МИНОБРНАУКИРОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Несепарабельный КМА на локальных полях положительной характеристики

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Фадеевой Алины Алексеевны

Научный руководитель
доцент, к.ф.-м.н. ____________________ Ю.С. Крусс
подпись, дата

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент ____________________ А.М. Водолазов
подпись, дата

Саратов 2025

Введение. Понятие кратномасштабного анализа (далее – КМА) было введено в конце 80-х годов XX века С. Малла и Й. Мейером. Основное предназначение КМА состоит в том, что на его основе можно построить ортогональный базис, полученный с помощью сжатий и сдвигов некоторой функции (или нескольки функций). Такие функции называются всплесками или вейвлетами, а базис – всплесковым базисом или вейвлет-базисом соответственно. В работах С. Малла и Й. Мейера рассматривается пространство $L^2(R)$. В дальнейшем понятие КМА было перенесено на другие алгебраические структуры: нульмерные группы, поля p-адических чисел, локальные поля. Локальным полем $F^{(s)}$ называется топологическое пространство, обладающее следующими свойствами: оно локально компактное, недискретное, полное, вполне несвязно, т.е. только пустое и одноточечное множество связны, также в $F^{(s)}$ определены операции сложения и умножения, удовлетворяющие аксиомам поля.

Целью данной работы является развитие теории несепарабельного кратномасштабного анализа на локальных полях положительной характеристики. В рамках исследования предполагается:

- построение масштабирующих уравнений и изучение их решений;

- изучить свойства масштабирующих функций и вейвлетов;

- разработать алгоритм нахождение неприводимых многочленов над заданным полем $GF(p)$.

В первой главе «Нульмерные группы, основные понятия» изложены основные определения и утверждения, необходимые для изложения результатов работы. Приведены основные сведения о нульмерных группах, включая вопросы меры и интегрирования. Также рассматривается двойственная к группе структура – группа характеров.

Во второй главе «Локальные поля» в начале формулируются основные определения и доказываются несложные общеизвестные теоермы, использующиеся потом для доказательств.

Параграф «Локальные поля положительной характеристики» посвящен вопросу о локальных полях положительной характеристики. Дается описание классического подхода к локальным полям в терминах образующего элемента, а также другого подхода, благодаря которому удается установить связь локальных полей и групп Виленкина. Так же рассматриваются конечные поля, а именно операции сложение и умножение в $GF(p)$.

В параграфе «Группа Виленкина как локальное поле и линейное пространство над полем $GF(p)$» рассматривается $(G, \dot{+})$ — p-ичная группа Виленкина.

В параграфе «Алгоритм построения масштабирующей функции на группах Виленкина G по N -валидному дереву» приводится алгоритм построения масштабирующей функции по N-валидному дереву на локальных полях положительной характеристики.

В третьей главе «Несепарабельный кратномасштабный анализ» рассматривается вопрос о том, будут ли хотя бы какие-то из построенных по алгоритму КМА несепарабельными.

В главе «Нахождение неприводимых многочленов над заданным полем $GF(p)$» для построения неприводимых многочленов над заданным полем в $Python$ используется библиотека $SymPy$. Показывается базовый способ генерации неприводимых многочленов над полем $GF(p)$. В таких полях используются неприводимые многочлены для описания структур и свойств объектов, таких как кривая или поверхность. В полях $GF(p)$ неприводимые многочлены служат основой для построения расширений полей, которые необходимы для реализации различных алгоритмов и теорем в алгебраической геометрии и других областях математики. Эти многочлены позволяют определить свойства объектов, анализируя их через поля.

Основное содержание работы. Введём необходимые определения.

Определение 1.1. Группа G называется топологической группой, если она обладает топологической структурой и при этом групповая операция и операция перехода к противоположному элементу непрерывны в данной топологии. Последнее означает, что:

1. для любой окрестности $U(x \dot{+} y)$ элемента $x \dot{+} y$ найдутся такие окрестности $U(x)$ и $U(y)$, что $U(x) \dot{+} U(y) \subset U(x \dot{+} y)$;
2. для любой окрестности $U(\dot{-}x)$ элемента x существует $U(x)$ такая что $\dot{-}\ U(x) \subset U(\dot{-}x)$.

