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
«01» мая _____2016 г.

ПЕРВООБРАЗНЫЕ КОРНИ

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

Курск 2016

УДК 511.172

Составитель М.А. Ефремов

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

Первообразные корни: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 15 с., Библиогр.: с. 15.

Содержат основные сведения о понятии показателя числа принадлежащего заданному показателю, первообразного корня, и способах их нахождения. 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

Цель лабораторной работы - научиться определять показатель, которому принадлежит заданное число, и находить наименьший первообразный корень по заданному модулю.

2. ЗАДАНИЕ

Ознакомьтесь с теоретическим материалом. Найти показатель, которому принадлежит заданное число по заданному модулю. Найти наименьший первообразный корень по заданному модулю.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание в соответствии с вариантом.
2. Изучить теоретическую часть с примерами.
3. Определить показатель, которому принадлежит заданное число a по заданному модулю m.
4. Найти наименьший первообразный корень по заданному модулю.
5. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Нахождение показателя, которому принадлежит заданное число a по заданному модулю m.
4. Нахождение наименьших первообразных корней по заданным модулям.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Принадлежность чисел заданному показателю

Говорят, что число a, взаимно простое с модулем m, принадлежит показателю $\delta \in N$, если δ - такое наименьшее число, что выполняется сравнение $a^{\delta+1} \equiv a(\mathrm{mod}\, m)$. Число, принадлежащее показателю $\phi(m)$, называется первообразным корнем по модулю m.

Свойства принадлежности чисел, взаимно простых с модулем m, показателю δ.

1) Числа $1, a, a^2, ..., a^{\delta-1}$ попарно несравнимы по модулю m.

2) Для того, чтобы $a^{\gamma} \equiv a^{\gamma'} (\mathrm{mod}\, m)$, необходимо и достаточно, чтобы $\gamma \equiv \gamma' (\mathrm{mod}\, \delta)$.

3) $\delta \mid \phi(m)$.

5.2 Свойства первообразные корней

Свойства первообразных корней.

1) По любому простому модулю p, а также по модулю 4, существует первообразный корень.

2) Пусть $C = \phi(m), \quad q_i, \quad i = \overline{1,k}$ - различные простые делители числа С. Для того, чтобы число a, взаимно простое с модулем m, было первообразным корнем, необходимо и достаточно невыполнения ни одного из сравнений: $a^{\frac{c}{q_i}+1} \equiv a(\mathrm{mod}\, m)$.

Теорема Гаусса.

Пусть p - нечётное простое число. Тогда по модулям вида $p^k, \quad 2p^k, \quad k \in N$, существуют первообразные корни.

Замечание.

Из свойства 1 первообразных корней и теоремы Гаусса следует, что первообразные корни существуют лишь по модулям $2, \quad 4, \quad p^k, \quad 2p^k, \quad k \in N$, где p - простое нечётное число.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Пример выполнения задания

Пример 1. Определить показатель, которому принадлежит 9 по модулю 10.

Решение.

$a = 9, m = 10.$

$\delta = 1 \quad 9^2 \equiv 9(\mathrm{mod}10) \quad \Leftrightarrow \quad 9 \equiv 1(\mathrm{mod}10)$

- неверно, т.к. $\frac{9-1}{10} = 0,8 \notin Z; \quad \delta = 2 \quad 9^3 \equiv 9(\mathrm{mod}10)$ - верно, т.к. 9^2-1/10=8, следовательно, $\delta = 2$ - показатель, которому принадлежит 9 по модулю 10.

Пример 2. Найти наименьший первообразный корень по модулю 23.

Решение.

$m = 23, \quad c = \phi(m) = 22 = 2*11; \quad q_1 = 2, \quad q_2 = 11.$ Таким образом, первообразный корень не должен удовлетворять двум сравнениям:

$$a^{\frac{22}{2}+1} \equiv a(\mathrm{mod}\,23), \quad m.e. \quad a^{12} \equiv a(\mathrm{mod}\,23) \quad \Leftrightarrow \quad a^{11} \equiv 1(\mathrm{mod}\,23);$$

$$a^{\frac{22}{11}+1} \equiv a(\mathrm{mod}\,23), \quad m.e. \quad a^{3} \equiv a(\mathrm{mod}\,23) \quad \Leftrightarrow \quad a^{2} \equiv 1(\mathrm{mod}\,23).$$

Испытываем числа 2,3,4,5,6,7,…

$$\frac{2^{11}-1}{23} = 89; \quad \frac{2^2-1}{23} = \frac{3}{23} \notin Z \quad \Rightarrow \quad 2^{11} \equiv 1(\mathrm{mod}\,23); \quad 2^2 \neq 1(\mathrm{mod}\,23).$$

$$\frac{3^2-1}{23} = \frac{8}{23} \notin Z; \quad \frac{3^{11}-1}{23} = 7702 \quad \Rightarrow \quad 3^{11} \equiv 1(\mathrm{mod}\,23); \quad 3^2 \neq 1(\mathrm{mod}\,23).$$

$$\frac{4^2-1}{23}=\frac{15}{23}\notin Z;\quad \frac{4^{11}-1}{23}=182361\quad\Rightarrow\quad 4^{11}\equiv 1(\mathrm{mod}\,23);\quad 4^2\neq 1(\mathrm{mod}\,23).$$

$$\frac{5^2-1}{23}=\frac{24}{23}\notin Z;\quad \frac{5^{11}-1}{23}=48828124\notin Z\quad\Rightarrow\quad 5^{11}\equiv 1(\mathrm{mod}\,23);\quad 5^2\neq 1(\mathrm{mod}\,23).$$

6.2 Варианты работ

Вариант 1.

