МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

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

Кафедра компьютерной алгебры и теории чисел

Лемма Гензеля и ее применения

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы

направление 02.04.01 — Математика и компьютерные науки

механико-математического факультета

Напыловой Дарьи Леонидовны

Научный руководитель
зав. каф., к.ф.-м.н., доцент А.М. Водолазов

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

Саратов 2019

Введение. Настоящая работа посвящена описанию алгоритма решения полиномиальных уравнений в кольце. Предложенный алгоритм является развитием идеи Курта Гензеля, впоследствии названной леммой Гензеля о подъеме решения полиномиального сравнения.

Решение уравнений и систем в различных кольцах и полях является одной из классических задач алгебры и теории чисел. Среди методов ее решения можно отдельно выделить связанные с подъемом. Идея данных алгоритмов состоит в том, чтобы сначала с помощью подъема решения полиномиального сравнения или системы найти корень по модулю степени некоторого простого числа, а потом с помощью оценки величины решения получить точный ответ.

Впервые идею подъема решения полиномиального сравнения высказал К. Гензель в 1904 г. в следующем виде:

Утверждение. *Пусть $F(x)$ - многочлен с целыми p-адическими коэффициентами, причем $p \nmid D(F)$, где $D(F)$ - дискриминант многочлена $F(x)$. Тогда при условии, что найдено разложение*

$$F(x) \equiv f_0(x)g_0(x) \ (mod\ p),$$

можно найти такие многочлены $f(x)$ и $g(x)$, что

$$F(x) = f(x)g(x)$$

в кольце целых p-адических чисел.

При доказательстве данного утверждения Гензель описал алгоритм нахождения многочленов $f_k(x)$ и $g_k(x), k \in \mathbb{N}$, удовлетворяющих условию

$$F(x) \equiv f_k(x)g_k(x) \ (mod\ p^{k+1}),$$

с помощью уже известных $f_{k-1}(x)$ и $g_{k-1}(x)$.

Основная часть. Основная часть данной работы состоит из 4 разделов, а именно:

1. p-адический анализ;

2. Подкоординатное представление функций;

3. Об обобщении леммы Гензеля;

4. Гензелевский подъем;

Первый раздел посвящен необходимым определениям и обозначениям из p-адического анализа. Приводятся определения p-адического числа, т.е. пусть p - простое число. Если

$$z = z_0 + z_1 p + z_2 p^2 + ...,$$

где $z_j \in \{0, 1, ..., p-1\}, j = 0, 1, 2, ...,$ — каноническая запись целого p-адического числа $z \neq 0$, то

$$ord_p z = min\{j : z_j \neq 0\}$$

- показатель максимальной степени p, делящей z. По определению,

$$\|z\|_p = p^{-ord_p z}$$

есть p-адическая норма z, $\|0\|_p = 0$. Норма $\|\cdot\|_p$ стандартным образом распространяется на все поле p-адических чисел Q_p, которое есть поле частных кольца целых p-адических чисел Z_p и задает на Q_p метрику

$$d_p(u, v) = \|u - v\|_p,$$

относительно которой Q_p является пополнением пространства рациональных чисел Q. Введенные К. Гензелем в конце XIX века p-адические числа составляют неотъемлемую часть теории чисел, алгебраической геометрии и других разделов современной математики.

Также повествуется о представлением p-адических функций в виде ряда Ван дер Пута, который определяются следующим образом[6]. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ - непрерывная функция. Тогда существует единственная последовательность p-адических коэффициентов $B_0, B_1, B_2, ...$ таких, что

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x)$$

для всех $x \in \mathbb{Z}_p$. Характеристическая функция $\chi(m, x)$ определяется как

$$\chi(m, x) = \begin{cases} 1, & \text{если } |x - m|_p \leqslant p^{-n}, \\ 0, & \text{в противоположном случае,} \end{cases}$$

где $n = 0$ при $m = 0$, и n определено единственным образом через неравенство $p^{n-1} \leqslant m \leqslant p^n - 1$ при $m \neq 0$ [7]. Число n из определения $\chi(m, x)$ обладает естественной интерпретацией. Это всего лишь число разрядов в каноническом представлении числа $m \in \mathbb{N}_0$ по основанию p.

