ФГБОУ ВО
Московский государственный университет имени М. В. Ломоносова
Механико–математический факультет

На правах рукописи
УДК 511.2

Зеленова Мария Евгеньевна

Решение систем уравнений в полях алгебраических чисел

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация

на соискание ученой степени
кандидата физико–математических наук

Научный руководитель:
член–корреспондент РАН,
профессор Ю. В. Нестеренко

Москва — 2015

Содержание

Введение **3**

1 Решение полиномиальных уравнений в поле алгебраических чисел **16**

1.1 Вспомогательные определения и утверждения 16

1.2 Алгоритм решения полиномиального уравнения в порядке без учета поиска простого числа p 21

1.3 Обоснование подъема решения полиномиального сравнения (шага 13 алгоритма 1.1) 24

1.4 Оценка коэффициентов решения полиномиального уравнения 27

1.5 Обоснование нахождения точных решений полиномиального уравнения (шагов 13, 14 алгоритма 1.1) 31

1.6 Алгоритм решения полиномиального уравнения в порядке с учетом поиска простого числа p 34

1.7 Оценка сложности работы алгоритма решения полиномиального уравнения в порядке 44

2 Решение однородных полиномиальных систем уравнений нулевой размерности в целых числах **52**

2.1 Постановка задачи 52

2.2 Основные теоретические сведения 53

2.3 Оценка модуля решений однородной полиномиальной системы 64

2.4 Нахождение решений неоднородной полиномиальной системы по модулю степени простого числа 69

2.5 Нахождение рациональных решений неоднородной полиномиальной системы 73

2.6 Алгоритм решения неоднородной полиномиальной системы в рациональных числах 80

2.7 Алгоритм решения однородной полиномиальной системы в целых числах 84

Список литературы **88**

Введение

Общая характеристика работы

Диссертация подготовлена на кафедре теории чисел механико-математического факультета Федерального государственного бюджетного образовательного учреждения высшего образования "Московский государственный университет имени М.В.Ломоносова".

Актуальность темы диссертации. Настоящая 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 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.

Саму идею подъема решения сравнения впервые описал К. Гензель в своей статье [22] в 1904 г. В 1905 г. в работе [23] он сформулировал другой вариант леммы. Позже, в 1968 г., Г. Цассенхауз [27] предложил более быстрый вариант подъема, а также выписал оценки, которые позволяли поднять разложение многочлена с целыми коэффициентами по модулю простого числа p до разложения в $\mathbb{Z}$. Данный алгоритм он более подробно описал в статье [28], изданной в 1978 г. Чуть позже, в 1982 г., в работе [24], А.К. Ленстра, Х.В. Ленстра и Л. Ловас опубликовали свой знаменитый LLL-алгоритм и использовали его для для факторизации многочленов с целыми коэффициентами. В алгоритме факторизации также производится подъем разложения многочлена на множители по модулю некоторого простого числа p до разложения по модулю p^k, где k — граница, которую можно эффективно вычислить. В 1993 г. в статье [25] Д. Бухлер, Х.В. Ленстра и К. Померанс использовали подъем решения сравнения для извлечения квадратного корня в порядке $\mathbb{Z}[\omega]$, где ω — целое алгебраическое число. Также, в 1982 г. в работе [19] Д.Д.

Диксон использовал метод подъема решения для нахождения рациональных решений произвольной линейной системы с целыми коэффициентами.

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 некотрых дополнительных предположениях найти целые решения однородной полиномиальной системы с целыми коэффициентами.

Научная новизна полученных результатов. Доказанные результаты являются новыми, полученными автором самостоятельно.

Основные положения диссертации, выносимые на защиту:

- получен алгоритм решения полиномиальных уравнений в произвольном порядке поля алгебраических чисел:
  - 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 решение исходного уравнения в порядке.
- получен алгоритм нахождения неособых целых решений однородных полиномиальных систем с целыми коэффициентами нулевой размерности:
  - 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 це-

лыми коэффициентами для того, чтобы найти рациональное решение соответствующей полиномиальной системы уравнений.

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

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

Личный вклад соискателя. Все результаты диссертации получены автором самостоятельно.

Апробация работы. Результаты настоящей диссертации докладывались автором на следующих семинарах и международных конференциях:

- научно–исследовательский семинар кафедры теории чисел под руководством чл.–корр. РАН, проф. Ю. В. Нестеренко и д.ф.–м.н., проф. Н. Г. Мощевитина неоднократно в 2013–2014 гг.;

- международная конференция "Indo-Russian conference on Algebra, Number Theory, Discrete Mathematics and their Applications" Москва, Россия, 15.11.2014–17.11.2014.

Опубликованность результатов диссертации. Результаты диссертации опубликованы в работах [29], [30], [31] списка использованных источников.

Структура и объем работы. Диссертация изложена на 90 страницах и состоит из введения, двух глав и списка использованных источников, включающего 31 наименование.

Благодарности. Соискатель считает своим приятным долгом поблагодарить своего научного руководителя, члена–корреспондента РАН, профессора Ю. В. Нестеренко за постоянный интерес и внимание к работе.

Содержание работы

Диссертация состоит из двух глав. В следующих параграфах формулируются основные результаты, а также дается исторический обзор по каждой задаче.

Решение полиномиальных уравнений в поле алгебраических чисел

Впервые идею подъема решения полиномиального сравнения высказал К. Гензель в своей программной статье 1904 г. [22] 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 [23] К. Гензель переформулировал свою лемму в следующей форме:

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 в статье [27] 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 можно найти многочлены $f_k(x)$ и $g_k(x)$, $k \in \mathbb{N}$, удовлетворяющих условию

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

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

Более подробно алгоритм нахождения многочленов $f_k(x)$ и $g_k(x)$ Г. Цассенхауз описал впоследствии спустя почти десять лет в статье [28].

Также в работе [27] 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 статье [24] 1982 г., написанной А.К. Ленстрой, Х.В. Ленстрой и Л.Ловасом, в которой был предложен алгоритм факторизации многочленов с целыми коэффициентами с помощью впервые описанного в той же работе LLL-алгоритма. В данном алгоритме существенную роль играет подъем разложения многочлена на множители, и авторы ссылаются на статьи [27] и [28].

В 1993 г. подъем решения сравнения использовали Д. Бухлер, Х.В. Ленстра и К. Померанс в своей работе [25], в которой 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.

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

Утверждение 4. *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

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

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

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

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

Далее авторами утверждается, 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.

Вышеизложенный алгоритм послужил отправной точкой для создания алгоритма 1.1 решения полиномиальных уравнений в произвольном порядке поля алгебраических чисел, являющегося основным результатом первой главы диссертации и опубликованного в статье [29]. Ниже сформулированы условия и основная идея данного алгоритма.

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

- $\|\delta_k\|$ — максимум модуля коэффициентов числа δ_k в базисе Ω.
- $\overline{g(x)}(p) \in \mathbb{F}_p[x]$ многочлен, получающийся из $g(x)$ заменой коэффициентов c_i их вычетами по модулю p,
- $R = \gamma_m D(f)$, $D(f)$ — дискриминант многочлена $f(x)$,
- $N(R)$ — норма алгебраического числа R,
- D_ω — дискриминант алгебраического числа ω,
- $B(x) \in \mathfrak{D}[x]$ — многочлен, удовлетворяющий равенству

$$R = A(x)f(x) + B(x)f'(x),$$

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

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

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

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

- $N_k \in \mathbb{Z}$, $k \geqslant 1$ определяются из рекуррентного соотношения

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

- $p > 2$ — 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 $\delta_k \in \mathfrak{D}$, $k \geqslant 0$, следующим образом:

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

$$\begin{gathered} f(\delta_0) \equiv 0 \pmod{p}, \\ \|\delta_0\| \leqslant \frac{p}{2}, \end{gathered} \tag{5}$$

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

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}}, \tag{6}$$
$$\|\delta_k\| \leqslant \frac{p^{2^k}}{2}.$$

Теорема 2. *При любом $k \geqslant 0$ для элементов $\delta_k \in \mathfrak{D}$, вычисляемых из соотношений (5) и (6), 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 3. *Имеет место неравенство*

$$\|\alpha\| \leqslant CU,$$

где

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

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

Теорема 4. *Если требуется найти α — корень уравнения $f(x) = 0$ в $\mathfrak{D}$, 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 5. *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 2–5.

Решение однородных полиномиальных систем в целых числах

В 1982 г. Д.Д. Диксон в статье [19] сформулировал алгоритм нахождения рациональных решений целочисленной квадратной линейной системы уравнений. Он в явном виде выписал формулы, позволяющие из целочисленного решения исходной системы по модулю p получить целочисленные решения по модулю p^k, где $k \in \mathbb{N}$.

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

Утверждение 5. *Пусть s, h — целые числа. Предположим, что существуют целые числа f и g, такие, что*

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

где λ — положительный корень уравнения

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

Пусть $\dfrac{w_i}{v_i}$ $(i = 1, 2, \ldots)$ — подходящие дроби к числу $\dfrac{s}{h}$. 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 $|u_k| < \sqrt{h}$.

Данное утверждение используется автором диссертации для нахождения рациональных решений полиномиальной системы.

Заметим, что изначально К. Гензель описал метод подъема (см. утв. 1 и 2) для уравнений, однако по сути лемма Гензеля является дискретным случаем метода касательных Ньютона (см. [1, гл. 7 §2]).

В частности, выражение (3) получено с помощью подстановки многочлена $f(x) = x^2 - \gamma$ в расчетную формулу, используемую в методе Ньютона:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

и последующем ее преобразовании.

Однако формула Ньютона существует и в многомерном варианте (см. [1, гл. 7 §2]). Идея подъема решения целочисленной системы полиномиальных сравнений во второй главе диссертации состоит в том, чтобы по аналогии с формулой Ньютона выписать и преобразовать формулу подъема в дискретном случае.

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

$$\overline{R}(\overline{x}) = 0, \text{ где } \overline{R} = \begin{pmatrix} R_1 \\ R_2 \\ \ldots \\ R_n \end{pmatrix}. \tag{7}$$

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 $k = 0, 1, 2, \ldots$.

Пусть p — простое число, удовлетворяющее условию

$$p \nmid \det A_0. \tag{8}$$

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

$$\overline{R}(\overline{\delta_0}) \equiv 0 \pmod{p}. \tag{9}$$

Пусть C_0 — матрица с целыми элементами, такая, что

$$A_0 C_0 \equiv E \pmod{p}. \tag{10}$$

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

$$\overline{\delta_k} \equiv \overline{\delta_{k-1}} - C_{k-1} \cdot \overline{R}(\overline{\delta_{k-1}}) \pmod{p^{2^k}}, \tag{11}$$

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

$$C_k \equiv 2C_{k-1} - C_{k-1} A_k C_{k-1} \pmod{p^{2^k}}, \tag{12}$$

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

Теорема 20. *При любом $k \in \mathbb{Z}$, $k \geqslant 0$ для векторов $\overline{R}$ и $\overline{\delta_k}$ и матриц A_k и C_k, определенных с помощью формул (8)–(12), выполняются следующие сравнения:*

$$A_k C_k \equiv E \pmod{p^{2^k}} \tag{13}$$

и

$$\overline{R}(\overline{\delta_k}) \equiv 0 \pmod{p^{2^k}}. \tag{14}$$

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

Пусть

$$\overline{P}(\overline{x}) = 0 \tag{15}$$

— однородная система уравнений, соответствующая системе (7), 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 19. *Рассмотрим систему (7) и предположим, что*

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

Тогда верны следующие оценки:

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

и

$$g \leqslant D^n,$$

где $\overline{\alpha}^{(1)}, \ldots, \overline{\alpha}^{(g)}$ — все решения системы (15) 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 (7), то верна оценка

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

где b=НОК$(b_1, \ldots, b_n)$.

Пусть

$$\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) = (\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}) \tag{16}$$

— одно из рациональных решений системы (7), удовлетворяющее условию

$$p \nmid b = \text{НОК}(b_1, \ldots, b_n). \tag{17}$$

Поскольку выполняется формула (17), то найдется вектор $\overline{\delta}_0$, такой, что

$$\overline{R}(\overline{\delta}_0) \equiv 0 \pmod{p} \tag{18}$$

и

$$\overline{\delta}_0 \equiv \overline{\alpha} \pmod{p}. \tag{19}$$

Во второй главе диссертации также доказывается следующий результат:

Теорема 21. *Для векторов* $\overline{\alpha}$ *и* $\overline{\delta}_0$*, определенных формулами* (16)–(19)*, и для любого числа* $K \in \mathbb{N}$ *выполняется следующее сравнение:*

$$\overline{\alpha} \equiv \overline{\delta_K} \pmod{p^{2^K}}, \tag{20}$$

где $\overline{\delta_K}$ *— вектор, полученный из* $\overline{\delta}_0$ *по формуле* (11)*.*

С помощью утверждения 5 и теоремы 21 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 23. *Если требуется найти*

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

— рациональное решение системы (7), удовлетворяющее условию

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

и $p \nmid b$*, где* p *задается 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* 5*, 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 24. *Алгоритм 2.1 находит все решения* $\overline{\alpha}$ *системы* (7)*, принадлежащие* $\mathbb{Q}^n$ *и удовлетворяющие условиям* $p \nmid b$ *и* $\nu_p(\det J|_{\overline{\alpha}}) = 0$*, где*

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

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 25. *Алгоритм 2.2 находит все решения* $\overline{\alpha}$ *системы* (15)*, 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*

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

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

1 Решение полиномиальных уравнений в поле алгебраических чисел

Получен алгоритм нахождения решений полиномиальных уравнений в произвольном порядке поля алгебраических чисел.

Обозначения, которые используются на протяжении всей главы, вводятся вне доказательств утверждений. Обозначения же, появляющиеся внутри доказательств, локальны.

1.1 Вспомогательные определения и утверждения

Более подробно с теорией, изложенной в данном параграфе, можно ознакомиться в книге [2].

Определение 1. *Пусть K — поле алгебраических чисел и $\mu_1, \ldots, \mu_n$ — произвольная конечная система чисел из K. Совокупность M всех линейных комбинаций $c_1\mu_1 + \ldots + c_m\mu_m$ с целыми рациональными коэффициентами c_i $(1 \leqslant i \leqslant m)$ называется модулем в поле K. Сами числа $\mu_1, \ldots, \mu_m$ называются при этом образующими модуля M.*

Определение 2. *Если модуль M в поле алгебраических чисел степени d содержит d линейно независимых чисел (над полем рациональных чисел), то он называется полным, в противном случае — неполным.*

Определение 3. *Полный модуль в поле алгебраических чисел K, содержащий число 1 и являющийся кольцом, называется порядком поля K.*

Пусть ω — целое алгебраическое число степени d,

$$\mu_\omega(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Z}[x],\ c_d = 1$$

— его минимальный многочлен и $\mathfrak{D}$ — произвольный порядок поля $K = \mathbb{Q}(\omega)$.

Пусть также

$$f(x) = \sum_{i=0}^{m} \gamma_i x^i,\ \gamma_i \in \mathfrak{D},\ \gamma_m \neq 0$$

— многочлен без кратных корней.

Введем следующее обозначение:

$$R = \gamma_m D(f), \tag{1.1}$$

где $D(f)$ — дискриминант многочлена $f(x)$.

Через $R(f_1, f_2)$ будем обозначать результант произвольных многочленов $f_1(x)$ и $f_2(x)$.

Лемма 1. *Верна следующая формула:*

$$R(f, f') = \gamma_m^{2m-1} \prod_{i \neq j} (\alpha_i - \alpha_j), \tag{1.2}$$

где $f'(x)$ — производная многочлена $f(x)$, а $\alpha_1, \ldots, \alpha_m$ — все корни уравнения $f(x) = 0$.

