Министерство образования и науки Российской Федерации

## САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

## ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО

Кафедра дискретной математики и

информационных технологий

## **ДИНАМИЧЕСКИЕ СИСТЕМЫ ФЕРМА-ЭЙЛЕРА**

## КУРСОВАЯ РАБОТА

Cтудента 3 курса, 321 гр.

Дневного отделения факультета КНиИТ

Решетникова Дмитрия Сергеевича

### Научный руководитель

доцент кафедры ДМиИТ к.ф.-м.н. \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ Кузнецова Л.В.

### Зав. кафедрой ДМиИТ

к.ф.-м.н., доцент \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ Тяпаев Л.Б.

#### Саратов 2011

Содержание

**Введение…………………………………………………………………………..3**

## **1 Теоретическая часть…………………………………………………..….4**

## **Группы Эйлера……………….…………………………………………...4**

* 1. **Функция Эйлера…………………………………………………………..5**
  2. **Теорема Ферма-Эйлера…………………………………………………..6**

1. **Динамическая система Ферма-Эйлера……………………………...…7**
   1. **Измерение степени случайности подмножества……………………...7**
2. **Описание работы программы…………………………………………..9**

**3.1 Результаты эксперимента………..……………………………………..10**

**Заключение……………………………………………………………………...11**

**Список использованных источников………………………………………..13**

**Приложение 1…………………………………………………………………...14**

**Приложение 2…………………………………………………………………...18**

## **Введение**

В данной курсовой работе изучается геометрическая прогрессия вида , где a = 2, t, её период T(n), а также параметры стохастичности её орбит.

## **Теоретическая часть**

### **1.1 Группы Эйлера**

**Определение.** Группой Эйлера Γ(n) называется мультипликативная группа взаимно простых с n вычетов по модулю n.

**Теорема 1**. Если числа a и b взаимно просты, то группа Эйлера их произведения — прямое произведение их групп Эйлера:

Г(ab) = Г (a) × Г (b).

**Теорема 2.** Если число n= p простое, то группа Эйлера Г (p) =Zp−1—циклическая группа.

**Теорема 3.** Если число n= pa  - степень нечетного простого числа, то его группа Эйлера - циклическая группа,

Г (pa) =

**Теорема 4.** Если число n=2a, a>2, — степень двойки, то его группа Эйлера есть произведение циклических групп порядков 2 и 2a−2:

Эти четыре теоремы доставляют все группы Эйлера, так как любое натуральное число можно разложить на простые множители.

**Следствие.** Группа Эйлера 􀀀(n) является циклической если и только если число n равно либо 2, либо 4, либо степени нечетного простого числа, либо удвоенной степени нечетного простого числа.

* 1. **Функция Эйлера**

**Определение.** Функция Эйлера , где n —натуральное число, равна количеству натуральных чисел, не больших n и взаимно простых с ним.

**Свойства**.

1. ,

если p — простое число. В частности, при n = 1 имеем ;

1. ,

если m и n взаимно просты. То есть Функция Эйлера мультипликативна;

1. ,

если a и m взаимно просты. Так называемая теорема Эйлера;

1. ;

,

если  — наименьшее общее кратное, a  — наибольший общий делитель.

При больших значениях аргумента n значение ϕ(n) растет, в среднем,

как cn, где близко к 2/3.

