БЫСТРАЯ ПРОВЕРКА МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ НА НЕПРИВОДИМОСТЬ И ПРИМИТИВНОСТЬ

СТУДЕНТ	ПИВЕНЬ ВАДИМ НИКОЛАЕВИЧ	КМБО-01-16
РУКОВОДИТЕЛЬ	ПАРФЕНОВ ДЕНИС ВАСИЛЬЕВИЧ	К.Т.Н., ДОЦЕНТ

АЛГОРИТМ БЕРЛЕКЭМПА

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: $n = deg(poly)$
5: if $n = 0$ or $(poly[0] = 0$ and $n > 1)$ then
6: return $false$
7: end if
8: if $n = 1$ then
9: return $true$
10: end if
11:
12: $poly' = \frac{\partial poly}{\partial x}$
13: if $poly' = 0$ then
14: return $false$
15: end if
16: if $deg\left(gcd\left(poly, poly'\right)\right) = 0$ then
17: return $false$
18: end if
19: $B = \begin{pmatrix} x^0 & mod & poly \\ x^P & mod & poly \\ \dots & \dots & \dots \\ x^{P \times (P-1)} & mod & poly \end{pmatrix}$
20: $B = B - E$
21: $r = rank(B)$
22: if $r = deg(poly) - 1$ then
23: return $true$
24: else
25: return $false$
26: end if

АЛГОРИТМ РАБИНА

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$ степени n,
$p_1, ..., p_k$ – простые делители n
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: if $n = 0$ or $(poly[0] = 0$ and $n > 1)$ then
5: return $false$
6: end if
7: if $n = 1$ then
8: return $true$
9: end if
10:
11: for $i = 1..k$ do
12: $n_i = \frac{n}{p_j}$
13: $g = gcd\left(poly, x^{P^{n_i}} - x \ (mod\ poly)\right)$
14: if $g = 0$ or $deg(g) > 0$ then
15: return $false$
16: end if
17: end for
18: $g = gcd\left(poly, x^{P^{n}} - x \ (mod\ poly)\right)$
19: if $g = 0$ then
20: return $true$
21: else
22: return $false$
23: end if

АЛГОРИТМ БЕН-ОРА

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

1: if $poly = 0$ then
2: return $false$
3: end if
4: $n = deg(poly)$
5: if $n = 0$ or $(poly[0] = 0$ and $n > 1)$ then
6: return $false$
7: end if
8: if $n = 1$ then
9: return $true$
10: end if
11:
12: $n = deg(poly)$
13: for $i = 1..\left[\frac{m}{2}\right]$ do
$g = gcd\left(poly, x^{P^i} - x \ (mod\ poly)\right)$
if $g = 0$ or $deg(g) > 0$ then
16: return $false$
17: end if
18: end for
19: return $true$

АЛГОРИТМ ПРОВЕРКИ НА ПРИМИТИВНОСТЬ

ВХОД: $poly$ - многочлен над полем Галуа $GF[P]$,
$p_1, ..., p_k$ – простые дилители $P-1$ за исключением 1 и самого $P-1$
РЕЗУЛЬТАТ: $true$ если многочлен неприводим, иначе $false$

```
1:  if poly = 0 then
2:      return false
3:  end if
4:  n = deg(poly)
5:  if n = 0 or (poly[0] = 0 and n > 1) then
6:      return false
7:  end if
8:
9:  poly = noramlize(poly)
10: if poly = x then
11:     return true
12: end if
13: if P = 2 and poly = 1 + x then
14:     return false
15: end if
16:
17: if P > 2 then
18:     for i = 1..k do
19:         l = (-1)^n (mod P)
            el = l^((P-1)/p_i)
            if el = 1 then
                return false
--.
23:         end if
24:     end for
25: end if
26:
27: l = (-1)^n (mod P)
28: r = (p^n - 1)/(p - 1)
29: if x^r ≠ l then
30:     return false
31: end if
32:
33: for i = 1..k do
34:     tmp = x^(r/q_i) (mod poly)
35:     if deg(tmp) = 0 then
36:         return false
37:     end if
38: end for
39: return true
```