Доказательство. См. [10, гл. 5 §10]. □

Замечание 1. *Из определения дискриминанта многочлена $f(x)$ и формулы* (1.2) *следует, что*

$$R = (-1)^{\frac{m(m-1)}{2}} R(f, f').$$

Обозначим через $N(\xi)$ норму произвольного алгебраического числа $\xi \in \mathbb{Q}(\omega)$, а через $\phi_\xi(x)$ — его характеристический многочлен в $\mathbb{Q}(\omega)$ (см. [2]).

Лемма 2. *Пусть ξ — произвольное алгебраическое число, а*

$$\phi_\xi(x) = x^d + v_{d-1}x^{d-1} + \ldots + v_1 x + v_0$$

— его характеристический многочлен. Тогда верно следующее равенство:

$$N(\xi) = (-1)^d v_0.$$

Доказательство. См. [2, гл. “Алгебраическое дополнение”, §2]. □

Лемма 3. *Если число $\zeta \in \mathfrak{D}$, то его характеристический и минимальный многочлен имеют целые коэффициенты. В частности,*

$$N(\zeta) \in \mathbb{Z}.$$

Доказательство. См. [2, гл. 2 §2]. □

Лемма 4. *Пусть число* $\zeta \in \mathfrak{D}$, $\zeta \neq 0$ *и*

$$\phi_\zeta(x) = u_0 + u_1 x + \ldots + u_{d-1}x^{d-1} + x^d.$$

Тогда $N(\zeta)$ *делится в кольце* $\mathfrak{D}$ *на* ζ, *причем*

$$\frac{N(\zeta)}{\zeta} = (-1)^{d-1}(\zeta^{d-1} + u_{d-1}\zeta^{d-2} + \ldots + u_1). \tag{1.3}$$

Доказательство. См. [2, гл. 2 §2]. □

Следствие 1. *Для числа* R, *определенного равенством* (1.1), *существует число* $R' \in \mathfrak{D}$, *такое, что*

$$N(R) = R \cdot R'. \tag{1.4}$$

Доказательство. Достаточно воспользоваться формулой (1.3) и положить

$$R' = (-1)^{d-1}(R^{d-1} + r_{d-1}R^{d-2} + \ldots + r_1),$$

где

$$\phi_R(x) = x^d + r_{d-1}x^{d-1} + \ldots + r_1 x + r_0.$$

□

Лемма 5. *Пусть* $f_1(x), f_2(x) \in \mathfrak{D}[x]$, *где* $\deg f_1 = n_1$ *и* $\deg f_2 = n_2$. *Тогда существуют многочлены* $A(x), B(x) \in \mathfrak{D}[x]$, *такие, что*

$$R(f_1, f_2) = A(x)f_1(x) + B(x)f_2(x).$$

При этом многочлены $A(x)$ *и* $B(x)$ *можно выписать в виде*

$$A(x) = x^{n_2-1}M_{1,n_1+n_2-1} + x^{n_2-2}M_{2,n_1+n_2-1} + \ldots + M_{n_2,n_1+n_2-1},$$

$$B(x) = x^{n_1-1}M_{n_2+1,n_1+n_2-1} + x^{n_1-2}M_{n_2+2,n_1+n_2-1} + \ldots + M_{n_1+n_2-1,n_1+n_2-1},$$

где $M_{i,j}$ — *алгебраические дополнения матрицы Сильвестра многочленов* $f_1(x)$ *и* $f_2(x)$.

Доказательство. См. [3, гл. 5 §34]. □

Следствие 2. *Существуют многочлены* $A(x), B(x) \in \mathfrak{D}[x]$*, такие, что*

$$R = A(x)f(x) + B(x)f'(x). \tag{1.5}$$

При этом многочлены $A(x)$ *и* $B(x)$ *можно выписать в виде*

$$A(x) = (-1)^{\frac{m(m-1)}{2}}(x^{m-2}M_{1,2m-1} + x^{m-3}M_{2,2m-1} + \ldots + M_{m-1,2m-1}),$$

$$B(x) = (-1)^{\frac{m(m-1)}{2}}(x^{m-1}M_{m,2m-1} + x^{m-2}M_{m+1,2m-1} + \ldots + M_{2m-1,2m-1}),$$

где $M_{i,j}$ *— алгебраические дополнения матрицы Сильвестра многочленов* $f(x)$ *и* $f'(x)$*.*

Доказательство. Воспользуемся леммой 5. Из нее следует, что существуют многочлены $A_1(x), B_1(x) \in \mathfrak{D}[x]$, такие, что

$$R(f, f') = A_1(x)f(x) + B_1(x)f'(x).$$

Тогда, по замечанию 1,

$$R = (-1)^{\frac{m(m-1)}{2}}A_1(x)f(x) + (-1)^{\frac{m(m-1)}{2}}B_1(x)f'(x).$$

□

Согласно определению порядка, он обладает базисом. Обозначим через

$$\Omega = \{\omega_1, \ldots, \omega_d\}$$

базис порядка $\mathfrak{D}$. Тогда каждый элемент $\beta \in \mathfrak{D}$ можно единственным образом представить в виде

$$\beta = b_1\omega_1 + \cdots + b_d\omega_d,$$

где $b_i \in \mathbb{Z}$.

Будем использовать обозначение

$$\|\beta\| = \max_{1 \leqslant i \leqslant d} |b_i|.$$

Также через $\mathrm{Tr}(\xi)$ будем обозначать след произвольного алгебраического числа $\xi \in \mathbb{Q}(\omega)$.

Лемма 6. *Пусть $E \supset F$ — конечное расширение и $\eta_1, \ldots, \eta_n$ — базис поля E над F. Существует базис $\eta'_1, \ldots, \eta'_n$ поля E с условием*

$$\mathrm{Tr}(\eta_i \eta'_j) = \begin{cases} 1, & \text{если} \quad i = j, \\ 0, & \text{если} \quad i \neq j. \end{cases} \tag{1.6}$$

Доказательство. См. [2, гл. 6 §2]. □

Определение 4. *Два базиса, связанные соотношениями* (1.6)*, называются взаимными.*

Обозначим через

$$\Omega' = \{\omega'_1, \ldots, \omega'_d\}$$

взаимный к Ω базис поля $\mathbb{Q}(\omega)$.

Определение 5. *Для любого набора алгебраических чисел $\xi_1, \ldots, \xi_d \in \mathbb{Q}(\omega)$ его дискриминант определяется следующим образом:*

$$\Delta(\xi_1, \ldots, \xi_d) = \det\left(\mathrm{Tr}(\xi_i \xi_j)\right)_{1 \leqslant i,j \leqslant d}.$$

Определение 6. *Дискриминантом алгебраического числа ω называется выражение*

$$\Delta(1, \omega, \ldots, \omega^{d-1}).$$

Будем обозначать дискриминант числа ω через D_ω.

Лемма 7. *Верно следующее равенство:*

$$D_\omega = D(\mu_\omega).$$

Доказательство. См. [17, §4.4.1]. □

Определение 7. *Индексом числа ω называется индекс подгруппы $\mathbb{Z}[\omega]$ в $\mathbb{Z}_K$.*

Будем обозначать индекс числа ω через z.

Лемма 8. *Верно следующее равенство:*

$$D_\omega = z^2 D,$$

где D — дискриминант поля K.

Доказательство. См. [6, гл. 2 §11]. □

Определение 8. *Пусть* $\{\xi_1, \ldots, \xi_d\}$ *— базис кольца* $\mathbb{Z}_K$*. Дискриминантом поля* K *называется величина* $\Delta(\xi_1, \ldots, \xi_d)$*.*

Будем обозначать через D дискриминант поля $\mathbb{Q}(\omega)$.

Для произвольного алгебраического числа ξ положим

$$\boxed{\xi} = \max_{1 \leqslant k \leqslant d} |\xi^{(k)}|,$$

где $\xi^{(k)}$ — числа, сопряженные с ξ.

Пусть $g(x) = g_l x^l + \ldots + g_1 x + g_0 \in \mathbb{Z}[x]$.

Обозначим через $\overline{g(x)}(p) \in \mathbb{F}_p[x]$ многочлен, получающийся из $g(x)$ заменой коэффициентов c_i их вычетами по модулю p, где p — некоторое простое число.

1.2 Алгоритм решения полиномиального уравнения в порядке без учета поиска простого числа p

В алгоритме, описанном ниже, не говорится о способе нахождения простого числа p *на шаге 8. Модификация данного алгоритма, позволяющая обойти поиск простого числа* p *в тех случаях, когда найти его не удается, описана в параграфе* 1.6*.*

Алгоритм 1.1.

Дано: ω — целое алгебраическое число степени d;

$\mathfrak{D}$ — порядок в поле $\mathbb{Q}(\omega)$;

$\mu_\omega(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Z}[x], c_d = 1$, — минимальный многочлен ω;

$f(x) = \sum_{i=0}^{m} \gamma_i x^i$, $\gamma_i \in \mathfrak{D}$ — многочлен без кратных корней.

Найти: множество решений уравнения $f(x) = 0$ в $\mathfrak{D}$ или дать ответ, что решений нет.

1. Положить $S' = \emptyset$. [*на выходе алгоритма множество* S' *будет состоять из решений исходного уравнения*]

2. Вычислить $R = \gamma_m D(f)$.

3. Вычислить $\phi_R(x) = r_0 + r_1 x + \ldots + r_{d-1}x^{d-1} + x^d$. [$\phi_R(x)$ — *характеристический многочлен числа* $R \in \mathfrak{D}$]

4. Положить $N(R) = (-1)^d r_0$. [*см. лемму* 2]

5. Положить

$$R' = (-1)^{d-1}(r_1 + r_2 R + \ldots + r_{d-1}R^{d-2} + R^{d-1}).$$

[*см. следствие* 1]

6. Вычислить $A(x), B(x) \in \mathfrak{D}[x]$, такие, что

$$R = A(x)f(x) + B(x)f'(x).$$

[*см. следствие* 2]

7. Вычислить $D_\omega = D(\mu_\omega)$. [*см. лемму* 7]

8. Найти простое число $p > 2$, такое, что $\overline{\mu_\omega(x)}(p)$ неприводим,

$$(p, N(R)) = 1 \text{ и } (p, D_\omega) = 1.$$

9. Найти все решения сравнения $f(x) \equiv 0 \pmod p$ в порядке $\mathfrak{D}$.

   Если оно неразрешимо, то уравнение $f(x) = 0$ неразрешимо в $\mathfrak{D}$.

   Если сравнение разрешимо, то обозначим через S множество всех элементов из $\mathfrak{D}$, таких, что для каждого $\delta \in S$

$$f(\delta) \equiv 0 \pmod p.$$

   Выбрать δ так, чтобы выполнялось $\|\delta\| \leqslant \frac{p}{2}$.

10. Положить $V = 1 + \lfloor \log_2(\log_p(2CU)) \rfloor$, где

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

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

   Здесь ω'_j — элементы базиса, взаимного к Ω.

11. Найти решение N_0 сравнения

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

для которого выполняется условие $|N_0| \leqslant \frac{p}{2}$.

12. Для каждого $k = 1, \ldots, V$ вычислить $N_k \in \mathbb{Z}$, такие, что

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

$$|N_k| \leqslant \frac{p^{2^k}}{2}.$$

13. Для каждого $\delta \in S$ выполнять следующие действия:

13.1. Положить $\delta_0 = \delta$.

13.2. Для каждого $k = 1, \ldots, V$ вычислить

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}},$$

$$\delta_k \in \mathfrak{D},\ \|\delta_k\| \leqslant \frac{p^{2^k}}{2}.$$

13.3. Проверить, удовлетворяет ли число δ_V равенству

$$f(\delta_V) = 0.$$

Если равенство выполняется, то

$$S' = S' \cup \{\delta_V\}.$$

14. Если $S' = \emptyset$, то дать ответ, что уравнение $f(x) = 0$ неразрешимо в $\mathfrak{D}$.

Замечание 2. *Для того, чтобы решить сравнение $f(x) \equiv 0 \pmod{p}$, достаточно решить уравнение $f(x) = 0$ в поле $\mathbb{F}_{p^d}$. Алгоритмы нахождения корней многочленов в конечных полях можно найти в книге [5, гл. 3].*

Замечание 3. *Для того, чтобы перейти к случаю, когда многочлен $f(x)$ не имеет кратных корней, достаточно рассмотреть*

$$d(x) = (f(x), f'(x)).$$

Если $\deg d(x) = 0$, *то многочлен* $f(x)$ *не имеет кратных корней.*

В противном случае вместо уравнения $f(x) = 0$ *можно рассматривать уравнение*

$$f_0(x) = 0, \ \text{где } f_0(x) = \frac{f(x)}{d(x)}. \tag{1.7}$$

Уравнение (1.7) *имеет те же решения, что и исходное уравнение.*

1.3 Обоснование подъема решения полиномиального сравнения (шага 13 алгоритма 1.1)

Пусть p — простое число, которое определяется в алгоритме 1.1. Определим числа N_k, $k \geqslant 0$, следующим образом:

1. $N_0 \in \mathbb{Z}$ находится как решение сравнения

$$\begin{gathered} N(R) \cdot x \equiv 1 \pmod{p}, \\ |N_0| \leqslant \frac{p}{2}. \end{gathered} \tag{1.8}$$

2. $N_k \in \mathbb{Z}$, $k \geqslant 1$ вычисляются из рекуррентных соотношений

$$\begin{gathered} N_k \equiv \ 2N_{k-1} - N(R)N_{k-1}^2 \pmod{p^{2^k}}, \\ |N_k| \leqslant \frac{p^{2^k}}{2}. \end{gathered} \tag{1.9}$$

Теорема 1. *При любом* $k \geqslant 0$ *для чисел* N_k, *вычисляемых из соотношений* (1.8) *и* (1.9), *выполняется сравнение*

$$N(R) \cdot N_k \equiv 1 \pmod{p^{2^k}}. \tag{1.10}$$

Доказательство. Поскольку простое число p, которое выбирается на шаге 8 алгоритма, удовлетворяет условию

$$(N(R), p) = 1,$$

то сравнение (1.8) разрешимо.

Дальнейшее доказательство проведем индукцией по k. При $k = 0$ теорема верна по построению N_0. Пусть теперь $k > 0$, и сравнение выполнено для всех N_i при $i < k$.

Согласно предположению индукции,

$$N(R) \cdot N_{k-1} - 1 \equiv 0 \pmod{p^{2^{k-1}}}.$$

Следовательно,

$$(N(R) \cdot N_{k-1} - 1)^2 \equiv 0 \pmod{(p^{2^{k-1}})^2 = p^{2^k}}. \tag{1.11}$$

Перепишем сравнение (1.11) в следующем виде:

$$(N(R) \cdot N_{k-1} - 1)^2 = N(R)^2 N_{k-1}^2 - 2N(R)N_{k-1} + 1 =$$

$$= N(R)(N(R)N_{k-1}^2 - 2N_{k-1}) + 1 \equiv 0 \pmod{p^{2^k}}$$

и применим к получившемуся сравнению соотношение (1.9). Таким образом, верно сравнение

$$-N(R) \cdot N_k + 1 \equiv 0 \pmod{p^{2^k}},$$

и, следовательно, выполняется утверждение теоремы 1. □

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

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

$$f(\delta_0) \equiv 0 \pmod{p}, \tag{1.12}$$
$$\|\delta_0\| \leqslant \frac{p}{2},$$

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

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}}, \tag{1.13}$$
$$\|\delta_k\| \leqslant \frac{p^{2^k}}{2},$$

где $B(x)$, R' и N_k определяются в следствиях 2, 1 и теореме 1 соответственно.