Замечание 1. В обозначении операции $\dot{+}$ точка ставится для того, чтобы отличать операцию сложения на группе от обычной операции сложения.

Замечание 2. В данной работе рассматриваются только коммутативные группы.

Теорема 1.1. Пусть $(G, \dot{+})$ – топологическая группа, $\mathfrak{B}_0$ – некоторая полная система окрестностей нуля. Тогда $\mathfrak{B} = a\dot{+}U \quad | \quad U \in \mathfrak{B}, a \in G$ – есть полная система окрестностей в группе $(G, \dot{+})$, а система $\mathfrak{B}_0$ удовлетворяет следующим условиям:

1. $\bigcap\limits_{U \in \mathfrak{B}_0} U = 0$;
2. $\forall\, U,\, V \in \mathfrak{B}_0 \;\exists\, W \in \mathfrak{B}_0$: $W \subset U \cap V$;
3. $\forall\, U \in \mathfrak{B}_0 \;\exists\, V \in \mathfrak{B}_0$: $V\dot{+}(\dot{-}V) \subset U$;
4. $\forall\, U \in \mathfrak{B}_0, \forall\, a \in U \;\exists\, V \in \mathfrak{B}_0$: $V\dot{+}a \subset U$.

Справедливо и обратное утверждение.

Теорема 1.2. Пусть $(G, \dot{+})$ – алгебраическая группа и $\mathfrak{B}_0$ – некоторая система подмножеств множества G, удовлетворяющая условиям теоремы 1 Тогда в множестве G можно ввести топологию и притом единственным способом, так что при этом групповая операция $\dot{+}$ будет непрерывна в этой топологии и система $\mathfrak{B}_0$ будет полной системой окрестностей нуля.

Для топологических групп, как и для алгебраических, вводятся понятия подгруппы, смежного класса, фактор-группы.

Определение 1.2 Множество $H \subset G$ называется подгруппой топологической группы G, если

1. H – подгруппа G в алгебраическом смысле;
2. H – замкнутое подмножество в топологии G.

Одно из важных свойств подгрупп топологической группы G отражено в следующей теореме.

Теорема 1.3. Всякая открытая подгруппа H топологической группы G замкнута.

Теорема 1.4.(теорема Силова) Пусть G – конечная группа, p – порядок группы. Если число q^α делит p (q - простое, $\alpha \in \mathbb{N}$), то в группе G существуют подгруппы порядка q^α.

Определение 1.3. Наличие топологии в группе $(G, \dot{+})$ позволяет нам рассматривать непрерывные функции, определенные на G. Непрерывную функцию $\chi : G \to \Delta$ (Δ – граница единичного круга в комплексной плоскости), удовлетворяющую условию

$$\chi(x_1 \dot{+} x_2) = \chi(x_1)\chi(x_2). \tag{1.1}$$

называют характером группы G. Выберем в качестве x_2 ноль и подставим в 1.6, получим $\chi(0) = 1$. Выберем в качестве $x_2 = \dot{-}x_1$ получим, что $\chi(x_1)\chi(\dot{-}x_1) = \chi(0) = 1$, и как следствие получим следующую формулу

$$\chi(\dot{-}x_1) = \frac{1}{\chi(x_1)} = \overline{\chi(x_1)}.$$

Теорема 1.5. Характеры компактной нульмерной группы G образуют группу $(\chi, \cdot)$ относительно операции умножения.
Теорема 1.6. Совокупность характеров компактной нульмерной группы G образует ортонормированный базис в $L_2(G)$.
Теорема 1.7. Характеры локально компактной нульмерной группы G образуют группу $(X, \cdot)$ относительно операции умножения.
Теорема 1.8. Пусть G – нульмерная локально компактная коммутативная группа и f – гладкая финитная функция на G. Тогда имеет место равенство

$$f(x) = \int_X \hat{f}(\chi)(\chi, x)d\nu(\chi),$$

где $\hat{f}$ – преобразование Фурье функции f.
Теорема 1.9.(Равенство Планшереля для гладких финитных функций) Пусть f, g – гладкие финитные функции. Тогда справедливо равенство

$$\int_G f(x)\overline{g(x)}d\mu(x) = \int_X \hat{f}(\chi)\overline{\hat{g}(\chi)}d\nu(\chi).$$

