ДОКЛАДЫ АКАДЕМИИ НАУК, *2019*, *том 489*, *№ 3*, *с. 232–234*

МАТЕМАТИКА

УДК 513.6+518.5

ОБ ОЦЕНКЕ КОЭФФИЦИЕНТОВ НЕПРИВОДИМЫХ МНОЖИТЕЛЕЙ МНОГОЧЛЕНОВ НАД ПОЛЕМ ФОРМАЛЬНЫХ СТЕПЕННЫХ РЯДОВ В НЕНУЛЕВОЙ ХАРАКТЕРИСТИКЕ

А. Л. Чистов

Представлено академиком РАН С.В. Кисляковым 21.07.2019 г.

Поступило 21.07.2019 г.

Мы обсуждаем некоторые результаты и проблемы, относящиеся к алгоритму Ньютона—Пюизё и его обобщению на случай ненулевой характеристики, предложенному автором ранее. Предлагается новый метод для получения эффективных оценок корней многочлена в поле дробно-степенных рядов в случае произвольной характеристики.

Ключевые слова: формальные степенные ряды, ненулевая характеристика, алгоритм Ньютона—Пюизё, оценки неприводимых множителей.

DOI: https://doi.org/10.31857/S0869-56524893232-234

В статье [1] мы обобщили алгоритм Ньютона–Пюизё на случай основного поля k ненулевой характеристики. Там мы получили канонический алгоритм для разложения многочленов над максимальным слабо разветвлённым расширением поля степенных рядов $k((X))$ (т.е. объединением полей дробно-степенных рядов $k_s((X^{1/\nu}))$ по всем ν взаимно простым с $p = \mathrm{char}(k)$, где k_s — сепарабельное замыкание поля k в его алгебраическом замыкании $\overline{k}$). До сих пор считалось, что такой алгоритм либо невозможен в принципе, либо если и существует, то он должен быть очень сложным. Поэтому результат из [1] является весьма важным.

Однако с точки зрения сложности вычислений здесь остаётся одна принципиальная проблема: оценить длины записи коэффициентов из конечных расширений поля k, появляющихся в этой естественной конструкции. То есть получить оценки, аналогичные оценкам из [2] (там поле k имеет нулевую характеристику). Но в рассматриваемом случае $\mathrm{char}(k) = p > 1$, по-видимому, нет прямого аналога результатов из [2], достаточного для того, чтобы получить требуемые оценки на длины записи коэффициентов. Здесь, по нашему мнению, следует вернуться к более классическому подходу и оценивать знаменатели этих коэффициентов. Точнее, мы хотели бы сформулировать следующую гипотезу.

Санкт-Петербургское отделение
Математического института им. В.А. Стеклова
Российской Академии наук
E-mail: *alch@pdmi.ras.ru*

Пусть $k = \mathbb{F}_{p^m}(t_1, \ldots, t_l)$, где $t_1, \ldots, t_l$ алгебраически независимы над конечным полем $\mathbb{F}_{p^m}$ из p^m элементов, $m \geq 1$ — целое число. Пусть $f \in k[X, Y]$ — сепарабельный многочлен относительно Y (т.е. степень $\deg_Y f \geq 1$ и дискриминант многочлена f относительно Y не равен нулю) со старшим коэффициентом $\mathrm{lc}_Y f = 1$. Предположим, что $f \in \mathbb{F}_{p^m}[t_1, \ldots, t_l, X, Y]$ и степени $\deg_{X,Y} f \leq d$, $\deg_{t_1,\ldots,t_l} f \leq d_1$ для некоторых $d, d_1 \geq 2$.