Теорема 2. *При любом $k \geqslant 0$ для элементов $\delta_k \in \mathfrak{D}$, вычисляемых из соотношений* (1.12) *и* (1.13)*, выполняется следующее сравнение:*

$$f(\delta_k) \equiv 0 \pmod{p^{2^k}}. \tag{1.14}$$

Доказательство. Проведем доказательство индукцией по k. При $k = 0$ теорема верна по построению δ_0. Пусть теперь $k \geqslant 1$, и сравнение выполнено для всех δ_i при $i < k$.

Пусть $A(x), B(x) \in \mathfrak{D}[x]$ — многочлены, построенные на шаге 6 алгоритма.

Согласно предположению индукции, верно сравнение

$$f(\delta_{k-1}) \equiv 0 \pmod{p^{2^{k-1}}}. \tag{1.15}$$

Из формулы (1.13) и свойств сравнений следует, что

$$f(\delta_k) \equiv f\left(\delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k\right) \pmod{p^{2^k}}.$$

Разложим многочлен $f(x)$ в ряд Тейлора в окрестности точки δ_{k-1}, и рассмотрим значение $f(x)$ в точке δ_k. Получим следующее сравнение:

$$\begin{aligned} f(\delta_k) \equiv f(\delta_{k-1}) - f'(\delta_{k-1})f(\delta_{k-1})B(\delta_{k-1})R'N_k + \\ + \sum_{j=2}^{m}(-1)^j \frac{f^{(j)}(\delta_{k-1})}{j!}(f(\delta_{k-1})B(\delta_{k-1})R'N_k)^j \pmod{p^{2^k}}. \end{aligned} \tag{1.16}$$

Заметим, что $j-$ая производная многочлена $f(x)$ в точке δ_{k-1} имеет вид

$$f^{(j)}(\delta_{k-1}) = \sum_{s=0}^{m-j} \frac{(m-s)!}{(m-s-j)!}\gamma_{m-s}{\delta_{k-1}}^{m-j-s}.$$

Следовательно,

$$\frac{f^{(j)}(\delta_{k-1})}{j!} = \sum_{s=0}^{m-j} \frac{(m-s)!}{(m-s-j)!j!}\gamma_{m-s}{\delta_{k-1}}^{m-j-s} = \sum_{s=0}^{m-j} \binom{m-s}{j}\gamma_{m-s}{\delta_{k-1}}^{m-j-s},$$

где $\binom{m-s}{j}$ — биномиальный коэффициент.

Таким образом,

$$\frac{f^{(j)}(\delta_{k-1})}{j!} \in \mathfrak{D},$$

и, следовательно,

$$\sum_{j=2}^{m}(-1)^j \frac{f^{(j)}(\delta_{k-1})}{j!}(f(\delta_{k-1})B(\delta_{k-1})R'N_k)^j \in \mathfrak{D}. \tag{1.17}$$

Заметим, что, согласно предположению индукции, верно сравнение (1.15), откуда следует, что

$$(f(\delta_{k-1}))^2 \equiv 0 \pmod{(p^{2^{k-1}})^2 = p^{2^k}}, \tag{1.18}$$

то есть, и

$$(f(\delta_{k-1}))^j \equiv 0 \pmod{p^{2^k}} \text{ при } j = 2, \ldots, m. \tag{1.19}$$

Применим формулу (1.19) к сравнению (1.16), учитывая выполнение условия (1.17). Получим, что

$$f(\delta_k) \equiv f(\delta_{k-1}) - f'(\delta_{k-1})f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}}. \tag{1.20}$$

Из следствия 2 непосредственно вытекает, что для многочленов $A(x)$ и $B(x)$ выполняется равенство

$$A(\delta_{k-1})f(\delta_{k-1}) + B(\delta_{k-1})f'(\delta_{k-1}) = R. \tag{1.21}$$

Согласно полученному выше равенству (1.21), а также формулам (1.4), (1.10), (1.18) и (1.20), выполняется следующая цепочка сравнений по модулю p^{2^k}:

$$f(\delta_k) \equiv f(\delta_{k-1}) - f'(\delta_{k-1})f(\delta_{k-1})B(\delta_{k-1})R'N_k \equiv \tag{1.22}$$

$$\equiv f(\delta_{k-1})\left(1 - \frac{f'(\delta_{k-1})B(\delta_{k-1})R'}{N(R)}\right) \equiv \frac{f(\delta_{k-1})}{N(R)}(N(R) - f'(\delta_{k-1})B(\delta_{k-1})R') =$$

$$= \frac{f(\delta_{k-1})R'}{N(R)}(R - f'(\delta_{k-1})B(\delta_{k-1})) = \frac{(f(\delta_{k-1})^2 R'A(\delta_{k-1})}{N(R)} \pmod{p^{2^k}}.$$

Заметим, что на шаге 8 алгоритма простое число p выбирается таким образом, что $(p, N(R)) = 1$, и применим к (1.22) соотношение (1.18). Получим, что

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

Таким образом, теорема доказана. □

1.4 Оценка коэффициентов решения полиномиального уравнения

Пусть $\alpha \in \mathfrak{D}$ — корень уравнения $f(x) = 0$. Тогда число α имеет вид

$$\alpha = \sum_{i=1}^{d} a_i \omega_i,$$

где $a_i \in \mathbb{Z}$.

В данном параграфе найдем оценку $\|\alpha\|$ через величины, зависящие только от базиса порядка $\mathfrak{D}$, степени расширения $\mathbb{Q}(\omega)$ и коэффициентов данного многочлена $f(x)$.

Лемма 9. *Имеет место равенство*

$$|\alpha| \leqslant \frac{\max_{0 \leqslant i < m} |\gamma_i|}{|\gamma_m|} + 1, \tag{1.23}$$

где γ_i — коэффициенты многочлена $f(x)$.

Доказательство. См. [9, гл. 9 §39]. □

Замечание 4. *Лемма 9 остается верной для любого корня многочлена $f(x)$, в том числе и для не принадлежащего порядку $\mathfrak{D}$.*

Лемма 10. *Пусть ξ_1 и ξ_2 — произвольные алгебраические числа, а число $c \in \mathbb{Q}$. Тогда выполняются следующие равенства:*

$$\operatorname{Tr}(\xi_1 + \xi_2) = \operatorname{Tr}(\xi_1) + \operatorname{Tr}(\xi_2); \tag{1.24}$$

$$\operatorname{Tr}(c\xi_1) = c \operatorname{Tr}(\xi_1); \tag{1.25}$$

$$N(\xi_1 \xi_2) = N(\xi_1) N(\xi_2). \tag{1.26}$$

Доказательство. См. [2, гл. “Алгебраическое дополнение”, §2]. □

Лемма 11. *Пусть ξ — произвольное алгебраическое число, а σ — некоторое вложение поля $\mathbb{Q}(\omega)$ в $\mathbb{C}$. Тогда $\sigma(\xi)$ сопряжен с ξ.*

Доказательство. См. [2, гл. “Алгебраическое дополнение”, §2]. □

Лемма 12. *Пусть ξ — произвольное алгебраическое число, а $\sigma_1, \ldots, \sigma_d$ — все вложения поля $\mathbb{Q}(\omega)$ в $\mathbb{C}$. Тогда выполняются следующие равенства:*

$$\operatorname{Tr}(\xi) = \sigma_1(\xi) + \ldots + \sigma_d(\xi); \tag{1.27}$$

$$N(\xi) = \sigma_1(\xi) \ldots \sigma_d(\xi). \tag{1.28}$$

Доказательство. См. [2, гл. “Алгебраическое дополнение”, §2]. □

Теорема 3. *Имеет место неравенство*

$$\|\alpha\| \leqslant CU, \tag{1.29}$$

где

$$C = d \cdot \max_{1 \leqslant j \leqslant d} \overline{|\omega'_j|}, \tag{1.30}$$

$$U = \max_{0 \leqslant j < m} \overline{|\gamma_j|} \cdot \overline{|\gamma_m|}^{d-1} + 1. \tag{1.31}$$

Доказательство. Обозначим через

$$\Omega' = \{\omega'_1, \ldots, \omega'_d\}$$

базис, взаимный к Ω. Тогда для произвольного индекса i, $1 \leqslant i \leqslant d$, верно равенство

$$\alpha\omega'_i = a_1\omega_1\omega'_i + \ldots + a_i\omega_i\omega'_i + \ldots + a_d\omega_d\omega'_i. \tag{1.32}$$

Рассмотрим след левой и правой части равенства (1.32). Из определения взаимного базиса, а также лемм 10, 11 и 12 следует, что

$$a_i = Tr(\alpha\omega'_i) = \sum_{j=1}^{d} \sigma_j(\alpha\omega'_i) = \sum_{j=1}^{d} \sigma_j(\alpha)\sigma_j(\omega'_i) = \sum_{j=1}^{d} \alpha^{(j)}(\omega'_i)^{(j)},$$

где $\sigma_1, \ldots, \sigma_d$ — все вложения поля $\mathbb{Q}(\omega)$.

Через $(\omega'_i)^{(j)}$, $1 \leqslant i, j \leqslant d$ обозначены числа, сопряженные с ω'_i, а через $\alpha^{(j)}$, $1 \leqslant j \leqslant d$ — числа, сопряженные к α. При этом положим

$$(\omega'_i)^{(1)} = \omega'_i \text{ и } \alpha^{(1)} = \alpha.$$

Заметим, что $\alpha^{(j)}$, $1 \leqslant j \leqslant d$ являются корнями уравнений

$$\gamma_m^{(j)} x^m + \cdots + \gamma_0^{(j)} = 0,$$

где $\gamma_m^{(j)}, \ldots, \gamma_0^{(j)}$ сопряжены с $\gamma_m, \ldots, \gamma_0$ соответственно.

Следовательно, для любого i, $1 \leqslant i \leqslant d$ выполняется следующая цепочка неравенств:

$$|a_i| \leqslant \sum_{j=1}^{d} |\alpha^{(j)}| \cdot |(\omega'_i)^{(j)}| \leqslant \max_{1 \leqslant j \leqslant d} |\alpha^{(j)}| \sum_{j=1}^{d} |(\omega'_i)^{(j)}| = \overline{|\alpha|} \sum_{j=1}^{d} |(\omega'_i)^{(j)}| \leqslant$$

$$\leqslant \overline{|\alpha|} \cdot d \cdot \max_{1 \leqslant j \leqslant d} |(\omega'_i)^{(j)}| = \overline{|\alpha|} \cdot d \cdot \overline{|\omega'_i|} \leqslant \overline{|\alpha|} \cdot d \cdot \max_{1 \leqslant j \leqslant d} \overline{|\omega'_j|}. \tag{1.33}$$

Так как $\gamma_m^{(j)}$ — целое алгебраическое число и $\gamma_m^{(j)} \neq 0$, то по лемме 3

$$N\left(\gamma_m^{(j)}\right) \in \mathbb{Z}\backslash\{0\}.$$

Следовательно,

$$|N(\gamma_m^{(j)})| \geqslant 1. \tag{1.34}$$

Согласно леммам 11 и 12, для любого j, $1 \leqslant j \leqslant d$, выполняется

$$|N(\gamma_m^{(j)})| = |\gamma_m^{(1)}\gamma_m^{(2)}\dots\gamma_m^{(d)}| = |\gamma_m^{(j)}| \cdot |\gamma_m^{(1)}\dots\gamma_m^{(j-1)}\gamma_m^{(j+1)}\dots\gamma_m^{(d)}| \leqslant$$

$$\leqslant |\gamma_m^{(j)}|(\max_{1\leqslant j\leqslant d}|\gamma_m^{(j)}|)^{d-1} = |\gamma_m^{(j)}|\overline{|\gamma_m|}^{d-1}.$$

Применим к полученному неравенству формулу (1.34). Получим следующее неравенство:

$$|\gamma_m^{(j)}|\overline{|\gamma_m|}^{d-1} \geqslant 1.$$

Таким образом,

$$|\gamma_m^{(j)}| \geqslant \overline{|\gamma_m|}^{1-d}. \tag{1.35}$$

Применим лемму 9 к числам $\alpha^{(j)}$, где $1 \leqslant j \leqslant d$. Для них выполняется неравенство

$$|\alpha^{(j)}| \leqslant \frac{\max_{0\leqslant i<m}|\gamma_i^{(j)}|}{|\gamma_m^{(j)}|} + 1. \tag{1.36}$$

Заметим, что для любого индекса j, $1 \leqslant j \leqslant d$, верно

$$\max_{0\leqslant i<m}|\gamma_i^{(j)}| \leqslant \max_{0\leqslant i<m}\max_{1\leqslant j\leqslant d}|\gamma_i^{(j)}| = \max_{0\leqslant i\leqslant m}\overline{|\gamma_i|}. \tag{1.37}$$

Воспользовавшись неравенствами (1.35) и (1.37), перепишем соотношение (1.36) в виде

$$|\alpha^{(j)}| \leqslant \frac{\max_{0\leqslant i<m}|\gamma_i^{(j)}|}{|\gamma_m^{(j)}|} + 1 \leqslant \frac{\max_{0\leqslant i<m}\overline{|\gamma_i|}}{\overline{|\gamma_m|}^{1-d}} + 1 = \max_{0\leqslant i<m}\overline{|\gamma_i|}\cdot\overline{|\gamma_m|}^{d-1} + 1. \tag{1.38}$$

Поскольку формула (1.38) имеет место при любом j, таком, что $1 \leqslant j \leqslant d$, следовательно, справедливо и неравенство

$$\overline{|\alpha|} = \max_{1\leqslant j\leqslant d}|\alpha^{(j)}| \leqslant \max_{0\leqslant i<m}\overline{|\gamma_i|}\cdot\overline{|\gamma_m|}^{d-1} + 1.$$

Применим теперь полученное неравенство к формуле (1.33). Получим следующую оценку на коэффициенты числа α:

$$|a_i| \leqslant (\max_{0\leqslant j<m}\overline{|\gamma_j|}\cdot\overline{|\gamma_m|}^{d-1} + 1)\cdot d\cdot\max_{1\leqslant j\leqslant d}\overline{|\omega_j'|} \leqslant CU. \tag{1.39}$$

Так как формула (1.39) выполняется для любого i при $1 \leqslant i \leqslant d$, то и для $\|\alpha\|$ будет верна оценка

$$\|\alpha\| = \max_{1 \leqslant i \leqslant d} |a_i| \leqslant CU.$$

Теорема доказана. □

1.5 Обоснование нахождения точных решений полиномиального уравнения (шагов 13, 14 алгоритма 1.1)

В данном параграфе докажем, что алгоритм находит все решения уравнения $f(x) = 0$, принадлежащие $\mathfrak{D}$.

Лемма 13. *Пусть p — простое число, такое, что $p \nmid z$, где z — индекс числа ω. Рассмотрим разложение минимального многочлена ω на неприводимые сомножители в $\mathbb{F}_p$:*

$$\overline{\mu_\omega(x)}(p) = (\mu_1(x))^{e_1} \cdot \ldots \cdot (\mu_K(x))^{e_K}.$$

Тогда верно следующее разложение:

$$(p) = \prod_{i=1}^{K} \mathfrak{p}_i{}^{e_i},$$

где $\mathfrak{p}_i = (p, \mu_i(\omega))$, $1 \leqslant i \leqslant K$ — простые идеалы.

Доказательство. См. [17, §4.8.2]. □

Следствие 3. *Пусть p — простое число, такое, что $p \nmid z$, где z — индекс числа ω, и многочлен $\overline{\mu_\omega(x)}(p)$ неприводим в $\mathbb{F}_p$. Тогда (p) — простой идеал в $\mathfrak{D}$.*

Теорема 4. *Если требуется найти α — корень уравнения $f(x) = 0$ в $\mathfrak{D}$, удовлетворяющий условию*

$$\alpha \equiv \delta_0 \pmod{p}, \tag{1.40}$$

то либо $\alpha = \delta_V$, где $V = 1 + \lfloor \log_2(\log_p(2CU)) \rfloor$, либо такого решения не существует.