Теорема 1.10. Справедливо равенство

$$\hat{f}(\chi) = \lim_{n\to\infty} \hat{f}_n(\chi),$$

где $\hat{f}_n(\chi) = \int_{G_n} f(x)\overline{(\chi, x)}d\mu(x)$, и предел в понимается в смысле сходимости по норме $L_2(X)$, то есть

$$\lim_{n\to\infty} ||\hat{f}(\chi) - \hat{f}_n(\chi)||_{L_2(X)} = 0.$$

Для функций из $L_2(G)$ верно равенство Планшереля.

Теорема 1.11.(Равенство Планшереля) Пусть f, $g \in L_2(G)$, тогда справедливо равенство

$$\int_G f(x)\overline{g(x)}d\mu(x) = \int_X \hat{f}(\chi)\overline{\hat{g}(\chi)}d\nu(\chi).$$

Определение 2.1.

Оператор растяжения $\mathscr{A}$ определяем равенством
$\mathscr{A}x = x\frac{1}{\mathfrak{p}}$. Очевидно, что $|\mathscr{A}x| = |x|p^s$.

Определение 2.2. Множество сдвигов определяется равенством

$$I_K = \{g = a_{-1}p^{-1}\dot{+}a_{-2}p^{-2}\dot{+}\ldots\dot{+}a_{-\nu}p^{-\nu}: \quad \nu \in \mathbb{N}, a_{-j} \in GF(p^s)\}.$$

Имея оператор растяжения и множество сдвигов, можно определить КМА в $L_2(K)$ стандартным образом.

Определение 2.3. Пусть $F^{(s)}$ локальное поле положительной характеристики. Совокупность замкнутых подпространств $\{V_n\}_{n\in\mathbb{Z}} \in L_2(F^{(s)})$ называется КМА в $L_2(F^{(s)})$, если выполнены следующие аксиомы:

1. $V_n \subset V_{n+1}$;
2. $\overline{\bigcup_{n\in\mathbb{Z}} V_n} = L_2(F^{(s)})$;
3. $\bigcup_{n\in\mathbb{Z}} V_n =\{0\}$;
4. $f(x) \in V_n \Leftrightarrow f(\mathcal{A}x) \in V_{n+1}$, $\mathcal{A}$ - оператор растяжения;
5. существует функция $\varphi \in V_0$ такая, что система сдвигов $\{\varphi(x\dot{-}h)\}_{h\in H_0}$ образует ортонормированный базис в V_0. H_0 - множество сдвигов.

Функция φ из аксиомы 5 называется масштабирующей функцией для данного КМА.

Теорема 2.1. Пусть $F^{(s)}$ - локальное поле положительной характеристики p,

p – простое число. Если система замкнутых подпространств $\{V_j\}_{j\in\mathbb{Z}}$ в $L_2(F^{(s)})$ удовлетворяет аксиомам 1-5 определения 17 и существуют интегрально-периодические функции $m^{(\mathbf{l})}$ $\mathbf{l} \in GF(p^s)$, $\mathbf{l} \neq 0$ такие, что матрица
$M(\chi) = [m^{(\mathbf{l})}\ (\chi \mathbf{r}_0^{\mathbf{a_0}})]$ ($\mathbf{l}$, $\mathbf{a_0} \in GF(p^s)$, $\mathbf{r}_0$ - функция Радемахера), унитарна, то существует ортонормированный базис вейвлетов $\psi^{(\mathbf{l})}$ $(\mathcal{A}^n x \dot{-} h)$, $\mathbf{l} \in GF(p^s)$, $\mathbf{l} \neq 0$, $h \in H_0$ в $L_2(F^{(s)})$, где $\hat{\psi}^{(\mathbf{l})}(\chi) = m^{(0)}(\chi)\hat{\varphi}(\chi\mathcal{A}^{-1})$, $\mathbf{l} \in GF(p^s)$, $\mathbf{l} \neq 0$, $m^{(0)}$ – маска масштабирующего уравнения.