СУЩЕСТВУЮЩИЕ РЕШЕНИЯ

Название	Неприводимость	Примитивность	Бесплатное решение
Wolfram Mathematica	$IrreduciblePolynomialQ$	$PrimitivePolynomialQ$ *	–
MATLAB	$gfprimck$	$gfprimck$	–
PARI/GP	$polisirreducible$	–	+
FLINT	$nmod\_poly\_is\_irreducible$ $nmod\_poly\_is\_irreducible\_ddf$ $nmod\_poly\_is\_irreducible\_rabin$	–	+
Результат данной работы**	$is\_irreducible\_berlekamp$ $is\_irreducible\_rabin$ $is\_irreducible\_benor$	$is\_primitive\_definition$	+

*Данная функция возвращает некорректный результат для неприведённых многочленов

**Исходный код и документацию можно найти на GitHub:
https://github.com/irreducible-polynoms/irrpoly

РЕАЛИЗОВАННЫЕ КЛАССЫ

Класс, представляющий поле Галуа, содержит:

- Основание поля Галуа
- Вектора всех обратных по умножению элементов поля

Класс, представляющий число в поле Галуа, содержит:

- Указатель, на экземпляр класса, представляющего поле Галуа
- Значение числа

Класс, представляющий многочлен над полем Галуа, содержит:

- Указатель, на экземпляр класса, представляющего поле Галуа
- Вектор коэффициентов, являющихся числами в поле Галуа

РЕАЛИЗАЦИЯ МЕТОДОВ ПРОВЕРКИ

Потребовалось реализовать следующие вспомогательные функции:

- **gcd** – вычисление наибольшего общего делителя двух многочленов
- ***derivative*** – вычисление производной многочлена
- ***integer_power*** – быстрое возведение в степень целого числа
- ***x_pow_mod*** – вычисляет остаток от деления x в заданной степени на заданный многочлен

Также был реализован **многопоточный конвейер**, рассчитанный на проверку последовательностей многочленов

ТЕСТИРОВАНИЕ И БЕНЧМАРКИНГ

Тестируемый алгоритм	Тест 1	Тест 2	Тест 3	Тест 4	Тест 5
	$GF[2]$ 200	$GF[3]$ 300	$GF[5]$ 400	$GF[7]$ 500	$GF[11]$ 600
Берлекэмпа	38,1	53,6	56,8	71,5	73,0
Рабина	161,2	360,0	583,0	549,0	1153,3
Бэн-Ора	52,6	51,7	56,0	57,3	47,6
Проверка на примитивность	548,8	1207,4	1426,1	1978,7	2765,0

Для каждого теста указано поле и количество многочленов заданной характеристики, которые требовалось найти; время указано в миллисекундах

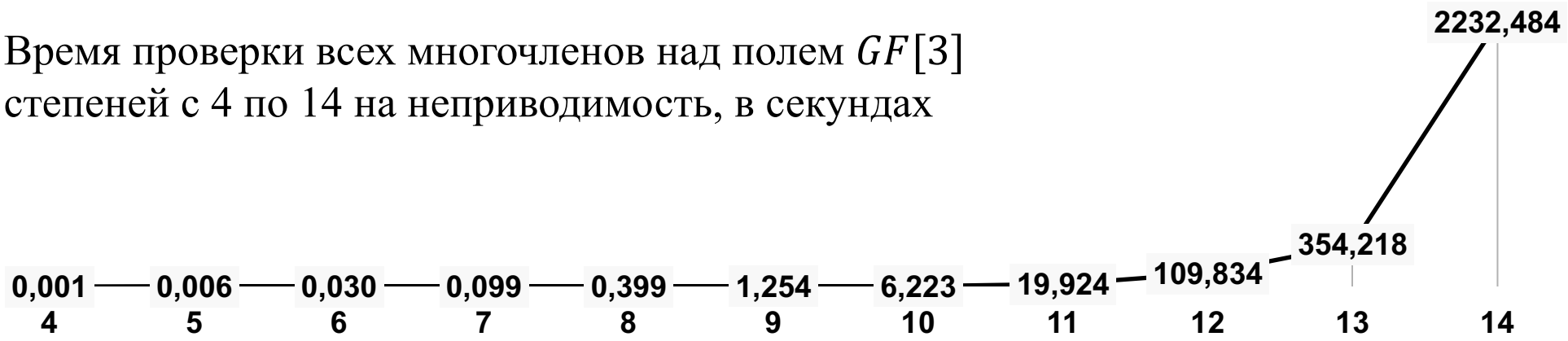
Приведённое время получено путём усреднения результатов 100 последовательных замеров