Доказательство. Поскольку при любом $k \geqslant 1$ верна формула

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}},$$

а $f(\delta_{k-1}) \equiv 0 \pmod{p^{2^{k-1}}}$, то

$$\delta_k \equiv \delta_{k-1} \pmod{p^{2^{k-1}}}$$

и, в частности,

$$\delta_k \equiv \delta_{k-1} \pmod{p}. \tag{1.41}$$

Из формул (1.50) и (1.51) можно заключить, что

$$\delta_V \equiv \delta_0 \equiv \alpha \pmod{p}.$$

Согласно теореме 2, верно сравнение

$$f(\alpha) - f(\delta_V) = -f(\delta_V) \equiv 0 \pmod{p^{2^V}}. \tag{1.42}$$

Для любых элементов ζ_1 и ζ_2 порядка $\mathfrak{D}$, а также для любого натурального числа l имеет место формула разности степеней

$$\zeta_1^l - \zeta_2^l = (\zeta_1 - \zeta_2)(\zeta_1^{l-1} + \zeta_1^{l-2}\zeta_2 + \ldots + \zeta_1\zeta_2^{l-2} + \zeta_2^{l-1}).$$

Применим ее к левой части сравнения (1.52). Получим следующее выражение:

$$f(\alpha) - f(\delta_V) = \gamma_m(\alpha^m - \delta_V^m) + \gamma_{m-1}(\alpha^{m-1} - \delta_V^{m-1}) + \ldots + \gamma_1(\alpha - \delta_V) =$$

$$= (\alpha - \delta_V)\sum_{i=1}^{m} \gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}). \tag{1.43}$$

Так как

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

то верно следующее сравнение по модулю p:

$$\sum_{i=1}^{m} \gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv \sum_{i=2}^{m}(i-1)\gamma_i(\delta_V)^{i-1} \equiv f'(\delta_V) \pmod{p}.$$

По следствию 2, выполняется равенство

$$R = A(\delta_V)f(\delta_V) + B(\delta_V)f'(\delta_V),$$

а из теоремы 2 непосредственно следует, что $f(\delta_V) \equiv 0 \pmod{p}$.

Следовательно,

$$B(\delta_V)f'(\delta_V) \equiv R \pmod{p}. \tag{1.44}$$

По условию, $(p, N(R)) = 1$, а, значит, из следствия 1 вытекает, что

$$p \nmid R. \tag{1.45}$$

Таким образом, из формул (1.57) и (1.45) следует, что

$$f'(\delta_V) \not\equiv 0 \pmod{p}. \tag{1.46}$$

По следствию 3, (p) — простой идеал в $\mathfrak{D}$. При этом, согласно формулам (1.52), (1.53) и (1.46), верно следующее:

$$(\alpha - \delta_V)\sum_{i=1}^{m}\gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv 0 \pmod{p^{2^V}}$$

и

$$\sum_{i=1}^{m}\gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \not\equiv 0 \pmod{p}.$$

Следовательно,

$$\alpha \equiv \delta_V \pmod{p^{2^V}}. \tag{1.47}$$

Оценим модуль коэффициентов разности α и δ_V, используя оценку на $\|\alpha\|$ из теоремы 3, а также неравенство

$$\|\delta_V\| \leqslant \frac{p^{2^V}}{2}.$$

Получим

$$\|\alpha - \delta_V\| \leqslant \|\alpha\| + \|\delta_V\| \leqslant CU + \frac{p^{2^V}}{2}. \tag{1.48}$$

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

$$CU < \frac{p^{2^V}}{2},$$

и, таким образом, $\|\alpha - \delta_V\| < p^{2^V}$.

Но из сравнения (1.60) следует, что каждый коэффициент элемента $\alpha - \delta_V$ есть целое число, делящееся на p^{2^V}. Следовательно, все коэффициенты равны нулю и $\delta_V = \alpha$. □

Теорема 5. *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.*

Доказательство. Пусть $\alpha \in \mathfrak{D}$ — корень многочлена $f(x)$. Поскольку

$$f(\alpha) = 0,$$

в том числе верно и сравнение

$$f(\alpha) \equiv 0 \pmod{p}.$$

Так как на шаге 9 алгоритма перебираются все возможные δ_0, удовлетворяющие условию

$$f(\delta_0) \equiv 0 \pmod{p},$$

то среди них обязательно окажется элемент, для которого

$$\alpha \equiv \delta_0 \pmod{p}. \tag{1.49}$$

Применим к данному δ_0 теорему 4. Получим, что либо $f(\delta_V) = 0$, либо не существует корня исходного уравнения, сравнимого с δ_0 по модулю p.

Таким образом, доказано, что каждый корень многочлена $f(x)$, лежащий в кольце $\mathfrak{D}$, содержится среди чисел, найденных на шаге 13.2 алгоритма.

На шаге же 13.3 выполняется проверка, поэтому алгоритм не может выдать лишних решений.

Если же не существует элементов $\delta_0 \in \mathfrak{D}$, таких, что

$$f(\delta_0) \equiv 0 \pmod{p},$$

то это значит, что уравнение $f(x) = 0$ заведомо не имеет решений, принадлежащих $\mathfrak{D}$. В этом случае алгоритм остановится на шаге 9. □

1.6 Алгоритм решения полиномиального уравнения в порядке с учетом поиска простого числа p

Более подробно с теорией, изложенной в данном параграфе, можно ознакомиться в книгах [13] и [18]; определение символа Артина для произвольного поля и формулировка теоремы 7 в более общем виде содержится в работе [15].

Заметим, что в алгоритме 1.1 не указан способ нахождения простого числа p, удовлетворяющего условиям: $\overline{\mu_\omega(x)}(p)$ неприводим, $p \nmid D_\omega$ и $p \nmid N(R)$. Более того, оказывается, что простое число, удовлетворяющее первому из этих условий, существует не всегда (например, такое простое число не существует в том случае, когда группа Галуа многочлена $\mu_\omega(x)$ не содержит цикла максимальной длины; это объясняется далее в тексте).

Алгоритм 1.2, описанный в данном параграфе, является модифицированной версией алгоритма 1.1, в которой от простого числа p не требуется условие неприводимости многочлена $\overline{\mu_\omega(x)}(p)$.

Для описания алгоритма 1.2 требуются некоторые вспомогательные определения и утверждения.

Определение 9. *Пусть $E \supset F$ — нормальное расширение. Подгруппа автоморфизмов поля E над полем F называется группой Галуа поля E над полем F и обозначается* $\mathrm{Gal}(E/F)$.

Определение 10. *Группой Галуа многочлена над полем F называется группа Галуа* $\mathrm{Gal}(E/F)$ *его поля разложения E и обозначается* $\mathrm{Gal}(g/F)$.

Теорема 6. *(теорема Дедекинда) Пусть $g(x) \in \mathbb{Z}[x]$ — унитарный сепарабельный многочлен степени l, а p — простое число, такое, что*

$$p \nmid D(g).$$

Рассмотрим разложение многочлена $\overline{g(x)}(p)$ на унитарные неприводимые множители в $\mathbb{F}_p[x]$:

$$\overline{g(x)}(p) = \overline{g_1(x)}(p) \dots \overline{g_r(x)}(p),\ d_i = \deg(\overline{g_i(x)}(p)).$$

Тогда

1. *Группа Галуа многочлена $\overline{g(x)}(p)$ над $\mathbb{F}_p$ является циклической группой порядка $НОК(d_1, \dots, d_r)$.*

2. *Группа Галуа многочлена $g(x)$ над $\mathbb{Q}$ содержит элемент, который действует на корни $g(x)$ как подстановка вида $\sigma_1 \dots \sigma_r$, где σ_i, $1 \leqslant i \leqslant r$ — цикл длины d_i.*

Доказательство. См. [18, §13.4, теор. 13.4.5]. □

Замечание 5. *Из доказательства теоремы* 6 *видно, что действие автоморфизма Фробениуса* $a \mapsto a^p$ *на корни многочлена* $\overline{g(x)}(p)$ *задается произведением непересекающихся циклов, имеющих длины* $d_1, \ldots, d_r$.

Определение 11. *Пусть* $g(x) \in \mathbb{Z}[x]$ *— унитарный сепарабельный многочлен с полем разложения* L, *а* p *— простое число, удовлетворяющее условию*

$$p \nmid D(g).$$

Тогда (см. теорему 6 *и замечание* 5*)* $\mathrm{Gal}(L/\mathbb{Q})$ *содержит элемент, соответствующий эндоморфизму Фробениуса* $a \mapsto a^p$ *в группе Галуа многочлена* $\overline{g(x)}(p)$ *над* $\mathbb{F}_p$. *Данный элемент группы* $\mathrm{Gal}(L/\mathbb{Q})$ *называется символом Артина и обозначается* $\left(\frac{L/\mathbb{Q}}{p}\right)$.

Расширенная гипотеза Римана. *Комплексные нули всех* L*–функций Дирихле, расположенные в полосе* $0 < \mathrm{Re}\, s < 1$, *лежат на прямой* $\mathrm{Re}\, s = \frac{1}{2}$.

Теорема 7. *Предположим, что справедлива расширенная гипотеза Римана. Пусть* $L \supset \mathbb{Q}$ *— нормальное расширение степени* n *с дискриминантом* D. *Тогда для произвольного элемента* $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ *существует простое число* p, $p \nmid D$, *удовлетворяющее условиям* $\left(\frac{L/\mathbb{Q}}{p}\right) = \sigma$ *и* $p \leqslant (4 \ln |D| + 2,5n + 5)^2$.

Доказательство. В более общем виде теорема сформулирована в [15, §8.8, теор. 8.8.21], полное доказательство можно найти в работе [16]. □

Введем обозначение D_{spl} для дискриминанта поля разложения многочлена $\mu_\omega(x)$.

Следствие 4. *Предположим, что справедлива расширенная гипотеза Римана. Если группа Галуа многочлена* $\mu_\omega(x)$ *содержит цикл длины* $d = \deg \mu_\omega(x)$, *то найдется простое число* p, *удовлетворяющее условиям:*

1. $p \nmid D_{spl}$.
2. *Многочлен* $\overline{\mu_\omega(x)}(p)$ *неприводим в* $\mathbb{F}_p$.
3. $p \leqslant (4 \ln |D_{spl}| + 2,5d + 5)^2$.

Доказательство. Обозначим через L поле разложения многочлена $\mu_\omega(x)$. По условию, группа $\mathrm{Gal}(\mu_\omega/\mathbb{Q})$ содержит цикл длины d. Обозначим его через σ_d. По теореме 7, существует простое число p, такое, что $\left(\frac{L/\mathbb{Q}}{p}\right) = \sigma_d$, $p \nmid D_{spl}$ и $p \leqslant (4 \ln |D_{spl}| + 2,5d + 5)^2$. □

Через $E_l(B)$ будем обозначать следующее множество:

$$E_l(B) = \{g(x) = g_l x^l + \ldots + g_1 x + g_0 \in \mathbb{Z}[x] \mid g_l = 1,\ \max(|g_0|, \ldots, |g_l|) \leqslant B, \\ \mathrm{Gal}(g/F) \neq S_l\}.$$

Теорема 8. *Справедлива оценка*

$$E_l(B) = \mathcal{O}(B^{l-\frac{1}{2}} \ln B).$$

Доказательство. См. [20]. □

Теорема 9 (китайская теорема об остатках)**.** *Пусть A — кольцо и $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ — такие идеалы, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при всех $i \neq j$. Для любого семейства элементов $x_1, \ldots, x_k$ кольца A существует такой элемент $x_0 \in A$, что $x_0 \equiv x_i \pmod{\mathfrak{a}_i}$ при всех i. Кроме того, существует алгоритм построения элемента x_0.*

Доказательство. См. [10, гл. 2 §2]. □

Через p_i будем обозначать i–ое простое число, через $\#\mathcal{M}$ — количество элементов в множестве $\mathcal{M}$, а через $\mathcal{M}_i$ — i–ый элемент множества $\mathcal{M}$.

Алгоритм 1.2.

Дано: ω — целое алгебраическое число степени d;
$\mathfrak{D}$ — порядок в поле $\mathbb{Q}(\omega)$;
$\mu_\omega(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Z}[x], c_d = 1$, — минимальный многочлен ω;
$f(x) = \sum_{i=0}^{m} \gamma_i x^i$, $\gamma_i \in \mathfrak{D}$ — многочлен без кратных корней.

Найти: множество решений уравнения $f(x) = 0$ в $\mathfrak{D}$ или дать ответ, что решений нет.

1. Положить $S' = \emptyset$. [*на выходе алгоритма множество S' будет состоять из решений исходного уравнения*]

2. Вычислить $R = \gamma_m D(f)$.

3. Вычислить $\phi_R(x) = r_0 + r_1 x + \ldots + r_{d-1}x^{d-1} + x^d$. [$\phi_R(x)$ — *характеристический многочлен числа* $R \in \mathfrak{D}$]

4. Положить $N(R) = (-1)^d r_0$. [*см. лемму* 2]

5. Положить

$$R' = (-1)^{d-1}(r_1 + r_2 R + \ldots + r_{d-1}R^{d-2} + R^{d-1}).$$

[*см. следствие* 1]

6. Вычислить $A(x), B(x) \in \mathfrak{D}[x]$, такие, что

$$R = A(x)f(x) + B(x)f'(x).$$

[*см. следствие* 2]

7. Вычислить $D_\omega = D(\mu_\omega)$. [*см. лемму* 7]

8. Вычислить D_{spl}.

9. Положить $W = [(4 \ln |D_{spl}| + 2, 5d + 5)^2]$.

10. Для каждого i, удовлетворяющего $p_i \leqslant W$ выполнять следующие действия:

    10.1. Положить $\mathcal{M} = \emptyset$ и $K = 0$.

    10.2. Проверить, выполняются ли условия

$$(p_i, N(R)) = 1 \text{ и } (p_i, D_\omega) = 1.$$

    Если нет, то перейти на начало шага 10.

    10.3. Разложить многочлен $\overline{\mu_\omega(x)}(p_i)$ на неприводимые множители в поле $\mathbb{F}_{p_i}$:

$$\overline{\mu_\omega(x)}(p_i) = \mu_{i,1}(x) \cdot \ldots \cdot \mu_{i,r_i}(x).$$

    Если $r_i = 1$, то положить $\mathcal{M} = \{\mu_{i,1}(\omega)\}$, $K = 1$, $P = p_i$ и перейти на шаг 12.

    10.4. Если $\mathcal{M} = \emptyset$ или $\#\mathcal{M} > r_i$, то положить

$$\mathcal{M} = \{\mu_{i,1}(\omega), \ldots, \mu_{i,r_i}(\omega)\}, K = r_i, P = p_i.$$

11. Если $\mathcal{M} = \emptyset$, то найти простое число $p > W$, такое, что

$$(p, N(R)) = 1 \text{ и } (p, D_\omega) = 1,$$

найти разложение многочлена $\overline{\mu_\omega(x)}(p)$ на неприводимые множители

$$\overline{\mu_\omega(x)}(p) = \mu_1(x) \cdot \ldots \cdot \mu_r(x)$$

и положить $\mathcal{M} = \{\mu_1(\omega), \ldots, \mu_r(\omega)\}$, $K = r$, $P = p$.

12. Для каждого $i = 1, \ldots, K$ решить сравнение $f(x) \equiv 0 \pmod{\mathfrak{p}_i}$, где $\mathfrak{p}_i = (P, \mathcal{M}_i)$. [*см. замечание* 6]

    Если оно неразрешимо, то уравнение $f(x) = 0$ неразрешимо в $\mathfrak{D}$.