Теорема 2.2. Обозначим через $U = \{r_1^{\mathbf{a_1}} \dots r_\nu^{\mathbf{a}_\nu}, \mathbf{a}_j \in GF(p^s), \nu \in \mathbb{N}_0\}$, $\mathbf{r}_j$ - функции Радемахера. Функция $\varphi \in L_2(F^{(s)})$ удовлетворяет аксиоме 5 КМА (определение 17) тогда и только тогда, когда для любых $\chi \in F_1^{(s)\perp}$

$$\sum_{\xi \in U} |\hat{\varphi}(\chi\xi)|^2 = 1,$$

$$\lim_{j\to\infty} |\hat{\varphi}(\chi)\mathcal{A}^{-j})| = 1 \quad \chi \in X$$

и существует интегрально-периодическая функция $m^{(0)}(\chi) \in L_2(F_1^{(s)\perp})$ такая, что для п.в. $\chi \in X$ справедливо равенство

$$\hat{\varphi}(\chi) = m^{(0)}(\chi)\hat{\varphi}(\chi\mathcal{A}^{-1}).$$

Лемма 2.3. Пусть $(g_n)_{n\in\mathbb{Z}}$ - фиксированная базисная последовательность в $F^{(s)}$, т.е. $g_n \in F_n^{(s)} \quad F_{n+1}^{(s)}$. Тогда любой элемент $a \in F^{(s)}$ можно представить в виде:

$$a = \sum_{k\in\mathbb{Z}} \lambda_k g_k, \quad \lambda_k \in GF(p^s).$$

Теорема 2.4. При $s > 1$ аддитивная группа $F^{(s)+}$ поля $F^{(s)}$ изоморфна произведению групп Виленкина, т.е.

$$F^{(s)} \cong F^{(1)+} \times F^{(1)+} \times \dots \times F^{(1)+} = (F^{(1)+})^s.$$

Этот изоморфизм переводит базу топологии группы $F^{(s)+}$ в базу топологии произведения $F^{(s)} \cong F^{(1)+} \times F^{(1)+} \times \dots \times F^{(1)+}$ групп Виленкина.

Теорема 2.5. Пусть $\varphi(x) \in \mathfrak{D}_M(F_{-N}^{(s)})$ решение масштабирующего уравнения. Тогда

$$\varphi(x) = \sum_{h \in H_0^{(N+1)}} c_h \varphi(\mathcal{A}x \dot{-} h).$$

Теорема 2.6. Пусть $\varphi(x) \in \mathfrak{D}_M(F_{-N}^{(s)})$. Система сдвигов $(\varphi(x \dot{-} h))_{h \in H_0}$ ортонормированна тогда и только тогда, когда $\forall \mathbf{a}_{-N}, \dots, \mathbf{a}_{-1} \in GF(p^s)$

$$\sum_{\mathbf{a}_0, \dots, \mathbf{a}_{M-1} \in GF(p^s)} |\hat{\varphi}(F_{-N}^{(s)\perp} r_{-N}^{\mathbf{a}_{-N}} \dots r_0^{\mathbf{a}_0} \dots r_{M-1}^{\mathbf{a}_{M-1}}|^2 = 1,$$

где r_k – функции Радемахера.

Лемма 2.7. Пусть функция $\varphi(x) \in \mathfrak{D}_M(F_{-N}^{(s)})$ – решение масштабирующего уравнения

$$\hat{\varphi}(\chi) = m^{(0)}(\chi)\hat{\varphi}(\chi \mathcal{A}^{-1}),$$

и система сдвигов $(\varphi(x \dot{-} h))_{h \in H_0}$ функции φ образует ортонормированную систему. Тогда для любых $\mathbf{a}_{-N}, \mathbf{a}_{-N+1}, \dots \mathbf{a}_{-1} \in GF(p^s)$ справедливо равенство

$$\sum_{\mathbf{a}_0 \in GF(p^s)} |m^{(0)}(F_{-N}^{(s)\perp} r_{-N}^{\mathbf{a}_{-N}} r_{-N+1}^{\mathbf{a}_{-N+1}} \dots r_{-1}^{\mathbf{a}_{-1}} r_0^{\mathbf{a}_0}|^2 = 1.$$

Определение 2.4 Пусть R – произвольное кольцо. Если существует такое число $n \in \mathbb{N}$, что для каждого $a \in R$ справедливо равенство $na = 0$, то наименьшее из таких чисел n_0 называется характеристикой кольца, а R – кольцом положительной характеристики n_0. Если же такого числа нет, то R называется кольцом нулевой характеристики.