Во втором разделе приведено описание способа представления p-адических функций, а именно, так называемое подкоординатное представление. Основной особенностью подкоординатного представления p-адических функций является то, что значения функции f заданы в канонической форме представления p-адического числа. При этом сама функция f определяется набором p-значных функций, отображающих множество $\{0, 1, ..., p-1\}$ в себя, и порядком использования этих функций для определения значения функции f. Также приведены соотношения, которые позволяют перейти от подкоординатного представления липшицевой функции класса 1 к ее представлению рядом Ван дер Пута. Эффективность использования подкоординатной формы представления p-адических функций проиллюстрирована на задаче исследования возможностей обобщения леммы Гензеля. В теореме 2.1 подкоординатное представление определяется для p-адических функций $f : \mathbb{Z}_p \to \mathbb{Z}_p$, которые удовлетворяют условию Липшица с константой 1. Однако подкоординатное представление может быть использовано и для липшицевых функций класса p^α $(\alpha \geqslant 1)$. Эта возможность следует из [12], теорема 3.1. В этой теореме утверждается, что липшицева функция класса p^α задается набором из p^α липшицевых функций класса 1 с помощью соотношения (1.2). Поэтому для задания p^α-липшицевых функций в подкоординатной форме достаточно за-

дать все липшицевы функции класса 1 $f_i, 0 \leqslant i \leqslant p^\alpha - 1$, в подкоординатной форме. Подкоординатная форма представления липшицевых функций класса 1 определяется в следующей теореме.

Теорема 2.1. *Пусть функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является 1-липшицевой. Тогда существуют p-значные функции*

$$\varphi_0 : \{0, 1, ..., p-1\} \to \{0, 1, ..., p-1\},$$
$$\varphi_{k,a} : \{0, 1, ..., p-1\} \to \{0, 1, ..., p-1\}, \quad a \in \{0, 1, ..., p^k - 1\}, \quad k \geqslant 1,$$

такие, что

$$f(x) = f(x_0 + p \cdot x_1 + ... + p^k \cdot x_k + ...) = \varphi_0(x_0) + \sum_{k=1}^{\infty} p^k \sum_{a=0}^{p^k-1} I_a([x]_k)\varphi_{k,a}(x_k), \quad (1)$$

где

$$I_a([x]_k) = \begin{cases} 1, & \text{если } [x]_k = a, \\ 0, & \text{иначе.} \end{cases}$$

При таком способе представления значение функции f есть p-адическое число, которое уже представлено в каноническом виде. В подкоординатном представлении могут быть записаны не только липшицевы функции класса 1, но и p-адические функции, удовлетворяющие условию Липшица с константой p^α, α - положительное целое число. Это следует из того, что липшицевы функции класса p^α однозначно определяются набором из p^α липшицевых функций класса 1 (теорема 3.1 из [12]). В утверждении 2.1 приводятся соотношения, которые позволяют перейти от подкоординатного представления липшицевой функции класса 1 к ее представлению рядом Ван дер Пута.

Третий раздел посвящен применению подкоординатного представления p-адических функций $f : \mathbb{Z}_p \to \mathbb{Z}_p$ для изучения вопроса о возможности обобщения p-адического варианта леммы Гензеля [13],[14]. В целом, лемма Гензеля может рассматриваться как критерий существования корня многочлена f над кольцом $\mathbb{Z}_p$. В частности, при определенных ограничениях на $f \in \mathbb{Z}_p[x]$ во-

прос о разрешимости уравнения $f(x) = 0$ над $\mathbb{Z}_p$ сводится к разрешимости сравнения $f(x) \equiv 0(mod\ p)$. Естественным образом возникает вопрос о возможности построения аналогичного утверждения для более широкого класса p-адических функций. Другими словами, рассматривается следующая задача. Для каких p-адических функций (например, в классе липшицевых функций класса 1) справедливо утверждение: существует натуральное число R такое, что уравнение $f(x) = M, M \in \mathbb{Z}_p$, разрешимо как только разрешимо сравнение $f(x) \equiv M(mod\ p^R)$. Для $M = 0$ (обобщение леммы Гензеля) эта задача была решена в теореме 2.4 из [12], и в теореме 3.3 из [12] для случая липшицевых функций класса p^α, $\alpha > 1$. В теореме 2.4 ограничения на f приведены в терминах коэффициентов ряда Ван дер Пута. Аналог теоремы 2.4 из [12] для подкоординатного представления приводится в теореме 3.2.

