ФГБОУ ВО
Московский государственный университет
имени М. В. Ломоносова

На правах рукописи

Зеленова Мария Евгеньевна

Решение систем уравнений в полях алгебраических чисел

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико–математических наук

Москва — 2015

Работа выполнена на кафедре теории чисел Механико–математического факультета ФГБОУ ВО Московского государственного университета имени М. В. Ломоносова.

Научный руководитель: член–корр. РАН, профессор
Нестеренко Юрий Валентинович

Официальные оппоненты: Степанов Сергей Александрович,
доктор физико–математических наук,
ведущий научный сотрудник лаборатории
№ 1 им. М.С. Пинскера
ФГБУН «Институт проблем передачи информации им. А.А. Харкевича Российской академии наук»

Михайлов Сергей Владимирович,
кандидат физико–математических наук
технический директор ООО «Мегаплан»

Ведущая организация: ФГБОУ ВПО «Московский педагогический государственный университет»

Защита диссертации состоится 25 декабря 2015 г. в 16^{45} на заседании диссертационного совета Д 501.001.84 при ФГБОУ ВО Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП–1, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, Механико-математический факультет, аудитория 14–08.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО МГУ имени М. В. Ломоносова (Москва, Ломоносовский проспект, д. 27, сектор А, $8^{\text{й}}$ этаж), http://mech.math.msu.su/ snark/index.cgi, http://istina.msu.ru/dissertations/10362590.

Автореферат разослан 25 ноября 2015 года.

Ученый секретарь диссертационного совета
Д 501.001.84 на базе ФГБОУ ВО МГУ,
доктор физико–математических наук,
профессор Иванов Александр Олегович

Общая характеристика работы

Актуальность темы

Диссертация посвящена построению алгоритмов решения полиномиальных уравнений и систем в полях алгебраических чисел, основанных на лемме 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. Данной задачей занимались Г. Цассенхауз, А. Ленстра, Х. Ленстра, Л. Ловас, Д.Бухлер, К. Померанс, Д. Диксон.

Впервые идею подъема решения полиномиального сравнения высказал К. Гензель[1] в 1904 г. в следующем виде:

Утверждение 1. *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*

$$F(x) \equiv f_0(x)g_0(x) \pmod{p},$$

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

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

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

В 1905 г. в работе К. Гензеля[2] лемма была переформулирована в следующей форме:

[1] Hensel K. Neue Grundlagen der Arithmetik // J. Reine Angew. Math. 1904, vol. 127, p. 51–84.

[2] Hensel K. Über eine neue Begründung der Theorie der algebraischen Zahlen // J. Reine Angew. Math. 1905, vol. 128, p. 1–32

Утверждение 2. *Пусть $F(x)$ — многочлен с целыми p–адическими коэффициентами, а γ — целое p–адическое число, удовлетворяющее условиям:* $F(\gamma) \equiv 0 \pmod{p}$ *и*

$$\left| \frac{F(\gamma)}{(F'(\gamma))^2} \right|_p < 1,$$

где $|\cdot|_p$ — p–адическая норма числа. Тогда можно найти целое p–адическое число γ_1, такое, что $\gamma_1 \equiv \gamma \pmod{p}$ *и*

$$F(\gamma_1) = 0$$

в кольце целых p-адических чисел.

В данном виде лемма Гензеля обычно формулируется в современной литературе.

В 1969 г. Г.Цассенхауз[3] модифицировал утверждение 1 таким образом, чтобы сделать подъем экспоненциальным:

Утверждение 3. *Пусть $F(x)$ — многочлен с целыми коэффициентами, причем известно разложение*

$$F(x) \equiv f_1(x)g_1(x) \pmod{p}.$$

Тогда с помощью уже известных $f_{k-1}(x)$ и $g_{k-1}(x)$ можно найти многочлены $f_k(x)$ и $g_k(x)$, $k \in \mathbb{N}$, удовлетворяющие условию

$$F(x) \equiv f_k(x)g_k(x) \pmod{p^{2^k}}. \tag{1}$$

Более подробно алгоритм нахождения многочленов $f_k(x)$ и $g_k(x)$ был описан Г. Цассенхаузом[4] впоследствии спустя почти десять лет.