Гипотеза. *Пусть* $g \in k((X))[Y]$ — *неприводимый* (*в этом кольце*) *множитель многочлена* f *такой*, *что старший коэффициент* $\mathrm{lc}_Y g = 1$. *Тогда существует многочлен* $0 \neq \delta \in \mathbb{F}_{p^m}[t_1, \ldots, t_l]$ *степени* $\deg_{t_1,\ldots,t_l} \delta = d_1 d^{O(1)}$ *и многочлен* $g_1 = g_1(t_1, \ldots, t_l, X, Y) \in \mathbb{F}_{p^m}[t_1, \ldots, t_l][[X]][Y]$ *такие*, *что*

$$g = g_1(t_1, \ldots, t_l, X/\delta, Y).$$

Заметим, что для доказательства этой гипотезы достаточно было бы получить хорошие оценки на аппроксимации в варианте леммы Гензеля (см. [3, гл. 4, § 3, теорема 1]). Но, к сожалению, такие оценки известны только в случае, когда многочлены $g|_{X=0}$ и $(f/g)|_{X=0}$ взаимно просты (возможно, ещё и в некоторых других подобных случаях, но не в общем случае).

Можно даже уточнить эту гипотезу. Именно, пусть $y_1, \ldots, y_n \in \overline{k((X))}$ — все попарно различные корни многочлена f (здесь $n = \deg_Y f$ и $\overline{k((X))}$ является алгебраическим замыканием поля $k((X))$). Положим полином $F = \prod_{1 \leq i \neq j \leq n} (Z - y_i + y_j)$, где Z — но-

вая переменная. Так что многочлен $F \in \mathbb{F}_{p^m}[t_1, \ldots, t_l, X, Z]$. Пусть $F = \sum_{i,j} F_{i,j} X^i Z^j$, где все коэффициенты $F_{i,j} \in \mathbb{F}_{p^m}[t_1, \ldots, t_l]$. Пусть V является множеством всех вершин ломаной Ньютона многочлена F, рассматриваемого как элемент $k[[X]][Z]$. Положим $\delta_1 = \prod_{(i,j)\in V} F_{i,j}$. Тогда дополнительно в формулировке гипотезы можно выбрать δ, делящим δ_1^N для некоторого целого числа $N = d^{O(1)}$.

Эта гипотеза (если она верна) является ключом к получению хороших оценок на длины записи коэффициентов из k_s в конструкции из [1]. Для доказательства этой гипотезы надо тщательно проанализировать алгоритм из [1] (сейчас мы не видим никакого другого подхода). У нас есть предварительный план для этого. Общий случай является сложным. Но кое-что здесь удаётся сделать уже сейчас. В настоящее время мы можем получить хорошие оценки в важном частном случае: $\deg_Y g = 1$ линейного множителя g. Мы доказываем следующую теорему.

Теорема. *Пусть многочлен f такой же, как и выше, и поле $k = \mathbb{F}_{p^m}(t_1, \ldots, t_l)$. Сформулированная гипотеза верна, если степень $\deg g = 1$. Более того, справедливы следующие утверждения*:

1. *Пусть $Y = u \in \overline{k((X))}$ — корень многочлена f такой, что расширение полей $k((X))[u] \supset k((X))$ является слабо разветвлённым. Тогда существует алгебраический сепарабельный над полем k элемент η с минимальным многочленом $\Phi \in \mathbb{F}_{p^m}[t_1, \ldots, t_l, Z]$, неприводимым в этом кольце со старшим коэффициентом $\mathrm{lc}_Z \Phi = 1$ и степенями $\deg_Y \Phi \le n$, $\deg_{t_1,\ldots,t_l} \Phi = d_1 d^{O(1)}$. Следовательно, $\Phi(t_1, \ldots, t_l, \eta) = 0$. Существует многочлен $0 \ne \delta \in \mathbb{F}_{p^m}[t_1, \ldots, t_l]$ такой, что $\deg_{t_1,\ldots,t_l} \delta = d_1 d^{O(1)}$ и целое число ν взаимно простое с p, $1 \le \nu \le n$. Далее можно представить*

$$u = \sum_{i \ge 0} \sum_{0 \le j < \deg_Z \Phi} u_{i,j} \eta^j (X/\delta)^{i/\nu},$$

где $u_{i,j} \in \mathbb{F}_{p^m}[t_1, \ldots, t_l]$ и степени $\deg_{t_1,\ldots,t_l} u_{i,j}$ ограничены сверху $(i+1)d_1 d^{O(1)}$ для всех i, j. Здесь везде константы в $O(1)$ абсолютные.