    Если оно разрешимо, то обозначим через S_i множество решений сравнения, а через s_i — их количество.

    Выберем ровно по одному элементу $a_i \in S_i$. Обозначим через T_k систему сравнений $x \equiv a_k \pmod{\mathfrak{p}_k}$, $1 \leqslant k \leqslant K$.

13. Если $K > 1$, то с помощью китайской теоремы об остатках получить все решения сравнения $f(x) \equiv 0 \pmod{p}$, решив системы T_k, где $1 \leqslant k \leqslant K$. [*см. теорему* 9]

14. Обозначим через S множество всех элементов из $\mathfrak{D}$, таких, что для каждого $\delta \in S$

$$f(\delta) \equiv 0 \pmod{p}.$$

    [*при* $K = 1$ *такие элементы были получены на шаге 12, а при* $K > 1$ *— на шаге 13*]

    Выбрать δ так, чтобы выполнялось $\|\delta\| \leqslant \frac{p}{2}$.

15. Положить $V = 1 + \lfloor \log_2(\log_p(2CU)) \rfloor$, где

$$C = d \cdot \max_{1 \leqslant j \leqslant d} \boxed{\omega'_j},$$

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

    Здесь ω'_j — элементы базиса, взаимного к Ω.

16. Найти решение N_0 сравнения

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

для которого выполняется условие $|N_0| \leqslant \frac{p}{2}$.

17. Для каждого $k = 1, \ldots, V$ вычислить $N_k \in \mathbb{Z}$, такие, что

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

$$|N_k| \leqslant \frac{p^{2^k}}{2}.$$

18. Для каждого $\delta \in S$ выполнять следующие действия:

18.1. Положить $\delta_0 = \delta$.

18.2. Для каждого $k = 1, \ldots, V$ вычислить

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}},$$

$$\delta_k \in \mathfrak{D},\ \|\delta_k\| \leqslant \frac{p^{2^k}}{2}.$$

18.3. Проверить, удовлетворяет ли число δ_V равенству

$$f(\delta_V) = 0.$$

Если равенство выполняется, то

$$S' = S' \cup \{\delta_V\}.$$

19. Если $S' = \emptyset$, то дать ответ, что уравнение $f(x) = 0$ неразрешимо в $\mathfrak{D}$.

Замечание 6. *Для того, чтобы решить сравнение* $f(x) \equiv 0 \pmod{\mathfrak{p}}$, *где* $\mathfrak{p} = (p, \mu(\omega))$, *достаточно решить уравнение* $f(x) = 0$ *в поле* $\mathbb{F}_{p^{\deg \mu(x)}}$. *Алгоритмы нахождения корней многочленов в конечных полях можно найти в книге [5, гл. 3].*

Лемма 14. *Пусть* p — *простое число, такое, что* $p \nmid D_\omega$. *Тогда* p *не разветвлено в* $\mathbb{Q}(\omega)$.

Доказательство. См. [2, гл. 3 §5]. □

Лемма 15. *Пусть* $\mathfrak{a} \subset \mathfrak{D}$ *— нетривиальный идеал порядка* $\mathfrak{D}$*. Тогда*

$$\mathfrak{a} \cap \mathbb{Z} \neq (0).$$

Если к тому же $\mathfrak{a}$ *— простой идеал, то*

$$\mathfrak{a} \cap \mathbb{Z} = (q),$$

где q *— некоторое простое число.*

Доказательство. См. [3, гл. 17 §136]. □

Теорема 10. *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.*

Доказательство. Пусть $\alpha \in \mathfrak{D}$ — корень многочлена $f(x)$. Поскольку

$$f(\alpha) = 0,$$

в том числе верно и сравнение

$$f(\alpha) \equiv 0 \pmod{p}.$$

Так как на шаге 14 алгоритма перебираются все возможные δ_0, удовлетворяющие условию

$$f(\delta_0) \equiv 0 \pmod{p},$$

то среди них обязательно окажется элемент, для которого

$$\alpha \equiv \delta_0 \pmod{p}. \tag{1.50}$$

Поскольку при любом $k \geqslant 1$ верна формула

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1})B(\delta_{k-1})R'N_k \pmod{p^{2^k}},$$

а $f(\delta_{k-1}) \equiv 0 \pmod{p^{2^{k-1}}}$, то

$$\delta_k \equiv \delta_{k-1} \pmod{p^{2^{k-1}}}$$

и, в частности,

$$\delta_k \equiv \delta_{k-1} \pmod{p}. \tag{1.51}$$

Из формул (1.50) и (1.51) можно заключить, что

$$\delta_V \equiv \delta_0 \equiv \alpha \pmod{p}.$$

Согласно теореме 2, верно сравнение

$$f(\alpha) - f(\delta_V) = -f(\delta_V) \equiv 0 \pmod{p^{2^V}}. \tag{1.52}$$

Для любых элементов ζ_1 и ζ_2 порядка $\mathfrak{D}$, а также для любого натурального числа l имеет место формула разности степеней

$$\zeta_1^l - \zeta_2^l = (\zeta_1 - \zeta_2)(\zeta_1^{l-1} + \zeta_1^{l-2}\zeta_2 + \ldots + \zeta_1\zeta_2^{l-2} + \zeta_2^{l-1}).$$

Применим ее к левой части сравнения (1.52). Получим следующее выражение:

$$f(\alpha) - f(\delta_V) = \gamma_m(\alpha^m - \delta_V^m) + \gamma_{m-1}(\alpha^{m-1} - \delta_V^{m-1}) + \ldots + \gamma_1(\alpha - \delta_V) =$$

$$= (\alpha - \delta_V)\sum_{i=1}^{m}\gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}). \tag{1.53}$$

Таким образом, из формул (1.52) и (1.53) вытекает, что верно следующее сравнение по модулю p^{2^k}:

$$(\alpha - \delta_V)\sum_{i=1}^{m}\gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv 0 \pmod{p^{2^V}}. \tag{1.54}$$

Разложим (p) в произведение простых идеалов:

$$(p) = \mathfrak{p}_1 \ldots \mathfrak{p}_K.$$

Согласно выбору p, $p \nmid D_\omega$, и, следовательно, по лемме 8 $p \nmid z$. Таким образом, можно применить леммы 13 и 14, откуда получаем, что все

$$\mathfrak{p}_i = (p, \mu_i(\omega)), 1 \leqslant i \leqslant K,$$

— различные простые идеалы.

Из формулы (1.54) следует, что

$$(\alpha - \delta_V)\sum_{i=1}^{m}\gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv 0 \pmod{{\mathfrak{p}_j}^{2^V}}, \tag{1.55}$$

где $1 \leqslant j \leqslant K$.

Так как $\delta_V \equiv \alpha \pmod{p}$, то верно, что

$$\delta_V \equiv \alpha \pmod{\mathfrak{p}_j},\ 1 \leqslant j \leqslant K,$$

и, таким образом,

$$\sum_{i=1}^{m} \gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv f'(\delta_V) \pmod{\mathfrak{p}_j}. \tag{1.56}$$

По следствию 2, выполняется равенство

$$R = A(\delta_V)f(\delta_V) + B(\delta_V)f'(\delta_V),$$

а из теоремы 2 непосредственно следует, что $f(\delta_V) \equiv 0 \pmod{p}$.

Следовательно, $B(\delta_V)f'(\delta_V) \equiv R \pmod{p}$, откуда получаем, что

$$B(\delta_V)f'(\delta_V) \equiv R \pmod{\mathfrak{p}_j},\ 1 \leqslant j \leqslant K. \tag{1.57}$$

Докажем от противного, что $R \not\equiv 0 \pmod{\mathfrak{p}_j}$, $1 \leqslant j \leqslant K$. Предположим, что это не так, и $R \in \mathfrak{p}_j$. Но тогда по следствию 1.4 и

$$N(R) \in \mathfrak{p}_j. \tag{1.58}$$

Однако $N(R)$ — целое число, откуда, из леммы 15 и из условия (1.58) следует, что

$$p \mid N(R).$$

Но это противоречит выбору простого числа p. Таким образом, доказано, что $R \not\equiv 0 \pmod{\mathfrak{p}_j}$, $1 \leqslant j \leqslant K$.

Теперь из выражения (1.57) следует, что

$$f'(\delta_V) \not\equiv 0 \pmod{\mathfrak{p}_j},\ 1 \leqslant j \leqslant K. \tag{1.59}$$

По лемме 13, $\mathfrak{p}_j$ — простой идеал в $\mathfrak{D}$. При этом, согласно формулам (1.55), (1.59) и (1.56), верно следующее:

$$(\alpha - \delta_V)\sum_{i=1}^{m} \gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv 0 \pmod{{\mathfrak{p}_j}^{2^V}}$$

и

$$\sum_{i=1}^{m} \gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \not\equiv 0 \pmod{\mathfrak{p}_j},\ 1 \leqslant j \leqslant K.$$

Следовательно, $\alpha \equiv \delta_V \pmod{\mathfrak{p}_j{}^{2^V}}$ для любого индекса $1 \leqslant j \leqslant K$, и, таким образом,

$$\alpha \equiv \delta_V \pmod{p^{2^V}}. \tag{1.60}$$

Оценим модуль коэффициентов разности α и δ_V, используя оценку на $\|\alpha\|$ из теоремы 3, а также неравенство

$$\|\delta_V\| \leqslant \frac{p^{2^V}}{2}.$$

Получим

$$\|\alpha - \delta_V\| \leqslant \|\alpha\| + \|\delta_V\| \leqslant CU + \frac{p^{2^V}}{2}. \tag{1.61}$$

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

$$CU < \frac{p^{2^V}}{2},$$

и, таким образом, $\|\alpha - \delta_V\| < p^{2^V}$.

Однако из сравнения (1.60) следует, что каждый коэффициент элемента $\alpha - \delta_V$ есть целое число, делящееся на p^{2^V}. Следовательно, все коэффициенты равны нулю и $\delta_V = \alpha$.

Таким образом, доказано, что каждый корень многочлена $f(x)$, лежащий в кольце $\mathfrak{D}$, содержится среди чисел, найденных на шаге 18.2 алгоритма.

На шаге же 18.3 выполняется проверка, поэтому алгоритм не может выдать лишних решений.

Если же не существует элементов $\delta_0 \in \mathfrak{D}$, таких, что

$$f(\delta_0) \equiv 0 \pmod{p},$$

то это значит, что уравнение $f(x) = 0$ заведомо не имеет решений, принадлежащих $\mathfrak{D}$. В этом случае алгоритм остановится на шаге 12. □

1.7 Оценка сложности работы алгоритма решения полиномиального уравнения в порядке

Предположим, что целое алгебраическое число ω и порядок $\mathfrak{D}$ фиксированы. Тогда можно считать, что сложность вычислений, связанных с подсчетом D_ω, D_{spl}, $\phi_R(x)$, R, R' и разложением $\mu_\omega(x)$ на множители в конечном поле,

является константой. Также в таком случае можно считать, что сложность арифметических операций в данном порядке поля алгебраических чисел составляет $\mathcal{O}(1)$.

Будем вычислять сложность описанного в параграфе 1.2 алгоритма в зависимости от параметров многочлена $f(x) = \sum_{i=0}^{m} \gamma_i x^i$, а именно, его степени и коэффициентов.

Утверждение 6. *Определитель матрицы размера $l \times l$ можно вычислить за $\mathcal{O}(l^3)$ арифметических операций.*

Доказательство. См. [17, гл. 2 §2.2]. □

Утверждение 7. *Сложность алгоритма Берлекэмпа (разложения унитарного многочлена на множители в конечном поле) составляет $\mathcal{O}(m^3 + kqm)$, где m — степень раскладываемого на множители многочлена, k — число его неприводимых различных унитарных сомножителей, а q — количество элементов в поле.*

Доказательство. См. [4, гл. 6 §6.3]. □

Утверждение 8 (неравенство Адамара)**.** *Для произвольной матрицы $T = (t_{i,j})_{1 \leqslant i,j \leqslant n}$ выполняется неравенство*

$$(\det T)^2 \leqslant \prod_{j=1}^{n} \left(\sum_{i=1}^{n} (t_{i,j})^2 \right).$$

Доказательство. См. [8, гл. 8 §7]. □

Следствие 5. *Для произвольной матрицы $T = (t_{i,j})_{1 \leqslant i,j \leqslant n}$, такой, что $\max_{1 \leqslant i,j \leqslant n} |t_{i,j}| \leqslant B$, выполняется неравенство*

$$(\det T)^2 \leqslant B^{2n} n^n.$$

Утверждение 9. *Для любого простого числа $p > 2$ существует константа A, для которой верно неравенство*

$$\prod_{q<p} q > e^{Ap}.$$

Здесь произведение берется по всем простым числам q, меньшим p.

Доказательство. См. [21, §22.2]. □

Утверждение 10. *Существуют константы C_1 и C_2, такие, что*

$$C_1\frac{x}{\ln x} < \pi(x) < C_2\frac{x}{\ln x},$$

где $\pi(x) = \sum_{p\leqslant x} 1$. Здесь сумма берется по всем простым числам p, не превосходящим x.

Доказательство. См. [21, §22.4]. □

Утверждение 11. *Существует алгоритм нахождения корней многочлена степени m в конечном поле $\mathbb{F}_{p^l}$, имеющий сложность*

$$\mathcal{O}(m^2 l^2 p \ln p)$$

арифметических операций в поле $\mathbb{F}_{p^l}$.

Доказательство. См. [5, гл. 3 §3]. □

Утверждение 12. *Сложность алгорима Евклида, как и обобщенного алгоритма Евклида, составляет $\mathcal{O}(\ln b)$ операций, где b — наименьшее из чисел, подаваемых алгоритму на вход.*

Доказательство. См. [4, приложение]. □

Теорема 11. *Существует хотя бы одно простое число $p > 2$, удовлетворяющее условию*

$$p < \frac{d(2m-1)(\ln m + \frac{1}{2}\ln(2m-1) + \ln(\max_{0\leqslant i\leqslant m}\lceil\gamma_i\rceil))}{A},$$

Для которого верно, что $(p, N(R)) = 1$, где $N(R)$ — норма алгебраического числа R, определенного формулой (1.1).

Доказательство. Согласно лемме 12, выполняется следующее равенство:

$$N(R) = R \cdot R^{(2)} \cdot \ldots \cdot R^{(d)}, \tag{1.62}$$

где $R^{(i)}$, $2 \leqslant i \leqslant d$ — числа, сопряженные с R.