Также в данных работах он нашел оценку на коэффициенты многочленов $f(x)$ и $g(x)$, удовлетворяющих равенству $F(x) = f(x)g(x)$, и таким образом смог оценить число k, до которого следует поднимать сравнение (1) для того, чтобы найти разложение $F(x)$ на множители над $\mathbb{Z}$. Являются ли полученные многочлены $f_k(x)$ и $g_k(x)$ настоящими делителями $F(x)$, Цассенхауз проверял делением.

Лемма Гензеля в форме утверждения 1 была также использована в 1982 г. А.К. Ленстрой, Х.В. Ленстрой и Л.Ловасом[5]. В данной статье был предложен алгоритм факторизации многочленов с целыми коэффициентами с

[3]Zassenhaus H. On Hensel Factorization, I // J. Number Theory. 1969, vol. 1, p. 291–311

[4]Zassenhaus H. A Remark on the Hensel Factorization Method // Math. Comp. 1978, vol. 32, № 141, p. 287–292

[5]Lenstra A. K., Lenstra H. W., Lovász L. Factoring Polynomials with Rational Coefficients // Math. Annalen, 1982, vol. 261, p. 515–534

помощью впервые описанного в той же работе LLL-алгоритма. В данном алгоритме существенную роль играет подъем разложения многочлена на множители, и авторы ссылаются на вышеуказанные статьи Г. Цассенхауза.

В 1982 г. Д.Д. Диксон[6] сформулировал алгоритм нахождения рациональных решений целочисленной квадратной линейной системы уравнений. Он в явном виде выписал формулы, позволяющие из решения системы сравнений по модулю p получить решения по модулю p^k, где $k \in \mathbb{N}$.

Также Д.Д. Диксон сформулировал в своей работе утверждение, позволяющее из целочисленного решения системы сравнений по модулю p^k с помощью оценки на модули числителей и знаменателей рациональных решений исходной системы их восстановить:

Утверждение 4. *Пусть s, h — целые числа. Предположим, что существуют целые числа f и g, такие, что*

$$gs \equiv f \pmod{h} \text{ и } |f|, |g| \leq \lambda\sqrt{h},$$

где λ — положительный корень уравнения

$$\lambda^2 + \lambda - 1 = 0.$$

Пусть $\frac{w_i}{v_i}$ $(i = 1, 2, \ldots)$ — подходящие дроби к числу $\frac{s}{h}$. Положим

$$u_i = v_i s - w_i h.$$

Тогда

$$\frac{f}{g} = \frac{u_k}{v_k},$$

где k — наименьшее целое число, для которого выполняется неравенство $|u_k| < \sqrt{h}$.

В 1993 г. подъем решения сравнения использовали Д. Бухлер, Х.В. Ленстра и К. Померанс[7]. В своей работе они описали алгоритм извлечения квадратного корня в порядке $\mathbb{Z}[\omega]$ поля алгебраических чисел, где ω — целое алгебраическое число степени d. Точнее, описанный алгоритм находит такое число $\beta \in \mathbb{Z}[\omega]$, что

$$\beta^2 = \gamma, \tag{2}$$

где γ — наперед заданное число, принадлежащее кольцу $\mathbb{Z}[\omega]$. Также алгоритм определяет случаи, когда такого числа β не существует.

[6]Dixon J. D. Exact Solution of Linear Equations Using P-Adic Expansions // Numerische Mathematik. 1982, vol. 40, p. 137–141

[7]Lenstra A. K., Lenstra H. W. The Development of the Number Field Sieve, Lecture Notes in Mathematics, vol. 1554. Berlin: Springer, 1993. 140 p.