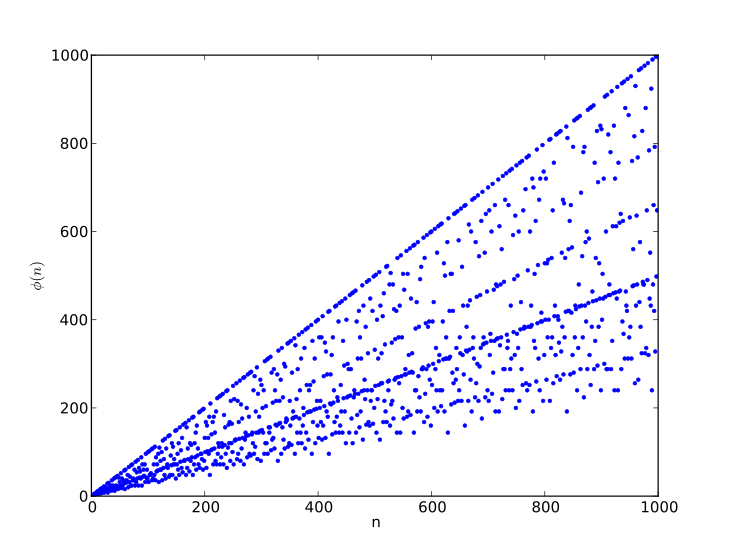


Рис 1. График функции Эйлера для значений n < 1000

* 1. **Теорема Ферма-Эйлера**

Зафиксируем взаимно простое с n число a и рассмотрим умножение на a как преобразование A множества Γ(n) взаимно простых с n вычетов по модулю n в себя: оно переводит вычет числа x в вычет числа ax (которое, как и x, взаимно просто с n). Мы определили перестановку A: Γ(n)→Γ(n), x →ax.

Преобразование A множества Γ(n) в себя, как и любое взаимно-однозначное преобразование, разбивается на циклы этой перестановки ϕ(n) элементов.

**Теорема.** Все циклы перестановки Ферма-Эйлера A: Γ(n)→Γ(n) имеют одинаковый период T(n, a).

**Следствие**. Множество Γ(n) взаимно простых с n вычетов по модулю n разбивается на N(n, a) =ϕ(n)/T(n, a) непересекающихся орбит преобразования Ферма—Эйлера, так что число орбит N, как и период T , является делителем значения функции Эйлера, ϕ(n) =NT ; и выполняется сравнение Ферма-Эйлера

**Пример.** Рассмотрим все циклы перестановки Γ(31), при а=2.

1\*2 mod 31= 2\*4 mod 31= 8\*2 mod 31= 16\*2 mod 31 = 1

3\*2 mod 31 = 6\*2 mod 31 = 12\*2 mod 31 = 24\*2 mod 31 = 17\*2 mod 31 = 3

9\*2 mod 31 = 18\*2 mod 31 = 5\*2 mod 31 = 10\*2 mod 31 = 20\*2 mod 31 = 9

27\*2 mod 31 = 23\*2 mod 31 = 15\*2 mod 31 = 30\*2 mod 31 =29\*2 mod 31 = 27

19\*2 mod 31 = 7\*2 mod 31 = 14\*2 mod 31 = 28\*2 mod 31 = 25\*2 mod 31 = 19

26\*2 mod 31 = 21\*2 mod 31 = 11\*2 mod 31= 22\*\*2 mod 31= 13\*\*2 mod 31 = 26

В этом случае получаем 6 орбит с циклами T(31, 2) = 5 (табл. 1.1)

Таблица 1.1

Орбиты для группы Эйлера Г (31)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 4 | 8 | 16 |
| 3 | 6 | 12 | 24 | 17 |
| 9 | 18 | 5 | 10 | 20 |
| 27 | 23 | 15 | 30 | 29 |
| 19 | 7 | 14 | 28 | 25 |
| 26 | 21 | 11 | 22 | 13 |

1. **Динамическая система Ферма-Эйлера**

**Определение.** Динамическая система - математическая абстракция, предназначенная для описания и изучения систем, эволюционирующих с течением времени.

Динамической системой называется отображение  вида A(x)=ax, где (a,n)=1, то есть a и n взаимно простые числа.

**2.1 Измерение степени случайности подмножества.**

Для того, чтобы исследовать, насколько случайно расположены точки орбиты {at } преобразования Ферма—Эйлера среди всех вычетов, входящих в Zn (или среди m=(n) взаимно простых с n вычетов, составляющих 18 группу Эйлера Г(n)), измеряется «расталкивание» элементов T - элементного множества точек отрезка друг другом.

Обозначим через {x1, . . . , xT } последовательность расстояний между соседними точками.

Cклеиваем концы отрезка в окружность, так что сумма положительных чисел xi равна длине L этого отрезка или окружности.

Для измерения присутствия или отсутствия близких сближений точек множества используем «параметр стохастичности»

Чтобы сделать параметр безразмерным (не зависящим от единиц измерения, т. е. от длины L), нормализуем его, преобразовав отрезок, к случаю L=1:

Параметр стохастичности r является моментом инерции точки x относительно начала координат (квадратом расстояния от x до 0). Поэтому его наименьшее значение соответствует центру симплекса: xi =1/T , rmin =T(1/T)2 =1/T , а наибольшее значение - вершине (x1 =1, остальные нули): rmax =1.

