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.

ФУНКЦИЯ ЭЙЛЕРА

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

Курск 2016

УДК 511.17

Составитель М.А. Ефремов

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

Функция Эйлера: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 8 с., Библиогр.: с. 8.

Содержат основные сведения о функции Эйлера и ее свойствах как мультипликативной функции, а также способах ее нахождения. Указывается порядок выполнения лабораторной 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
6. Пример выполнения работы.. 6
7. Варианты заданий... 6
8. Контрольные вопросы.. 7
9. Список использованных источников и литературы 8

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – научиться использовать функцию Эйлера для нахождения количества взаимно простых чисел с заданным числом.

2. ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Ознакомиться с примерами решения. Выбрать свой вариант задания и, учитывая форму выполнения, вычислить функцию Эйлера.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Выбрать свой вариант задания.
4. Вычислить функцию Эйлера для заданного числа.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Вычисление функции Эйлера.
4. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Функция Эйлера.

Количество классов вычетов в приведённой системе вычетов обозначается через $\varphi(m)$ и называется функцией Эйлера. Она определена для всех натуральных чисел и представляет собой количество чисел ряда $1,2,...,a$, взаимно простых с $(a,m)=1$ и x пробегает полную систему вычетов по модулю m, то $ax+b, \quad b\in Z$, также пробегает полную систему вычетов по модулю a.

Примеры. $\varphi(1)=1; \quad \varphi(2)=1; \quad \varphi(3)=2; \quad \varphi(4)=2; \quad \varphi(5)=4; \quad \varphi(6)=2.$

Свойства функции Эйлера.

Пусть p - простое число. Тогда:

$$\varphi(p)=p-1;$$

$$\varphi(p^k)=p^k-p^{k-1}=p^k(1-\frac{1}{p}), \quad k\in N.$$

Мультипликативные функции.

Определение. Функция $\Theta(a)$ называется мультипликативной, если она удовлетворяет условиям:

$\Theta(a)$ определена для всех $a\in N$ и $\Theta(a)\neq 0$, по меньшей мере, при одном таком a;

любые $a_1,a_2 \rhd 0, \quad (a_1,a_2)=1 \Rightarrow \Theta(a_1,a_2)=\Theta(a_1)\ \Theta(a_2)$.

Пример. $\Theta(a)=a^s, \quad s\in R$, - мультипликативная функция.

Лемма о мультипликативной функции Эйлера.

Если $(a,b)=1$, то $\varphi(ab)=\varphi(a)\varphi(b).$

Использую эту лемму, каноническое разложение числа на простые множители $a=p_1^{k1}p_2^{k2}...p_s^{ks}$ и свойство 2 функции Эйлера, получим:

$$\varphi(a)=\varphi(p_1^{k1})\varphi(p_2^{k2})...\varphi(p_s^{ks})=p_1^{k1}(1-\frac{1}{p_1})p_2^{k2}(1-\frac{1}{p_2})...p_s^{ks}(1-\frac{1}{p_s})=$$

$$\underbrace{p_1^{k1}p_2^{k2}...p_s^{ks}}_{a}(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_s}).$$

$$\varphi(a)=a\prod_{p|a}(1-\frac{1}{p})$$

6. ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

1. Пусть n=16. Так как $16 = 2^4$, то $\varphi(16) = 2^{4-1} \cdot (2-1)=8$.

2. Пусть n=30 . Так как $30=2\cdot 3\cdot 5$, то $\varphi(30)=\varphi(2)\varphi(3)\varphi(5)=$ $=(2-1)\cdot(3-1)\cdot(5-1)=8$.

3. Пусть n=2025. Так как $2025=3^4\cdot 5^2$, то $\varphi(2025)=\varphi(3^4)\cdot\varphi(5^2)=$ $= 3^{4-1}\cdot(3-1)\cdot 5^{2-1}\cdot(5-1)=1080$.

7. ВАРИАНТЫ ЗАДАНИЙ

№ вар.	*Число*
1	4448
2	5362
3	3347
4	2346
5	3753
6	5125
7	2750
8	4450
9	3531
10	3488
11	2332
12	2391
13	3399
14	7154
15	6148
16	7186
17	5452
18	5245
19	4214
20	5178
21	3823
22	6274
23	3842

24	5275
25	3318
26	4438
27	2423
28	6186
29	4286
30	7268

8. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что указывает функция Эйлера?
2. Что такое мультипликативная функция?
3. Что такое каноническое разложение составного числа?
4. Как находится функция Эйлера для простого числа?
5. Как находится функция Эйлера для составного числа?

9. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Виноградов И.М. Основы теории чисел. М.: Наука,1995.
2. Галочкин А.И., Нестеренко Н.В., Шидловский А.Б. Введение в теорию чисел. Изд - во МГУ, 1995.
3. Кудреватов Г.А. Сборник задач по теории чисел. М.: Просвещение,1970.
4. Ляпин С.Е., Баранова И.В., Борчугова З.Г. Сборник задач по элементарной математике. М.: Просвещение, 1973.
5. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999
6. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993
7. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003