В данном алгоритме авторы в явном виде выписали итерационную формулу без деления для вычисления каждого последующего шага при подъеме решения:

Утверждение 5. *Пусть p — простое число, $p > 2$, $\gamma \in \mathbb{Z}[\omega]$,*

$$\delta_0 = \sum_{i=0}^{d-1} d_{0,i}\omega^i \in \mathbb{Z}[\omega],$$

причем

$$\max_{0 \le i \le d-1} |d_{0,i}| \le \frac{p}{2}$$

и $\delta_0 \pmod p$ является решением сравнения

$$\gamma z^2 \equiv 1 \pmod p$$

в $\mathbb{Z}[\omega]$. Тогда элемент

$$\delta_j = \sum_{i=0}^{d-1} d_{j,i}\omega^i \in \mathbb{Z}[\omega],$$

определяемый из условий

$$\delta_j \equiv \frac{\delta_{j-1}(3 - \delta_{j-1}^2\gamma)}{2} \pmod{p^{2^j}} \text{ и } \max_{0 \le i \le d-1} |d_{j,i}| \le \frac{p^{2^j}}{2}, \tag{3}$$

является решением сравнения $\delta_j^2\gamma \equiv 1 \pmod{p^{2^j}}$.

Далее авторы доказали, что для некоторой эффективно вычислимой границы V выполняется следующее утверждение: либо $\delta_V^2\gamma = 1$ в $\mathbb{Z}[\omega]$, либо уравнение $z^2\gamma = 1$ не имеет решений в $\mathbb{Z}[\omega]$. В первом случае можно положить $\beta = \delta_V\gamma$, а во втором случае исходное уравнение (2) неразрешимо.

В настоящей диссертации описан алгоритм, обобщающий метод Д. Бухлера, Х.В. Ленстры и К. Померанса на многочлены произвольной степени с коэффициентами, лежащими в произвольном порядке поля алгебраических чисел. Также описан алгоритм, позволяющий при некоторых дополнительных предположениях найти целые решения однородной полиномиальной системы уравнений с целыми коэффициентами. Алгоритм основан на разработанной в диссертации формуле подъема решения полиномиальной системы сравнений.

Цель работы

Диссертационная работа преследует следующие цели:

1. Разработать алгоритм для решения полиномиальных уравнений от одной неизвестной в произвольных порядках поля алгебраических чисел.

2. Разработать алгоритм для нахождения при некоторых условиях целых решений однородной полиномиальной системы уравнений нулевой размерности с целыми коэффициентами.

Методы исследования

В диссертации используются методы коммутативной алгебры и методы построения решений в полях p–адических чисел с помощью подъема по степеням простых идеалов.

Научная новизна

Результаты диссертации являются новыми, получены автором самостоятельно и заключаются в следующем:

1. Получен алгоритм решения полиномиальных уравнений в произвольном порядке поля алгебраических чисел, в том числе:

   - найдена оценка на высоту решения полиномиального уравнения в произвольном порядке поля алгебраических чисел;
   - найдена итерационная формула, позволяющая сделать подъем решения полиномиального сравнения в порядке по модулю некоторого простого числа p до решения по модулю p^{2^k}, где $k \in \mathbb{N}$;
   - вычислена эффективная граница, до которой следует поднимать решение сравнения для того, чтобы найти точное решение исходного уравнения в порядке.

2. Получен алгоритм нахождения неособых целых решений однородных полиномиальных систем с целыми коэффициентами нулевой размерности, в том числе:

   - найдена оценка на высоту рационального решения неоднородной полиномиальной системы уравнений с целыми коэффициентами;

- найдена итерационная формула, позволяющая сделать подъем целого решения неоднородной полиномиальной системы сравнений с целыми коэффициентами по модулю некоторого простого числа p до решения по модулю p^{2^k}, где $k \in \mathbb{N}$;
- вычислена эффективная граница, до которой следует поднимать решение неоднородной полиномиальной системы сравнений с целыми коэффициентами для того, чтобы найти рациональное решение соответствующей полиномиальной системы уравнений.

Теоретическая и практическая ценность

Диссертация носит теоретический характер. Ее результаты могут быть полезны специалистам в области алгоритмической и алгебраической теории чисел.

Апробация диссертации

Результаты диссертации докладывались на следующей международной научной конференции:

1. Международная конференция "Indo–Russian Conference on Algebra, Number Theory, Discrete Mathematics and their Applications" (Москва, 15–17 ноября 2014).

Результаты диссертации докладывались и обсуждались на заседаниях следующего научного семинара:

1. Научно–исследовательский семинар кафедры теории чисел под руководством чл.–корр. РАН. проф. Ю. В. Нестеренко, проф. Н. Г. Мощевитина неоднократно в 2013–2014 годах.