По замечанию 1, R можно записать в виде

$$R = (-1)^{\frac{m(m-1)}{2}} R(f, f'), \tag{1.63}$$

где

$$f(x) = \gamma_m x^m + \ldots + \gamma_1 x + \gamma_0.$$

Заметим, что $R(f, f')$ — это определитель матрицы размера $(2m-1) \times (2m-1)$, элементы которой ограничены числом

$$m \cdot \max_{0 \leqslant i \leqslant m} |\gamma_i|.$$

Таким образом, по следствию 5 и формуле (1.63), получаем неравенство

$$|R| = |(R(f, f'))| \leqslant (m \cdot \max_{0 \leqslant i \leqslant m} |\gamma_i|)^{2m-1} (2m-1)^{m-\frac{1}{2}}. \tag{1.64}$$

Аналогично можно показать, что верны соотношения

$$|R^{(j)}| \leqslant (m \cdot \max_{0 \leqslant i \leqslant m} |\gamma_i^{(j)}|)^{2m-1} (2m-1)^{m-\frac{1}{2}},\ 2 \leqslant j \leqslant d, \tag{1.65}$$

где $\gamma_i^{(j)}$ — числа, сопряженные с γ_i. Теперь из формул (1.62), (1.64) и (1.65) следует, что

$$|N(R)| \leqslant (m^2(2m-1))^{d(m-\frac{1}{2})} \max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil^{(2m-1)d}. \tag{1.66}$$

Предположим теперь, что p — наименьшее простое число, удовлетворяющее условию $p \nmid N(R)$. Тогда для него должно выполняться неравенство

$$\prod_{q<p} q \leqslant N(R).$$

Применим к вышеуказанному соотношению формулу (1.66) и утверждение 9. Получим следующую цепочку неравенств:

$$e^{Ap} < \prod_{q<p} q \leqslant N(R) \leqslant (m^2(2m-1))^{d(m-\frac{1}{2})} \max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil^{(2m-1)d}, \tag{1.67}$$

откуда следует, что

$$p < \frac{d(2m-1)(\ln m + \frac{1}{2}\ln(2m-1) + \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil))}{A}.$$

□

Теорема 12. *Наихудшая сложность описанного в параграфе 1.2 алгоритма в зависимости от параметров многочлена $f(x)$ составляет*

$$\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) + m^3 \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) \ln\ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) +$$

$$+m^d \ln\ln(\max_{0\leqslant i\leqslant m}\lceil\gamma_i\rceil))$$

арифметических операций.

Доказательство. Сложность шага 2 алгоритма равна количеству операций, требуемых для вычисления определителя матрицы размера $(2m-1)\times(2m-1)$ и поэтому, согласно утверждению 6, равна

$$\mathcal{O}(m^3). \tag{1.68}$$

Для шага 6 требуется вычислить m и $m-1$ определителей такого же вида, откуда сложность шага 6 получается равной

$$\mathcal{O}(m^4). \tag{1.69}$$

На шаге 10 требуется для каждого $p_i < W$, где W — граница, зависящая только от исходного порядка, раскладывать на множители многочлены степени d. Следовательно, временная сложность шага 10 не зависит от многочлена $f(x)$.

На шаге 11 нужно, во-первых, найти такое простое число $p > W$, что $p \nmid N(R)$ и $p \nmid D_\omega$. На это требуется

$$\mathcal{O}(\pi(p) - \pi(W))$$

операций. Из теоремы 11 и утверждения 10 теперь следует, что на поиск числа p нужно не больше, чем

$$\mathcal{O}\left(\frac{C_3}{\ln C_3}\right),\ C_3 = \frac{d(2m-1)(\ln m + \frac{1}{2}\ln(2m-1) + \ln(\max_{0\leqslant i\leqslant m}\lceil\gamma_i\rceil))}{A} \tag{1.70}$$

арифметических выражений. Выражение (1.70) можно преобразовать с учетом того, что, по предположению, порядок $\mathfrak{D}$ фиксирован. Получим следующее:

$$\mathcal{O}\left(\frac{C_3}{\ln C_3}\right) = \mathcal{O}\left(\frac{m\ln m + m\ln(\max_{o\leqslant i\leqslant m}\lceil\gamma_i\rceil)}{\ln m + \ln\ln(\max_{o\leqslant i\leqslant m}\lceil\gamma_i\rceil)}\right). \tag{1.71}$$

Во-вторых, на шаге 11 требуется разложить на неприводимые множители в конечном поле $\mathbb{F}_p$ многочлен $\overline{\mu_\omega(x)}(p)$, причем $\deg(\overline{\mu_\omega(x)}(p)) = d$. Здесь p — простое число, удовлетворяющее неравенству $p < C_3$. Согласно утверждению 7, для этого требуется не более, чем

$$\mathcal{O}(d^3 + d^2 p)$$

арифметических операций. Из теоремы 11 теперь можно получить, что на вторую часть шага 11 нужно не более

$$\mathcal{O}(m \ln m + m \ln(\max_{o \leqslant i \leqslant m} \lceil \gamma_i \rceil)) \tag{1.72}$$

операций.

На шаге 12 требуется K раз ($K \leqslant d$) решить уравнение $f(x) = 0$ в полях вида $\mathbb{F}_{p^l}$, где $l \leqslant d$. По утверждению 11, на выполнение вышеуказанных действий требуется

$$\mathcal{O}(m^2 p \ln p), p < C_3$$

арифметических операций. С учетом формулы (1.70) можно заключить, что сложность шага 12 составляет

$$\mathcal{O}(m^3 (\ln m)^2 + m^3 \ln m \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) + m^3 \ln(\max_{o \leqslant i \leqslant m} \lceil \gamma_i \rceil) \ln \ln(\max_{o \leqslant i \leqslant m} \lceil \gamma_i \rceil)). \tag{1.73}$$

Поскольку по условию минимальный многочлен $\mu_\omega(x)$ фиксирован, то и на нахождение каждого решения системы T_k по китайской теореме об остатках на шаге 13 потребуется фиксированное время. Поскольку количество решений каждого уравнения на шаге 12 не превосходит m, то всего таких систем требуется решить не более чем m^K, где K — количество неприводимых сомножителей при разложении многочлена $\overline{\mu_\omega(x)}(p)$ на множители в $\mathbb{F}_p$, $K \leqslant d$. Соответственно, в наихудшем случае сложность шага 13 составляет

$$\mathcal{O}(m^d) \tag{1.74}$$

арифметических операций.

Для оценки числа V, выбираемого на шаге 15, заметим, что из того, что $p > 2$, следует, что

$$V \leqslant 1 + \lfloor \log_2 \log_3 (2CU) \rfloor. \tag{1.75}$$

Для выполнения шага 16 требуется применить обобщенный алгоритм Евклида для чисел $N(R)$ и p. Заметим, что из формулы (1.67) следует, что $p < N(R)$, следовательно, согласно утверждению 12, сложность шага 16 составляет

$$\mathcal{O}(\ln p) = \mathcal{O}(\ln m + \ln \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) \tag{1.76}$$

арифметических операций.

Шаги 17 и 18 выполняются за $\mathcal{O}(Vm^d)$ операций. Из формулы (1.75) получаем, что

$$\mathcal{O}(Vm^d) = \mathcal{O}(m^d \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil)) \tag{1.77}$$

операций.

Объединим выражения (1.68), (1.69), (1.71), (1.72), (1.73), (1.74), (1.76), (1.77). Получим, что суммарная сложность всего алгоритма составляет

$$\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil) + m^3 \ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil) \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil) +$$

$$+ m^d \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil))$$

арифметических операций. □

Замечание 7. *Заметим, что по теореме* 8 *доля унитарных многочленов с целыми коэффициентами степени* l*, группа Галуа которых меньше, чем* S_l*, а коэффициенты ограничены* B*, составляет*

$$\mathcal{O}\left(\frac{B^{l-\frac{1}{2}} \ln B}{(2B+1)^l}\right) = \mathcal{O}\left(\frac{\ln B}{\sqrt{B}}\right),$$

а эта величина стремится к нулю при $B \to \infty$*. Таким образом, можно ожидать, что большое количество многочленов, возникающих в качестве* $\mu_\omega(x)$*, имеет группу Галуа* S_d*, откуда следует, что* $\sigma_d \in \mathrm{Gal}(\mu_\omega/\mathbb{Q})$*, и тогда при условии справедливости расширенной гипотезы Римана верны утверждения теоремы* 7*.*

Тогда в алгоритме появляется возможность сократить количество вычислений, перепрыгнув с шага 10 на шаг 14, поскольку по следствию 3 (p) *будет являться простым идеалом в* $\mathfrak{D}$*, и для решения сравнения* $f(x) \equiv 0 \pmod p$ *в* $\mathfrak{D}$ *достаточно будет решить уравнение* $f(x) = 0$ *в поле* $\mathbb{F}_{p^d}$*. В таком случае сложность алгоритма будет составлять*

$$\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil) + m^3 \ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil) \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\gamma_i\rceil)$$

арифметических операций.

Замечание 8. *Существует полиномиальный алгоритм факторизации многочленов в* $\mathbb{Q}$*, описанный в статье* [24] *и использующий в качестве*

основной идеи LLL–алгоритм. С его помощью, в частности, можно находить целые корни уравнения $f(x) = 0$. *Сложность данного алгоритма составляет*

$$\mathcal{O}(m^6 + m^5 \ln |f|),$$

где m *— степень раскладываемого на множители многочлена* $f(x) \in \mathbb{Z}[x]$, *а* $|f|$ *— корень из суммы квадратов коэффициентов исходного многочлена.*

2 Решение однородных полиномиальных систем уравнений нулевой размерности в целых числах

Получен алгоритм нахождения целых решений однородной полиномиальной системы с целыми коэффициентами, имеющей конечное число решений в проективном пространстве над полем комплексных чисел.

Обозначения, которые используются на протяжении всей главы, вводятся вне доказательств утверждений. Обозначения же, появляющиеся внутри доказательств, локальны.

Обозначения, введенные в первой главе, в данной главе не используются.

2.1 Постановка задачи

Рассмотрим однородную систему уравнений

$$\begin{cases} P_1(x_0, x_1, \ldots, x_m) &= 0 \\ P_2(x_0, x_1, \ldots, x_m) &= 0 \\ \ldots \\ P_n(x_0, x_1, \ldots, x_m) &= 0, \end{cases} \tag{2.1}$$

где

$$P_i \in \mathbb{Z}[x_0, x_1, \ldots, x_m], i = 1, \ldots, n$$

— однородные многочлены.

С ней можно связать неоднородную систему уравнений

$$\begin{cases} R_1(x_1, \ldots, x_m) &= 0 \\ R_2(x_1, \ldots, x_m) &= 0 \\ \ldots \\ R_n(x_1, \ldots, x_m) &= 0, \end{cases} \tag{2.2}$$

воспользовавшись соотношением

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

Обратно к системе (2.1) можно вернуться, положив

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

Пусть

$$J = (P_1, \ldots, P_n)$$

— идеал, порожденный многочленами, задающими левую часть однородной системы (2.1). Тогда нули идеала J совпадают с нулями системы (2.1) в m-мерном проективном пространстве над полем $\mathbb{C}$, а если положить $x_0 = 1$, то и с нулями системы (2.2) в $\mathbb{C}^m$.

Предположим, что система (2.1) имеет конечное число решений в m-мерном проективном пространстве над $\mathbb{C}$, то есть,

$$\dim J = 0.$$

Тогда и система (2.2) имеет конечное число решений в $\mathbb{C}^m$. Предположим также, что $n = m$. Предложенный в работе алгоритм позволяет при данных предположениях найти целые решения $\overline{\alpha}$ системы (2.1), обладающих следующим свойством: существует минор M_j порядка n матрицы Якоби системы (2.1), такой, что в точке $\overline{\alpha}$ выполняется условие

$$\nu_p(M_j|_{\overline{\alpha}}) = 0,$$

где p — некоторое фиксированное простое число.

Через $\nu_p(\xi)$ здесь обозначена степень вхождения простого числа p в рациональное число ξ.

2.2 Основные теоретические сведения

Пусть $I \subset \mathbb{Q}[x_0, \ldots, x_m]$ — идеал соответствующего кольца.

Определение 12. *Идеал I называется примарным, если из условий $ab \in I$ и $a \notin I$ следует, что для некоторого $n \in \mathbb{N}$ выполняется*

$$b^n \in I.$$

Определение 13. *Радикалом кольца I называется множество*

$$\sqrt{I} = \{a \in \mathbb{Q}[x_0, \ldots, x_m] | \exists n \in \mathbb{N} : a^n \in I\}.$$

Замечание 9. *Если I — примарный идеал, то $\sqrt{I}$ является простым идеалом кольца $\mathbb{Q}[x_0, \ldots, x_m]$.*

Теорема 13 (существование примарного разложения)**.** *Для любого идеала*

$$I \subset \mathbb{Q}[x_0, \ldots, x_m]$$

существуют примарные идеалы $I_1, \ldots, I_s$*, такие, что*

1. $I = I_1 \cap \ldots \cap I_s$.
2. *Представление из пункта (1) минимально по отношению к* s*, то есть ни один из идеалов* I_j *нельзя из него исключить.*
3. *При* $j \neq k$ $\sqrt{I_j} \neq \sqrt{I_k}$.

Доказательство. См. [26, гл. 5 §1]. □

Теорема 14 (единственность примарного разложения)**.** *Предположим, что идеал*

$$I \subset \mathbb{Q}[x_0, \ldots, x_m]$$

имеет два неприводимых примарных разложения

$$I = I_1 \cap \cdots \cap I_s = I'_1 \cap \cdots \cap I'_t,$$

где $\sqrt{I_j} = \mathfrak{p}_j$, $\sqrt{I'_k} = \mathfrak{p}'_k$, $1 \leqslant j \leqslant s$, $1 \leqslant k \leqslant t$. *Тогда*

$$s = t,$$

и примарные компоненты можно поменять местами таким образом, что

$$\mathfrak{p}_j = \mathfrak{p}'_j, 1 \leqslant j \leqslant s.$$

Доказательство. См. [26, гл. 5 §1]. □

Определение 14. *Идеалы* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$*, определенные в теореме* 14*, называются простыми идеалами, ассоциированными с* I.

Определение 15. *Идеал* $I \subset \mathbb{Q}[x_0, \ldots, x_m]$ *называется однородным, если существуют однородные многочлены* $P_1, \ldots, P_n \in \mathbb{Q}[x_0, \ldots, x_m]$*, такие, что* $I = (P_1, \ldots, P_n)$.

Определение 16. *Пусть* $\mathfrak{p}$ *— однородный простой идеал. Тогда проективная размерность* $\mathfrak{p}$ *определяется как*

$$\dim \mathfrak{p} = \ \mathrm{tr.deg}(\mathbb{Q}[x_0, \ldots, x_m]/\mathfrak{p}) - 1.$$

Если I *— однородный идеал с ассоциированными простыми идеалами* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$*, то проективная размерность идеала* $\dim I$ *определяется следующим образом:*

$$\dim I = \max_{1 \leqslant j \leqslant s} (\dim \mathfrak{p}_j).$$

Определение 17. *Пусть* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ *— все простые идеалы, ассоциированные с* I*. Идеал* I *называется несмешанным, если*

$$\dim \mathfrak{p}_j = \dim I$$

для всех $1 \leqslant j \leqslant s$*.*

Определение 18. *Пусть*

$$I \subset \mathbb{Q}[x_0, \ldots, x_m]$$

— однородный несмешанный идеал. Для произвольного целого числа r*,* $1 \leqslant r \leqslant m$ *и переменных* $u_{i,j}$*,* $1 \leqslant i \leqslant r$*,* $0 \leqslant j \leqslant m$ *определим линейные формы*

$$L_i = \sum_{j=0}^{m} u_{i,j} x_j, \ \text{где } 1 \leqslant i \leqslant r.$$

Обозначим через $\overline{I}(r)$ *множество всех многочленов*

$$G \in \mathbb{Q}[u_{1,0}, \ldots, u_{r,m}],$$

таких, что

$$G x_i^M \in (I, L_1, \ldots, L_r)$$

при $0 \leqslant i \leqslant m$*, где* M *— некоторое натуральное число.*

Теорема 15. *Пусть* I *— однородный несмешанный идеал кольца* $\mathbb{Q}[x_0, \ldots, x_m]$ *и* $\dim I = r - 1$*. Пусть*

$$I = I_1 \cap \cdots \cap I_t$$

— неприводимое примарное разложение I, $\sqrt{I_j} = \mathfrak{p}_j$ и k_j — показатель I_j, где $1 \leqslant j \leqslant t$. Тогда $\overline{I}(r)$ — главный идеал кольца $\mathbb{Q}[u_{1,0}, \ldots, u_{r,m}]$, и, если обозначить

$$\overline{\mathfrak{p}}_j = (F_j),$$

то все F_j неприводимы, и

$$F = F_1^{k_1} \ldots F_s^{k_s}$$

— порождающий элемент идеала $\overline{I}(r)$.