Для сравнения множеств с разным числами элементов T естественно ввести бинормализованный параметр стохастичности:

Интервал изменения этого параметра при различных выборах подмножеств окружности из T элементов есть:

Минимальное значение, s =1, достигается при равноудаленном положении вершин правильного T - угольника xi =1/T (считая L=1). В этом случае можно говорить о «сильном расталкивании», не допускающем сближения точек.

Максимальное значение, s =T , достигается на скученном кластере из T слившихся точек, для которого все расстояния xi равны нулю, кроме одного, равного единице. В этом случае можно говорить о «сильном притяжении», собравшем все точки в одно место.

Подмножество наиболее стохастично, если его бинормализованный параметр стохастичности s 2.

1. **Описание работы программы.**

Программа подсчитывает бинормализованный параметр стохастичности для распределения орбиты на множестве Г(n), где и n – нечетное число.

нет

Начало

Поиск всех делителей числа n

Получение группы Эйлера для n

Получение одной орбиты для данной группы Эйлера

Сортировка полученной орбиты по возрастанию

Подсчет параметра стохастичности

Подсчет нормализованного параметра стохастичности

Подсчет бинормализованного параметра стохастичности

Вывод полученных результатов

n = 3; NMAX = 32000;

N<=NMAX

Конец

да

Программа работает по следующему алгоритму:

1. Проводится поиск все делителей числа n. Проверяется остаток от деления n на все числа меньше него, если остаток равен 0, значит, текущее число является делителем числа n, и оно добавляется в список делителей.
2. Поиск группы Эйлера, то есть получение всех чисел, которые меньше n и являются взаимно простыми с n. В этом пункте ведется поиск общих делителей числа n и текущего числа, если их не оказалось, то делается вывод, что число взаимно простое с n, и добавляется в группу Эйлера Г(n).
3. Генерируем орбиту, по формуле , начиная с t = 0.
4. Сортируем полученную орбиту по возрастанию для удобства обработки.
5. Подсчет параметра стохастичности, нормализованного параметра стохастичности и бинормализованного параметра стохастичности по соответствующим формулам.
6. Повторение первых пяти пунктов для всех n
   1. **Результаты эксперимента**

13,755% всех подмножеств имеют бинормализованный параметр стохастичности , т.е. они стохастичны.

9,72% всех подмножеств имеют бинормализованный параметр стохастичности т.е. они “стягиваются”

76,525% всех подмножеств имеют бинормализованный параметр стохастичности , т.е. они “расталкиваются”

Список орбит, с s:

n = 1541 s = 1.9991860756323567 T = 1435

n = 2849 s = 1.9998456790123456 T = 2092

n = 4395 s = 1.9993578767123288 T = 2332

n = 4959 s = 1.9993937389770722 T = 2998

n = 11633 s = 2.000386863823934 T = 11631

n = 13185 s = 1.999357876712329 T = 7004

n = 15229 s = 1.999599358974359 T = 14911

n = 16269 s = 1.9995396205357143 T = 8941

n = 17401 s = 2.0002758620689653 T = 17399

n = 17673 s = 2.0003209617180207 T = 11381

n = 19527 s = 2.000174618525682 T = 12374

n = 19943 s = 1.9998456790123456 T = 15052

n = 21975 s = 1.9993578767123288 T = 11676

n = 22763 s = 1.9991255616830066 T = 19495

n = 23279 s = 1.9998511032125839 T = 23221

n = 24949 s = 1.9999931917211327 T = 24479

n = 25987 s = 2.000176102027954 T = 23936

n = 29371 s = 1.999860747687764 T = 28036

n = 31135 s = 1.9991174163179917 T = 22902

n = 31301 s = 2.000916580400276 T = 30911

n = 31339 s = 1.9998456790123456 T = 23692

**Заключение**

Из проделанного эксперимента видно, что в большинстве случаев точки орбит {2t} “расталкиваются”, то есть бинормализованный параметр стохастичности меньше 1,9. Количество “расталкивающихся” орбит уменьшается с ростом n. Для n<1000 их количество составляет 84,2%, а для 20000 < n < 25000 их количество падает до 74,32%.