Публикации

Основные результаты диссертации представлены в 3 работах [1–3], 2 из которых из списка ВАК, список работ приведен в конце автореферата.

Структура и объем

Диссертация состоит из введения и двух глав. Текст диссертации изложен на 90 страницах. Список литературы содержит 31 наименование.

Содержание работы

Во **введении** описывается структура диссертации и история рассматриваемых вопросов; обосновывается актуальность темы и научная новизна полученных результатов; описываются основные результаты диссертации.

В **первой главе** описывается алгоритмы 1.1 и 1.2 решения полиномиальных уравнений в произвольном порядке поля алгебраических чисел. А именно, пусть ω — целое алгебраическое число степени d с минимальным многочленом $g(x)$. Обозначим через $\mathfrak{D}$ произвольный порядок поля $\mathbb{Q}(\omega)$ и зафиксируем в нем произвольный базис $\Omega = \{\omega_1, \ldots, \omega_d\}$. Рассмотрим полиномиальное уравнение

$$f(x) = 0, \text{ где } f(x) = \sum_{i=0}^{m} \gamma_i x^i \in \mathfrak{D}[x], \gamma_m \neq 0 \tag{4}$$

— многочлен без кратных корней. Алгоритм 1.1 позволяет найти решения уравнения (4) в порядке $\mathfrak{D}$, а также определяет случаи, когда решений не существует.

Теоремы, приведенные ниже, описывают суть данного алгоритма. Итак, пусть

- $\|\delta\|$ — максимум модулей коэффициентов произвольного числа $\delta \in \mathfrak{D}$ в базисе Ω.
- $\overline{g(x)}(p) \in \mathbb{F}_p[x]$ многочлен, получающийся из $g(x)$ заменой коэффициентов их вычетами по модулю p,
- $\boxed{\xi} = \max_{1 \leq k \leq d} |\xi^{(k)}|$, где $\xi^{(k)}$ — числа, сопряженные с произвольным алгебраическим числом ξ,
- $R = \gamma_m D(f)$, $D(f)$ — дискриминант многочлена $f(x)$,
- $N(R)$ — норма алгебраического числа R,
- D_ω — дискриминант алгебраического числа ω,
- $A(x), B(x) \in \mathfrak{D}[x]$ — многочлены, удовлетворяющие условиям

$$R = A(x)f(x) + B(x)f'(x), \deg A(x) < m - 1, \deg B(x) < m,$$

- $R' \in \mathfrak{D}$ — элемент порядка, удовлетворяющий условию

$$N(R) = R \cdot R',$$

- $N_0 \in \mathbb{Z}$ определяется как решение сравнения

$$N(R) \cdot x \equiv 1 \pmod{p},$$

- $N_k \in \mathbb{Z}$, $k \geq 1$, являющиеся элементами, обратными к $N(R)$ по модулю p^{2^k}, определяются из рекуррентного соотношения

$$N_k \equiv 2N_{k-1} - N(R)N_{k-1}^2 \pmod{p^{2^k}}, \tag{5}$$

- $p > 2$ — простое число, такое, что $p \nmid D_\omega$, $p \nmid N(R)$ и многочлен $\overline{\mu_\omega(x)}(p)$ неприводим, где $\mu_\omega(x)$ — минимальный многочлен числа ω.

Определим элементы порядка $\delta_k \in \mathfrak{D}$, $k \geq 0$, следующим образом:

1. δ_0 — элемент порядка $\mathfrak{D}$, удовлетворяющий условиям

$$f(\delta_0) \equiv 0 \pmod{p}, \tag{6}$$
$$\|\delta_0\| \leq \frac{p}{2},$$

2. δ_k — элемент порядка $\mathfrak{D}$, удовлетворяющий соотношениям

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}}, \tag{7}$$
$$\|\delta_k\| \leq \frac{p^{2^k}}{2}.$$

Теорема 1. *При любом $k \geq 0$ для элементов $\delta_k \in \mathfrak{D}$, вычисляемых из соотношений* (5), (6) *и* (7), *выполняется следующее сравнение:*

$$f(\delta_k) \equiv 0 \pmod{p^{2^k}}.$$

Обозначим через $\{\omega'_1, \ldots, \omega'_d\}$ — базис порядка $\mathfrak{D}$, взаимный к Ω.

