{mod}\,44)$.

Вариант 19.

1. Составить таблицу индексов по модулю 19.
2. Решить сравнение: $x^{8} \equiv 8(\mathrm{mod}\,28)$.

Вариант 20.

1. Составить таблицу индексов по модулю 17.
2. Решить сравнение: $x^{10} \equiv 19(\mathrm{mod}\,51)$.

Вариант 21.

1. Составить таблицу индексов по модулю 73.
2. Решить сравнение: $x^{16} \equiv 25(\mathrm{mod}\,36)$.

Вариант 22.

1. Составить таблицу индексов по модулю 74.
2. Решить сравнение: $x^{21} \equiv 27(\mathrm{mod}\,42)$.

Вариант 23.

1. Составить таблицу индексов по модулю 78.
2. Решить сравнение: $x^{13} \equiv 25(\mathrm{mod}\,54)$.

Вариант 24.

1. Составить таблицу индексов по модулю 79.
2. Решить сравнение: $x^{17} \equiv 46(\mathrm{mod}\,59)$.

Вариант 25.

1. Составить таблицу индексов по модулю 82.
2. Решить сравнение: $x^{9} \equiv 5(\mathrm{mod}\,83)$.

Вариант 26.

1. Составить таблицу индексов по модулю 83.
2. Решить сравнение: $x^{19} \equiv 22 (\mathrm{mod}\, 29)$.

Вариант 27.

1. Составить таблицу индексов по модулю 86.
2. Решить сравнение: $x^{17} \equiv 8 (\mathrm{mod}\, 67)$.

Вариант 28.

1. Составить таблицу индексов по модулю 89.
2. Решить сравнение: $x^{4} \equiv 20 (\mathrm{mod}\, 31)$.

Вариант 29.

1. Составить таблицу индексов по модулю 92.
2. Решить сравнение: $x^{22} \equiv 15 (\mathrm{mod}\, 71)$.

Вариант 30.

1. Составить таблицу индексов по модулю 97.
2. Решить сравнение: $x^{23} \equiv 40 (\mathrm{mod}\, 53)$.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое дискретный логарифм?
2. По каким модулям существуют индексы?
3. Каково условие разрешимости степенного сравнения?
4. Как решаются степенные сравнения?
5. Сколько решений может иметь степенное сравнение?

8. СПИСОК ИСПОЛЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Александров В.А., Горшенин С.М. Задачник – практикум по теории чисел. М.: Учпедгиз, 1972.

2. Виноградов И.М. Основы теории чисел. М.: Наука,1995.

3. Гайнов А.Т. Теория чисел. Изд - во НГУ, 1995.

4. Галочкин А.И., Нестеренко Н.В., Шидловский А.Б. Введение в теорию чисел. Изд - во МГУ, 1995.

5. Кудреватов Г.А. Сборник задач по теории чисел. М.: Просвещение,1970.

6. Ляпин С.Е., Баранова И.В., Борчугова З.Г. Сборник задач по элементарной математике. М.: Просвещение, 1973.

7. Пензин Ю.Г., Клейменов В.Ф. Сравнения. Учебно-методические разработки (тексты лекций). Изд-во ИГУ, 1998.

8. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999

9. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993

10. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003