Количество стохастичных орбит колеблется от 6,8% (для 3 < n < 1000) до 16,36% (для 20000 < n < 25000). Также процентное содержание стохастичных орбит увеличивается с ростом n. В среднем количество стохастических орбит равно 13,755%.

“Стягивающиеся” орбиты составляют в среднем 9,72%, и колеблются от 8,97% (для 25000 < n < 32000) до 10,16% (для n < 5000).

**Список использованных источников**

1. В.И. Арнольд «Группы Эйлера и арифметика геометрических прогрессий»
2. <http://ru.wikipedia.org/wiki/Функция_Эйлера>

**Приложение 1**

package cursovaya;

import java.util.ArrayList;

import java.util.Iterator;

public class CourseWork {

public static ArrayList findDeviders(int n) //Опеределение делителей числа:

{

int k=2;

ArrayList deviders = new ArrayList();

while (k<n) {

if (n%k==0)

{ deviders.add(k); }

k++; }

return deviders;

}

public static boolean isRelativelyPrime(ArrayList deviders, int i) {

Iterator iterator = deviders.iterator();

for (int l=0;iterator.hasNext();l++) {

Integer h = (Integer) iterator.next();

if (i%h==0) {return false;}

}

return true;

}

public static ArrayList findGauss(int n)

//поиск множества взаимно простых с n

{

ArrayList deviders = PartThree.findDeviders(n);

ArrayList list = new ArrayList();

for(int i=1; i<n; i++) {

if (PartThree.isRelativelyPrime(deviders, i))

{ list.add(i); }

}

return list;

}

public static Integer[] toArray (ArrayList gaussList)

{

Iterator iterator = gaussList.iterator();

Integer[] gaussArray = new Integer[gaussList.size()];

for (int i=0;i<gaussList.size();i++)

{

gaussArray[i] = (Integer) iterator.next();

}

return gaussArray;

}

public static ArrayList getOrbita(int q, int n)//получаем последоватеьлность

//начиная с единицы

{

int h = 1;

ArrayList orbita = new ArrayList();

for(int i=0;h\*2%n!=1 ;i++)

{

orbita.add(h);

h = h\*q;

h = h%n;

}

orbita.add(h);

return orbita;

}

public static Integer[] sort(Integer[] array)//сортировка по возрастанию

{

for (int i=0;i<array.length;i++) {

for( int j=0; j<array.length;j++) {

if (array[i]<array[j]) {

Integer t = array[i];

array[i] = array[j];

array[j] = t;

}

}

}

return array;

}

public static void doCourseWork(int q) {

for (int n =3; n<=10000;n++) {

if (n%q==0){n++;}

Integer[] gaussArray = toArray(findGauss(n));//получаем Гаусово множество

Integer[] orbita = toArray(getOrbita(q, n));//получаем один из периодов

orbita = sort(orbita);//СОРТИРОВКА ПОЛУЧЕННОГО периода

ArrayList<Integer> index = new ArrayList<Integer>();

for (int j=0; j<orbita.length; j++)//Получение индексов элементов

// внутри Гаусовского мн-ва

{ int i;

for (i=0; i<gaussArray.length; i++)

{ if (gaussArray[i].equals(orbita[j])) break; }

index.add(i);

}

double R = 0;//Параметр стохастичности

Integer T;

for (int j=1; j+1<index.size(); j++) {

R = R + (index.get(j+1) - index.get(j))\*( index.get(j+1) - index.get(j));

T = index.get(j);

}

T = index.get(index.size()-1);

R+=(gaussArray.length - index.get(index.size()-1))\*(gaussArray.length - index.get(index.size()-1))+1;

double r; //Нормализованный параметр стохастичности

r = R/gaussArray.length/gaussArray.length;

double s = r\*orbita.length;//бинормализованный параметр стохастичности

double s1 = 2\*(double)gaussArray.length/((double)gaussArray.length+1);

System.out.print( " R = " + R + " r = " + r + " s = " + s + " s1 = " + s1 + " n = "+ n + " T = "+ orbita.length + "\n");

}

}

}

**Приложение 2**

График зависимости s(n) для n < 1000

График зависимости T(n) для n < 2000