2. *Для всякого целого числа $N \ge 0$ можно построить семейство шестёрок*

$$(u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)}, \{u_{i,j}^{(r)}\}_{0 \le i \le N,\ 0 \le j < \deg_Z \Phi^{(r)}}), \quad 1 \le r \le \mu, \tag{1}$$

(здесь все $u^{(r)}$, $\eta^{(r)}$, $\Phi^{(r)}$, $\delta^{(r)}$, $\nu^{(r)}$, $u_{i,j}^{(r)}$ не зависят от N; элементы $\eta^{(r)} \in \overline{k}$), удовлетворяющее следующим свойствам. Для всякого корня и из утверждения 1 *существует $1 \le r \le \mu$ и вложение полей $\sigma\colon k[\eta^{(r)}] \to \overline{k}$ над k такие, что*

$$(u, \eta, \Phi, \delta, \nu, \{u_{i,j}\}_{0 \le i \le N,\ 0 \le j < \deg_Z \Phi}) =$$
$$= (u^{(r)}, \sigma(\eta^{(r)}), \Phi^{(r)}, \delta^{(r)}, \nu^{(r)}, \{u_{i,j}^{(r)}\}_{0 \le i \le N,\ 0 \le j < \deg_Z \Phi^{(r)}}).$$

Обратно, пусть $1 \le r \le \mu$ — произвольное. Положим $(u, \eta, \Phi, \delta, \nu) = (u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)})$ и $u_{i,j} = u_{i,j}^{(r)}$ для всех i, j. Тогда выполняется утверждение 1 *для этих u, η, Φ, δ, ν и $u_{i,j}$.*

Для всякого $N \ge 0$ время работы алгоритма для построения семейства всех шестёрок (1) *полиномиально от $((N+1)d_1 d)^{l+1}$, m и p. Следовательно, время работы алгоритма для построения семейства всех пятёрок $(u^{(r)}, \eta^{(r)}, \Phi^{(r)}, \delta^{(r)}, \nu^{(r)})$, $1 \le r \le \mu$, полиномиально от $(d_1 d)^{l+1}$, m и p.*

Сформулированная теорема обобщает результат из [2] на случай ненулевой характеристики. Но здесь ещё важно, что доказать её стало возможным благодаря предложенному новому методу, который можно применить также и в нулевой характеристике и получить другим способом результат из [2]. Грубо говоря, суть этого метода состоит в использовании теоремы о производных неявной функции в общей точке с последующей специализацией значений этой общей точки.

Опишем его вкратце (но сейчас основной случай — ненулевая характеристика). Рассмотрим сепарабельную алгебру $A = K[Y]/(f)$, где $K = k((X))$. Положим $y = Y \bmod f \in A$. Пусть Z, W — новые переменные. Для всякого $\varphi \in k[[X]]$ элемент $\varphi(X+Z) \in k[[X, Z]] \subset K[[Z]]$ определяется естественным образом. Так что $f(X+Z, W) \in K[[Z]][W]$. Положим

$$B = K[[Z]][W]/(f(X+Z, W))$$

и $w = W \bmod f(X+Z, W) \in B$. Неформально мы имеем $w = y(X+Z) = y|_{X:=X+Z}$. Мы находим вложение $K[[Z]]$-алгебр $K[[Z]][w] \to K[y][[Z]]$ такое, что $w \mapsto \sum_{i \ge 0} w_i Z^i$, где все $w_i \in K[y] = A$ и $w_0 = y$. Положим $D_i(y) = w_i$ для всякого $i \ge 0$. В нулевой характеристике очевидно имеем

$$D_i(y) = \frac{1}{i!} \frac{d^i y}{dX^i}.$$

В ненулевой характеристике для $D_i(y)$ также можно получить некоторую формулу. Именно для целого

