МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра системного анализа и автоматического управления

Отчет по заданию 2. Вариант $10(29 \bmod 20 + 1 = 10)$

Студента 3 курса 321 группы направления 09.03.01 ИВТ

Факультета компьютерных наук и информационных технологий

Чесакова Максима Евгеньевича

Задача №1 Проверить на биективность/транзитивность полиномы $f(x) = 18 + x - 7x^2$ и $g(x) = \frac{17}{19}x - \frac{1}{15}$ на $\mathbb{Z}_2$. Решить задачу аналитически, затем проверить с помощью программной реализации.

Аналитическое решение.

Теорема Ларина. *Многочлен F с целыми или рациональными 2-адическими коэффициентами биективен (транзитивен) на $\mathbb{Z}_2$, тогда и только тогда, когда F биективен (транзитивен) по модулю 4, т. е. редукция $F \mod 4$ является перестановкой (транзитивен по модулю 8, т. е. редукция $F \mod 8$ одноцикловая перестановка)*

Найдём редукцию $f \mod 4$:

$18 = (0)^\infty 10010, \quad 1 = (0)^\infty 1, \quad -7 = (1)^\infty 001, \quad \Rightarrow \quad f \mod 4 = 2 + x + x^2.$

$f(0) \mod 4 = 2, \quad f(1) \mod 4 = 0, \quad f(2) \mod 4 = 0, \quad f(3) \mod 4 = 2.$

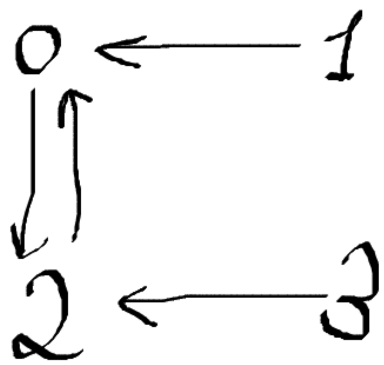

Рисунок 1 – диаграмма $f \mod 4$

Следовательно, f не биективна на $\mathbb{Z}_2$. Следовательно не транзитивна на $\mathbb{Z}_2$.

Найдём редукцию $g \mod 4$:

Для разложения дробей в 2-адические числа используем лемму Малера:

Лемма Малера. *Пусть* $r, s, p \in \mathbb{Z}$; $s \geq 1$ *и пусть* $p \geq 2$, *НОД*$(p, s) = 1$. *Тогда существуют уникальные* $A, R \in \mathbb{Z}$ *такие, что* $\frac{r}{s} = A + p\frac{R}{s}$, *где* $0 \leq A \leq p-1$.
С помощью леммы имеем:

– –

$$\frac{17}{19} = 1 + 2 \cdot \frac{-1}{19},$$
$$\frac{-1}{19} = 1 + 2 \cdot \frac{-10}{19},$$
$$\frac{-10}{19} = 0 + 2 \cdot \frac{-5}{19},$$
$$\frac{-5}{19} = 1 + 2 \cdot \frac{-12}{19},$$
$$\frac{-12}{19} = 0 + 2 \cdot \frac{-6}{19},$$
$$\frac{-6}{19} = 0 + 2 \cdot \frac{-3}{19},$$
$$\frac{-3}{19} = 1 + 2 \cdot \frac{-11}{19},$$
$$\frac{-11}{19} = 1 + 2 \cdot \frac{-15}{19},$$
$$\frac{-15}{19} = 1 + 2 \cdot \frac{-17}{19}, \qquad \Longrightarrow \quad \frac{17}{19} = (000011010111100101)^{\infty}1$$
$$\frac{-17}{19} = 1 + 2 \cdot \frac{-18}{19},$$
$$\frac{-18}{19} = 0 + 2 \cdot \frac{-9}{19}.$$
$$\frac{-9}{19} = 1 + 2 \cdot \frac{-14}{19},$$
$$\frac{-14}{19} = 0 + 2 \cdot \frac{-7}{19},$$
$$\frac{-7}{19} = 1 + 2 \cdot \frac{-13}{19},$$
$$\frac{-13}{19} = 1 + 2 \cdot \frac{-16}{19},$$
$$\frac{-16}{19} = 0 + 2 \cdot \frac{-8}{19}.$$
$$\frac{-8}{19} = 0 + 2 \cdot \frac{-4}{19},$$
$$\frac{-4}{19} = 0 + 2 \cdot \frac{-2}{19}.$$
$$\frac{-2}{19} = 0 + 2 \cdot \frac{-1}{19}.$$

– –

$$\frac{-1}{15} = 1 + 2 \cdot \frac{-8}{15},$$
$$\frac{-8}{15} = 0 + 2 \cdot \frac{-4}{15},$$
$$\frac{-4}{15} = 0 + 2 \cdot \frac{-2}{15}, \qquad \Longrightarrow \quad \frac{-1}{15} = (0001)^{\infty}$$