1. Найти показатель, которому принадлежит заданное число *a* по заданному модулю *m*:
   a = 7, *m* = 43;
2. Найти наименьшие первообразные корни по заданным модулям:
   m =17;

Вариант 2.

1. Найти показатель, которому принадлежит заданное число *a* по заданному модулю *m*:
   a = 5, *m* = 108;
2. Найти наименьшие первообразные корни по заданным модулям:
   m = 19;

Вариант 3.

1. Найти показатель, которому принадлежит заданное число *a* по заданному модулю *m*:
   a = 13, *m* = 47;
2. Найти наименьшие первообразные корни по заданным модулям:
   m =23;

Вариант 4.

1. Найти показатель, которому принадлежит заданное число *a* по заданному модулю *m*:
   a = 9, *m* = 13;
2. Найти наименьшие первообразные корни по заданным модулям:
   m = 29;

Вариант 5.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   $a = 3$, $m = 25$;
2. Найти наименьшие первообразные корни по заданным модулям:
   $m = 31$;

Вариант 6.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   $a = 7$, $m = 20$;
2. Найти наименьшие первообразные корни по заданным модулям:
   $m = 34$;

Вариант 7.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   $a = 13$, $m = 43$;
2. Найти наименьшие первообразные корни по заданным модулям:
   $m = 37$;

Вариант 8.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   $a = 11$, $m = 56$;
2. Найти наименьшие первообразные корни по заданным модулям:
   $m = 38$;

Вариант 9.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   $a = 9$, $m = 49$;

2. Найти наименьшие первообразные корни по заданным модулям:
   m =41

Вариант 10.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   a = 11, m = 37;
2. Найти наименьшие первообразные корни по заданным модулям:
   m =43;

Вариант 11.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   a = 7, m = 45;
2. Найти наименьшие первообразные корни по заданным модулям:
   m =47;

Вариант 12.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   а) a = 10, m = 51;
2. Найти наименьшие первообразные корни по заданным модулям:
   m =46;

Вариант 13.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:
   a = 5, m = 17;
2. Найти наименьшие первообразные корни по заданным модулям:
   m =53;

Вариант 14.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 5, m = 23;

2. Найти наименьшие первообразные корни по заданным модулям:

m =58;

Вариант 15.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 11, m = 59;

2. Найти наименьшие первообразные корни по заданным модулям:

m =59;

Вариант 16.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 13, m = 23;

2. Найти наименьшие первообразные корни по заданным модулям:

m =61;

Вариант 17.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 13, m = 29;

2. Найти наименьшие первообразные корни по заданным модулям:

m =62;

Вариант 18.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 10, m = 61;

2. Найти наименьшие первообразные корни по заданным модулям:

m =67;

Вариант 19.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 5, m = 31;

2. Найти наименьшие первообразные корни по заданным модулям:

m =68;

Вариант 20.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 11, m = 73;

2. Найти наименьшие первообразные корни по заданным модулям:

m =71;

Вариант 21.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 17, m = 97;

2. Найти наименьшие первообразные корни по заданным модулям:

m =73;

Вариант 22.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 11, m = 83;

2. Найти наименьшие первообразные корни по заданным модулям:

m =74;

Вариант 23.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 19, m = 108;

2. Найти наименьшие первообразные корни по заданным модулям:

m =78;

Вариант 24.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 23, m = 108;

2. Найти наименьшие первообразные корни по заданным модулям:

m =79;

Вариант 25.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 11, m = 83;

2. Найти наименьшие первообразные корни по заданным модулям:

m =82;

Вариант 26.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 15, m = 71;

2. Найти наименьшие первообразные корни по заданным модулям:

m =83;

Вариант 27.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 14, m = 81;

2. Найти наименьшие первообразные корни по заданным модулям:

m =86;

Вариант 28.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 19, m = 67;

2. Найти наименьшие первообразные корни по заданным модулям:

m =89;

Вариант 29.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 8, m = 129;

2. Найти наименьшие первообразные корни по заданным модулям:

m =92;

Вариант 30.

1. Найти показатель, которому принадлежит заданное число a по заданному модулю m:

a = 11, m = 120;

2. Найти наименьшие первообразные корни по заданным модулям:

m =97;

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое показатель числа?
2. Что такое первообразный корень?
3. Свойства первообразных корней, назовите их.
4. По каким модулям существуют первообразные корни?
5. Что необходимо для того, чтобы число, взаимно простое с модулем, было первообразным корнем?

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