Доказательство. См. [26, гл. 5 §2]. □

Определение 19. *Для любого однородного несмешанного идеала I, где $I \subset \mathbb{Q}[x_0, \ldots, x_m]$, многочлен*

$$F \in \mathbb{Q}[u_{1,0} \ldots, u_{r,m}],$$

такой, что

$$\overline{I}(r) = (F),$$

называется ассоциированной формой идеала I.

Определение 20. *Логарифмической высотой многочлена*

$$P = \sum a_{\overline{\gamma}} T_1^{\gamma_1} \cdots T_m^{\gamma_m} \in \mathbb{Q}[T_1, \ldots, T_m]$$

называется следующая величина:

$$h(P) = \sum_{v \in \mathcal{M}} \log |P|_v,$$

где $\mathcal{M}$ — множество индексов, таких, что для любого $v \in \mathcal{M}$ существует абсолютное значение $|\quad|_v$ на поле $\mathbb{Q}$ (то есть в данном случае $\mathcal{M}$ состоит из всех простых чисел и ∞), а

$$|P|_v = \max_{\overline{\gamma}} |a_{\overline{\gamma}}|_v.$$

Замечание 10. *Если многочлен*

$$P \in \mathbb{Z}[T_1, \ldots, T_m]$$

и имеет взаимно простые в совокупности коэффициенты, то

$$h(P) = \log |P|_{\mathbb{C}}.$$

Определение 21. *Пусть*

$$I \subset \mathbb{Q}[x_0, \ldots, x_m]$$

— однородный несмешанный идеал, $r = \dim I + 1$ *и*

$$\overline{I}(r) = (F).$$

Тогда степенью и логарифмической высотой идеала I *называются величины*

$$\deg I = \deg_{\overline{u}_1} F \text{ и } h(I) = h(F)$$

соответственно.

Лемма 16. *Если* M *— целозамкнутая конечная область целостности степени трансцендентности* r*, то каждый собственный главный идеал в* M *является несмешанным идеалом размерности* $r - 1$*.*

Доказательство. См. [7, гл. 7 §7]. □

Лемма 17. *Пусть* $P \in \mathbb{Q}[x_0, \ldots, x_m]$ *— однородный многочлен и* $I = (P)$*. Тогда*

1. $\deg I = \deg P$.

2. $h(I) \leqslant h(P) + m^2 \deg P$.

Доказательство. См. [26, гл. 5 §5]. □

Лемма 18. *Пусть* $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ *— простые однородные идеалы кольца* $\mathbb{Q}[x_0, \ldots, x_m]$*, а*

$$Q_1, \ldots, Q_t \in \mathbb{Q}[x_0, \ldots, x_m]$$

— однородные многочлены, такие, что при $1 \leqslant j \leqslant t$ *выполнены условия*

$$Q_j \notin \mathfrak{p}_j, \ \deg Q_j \leqslant D, \ h(Q_j) \leqslant h. \tag{2.3}$$

Тогда существует однородный многочлен

$$Q \in \mathbb{Q}[x_0, \ldots, x_m],$$

такой, что для него выполняются условия

$$Q \notin \mathfrak{p}_j, \ 1 \leqslant j \leqslant t$$

и

$$\deg Q = D, \ h(Q) \leqslant h + 2 \log t. \tag{2.4}$$

Доказательство. Заметим, что поскольку для всех i, $1 \leqslant i \leqslant t$, идеалы $\mathfrak{p}_i$ являются собственными, то для каждого i существует некоторый одночлен S_i вида

$$x_0^{k_0} \dots x_m^{k_m},$$

где $k_n \in \mathbb{Z}_+$, $0 \leqslant n \leqslant m$, обладающий свойствами

$$\deg S_i = D - \deg Q_i \text{ и } S_i \notin \mathfrak{p}_i. \tag{2.5}$$

Дальнейшее доказательство проведем с помощью индукции по количеству идеалов.

Докажем индукцией по l, где $1 \leqslant l \leqslant t$, что существуют целые числа $\lambda_1, \dots, \lambda_l$, $0 \leqslant \lambda_j \leqslant j$, такие, что

$$\sum_{j=1}^{l} \lambda_j S_j Q_j \notin \mathfrak{p}_i, \ i = 1, \dots, l.$$

Докажем сначала базу индукции. Действительно, при $l = 1$ положим $\lambda_1 = 1$. Исходя из формул (2.3) и (2.5), а также учитывая простоту идеала $\mathfrak{p}_1$, можно заключить, что

$$S_1 Q_1 \notin \mathfrak{p}_1.$$

Пусть теперь $l \geqslant 2$, и доказано существование целых чисел $\lambda_1, \dots, \lambda_{l-1}$, таких, что

$$\sum_{j=1}^{l-1} \lambda_j S_j Q_j \notin \mathfrak{p}_i, \ i = 1, \dots, l-1. \tag{2.6}$$

Положим

$$Q_0 = \sum_{j=1}^{l-1} \lambda_j S_j Q_j.$$

Покажем, что существует не более одного числа λ, такого, что

$$Q_0 + \lambda S_l Q_l \in \mathfrak{p}_l. \tag{2.7}$$

Действительно, предположим, что помимо λ, существует еще число $\mu \neq \lambda$, такое, что

$$Q_0 + \mu S_l Q_l \in \mathfrak{p}_l. \tag{2.8}$$

Вычтем из (2.7) соотношение (2.8). Получим, что выполняется следующее условие:

$$(\lambda - \mu) S_l Q_l \in \mathfrak{p}_l, \tag{2.9}$$

значит, в силу простоты идеала $\mathfrak{p}_l$, должно выполняться либо условие $S_l \in \mathfrak{p}_l$, либо $Q_l \in \mathfrak{p}_l$. Но, согласно формулам (2.3) и (2.5), данные условия не могут выполняться. Следовательно, числа μ, удовлетворяющего (2.8), не существует.

Можно заметить, что аналогично предыдущему существует не более $l-1$ чисел λ, таких, что

$$Q_0 + \lambda S_l Q_l \in \bigcup_{j=1}^{l-1} \mathfrak{p}_j. \tag{2.10}$$

Действительно, пусть существуют числа $\lambda^{(1)}, \ldots, \lambda^{(l)}$, такие, что

$$Q_0 + \lambda^{(r)} S_l Q_l \in \bigcup_{j=1}^{l-1} \mathfrak{p}_j,\ 1 \leqslant r \leqslant l.$$

Но тогда среди них можно найти как минимум два числа $\lambda^{(r_1)}$ и $\lambda^{(r_2)}$, удовлетворяющих для некоторого индекса i, $1 \leqslant i \leqslant l-1$, условию

$$Q_0 + \lambda^{(r_n)} S_l Q_l \in \mathfrak{p}_i,\ n = 1, 2.$$

Отсюда аналогично (2.9) можно заключить, что

$$S_l Q_l \in \mathfrak{p}_i. \tag{2.11}$$

Из формул (2.10) и (2.11) следует, что

$$Q_0 \in \mathfrak{p}_i \tag{2.12}$$

для некоторого i, удовлетворяющего неравенствам $1 \leqslant i \leqslant l-1$. Но условие (2.12) противоречит предположению индукции (2.6).

Следовательно, существует не более $l-1$ чисел λ, удовлетворяющих соотношению (2.10), и, таким образом, среди $l+1$ чисел $0, 1, \ldots, l$ найдется число λ_l, такое, что

$$\sum_{j=1}^{l} \lambda_j S_j Q_j \notin \mathfrak{p}_i,\ i = 1, \ldots, l.$$

Положим

$$Q = \sum_{j=1}^{t} \lambda_j S_j Q_j.$$

Выполнение формул (2.4) следует из построения многочленов S_j, а также того факта, что по построению $\lambda_j \leqslant j < t$. $\square$

Лемма 19. *Пусть* $\mathfrak{a}$ *— несмешанный однородный идеал кольца* $\mathbb{Q}[x_0, \ldots, x_m]$. *Пусть*

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_t$$

— неприводимое примарное разложение идеала $\mathfrak{a}$, $\sqrt{\mathfrak{a}_i} = \mathfrak{p}_i$ *и* k_i *— показатель* $\mathfrak{a}_i$, $1 \leqslant i \leqslant t$. *Тогда*

1. $\sum_{j=1}^{t} k_j \deg \mathfrak{p}_j = \deg \mathfrak{a}$.
2. $\sum_{j=1}^{t} k_j h(\mathfrak{p}_j) \leqslant h(\mathfrak{a}) + m^2 \deg \mathfrak{a}$.

Доказательство. См. [26, гл. 5 §4]. □

Обозначим через $\mathfrak{R}(\mathfrak{a})$ множество нулей идеала $\mathfrak{a}$ в m-мерном проективном пространстве над полем $\mathbb{C}$.

Лемма 20. *Пусть* $\mathfrak{a}$ *— однородный несмешанный идеал кольца* $\mathbb{Q}[x_0, \ldots, x_m]$, $\dim \mathfrak{a} = r - 1$. *Пусть*

$$Q \in \mathbb{Q}[x_0, \ldots, x_m]$$

— однородный многочлен, не содержащийся ни в каком простом идеале, ассоциированном с $\mathfrak{a}$. *Тогда при* $r \geqslant 2$ *существует однородный несмешанный идеал* I *кольца* $\mathbb{Q}[x_0, \ldots, x_m]$, $\dim I = r - 2$, *удовлетворяющий условиям*

1. $\deg I \leqslant \deg \mathfrak{a} \deg Q$.
2. $h(I) \leqslant h(\mathfrak{a}) \deg Q + h(Q) \deg \mathfrak{a} + 4m^2 \deg Q \deg \mathfrak{a}$.
3. $\mathfrak{R}(I) = \mathfrak{R}((\mathfrak{a}, Q))$.

Доказательство. См. [11, лемма 11]. □

Теорема 16. *Пусть* D *— натуральное число,* h *— действительное. Пусть*

$$\mathfrak{a}, \mathfrak{b} = (P_1, \ldots, P_n) \subset \mathbb{Q}[x_0, \ldots, x_m]$$

— однородные идеалы, причем $\mathfrak{a}$ *несмешан и выполняются следующие условия:*

1. $\mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(\mathfrak{a})$,
2. $p = \dim \mathfrak{a} \geqslant r = \dim \mathfrak{b}$,

3. $\deg \mathfrak{a} \leqslant D^{m-p}$,

4. P_i *однородны и*

$$\deg P_i \leqslant D,\ h(P_i) \leqslant h.$$

Тогда существует однородный несмешанный идеал

$$I \subset \mathbb{Q}[x_0, \ldots, x_m],$$

такой, что $\dim I = \dim \mathfrak{b}$ *и*

1. $\deg I \leqslant \deg \mathfrak{a} \cdot D^{p-r}$.

2. $h(I) \leqslant ((p-r)\deg \mathfrak{a} \cdot h + D \cdot h(\mathfrak{a}) + 6m^2(p-1)\deg \mathfrak{a} \cdot D)D^{p-r-1}$.

3. $\mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(I)$.

Замечание 11. *При* $\dim \mathfrak{a} = m$ *следует считать* $\deg \mathfrak{a} = 1, h(\mathfrak{a}) = 0$.

Доказательство. Докажем теорему 16 от противного.

Предположим, что существуют пары идеалов $\mathfrak{a}$, $\mathfrak{b}$, для которых теорема неверна. Фиксируем одну из них с наименьшим возможным значением $\dim \mathfrak{a}$.

Рассмотрим два случая: $\dim \mathfrak{a} = \dim \mathfrak{b}$ и $\dim \mathfrak{a} > \dim \mathfrak{b}$.

В первом случае можно положить $I = \mathfrak{a}$. Тогда утверждения теоремы будут выглядеть следующим образом:

$$\deg I \leqslant \deg I,\ h(I) \leqslant h(I) + 6m^2(p-1),\ \mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(I).$$

Данные условия, очевидно, выполняются, следовательно, первый случай невозможен.

Рассмотрим теперь второй случай: $\dim \mathfrak{a} > \dim \mathfrak{b}$ и, в свою очередь, разобьем его на два подслучая:

$$\dim \mathfrak{a} = m \text{ и } 1 \leqslant \dim \mathfrak{a} \leqslant m-1.$$

Рассмотрим первый из них.

Если $\dim \mathfrak{a} = m$, то положим $I = (P)$, где P — один из ненулевых многочленов P_i. Тогда, согласно лемме 16, I — несмешанный идеал, и

$$\dim I = m - 1 < \dim \mathfrak{a}.$$

По лемме 17,

$$\deg I = \deg P \leqslant D,\ h(I) \leqslant h(P) + m^2 \deg P \leqslant h + m^2 D,$$

следовательно, в данном случае идеал I удовлетворяет утверждениям теоремы.

Значит, осталось рассмотреть только второй подслучай:

$$1 \leqslant \dim \mathfrak{a} \leqslant m - 1.$$

Обозначим через $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ примарные компоненты идеала $\mathfrak{a}$. Через $\mathfrak{p}_i$ обозначим радикалы соответствующих примарных компонент $\mathfrak{a}_i$, а через k_i — их показатели. Поскольку $\dim \mathfrak{p}_i = \dim \mathfrak{a}_i > \dim \mathfrak{b}$, то ни один из идеалов $\mathfrak{p}_i$ не может содержать $\mathfrak{b}$. Следовательно, для каждого i, $1 \leqslant i \leqslant t$ среди многочленов P_k содержится многочлен Q_i, такой, что $Q_i \notin \mathfrak{p}_i$.

Применим лемму 18 к многочленам $Q_1, \ldots, Q_t$ и идеалам $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Они удовлетворяют условиям леммы, и, следовательно, существует однородный многочлен

$$Q \in \mathbb{Q}[x_0, \ldots, x_m],$$

удовлетворяющий условиям $Q \notin \mathfrak{p}_j$, $1 \leqslant j \leqslant t$, а также

$$\deg Q = D \tag{2.13}$$

и

$$h(Q) \leqslant h + 2 \log t. \tag{2.14}$$

По лемме 19, примененной к идеалу $\mathfrak{a}$, верно равенство

$$\sum_{i=1}^{t} k_i \deg \mathfrak{p}_i = \deg \mathfrak{a}. \tag{2.15}$$

Но все $k_i \deg \mathfrak{p}_i \in \mathbb{N}$ при $1 \leqslant i \leqslant t$, следовательно, имеет место неравенство

$$t \leqslant \sum_{i=1}^{t} k_i \deg \mathfrak{p}_i. \tag{2.16}$$

С другой стороны, по условию,

$$\deg \mathfrak{a} \leqslant D^{m-p} \tag{2.17}$$

Объединив формулы (2.15), (2.16) и (2.17), можно заключить, что верно неравенство

$$t \leqslant D^{m-p}.$$

Теперь можно преобразовать формулу (2.14) следующим образом:

$$h(Q) \leqslant h + 2(m-p)\log D. \tag{2.18}$$

Применим лемму 20 к идеалу $\mathfrak{a}$ и многочлену Q. Полученный в лемме 20 идеал J должен иметь размерность

$$\dim J = \dim \mathfrak{a} - 1$$

и удовлетворять условиям

$$\deg J \leqslant \deg \mathfrak{a} \deg Q \leqslant D^{m-p} \cdot D = D^{m+1-p} \tag{2.19}$$

и

$$h(J) \leqslant h(\mathfrak{a}) \deg Q + h(Q) \deg \mathfrak{a} + 4m^2 \deg Q \deg \mathfrak{a}. \tag{2.20}$$

Разобъем оставшееся доказательство еще на два случая: $\dim \mathfrak{a} = \dim \mathfrak{b} + 1$ и $\dim \mathfrak{a} > \dim \mathfrak{b} + 1$.