Лемма 2.8. Пусть $(g_n)_{n \in \mathbb{Z}}$ - фиксированная базисная последовательность в $F^{(s)}$, $g_n \in F_n^{(s)} \setminus F_{n+1}^{(s)}$. Тогда любой элемент $a \in F^{(s)}$ можно представить в виде:

$$a = \sum_{k \in \mathbb{Z}} \lambda_k g_k, \lambda_k \in GF(p^s).$$

В дальнейшем будем считать, что
$g_k = (\dots, 0_{k-1}, (1^{(0)}, 0^{(1)}, \dots, 0^{(s-1)})_k, 0_{k+1}, \dots)$.В этом случае $\lambda_k = \mathbf{a}_k$.

Рассмотрим аддитивную группу $F^{(s)+}$ поля $F^{(s)}$. Окрестности $F_n^{(s)}$ являются компактными подгруппами группы $F^{(s)+}$, обозначим их через $F_n^{(s)+}$. Они обладают следующими свойствами:

1. $\dots \subset F_1^{(s)+} \subset F_0^{(s)+} \subset F_{-1}^{(s)+} \dots$
2. $F_n^{(s)+}/F_{n+1}^{(s)+} \cong GF(p^s)^+$ и $F_n^{(s)+}/F_{n+1}^{(s)+} = p^s$.

Отсюда сразу следует, что при $s = 1$ $F^{(1)+}$ есть группа Виленкина с постоянной образующей последовательностью $p_n = p$.

Верно и обратное.

Теорема 2.9. При $s > 1$ аддитивная группа $F^{(s)+}$ поля $F^{(s)}$ изоморфна произведению групп Виленкина, т.е.

$$F^{(s)+} \cong F^{(1)+} \times F^{(1)+} \times \dots \times F^{(1)+} = (F^{(1)+})^s.$$

Этот изоморфизм переводит базу топологии группы $F^{(s)+}$ в базу топологии произведения $F^{(1)+} \times F^{(1)+} \times \dots \times F^{(1)+}$ групп Виленкина.

Данная теорема позволяет использовать для локальных полей положительной характеристики весь математический аппарат, разработанный для групп Виленкина. В частности, поскольку определение меры и интеграла связаны только с операцией сложения, то уже фактически определены мера и интеграл на локальном поле положительной характеристики. Более того можно рассматривать группу характеров X аддитивной группы $F^{(s)+}$ и функции Радемахера в локальных полях положительной характеристики.

Теорема 2.10. Пусть $g_j = (\dots, 0_{j-1}, (1, 0, \dots, 0)_j, 0_{j+1}, \dots) \in F^{(s)}$,
$\mathbf{a}_k, \mathbf{u} \in GF(p^s)$. Тогда для любых $k \neq j : (r_k^{\mathbf{a}_k}, \mathbf{u}g_j) = 1$.

Оператор растяжения $\mathcal{A}$ в локальном поле $F^{(s)}$ положительной характеристики p определяется равенством

$$\mathcal{A}x := \sum_{n=-\infty}^{+\infty} \mathbf{a}_n g_{n-1},$$

где $x = \sum_{n=-\infty}^{+\infty} \mathbf{a}_n g_n \in F^{(s)}$, в группе характеров - равенством
$(\chi\mathcal{A}, x) = (\chi, \mathcal{A}x)$.

Определение 2.5. Пусть N натуральное число. Обозначим
$V = \{0, 1, \dots, p-1\}$ и построим дерево T следующим образом:

1. Вершинами дерева являются элементы множества V .
2. Корень дерева и все вершины вплоть до $N-1$ уровня принимают значение 0.
3. Дерево содержит всевозможные пути $(\alpha_{k+1} \to \cdots \to \alpha_{k+N})$, $\alpha_k \in V$ длины $N-1$, и при чем каждый из них встречается только один раз. При этом рассматриваем только те пути, которые идут от вершин большего уровня к вершинам меньшего уровня.

Такое дерево называется N-валидным.