Теорема 2. *Пусть $\alpha \in \mathfrak{D}$ — произвольное решение уравнения $f(x) = 0$. Тогда имеет место неравенство*

$$\|\alpha\| \leq CU,$$

где

$$C = d \cdot \max_{1 \leq j \leq d} \overline{|\omega'_j|},$$

$$U = \max_{0 \leq j < m} \overline{|\gamma_j|} \cdot \overline{|\gamma_m|}^{d-1} + 1.$$

Теорема 3. *Если требуется найти $\alpha \in \mathfrak{D}$ — корень уравнения $f(x) = 0$, удовлетворяющий условию*

$$\alpha \equiv \delta_0 \pmod{p},$$

где p выбирается в алгоритме 1.1, то либо $\alpha = \delta_V$, где

$$V = 1 + \lfloor \log_2(\log_p(2CU)) \rfloor,$$

либо такого решения не существует.

Теорема 4. *Алгоритм 1.1 находит все корни уравнения $f(x) = 0$, принадлежащие порядку $\mathfrak{D}$, если они есть, а также выдает ответ, что таких корней нет, если их не существует.*

Также в первой главе диссертации описывается алгоритм 1.2, являющийся модифицированной версией алгоритма 1.1. Он позволяет отказаться от условия неприводимости многочлена $\overline{\mu_\omega(x)}(p)$, и для него остаются верными теоремы 1–4.

Во **второй главе** описывается алгоритм нахождения неособых целых решений однородных полиномиальных систем уравнений нулевой размерности с целыми коэффициентами.

Полученный результат можно сформулировать следующим образом: пусть $R_i(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, $1 \leq i \leq n$. Рассмотрим систему уравнений

$$\overline{R}(\overline{x}) = 0, \text{ где } \overline{R} = \begin{pmatrix} R_1 \\ R_2 \\ \ldots \\ R_n \end{pmatrix}. \tag{8}$$

Введем следующие обозначения:

$$\overline{\delta_k} = \begin{pmatrix} \delta_{k,1} \\ \delta_{k,2} \\ \ldots \\ \delta_{k,n} \end{pmatrix}, \; A_k = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\overline{\delta_k}) & \ldots & \frac{\partial R_1}{\partial x_n}(\overline{\delta_k}) \\ \ldots & & \\ \frac{\partial R_n}{\partial x_1}(\overline{\delta_k}) & \ldots & \frac{\partial R_n}{\partial x_n}(\overline{\delta_k}) \end{pmatrix},$$

где $\delta_{k,i} \in \mathbb{Z}$ и $k = 0, 1, 2, \ldots$.

Пусть p — простое число, удовлетворяющее условию

$$p \nmid \det A_0. \tag{9}$$

Пусть также $\overline{\delta_0}$ — вектор, удовлетворяющий условию

$$\overline{R}(\overline{\delta_0}) \equiv 0 \pmod{p}. \tag{10}$$

Пусть C_0 — матрица с целыми элементами, такая, что

$$A_0 C_0 \equiv E \pmod{p}. \tag{11}$$

Зададим $\overline{\delta_k}$ и C_k, где $k \in \mathbb{N}$, следующими формулами:

$$\overline{\delta_k} \equiv \overline{\delta_{k-1}} - C_{k-1} \cdot \overline{R}(\overline{\delta_{k-1}}) \pmod{p^{2^k}}, \tag{12}$$

где $\max |\delta_{k,i}| \leq \frac{p^{2^k}}{2}$, и

$$C_k \equiv 2C_{k-1} - C_{k-1} A_k C_{k-1} \pmod{p^{2^k}}, \tag{13}$$

где $\max |C_{k,i}| \leq \frac{p^{2^k}}{2}$.

Теорема 5. *При любом $k \in \mathbb{Z}$, $k \geq 0$ для векторов $\overline{R}$ и $\overline{\delta_k}$ и матриц A_k и C_k, определенных с помощью формул (9)–(13), выполняются следующие сравнения:*

$$A_k C_k \equiv E \pmod{p^{2^k}} \tag{14}$$

и

$$\overline{R}(\overline{\delta_k}) \equiv 0 \pmod{p^{2^k}}. \tag{15}$$

Еще одним основополагающим результатом второй главы диссертации является оценка модуля решения системы полиномиальных уравнений, полученная с помощью теории полиномиальных идеалов.