Теорема 3.2. *Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является 1-липшицевой функцией, заданной в подкоординатноой форме (2.1). Если справедливо, что:*

1. *для некоторого натурального числа R существует $\bar{a} \in \{0, 1, ..., p^R - 1\}$ такое, что $f(\bar{a}) \equiv 0\ (mod\ p^R)$;*
2. *для любых $k \geqslant R$ и $a \geqslant p^R$, где $a \equiv \bar{a}\ (mod\ p^R)$, функции $\varphi_{k,a}$ биективны.*

Тогда существует единственное целое p-адическое число $r \in \mathbb{Z}_p$ такое, что $f(r) = 0$ и $r \equiv \bar{a}\ (mod\ p^R)$.

Содержательность поставленной задачи определяется следующим обстоятельством. В общем случае (т. е. никакие дополнительные ограничения на липшицевы функции класса 1 не накладывается) для решения вопроса о разрешимости уравнения $f(x) = M, M \in \mathbb{Z}_p$, требуется проверить разрешимость бесконечного числа сравнений $f(x) \equiv M(mod\ p^k), k \geqslant 1$.

На основе использования подкоординатного представления в теореме 3.3 показано, что имеются следующие альтернативы. Если число небиективных функций $\varphi_{k,m}, m \in \{0, 1, ..., p^k - 1\}, k \geqslant 1$, из подкоординатного представления функции f, конечно, то существует $R \in \mathbb{N}$ такое, что разрешимость

уравнения $f(x) = M, M \in \mathbb{Z}_p$, сводится к проверке разрешимости сравнения $f(x) \equiv M \ (mod\ p^R)$. В частности, лемма Гензеля обобщается на такой класс липшицевых функций класса 1. Если число небиективных функций $\varphi_{k,m}, m \in \{0, 1, ..., p^k - 1\}, k \geqslant 1$, из подкоординатного представления функции f, бесконечно, то построить обобщение леммы Гензеля не удается в том смысле, что для любого $k \in \mathbb{N}$ найдется $C \in \mathbb{Z}_p$ такое, что $f(x) \equiv C(mod\ p^k)$, но $f(x) \neq C$. В частности, теорема 3.3 позволяет косвенным образом оценить границы возможного обощения леммы Гензеля.

Теорема 3.3.*Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является 1-липшицевой функцией, заданной в подкоординатноой форме (2.1). Тогда справедливы утверждения:*

1. *если $f \in \mathfrak{B}$, то существует $R \in \mathbb{N}$ такое, что уравнение $f(x) = C, C \in \mathbb{Z}_p$, разрешимо тогда и только тогда, когда разрешимо сравнение $f(x) \equiv C \ (mod\ p^R)$;*
2. *если $f \notin \mathfrak{B}$ (т.е. в (2.1) содержится бесконечное число небиективных функций $\varphi_{k,a}$), то для любого $k \in \mathbb{N}$ существует $C \in \mathbb{Z}_p$ такое, что $f(x) \equiv C \ (mod\ p^k)$, но $f(x) \neq C$;*
3. *функция f биективна на $\mathbb{Z}_p$ тогда и только тогда, когда любая функция $\varphi_0, \varphi_{k,a}, a \in \{0, 1, ..., p^k - 1\}, k \geqslant 1$, из (2.1) биективна.*

Так же в третьем разделе рассматривается случай, когда все функции $\varphi_0, \varphi_{k,m}, m \in \{0, 1, ..., p^k - 1\}, k \geqslant 1$, из подкоординатного представления липшицевой функции класса 1 f биективны. Этот случай имеет тесную связь с теорией p-адических динамических систем [15]–[17].

В заключительном, четвертом разделе рассматриваются условия, при которых функция, обладающая одним важным свойством равномерной дифференцируемости по модулю p^k, будет равновероятной, или эргодичной, или сохраняющей меру. Результаты этого раздела демонстрируют эффект: из того, что функция F обладает некоторым свойством по модулю p^{k_0} вытекает, что она обладает этим свойством по любому модулю p^n для всех $n \geqslant k_0$. Кроме того, уместно заметить, что результаты этого раздела позволяют строить сохраня-

ющие меру или эргодические функции, которые не обязательно аффинны по модулю p. Фактически, на основе результатов этого раздела может быть развита некоторая техника, позволяющая поднимать произвольное транзитивное преобразование кольца Z/p^{k_0} до функции на Z_p, транзитивной по модулю p^k для всех $k = k_0, k_0+1, k_0+2, ...$ Именно по этой причине вводим ниже понятие асимптотически совместимой функции.