Теорема 2.11. Пусть по N-валидному дереву T построены дерево $\tilde{T}$, граф Γ и определены значения маски $m^{(0)}$ так, как указано в равенствах

$$\sum_{\tilde{\alpha}_0} |\lambda_{\alpha_{-N},\alpha_{-N+1},\ldots,\alpha_{-1},\tilde{\alpha}_0}|^2 = 1, \quad \lambda_{\alpha_{-N},\alpha_{-N+1},\ldots,\alpha_{-1},\alpha_0} = 0 \qquad \alpha_0 \notin \{\tilde{\alpha}_0\}.$$

Определение 2.6. Пусть $F^{(s)}$ – локальное поле положительной характеристики p, N – натуральное число. Построим дерево T, удовлетворяющее следующим условиям:

1. Каждая вершина представляет собой элемент конечного поля $GF(p^s)$, т.е. имеет вид: $\mathbf{a}_i = (a_i^{(0)}, a_i^{(1)}, \ldots, a_i^{(s-1)})$, $a_i^{(j)} = \overline{0, p-1}$.
2. Корень и все вершины вплоть до N - 1-го уровня имеют значение равное нулевому элементу поля $GF(p^s)$: $0{=}(0^{(0)}, 0^{(1)}, \ldots, 0^{(s-1)})$.
3. Дерево содержит всевозможные пути $(\mathbf{a}_{k+1}, \ldots, \mathbf{a}_{k+N})$, $\mathbf{a}_k \in GF(p^s)$ длины N - 1 и при чем каждый из них встречается только один раз. При этом рассматриваем только те пути, которые идут от вершин большего уровня к вершинам меньшего уровня.

Такое дерево называется N-валидным деревом на локальном поле $F^{(s)}$ положительной характеристики p.

Лемма 2.12. В массиве $A^{(0)}$ на местах, соответствующих вершинам уровня $l \leq N$ в дереве $\tilde{T}$, стоят единицы.

Лемма 2.13. Пусть по N-валидному дереву T построены дерево $\tilde{T}$, граф Γ и определены значения маски $m^{(0)}(\chi)$. Пусть $(A^{(n)})_{n=0}^{\infty}$ - последовательность массивов, тогда в массиве $A^{(n)}$ элементы, соответствующие вершинам уровня $l \leq N+n$ в дереве $\tilde{T}$, равны единице.

Теорема 2.14. Пусть по N-валидному дереву T построены дерево $\tilde{T}$, граф Γ и определены значения маски $m^{(0)}(\chi)$. Пусть $\tilde{H} = \sqrt{(\tilde{T})}$. Тогда равенство

$$\hat{\varphi}(\chi) = \prod_{k=0}^{\infty} m^{(0)}(\chi \mathcal{A}^{-k}) \in \mathfrak{D}_M(F_{-N}^{(s)\perp})$$

определяет ортогональную масштабирующую функцию $\varphi(x) \in \mathfrak{D}_M(F_{-N}^{(s)})$, порождающую КМА, причем M не превышает $\tilde{H}$ - N.

Теорема 3.1. Функция $\varphi(x) \in \mathfrak{D}_M(F_{-N}^{(s)})$ порождает как сепарабельные так и несепарабельные КМА.

Заключение. В данной работе были исследованы вопросы, связанные с построением несепарабельного кратномасштабного анализа на локальных полях положительной характеристики.

В ходе работы были реализованы основные цели исследования, что подтверждает актуальность и научную ценность данного направления.

Основные результаты работы:

1. Изучена теоретическая база для построения кратномасштабного анализа.

2. Приведены основные свойства масштабирующих функций:

- установлено, что масштабирующая функция, построенная по изложенным выше алгоритмам, может порождать как сепарабельные так и несепарабельные КМА;

- установлены условия ортогональности базисных функций;

- приведен алгоритмы построения масштабирующей функции на группах Виленкина G по N - валидному дереву.

3. Разработан эффективный алгоритм нахождения неприводимых многочленов над полями $GF(p)$.

Программа эффективна, потому что:

1. Сокращает перебор за счёт моннических полиномов.
2. Использует быстрые алгоритмы *SymPy* (функцию *isirreducible*).
3. Работает только с корректными входами (простые p).
4. Минимизирует накладные расходы на вывод.