Пусть

$$\overline{P}(\overline{x}) = 0 \tag{16}$$

— однородная система уравнений, соответствующая системе (8), то есть

$$R_i(x_1, \ldots, x_n) = P_i(1, x_1, \ldots, x_n), i = 1, \ldots, n$$

и

$$P_i = x_0^{\deg R_i} R_i(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \in \mathbb{Z}[x_0, x_1, \ldots, x_n], i = 1, \ldots, n.$$

Теорема 6. *Рассмотрим систему (8) и предположим, что*

$$\max_{1 \leq i \leq n} \deg R_i \leq D \ \textit{и} \ \max_{1 \leq i \leq n} h(R_i) \leq h.$$

Тогда верны следующие оценки:

$$\log \max_{0 \leq k \leq n} |\alpha_k^{(j)}| \leq (nh + 6n^2(n-1)D)D^{n-1} + nD^n$$

и

$$g \leq D^n,$$

где $\overline{\alpha}^{(1)}, \ldots, \overline{\alpha}^{(g)}$ *— все решения системы (16) и*

$$\overline{\alpha}^{(j)} = (\alpha_0^{(j)}, \ldots, \alpha_n^{(j)}).$$

Если $\overline{\alpha} = (\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n})$ *— рациональное решение системы (8), то верна оценка*

$$\max\{\log \max_{1\leq k\leq n} |a_k|, \log \max_{1\leq k\leq n} |b|\} \leq (nh + 6n^2(n-1)D)D^{n-1} + nD^n,$$

где b=НОК$(b_1, \ldots, b_n)$.

С помощью результатов второй главы диссертации для неоднородных систем уравнений можно получить следующий результат, лежащий в основе алгоритма 2.1.

Введем обозначение $C = \exp((nh + 6n^2(n-1)D)D^{n-1} + nD^n)$.

Теорема 7. *Если требуется найти*

$$\overline{\alpha} = \left(\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\right)$$

— рациональное решение системы (8), удовлетворяющее условию

$$\overline{\alpha} \equiv \overline{\delta_0} \pmod{p}$$

и $p \nmid b$*, где* p *выбирается в алгоритме 2.1, то либо* $\dfrac{a_i}{b_i} = \dfrac{f_k}{g_k}$*, где* f_k *и* g_k *выбираются согласно условиям утверждения* 4*, а* $h = p^{2^V}$*, где*

$$V = \lfloor \log_2 \log_p \left(\frac{C^2}{\lambda^2}\right) \rfloor + 1,$$

либо такого решения не существует.

Для самого алгоритма 2.1 верно следующее.

Теорема 8. *Алгоритм 2.1 находит все решения* $\overline{\alpha}$ *системы* (8)*, принадлежащие* $\mathbb{Q}^n$ *и удовлетворяющие условиям* $p \nmid b$ *и* $\nu_p(\det J|_{\overline{\alpha}}) = 0$*, где*

$$J = \begin{pmatrix} \frac{\partial R_1}{\partial x_1} & \cdots & \frac{\partial R_1}{\partial x_n} \\ \cdots & & \\ \frac{\partial R_n}{\partial x_1} & \cdots & \frac{\partial R_n}{\partial x_n} \end{pmatrix},$$

если они есть, а также выдает ответ, что таких решений нет, если их не существует.

С помощью алгоритма 2.1 нахождения рациональных решений неоднородной системы уравнений с целыми коэффициентами можно получить алгоритм 2.2 нахождения целых решений соответствующей однородной системы. Для данного алгоритма верна следующая теорема.

Теорема 9. *Алгоритм 2.2 находит все решения* $\overline{\alpha}$ *системы* (16)*, принадлежащие* $\mathbb{Z}^n$ *и удовлетворяющие условию* $\exists j \in \overline{0,n} : \nu_p(M_j|_{\overline{\alpha}}) = 0$*, где* $M_j = \det M'_j$*, а*

$$M'_j = \begin{pmatrix} \frac{\partial P_1}{\partial x_0} & \cdots & \frac{\partial P_1}{\partial x_{j-1}} & \frac{\partial P_1}{\partial x_{j+1}} & \cdots & \frac{\partial P_1}{\partial x_n} \\ \cdots & & & & & \\ \frac{\partial P_n}{\partial x_0} & \cdots & \frac{\partial P_n}{\partial x_{j-1}} & \frac{\partial P_n}{\partial x_{j+1}} & \cdots & \frac{\partial P_n}{\partial x_n} \end{pmatrix},$$

если они есть, а также выдает ответ, что таких решений нет, если их не существует.