Вначале вводятся несколько определений, обобщающих некоторые из основных понятий (см. п. 5.1 из [7]).

Определение 4.1. *Пусть* $F = (f_1, ..., f_m) : Z_p^{(n)} \longrightarrow Z_p^{(m)}$ *- некоторая функция, не обязательно совместимая. Функция* F *называется (асимптотически) равновероятной, если для всех* $k = 1, 2, ...$ *(соответственно, для всех достаточно больших* $k \in N$*) она равновероятна по модулю* p^k*, то есть ограничение*

$$F\, mod\, p^k = (f_1\, mod\, p^k, ..., f_m\, mod\, p^k)$$

функции F *на множество* $\{0, 1, ..., p^k - 1\}^{(n)}$ *есть равновероятная функция.*

В случаях, когда это не вызывает недоразумений, отождествляем множество $\{0, 1, ..., p^k - 1\}^{(n)}$ с множеством всех элементов кольца $(Z/p^k)^{(n)}$.

Аналогично, F асимптотически сохраняет меру (соответственно, что F асимптотически эргодична), если $F\, mod\, p^k$ есть биективная (соответственно, транзитивная) функция на $(Z/p^k)^{(n)}$ для всех достаточно больших k. Наконец, F асимптотически совместима, если найдется положительное рациональное целое N такое, что для всех $a, b \in Z_p^{(n)}$ и всех $k \geqslant N$ из сравнения $a \equiv b(mod\, p^k)$ вытекает сравнение $F(a) \equiv F(b)(mod\, p^k)$.

По определению для $a = (a_1, ..., a_n)$ и $b = (b_1, ..., b_n)$ из $Q_p^{(n)}$ сравнение

$$a \equiv b(mod\, p^s)$$

означает, что $\|a_i - b_i\|_p \leqslant p^{-s}$ (или, что то же самое, что $a_i = b_i + c_i p^s$ для подходящих $c_i \in Z_p, i = 1, 2, ..., s$), то есть, что $\|a - b\|_p \leqslant p^{-s}$. Другими

словами, функция асимптотически совместима, если для некоторого $N \in N_0$ она удовлетворяет условию Липшица с коэффициентом 1 для всех пар точек, находящихся одна от другой на расстоянии, меньшем, чем p^{-N}. Ввиду компактности пространства $Z_p^{(n)}$ означает, что функция F асимптотически совместима тогда и только тогда, когда она удовлетворяет условию Липшица с константой 1 локально.

Заключение. В последние годы p-адические числа стали очень привлекательны для исследователей, создающих математические модели сложных иерархических систем: в физике, теории информации, криптографии, психологии, генетике, финансах. Ключевым моментом в использовании p-адических чисел для моделирования физических, биологических или социальных процессов является возможность закодировать иерархические структуры этих процессов с помощью алгебры или топологии.

В настоящее время p-адический анализ является одним из бурно развивающихся направлений математики. Многочисленные приложения p-адических чисел нашли свое отражение в теории p-адических дифференциальных уравнений, p-адической теории вероятностей, p-адической математической физике и т. д.

p-адические метрики используются при решении многих алгебраических и теоретико-числовых задач. В частности, p-адическая метрика оказывается более полезной, чем архимедова при факторизации полиномов.

Применение ее для решения задач факторизации стало возможным после того, как был получен достаточно эффективный метод разложения полиномов на множители над полем p - адических чисел. Этот метод состоит из двух ключевых алгоритмов: первый из них, алгоритм Берлекэмпа, позволяет достаточно быстро разлагать на множители полиномы с коэффициентами из конечного поля, что соответствует нахождению нулевого приближения разложения в описанном выше алгоритме; второй представляет p - адический аналог метода Ньютона. Математический результат, на котором он основан, как раз и

носит название леммы Гензеля. Метод факторизации, базирующийся на алгоритме Берлекэмпа и лемме Гензеля, принят во многих системах компьютерной алгебры.

На основе этого в приложении проиллюстрирован алгоритм линейного подъема Гензеля для двух сомножителей. Основу алгоритма составляет итерационный процесс перехода от сравнения по модулю некоторой степени числа p к сравнению по модулю большей степени p. Показывается, что этот переход можно выполнить за конечное число шагов.