числа $s \geq 0$ на кольце $k((X^{p^s}))[y^{p^s}]$ можно определить оператор дифференцирования $\delta_s = \dfrac{d}{dX^{p^s}}$. Далее, если $z \in k((X))[y]$, то представим $z = \sum\limits_{0 \leq i < p^s} z_i X^i$, где все $z_i \in k((X^{p^s}))[y^{p^s}]$. По определению положим $\delta_s(z) = \sum\limits_{0 \leq i < p^s} \delta_s(z_i) X^i \in A$. Здесь мы хотели бы подчеркнуть, что из этого определения следует, что для всех $z_1, z_2 \in A$ мы имеем

$$\delta_s(z_1 z_2^{p^{s+1}}) = \delta_s(z_1) z_2^{p^{s+1}}.$$

Теперь представим $i = i_0 + i_1 p + \ldots + i_r p^r$, где все i_j, $0 \leq j \leq r$, являются целыми числами, такими, что $0 \leq i_j < p$ и $i_r \neq 0$ (при $i \neq 0$). Тогда мы имеем

$$D_i(y) = \frac{1}{i_0! i_1! \ldots i_r!} \delta_0^{i_0} \delta_1^{i_1} \ldots \delta_r^{i_r}(y). \qquad (2)$$

Таким образом, получается интересный аналог формулы Тейлора для алгебраических функций в ненулевой характеристике.

Предположим, что многочлен $f \in k[X, Y]$ имеет корень $Y = u \in k_s[[X]]$, см. утверждение 1 (здесь $\nu = 1$ и всегда всё сводится к этому случаю заменой переменных $X^{1/\nu} \to X$). Мы вычисляем, решая некоторые линейные системы, многочлен $0 \neq \Phi_i \in k[X, Z]$ такой, что $\Phi_i(X, D_i(y)) = 0$ и X не делит Φ_i. Тогда $\sum\limits_{0 \leq j < \deg \Phi} u_{i,j} \eta^j / \delta^i$, см. утверждение 1, является корнем многочлена $\Phi_i(0, Z)$. Таким образом, для этого элемента можно получить хорошие оценки. Есть только технические сложности, чтобы построить δ и Φ.

СПИСОК ЛИТЕРАТУРЫ

1. *Чистов А.Л.* Расширение алгоритма Ньютона—Пюизе на случай ненулевой характеристики основного поля. I // Алгебра и анализ. 2016. Т. 28. № 6. С. 147–188.
2. *Chistov A.L.* Polynomial Complexity of the Newton–Puiseux Algorithm / In: Ed. J. Gruska, B. Rovan. Wiedermann International Symposium on Mathematical Foundations of Computer Science 1986. Lecture Notes in Computer Science. Springer-Verlag, 1986. V. 233. P. 247–255.
3. *Боревич З.И.*, *Шафаревич И.Р.* Теория чисел. М.: Наука, 1964.

ON THE ESTIMATION OF COEFFICIENTS OF IRREDUCIBLE FACTORS OF POLYNOMIALS OVER A FIELD OF FORMAL POWER SERIES IN NONZERO CHARACTERISTIC

A. L. Chistov

Saint-Petersburg Department of Steklov Mathematical Institute of the Russian Academy of Sciences, *Saint-Petersburg*, *Russian Federation*

Presented by Academician of the RAS S.V. Kislyakov July 21, 2019

Received July 21, 2019

We discuss some problems and results related to the Newton—Puiseux algorithm and its generalization for nonzero characteristic obtained by the author earlier. A new method is suggested for obtaining effective estimations of the roots of a polynomial in the field of fraction-power series in arbitrary characteristic.

Keywords: formal power series, nonzero characteristic, Newton–Puiseux algorithm, estimations of irreducible factors.