Заключение

В заключении перечислены основные результаты, полученные в диссертационой работе.

1. Получена оценка на максимум модулей коэффициентов решения полиномиального уравнения от одной неизвестной в произвольном порядке поля алгебраических чисел, зависящая от базиса порядка, степени и коэффициентов исходного многочлена.

2. Получена итерационная формула без деления, позволяющая произвести квадратичный подъем решения полиномиального сравнения от одной неизвестной по модулю степени некоторого простого числа.

3. Получена оценка, зависящая от простого числа p, базиса порядка, степени и коэффициентов исходного многочлена, которая гарантирует тот факт, что либо решение полиномиального сравнения, поднятое до вышеуказанной границы, является решением самого полиномиального уравнения, либо не существует решения решения исходного уравнения в порядке, сравнимого с данным решением полиномиального сравнения по модулю p.

4. Получен алгоритм решения полиномиального уравнения от одной неизвестной в произвольном порядке поля алгебраических чисел.

5. Получена оценка сложности алгоритма решения полиномиального уравнения от одной неизвестной в произвольном порядке поля алгебраических чисел.

6. Получена оценка на максимум модулей элементов решения однородной полиномиальной системы уравнений с целыми коэффициентами нулевой размерности, зависящая от числа неизвестных, а также максимума степеней и модулей коэффициентов исходной системы уравнений.

7. Получена оценка на максимум модулей числителей и знаменателей элементов решения неоднородной полиномиальной системы уравнений с целыми коэффициентами, обладающей тем свойством, что соответствующая ей однородная система имеет нулевую размерность, зависящая от числа неизвестных, а также от максимума степеней и модуля коэффициентов исходной системы уравнений.

8. Получена итерационная формула, позволяющая произвести квадратичный подъем решения неоднородной полиномиальной системы сравнений, в которой число сравнений равно числу неизвестных, по модулю степени некоторого простого числа.

9. Получена оценка, зависящая от простого числа p, количества уравнений, максимума степеней и максимума модулей коэффициентов неоднородной системы уравнений с целыми коэффицентами, обладающей тем свойством, что соответствующая ей однородная система имеет нулевую размерность, и количество уравнений равно число неизвестных, позволяющая получить с помощью подъема решение исходной полиномиальной системы уравнений, сравнимое с решением соответствующего полиномиального сравнения по модулю p, если такое решение есть.

10. Получен алгоритм нахождения неособых рациональных решений неоднородной полиномиальной системы уравнений, обладающей тем свойством, что соответствующая ей однородная система имеет нулевую размерность, в которой число уравнений равно числу неизвестных.

11. Получен алгоритм нахождения неособых целых решений однородной полиномиальной системы уравнений нулевой размерности, в которой число уравнений равно числу неизвестных.

Благодарности

Автор выражает глубокую благодарность своему научному руководителю члену–корреспонденту РАН, профессору Юрию Валентиновичу Нестеренко за постановку задачи и неоценимую помощь на всех этапах написа-

ния работы. Автор благодарен всем сотрудникам кафедры теории чисел механико–математического факультета МГУ за постоянное внимание.

Основные публикации автора по теме диссертации

[1] Зеленова М. Е. Решение полиномиальных уравнений в поле алгебраических чисел // Вестн. Моск. ун-та. Сер. 1. Матем., мех. 2014, № 1, с. 25–29.

[2] Зеленова М. Е. Решение полиномиальных систем уравнений нулевой размерности в целых числах. Деп. в ВИНИТИ 31.03.2015, №69 - В 2015, 32 с.

[3] Зеленова М. Е. О решении полиномиальных уравнений в произвольных порядках // Чебышевский сб. 2015, т. 16, № 2, с. 117–132.