$\dfrac{-2}{15} = 0 + 2 \cdot \dfrac{-1}{15},$

$g \mod 4 = 3x + 1.$

$g(0) \mod 4 = 1, \quad g(1) \mod 4 = 0, \quad g(2) \mod 4 = 3, \quad g(3) \mod 4 = 2.$

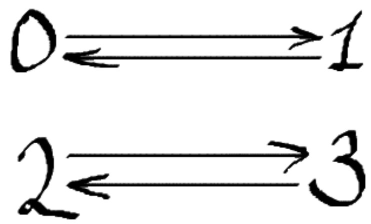

Рисунок 2 – диаграмма $g \mod 4$

Следовательно, g биективна на $\mathbb{Z}_2$. Проверим транзитивность. Найдём редукцию $g \mod 8$:

$g \mod 8 = 3x + 1.$

$g(0) \mod 8 = 1, \quad g(1) \mod 8 = 4, \quad g(2) \mod 8 = 7, \quad g(3) \mod 8 = 2,$

$g(4) \mod 8 = 5, \quad g(5) \mod 8 = 0, \quad g(6) \mod 8 = 3, \quad g(7) \mod 8 = 6.$

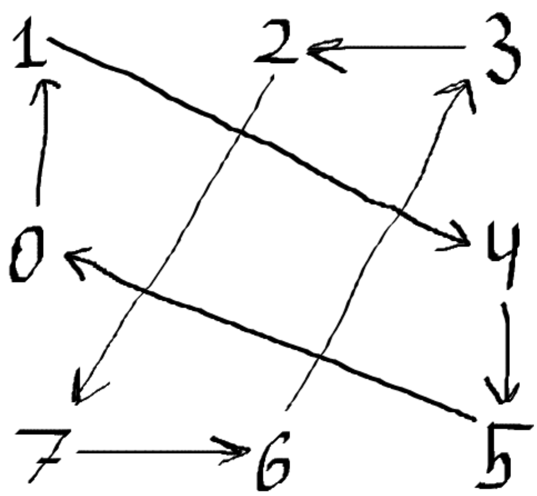

Рисунок 3 – диаграмма $g \mod 8$

Функция $g \mod 8$ имеет двухцикловую перестановку, следовательно g не транзитивна на $\mathbb{Z}_2$.

Ответ: f не биективна, не транзитивна на $\mathbb{Z}_2$, g биективна на $\mathbb{Z}_2$, но не транзитивна на $\mathbb{Z}_2$.

Программная реализация на Python.

Исходный код представлен в файле 2.py. Результаты его работы представлены на рисунках 3 — 6.

```
-----------------------------------
     f(x) = 18 + 1x - 7x^2

-----------------------------------
f mod 4 = 2 + 1x + 1x²
0 -> 2
1 -> 0
2 -> 0
3 -> 2
Не биекция => полином не транзитивен
```

Рисунок 4 – Проверка $f(x)$

```
------------------------------
     g(x) = (17/19)x - (1/15)

------------------------------
g mod 4 = 1 + 3x + 0x²
0 -> 1
1 -> 0
2 -> 3
3 -> 2
Полином является биекцией.
 ...Проверка транзитивности на Z8...
g mod 8 = 1 + 3x + 0x²
0 -> 1
1 -> 4
2 -> 7
3 -> 2
4 -> 5
5 -> 0
6 -> 3
7 -> 6
Не циклическая перестановка => полином не транзитивен
```

Рисунок 5 – Проверка $g(x)$

1

2

```
______________________________________
Разложение дробей по лемме (p=2)

______________________________________
a_0: 17/19
17/19 = 1 + 2*(-1/19)
-1/19 = 1 + 2*(-10/19)
-10/19 = 0 + 2*(-5/19)
-5/19 = 1 + 2*(-12/19)
-12/19 = 0 + 2*(-6/19)
-6/19 = 0 + 2*(-3/19)
-3/19 = 1 + 2*(-11/19)
-11/19 = 1 + 2*(-15/19)
-15/19 = 1 + 2*(-17/19)
-17/19 = 1 + 2*(-18/19)
-18/19 = 0 + 2*(-9/19)
-9/19 = 1 + 2*(-14/19)
-14/19 = 0 + 2*(-7/19)
-7/19 = 1 + 2*(-13/19)
-13/19 = 1 + 2*(-16/19)
-16/19 = 0 + 2*(-8/19)
-8/19 = 0 + 2*(-4/19)
-4/19 = 0 + 2*(-2/19)
-2/19 = 0 + 2*(-1/19)
Результат: (000011010111100101)1

a_0: -1/15
-1/15 = 1 + 2*(-8/15)
-8/15 = 0 + 2*(-4/15)
-4/15 = 0 + 2*(-2/15)
-2/15 = 0 + 2*(-1/15)
Результат: (0001)
```

Рисунок 6 – Разложение дробей в 2-адические числа