ПОВТОРНЫЙ БЕНЧМАРКИНГ

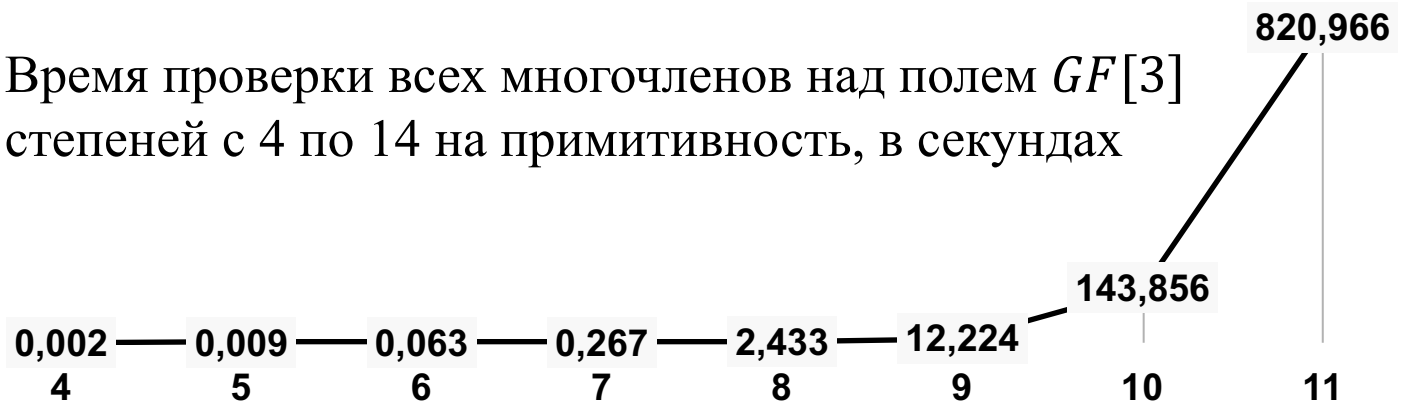
Тестируемый алгоритм	Тест 1	Тест 2	Тест 3	Тест 4	Тест 5
	$GF[2]$ 200	$GF[3]$ 300	$GF[5]$ 400	$GF[7]$ 500	$GF[11]$ 600
Берлекэмпа	38,9	56,8	59,6	75,7	78,1
Рабина	165,2	388,6	612,9	587,4	1280,6
Бэн-Ора	55,9	54,8	49,3	61,1	54,0
Проверка на примитивность	579,1	1288,5	1494,2	2102,6	3109,7
Рекомендуемая проверка на неприводимость	38,8	54,4	48,9	72,1	54,1
Рекомендуемая проверка на примитивность	255,8	728,7	973,3	1270,4	2370,8
Многопоточная проверка на неприводимость	74,5	71,1	67,4	81,7	64,8
Многопоточная проверка на примитивность	556,9	1114,5	1607,4	1917,6	3045,1

ЗАВИСИМОСТЬ ВРЕМЕНИ ВЫПОЛНЕНИЯ ПРОВЕРКИ ОТ СТЕПЕНИ ПРОВЕРЯЕМОГО МНОГОЧЛЕНА

Время проверки всех многочленов над полем $GF[3]$ степеней с 4 по 14 на неприводимость, в секундах



Время проверки всех многочленов над полем $GF[3]$ степеней с 4 по 14 на примитивность, в секундах



СРАВНЕНИЕ С АНАЛОГАМИ

Название проверяемой системы/библиотеки	Время выполнения проверок на неприводимость	Время выполнения проверок на примитивность
Wolfram Mathematica	25: 24.080	25: 27.077
MATLAB	39: 41.027	39: 41.027
PARI/GP	00: 02.187	–
FLINT*	00: 01.648	–
Реализованная в данной работе библиотека**	00: 06.776	02: 24.079

Время выполнения проверок тестовыми программами приведено в формате mm:ss.ms, где mm – минуты, ss – секунды, ms – миллисекунды

*Приведено время для метода Берлекэмпа-Цассенхауса, поскольку два других метода показали худшие результаты

**Приведено время работы рекомендованных методов проверки

БЫСТРАЯ ПРОВЕРКА МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ НА НЕПРИВОДИМОСТЬ И ПРИМИТИВНОСТЬ

СТУДЕНТ	ПИВЕНЬ ВАДИМ НИКОЛАЕВИЧ	КМБО-01-16
РУКОВОДИТЕЛЬ	ПАРФЕНОВ ДЕНИС ВАСИЛЬЕВИЧ	К.Т.Н., ДОЦЕНТ