Рассмотрим первый подслучай:

$$\dim \mathfrak{a} = \dim \mathfrak{b} + 1.$$

Тогда $\dim J = \dim \mathfrak{b}$, Проверим, что для J будут выполняться утверждения теоремы 16.

Воспользовавшись формулами (2.13) и (2.19), получим неравенство

$$\deg J \leqslant \deg \mathfrak{a} \cdot D = \deg \mathfrak{a} \cdot D^{p-r}.$$

Теперь применим формулы (2.13) и (2.18) к неравенству (2.20). Получим следующее неравенство:

$$h(J) \leqslant h(\mathfrak{a}) \cdot D + h \deg \mathfrak{a} + 2(m-p)\log D \deg \mathfrak{a} + 4m^2 D \deg \mathfrak{a} <$$

$$< h(\mathfrak{a}) \cdot D + h \deg \mathfrak{a} + 6m^2(m-p)D.$$

Также из леммы 20 следует, что

$$\mathfrak{R}(\mathfrak{a}) \subset \mathfrak{R}(J).$$

Таким образом, выполняются все утверждения теоремы 16, следовательно, можно положить $I = J$, и такой случай невозможен.

Осталось рассмотреть случай

$$\dim \mathfrak{a} > \dim \mathfrak{b} + 1.$$

Поскольку $\dim J < \dim \mathfrak{a}$, а $\mathfrak{a}$ — идеал наименьшей размерности, для которого утверждение теоремы 16 не выполняется, то теорема верна для идеалов J и $\mathfrak{b}$. Следовательно, существует несмешанный однородный идеал I, $\dim I = \dim b$, такой, что

$$\deg I \leqslant \deg J \cdot D^{\dim J - \dim \mathfrak{b}} \leqslant \deg J \cdot D^{p-1-r} \leqslant \deg \mathfrak{a} \deg Q \cdot D^{p-1-r} = \deg \mathfrak{a} \cdot D^{p-r}$$

и

$$h(I) \leqslant ((p-r-1)\deg J \cdot h + D \cdot h(J) + 6m^2(p-2)\deg J \cdot D) \cdot D^{p-r-2} \leqslant$$

$$\leqslant ((p-r-1)\deg \mathfrak{a} \cdot Dh + D \cdot (h(\mathfrak{a})D + (h + 2\ln t)\deg \mathfrak{a} + 2(m-p)\ln D) +$$

$$+6m^2(p-2)\deg \mathfrak{a} \cdot D^2) D^{p-r-2} \leqslant ((p-r-1)\deg \mathfrak{a} \cdot h + D \cdot h(\mathfrak{a}) + h \cdot \deg \mathfrak{a} +$$

$$+2(m-p)\deg \mathfrak{a} + 2(m-p)\ln D + 6m^2(p-2)\deg \mathfrak{a} \cdot D) D^{p-r-1} \leqslant$$

$$\leqslant ((p-r)\deg \mathfrak{a} \cdot h + D \cdot h(\mathfrak{a}) + 6m^2(p-1)\deg \mathfrak{a} \cdot D) D^{p-r-1}.$$

Кроме того,

$$\mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(I).$$

Таким образом, для идеала I выполняются все условия теоремы 16, что противоречит исходному предположению о том, что для идеала $\mathfrak{a}$ теорема 16 неверна. □

2.3 Оценка модуля решений однородной полиномиальной системы

В данном разделе оцениваются модули решений систем (2.1) и (2.2) через максимумы степеней и логарифмических высот исходных многочленов, входящих в данные системы.

Теорема 17. *Пусть* $\mathfrak{p} \subset \mathbb{Q}[x_0, \ldots, x_m]$ *— однородный простой идеал,* $r = 1 + \dim \mathfrak{p} \geqslant 1$, $x_0 \notin \mathfrak{p}$ *и*

$$\overline{\mathfrak{p}}(r) = (F) \in \mathbb{Q}[u_{1,0}, \ldots, u_{r,m}].$$

Тогда

1. *Существует конечное нормальное расширение*

$$\mathfrak{L}_1 \supset \mathbb{Q}[u_{1,0}, \ldots, u_{r-1,m}],$$

такое, что

$$F = a \prod_{j=1}^{g} (\alpha_0^{(j)} u_{r,0} + \alpha_1^{(j)} u_{r,1} + \cdots + \alpha_m^{(j)} u_{r,m}),$$

где $g = \deg \mathfrak{p} \geqslant 1$, $a \in \mathbb{Q}[u_{1,0}, \ldots, u_{r-1,m}]$, $\alpha_0^{(j)} = 1$ *и* $\alpha_i^{(j)} \in \mathfrak{L}_1$.

2. *Каждая точка*

$$\overline{\alpha}^{(j)} = (1 : \alpha_1^{(j)} : \cdots : \alpha_m^{(j)}) \in \mathbb{P}^m_{\mathfrak{L}_1},\ j = 1, \ldots, g$$

является общей точкой идеала $\mathfrak{p}$*, то есть для любого однородного многочлена* $Q \in \mathbb{Q}[x_0, \ldots, x_m]$ $Q \in \mathfrak{p}$ *тогда и только тогда, когда*

$$Q(\overline{\alpha}^{(j)}) = 0.$$

Доказательство. См. [26, гл. 5 §6]. □

Теорема 18. *Пусть* $P_1, \ldots, P_s \in \mathbb{Q}[T_1, \ldots, T_m]$ *и*

$$P = P_1 \ldots P_s.$$

Тогда

1. $h(P) \leqslant h(P_1) + \cdots + h(P_s) + m \deg P$.

2. $h(P_1) + \cdots + h(P_s) \leqslant h(P) + \sum_{i=1}^{m} \deg_{T_i} P$.

Доказательство. См. [26, гл. 5 §4]. □

Теорема 19. *Рассмотрим систему* (2.2) *и предположим, что*

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

Тогда верны следующие оценки:

$$\log\max_{0\leqslant k\leqslant m}|\alpha_k^{(j)}|\leqslant (mh+6m^2(m-1)D)D^{m-1}+mD^m \tag{2.21}$$

и

$$g\leqslant D^m, \tag{2.22}$$

где $\overline{\alpha}^{(1)},\dots,\overline{\alpha}^{(g)}$ *— все решения системы (2.1) и*

$$\overline{\alpha}^{(j)}=(\alpha_0^{(j)},\dots,\alpha_m^{(j)}).$$

Если $\overline{\alpha}=(\frac{a_1}{b_1},\dots,\frac{a_m}{b_m})$ *— рациональное решение системы (2.2), то верна оценка*

$$\max\{\log\max_{1\leqslant k\leqslant m}|a_k|,\log\max_{1\leqslant k\leqslant m}|b|\}\leqslant (mh+6m^2(m-1)D)D^{m-1}+mD^m, \tag{2.23}$$

где b=НОК$(b_1,\dots,b_m)$.

Доказательство. Рассмотрим систему (2.1) и идеал

$$J=(P_1,\dots,P_n).$$

Напомним, что, согласно постановке задачи, $\dim J=0$.

Заметим, что

$$\max_{1\leqslant i\leqslant n}\deg P_i=\max_{1\leqslant i\leqslant n}\deg R_i\leqslant D \text{ и } \max_{1\leqslant i\leqslant n}h(P_i)=\max_{1\leqslant i\leqslant n}h(R_i)\leqslant h.$$

Применим теорему 16 к идеалам $\mathfrak{a}=(0)$ и J. Согласно утверждениям теоремы, существует однородный несмешанный идеал $I\subset\mathbb{Q}[x_0,\dots,x_m]$, такой, что $\dim I=0$ и

1. $\deg I\leqslant D^m$.
2. $h(I)\leqslant (mh+6m^2(m-1)D)D^{m-1}$.
3. $\mathfrak{R}(J)\subset\mathfrak{R}(I)$.

Из пункта 3 следует, что оценка на величины нулей идеала I будет верна и для нулей идеала J.

Обозначим через F ассоциированную форму идеала I. Поскольку ее можно выбирать с точностью до константы, будем считать, что $F \in \mathbb{Z}[u_0, \ldots, u_m]$ и имеет взаимно простые в совокупности коэффициенты.

Согласно определению, $\deg_{u_i} F \leqslant D^m$ и

$$h(F) \leqslant (mh + 6m^2(m-1)D)D^{m-1}.$$

По теореме 15,

$$I = I_1 \cap \cdots \cap I_t,$$

где все I_i — примарные идеалы, $\mathfrak{p}_i$ — соответствующие радикалы, k_i — показатели I_i и $\overline{\mathfrak{p}}_i = (F_i)$. Тогда

$$F = F_1^{k_1} \ldots F_t^{k_t}.$$

При этом $\dim I_i = 0$ при $i = 1, \ldots, t$, поскольку $\dim I = 0$.

Применим к идеалу $\mathfrak{p}_i$ для каждого $i = 1, \ldots, t$ теорему 17. Многочлен F имеет целые коэффициенты, следовательно, и $F_i \in \mathbb{Z}[u_0, \ldots, u_m]$, следовательно, согласно теореме 17, можно выбрать F_i следующим образом:

$$F_i = a_i \prod_{j=g_{i-1}}^{g_i} (\alpha_0^{(j)} u_0 + \ldots + \alpha_m^{(j)} u_m) = L_{g_{i-1}} \cdots L_{g_i}, \tag{2.24}$$

$$a_i \in \mathbb{Z}, g_0 = 1, g_t = g.$$

Таким образом,

$$F = (L_1 \ldots L_{g_1})^{k_1} \cdot \ldots \cdot (L_{g_{t-1}} \ldots L_g)^{k_t} = W_1 \ldots W_w,$$

где каждый из многочленов W_j, $j = 1, \ldots, w$ совпадает с одним из многочленов $L_1, \ldots, L_g$. Тогда, по теореме 18, учитывая, что $\alpha_0^{(j)} = 1$, получим

$$\max_{0 \leqslant k \leqslant m} |\alpha_k^{(j)}| \leqslant \prod_{j=1}^{g} \max_{0 \leqslant k \leqslant m} |\alpha_k^{(j)}| \leqslant \prod_{j=1}^{g} \max |\text{коэф. } L_j| \leqslant$$

$$\leqslant \prod_{j=1}^{w} \max |\text{коэф. } W_j| \leqslant e^{h(F) + m \deg F}. \tag{2.25}$$

Таким образом,

$$\ln \max_{0 \leqslant k \leqslant m} |\alpha_k^{(j)}| \leqslant (mh + 6m^2(m-1)D)D^{m-1} + mD^m,$$

а само количество корней не превосходит D^m.

Докажем теперь второе утверждение теоремы. Пусть у системы (2.2) существует рациональное решение

$$\overline{\alpha} = (\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}),$$

где $(a_k, b_k) = 1, 1 \leqslant k \leqslant m$. Отсюда следует, что у системы (2.1) есть решение

$$\overline{\alpha}^{(l)} = (1, \alpha_1^{(l)}, \ldots, \alpha_m^{(l)}),$$

где $\alpha_j^{(l)} = \frac{a_j}{b_j}$, $1 \leqslant j \leqslant m$, или, что то же самое,

$$\overline{\alpha}^{(l)} = (b, \frac{b}{b_1}a_1, \ldots, \frac{b}{b_m}a_m),$$

где

$$\frac{b}{b_k}a_k \in \mathbb{Z} \text{ и } (b, \frac{b}{b_1}a_1, \ldots, \frac{b}{b_m}a_m) = 1.$$

Согласно теореме 17, $\overline{\alpha}^{(l)}$ является корнем многочлена F_i для некоторого $1 \leqslant i \leqslant t$. Напомним, что $F_i \in \mathbb{Z}[u_0, \ldots, u_m]$ и имеет взаимно простые в совокупности коэффициенты, а также, согласно формуле (2.24),

$$F_i = L_{g_{i-1}} \cdots L_{g_i},$$

где для любого j, $g_{i-1} \leqslant j \leqslant g_i$, $L_j \in \mathbb{Z}[u_0, \ldots, u_m]$, имеет взаимно простые в совокупности коэффициенты, и L_j имеет вид

$$L_j = qu_0 + p_1u_1 + \cdots + p_mu_m,$$

где $(q, p_1, \ldots, p_m)$ — решение системы (2.1) и $(q, p_1, \ldots, p_m) = 1$. Следовательно, существует индекс r, $g_{i-1} \leqslant r \leqslant g_i$, для которого верно следующее:

$$L_r = bu_0 + \frac{b}{b_1}a_1u_1 + \cdots + \frac{b}{b_m}a_mu_m.$$

Согласно формуле (2.3),

$$\max |\text{коэф. } L_r| \leqslant \prod_{j=1}^{g} \max |\text{коэф. } L_j| \leqslant \prod_{j=1}^{w} \max |\text{коэф. } W_j| \leqslant$$
$$\leqslant e^{h(F)+m\deg F} \leqslant e^{(mh+6m^2(m-1)D)D^{m-1}+mD^m}. \qquad (2.26)$$

Таким образом, мы показали, что

$$|b| \leqslant e^{(mh+6m^2(m-1)D)D^{m-1}+mD^m}$$

и

$$|a_j| \leqslant |\frac{b}{b_j}a_j| \leqslant e^{(mh+6m^2(m-1)D)D^{m-1}+mD^m},\ 1 \leqslant j \leqslant m.$$

Оценка (2.23) доказана. □

Замечание 12. *Теорема* 18 *верна для произвольной системы, имеющей конечное число решений в проективном пространстве над* $\mathbb{C}$*, а не только для квадратной.*

2.4 Нахождение решений неоднородной полиномиальной системы по модулю степени простого числа

В данном и дальнейших параграфах существенную роль играет тот факт, что число уравнений системы (2.2) равно числу ее неизвестных. Таким образом, далее положим $m = n$.

Для произвольной матрицы B обозначим

$$\|B\| = \max |\text{элем. } B|.$$

Введем следующие обозначения:

$$\overline{R} = \begin{pmatrix} R_1 \\ R_2 \\ \dots \\ R_n \end{pmatrix},\ \overline{\delta_k} = \begin{pmatrix} \delta_{k,1} \\ \delta_{k,2} \\ \dots \\ \delta_{k,n} \end{pmatrix},\ A_k = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\overline{\delta_k}) & \dots & \frac{\partial R_1}{\partial x_n}(\overline{\delta_k}) \\ \dots & & \\ \frac{\partial R_n}{\partial x_1}(\overline{\delta_k}) & \dots & \frac{\partial R_n}{\partial x_n}(\overline{\delta_k}) \end{pmatrix},$$

где $k = 0, 1, 2, \dots$.

Пусть p — простое число, удовлетворяющее условию

$$p \nmid \det A_0. \tag{2.27}$$

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

$$\overline{R}(\overline{\delta_0}) \equiv 0 \pmod{p}. \tag{2.28}$$

Поскольку выполняется условие (2.27), то существует матрица C_0 с целыми элементами, такая, что

$$A_0 C_0 \equiv E \pmod{p}. \tag{2.29}$$

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

$$\overline{\delta_k} \equiv \overline{\delta_{k-1}} - C_{k-1} \cdot \overline{R}(\overline{\delta_{k-1}}) \pmod{p^{2^k}}, \tag{2.30}$$

где $\|\delta_k\| \leqslant \frac{p^{2^k}}{2}$, и

$$C_k \equiv 2C_{k-1} - C_{k-1} A_k C_{k-1} \pmod{p^{2^k}}, \tag{2.31}$$

где $\|C_k\| \leqslant \frac{p^{2^k}}{2}$.

Теорема 20. *При любом $k \in \mathbb{Z}$, $k \geqslant 0$ для векторов $\overline{R}$ и $\overline{\delta_k}$ и матриц A_k и C_k, определенных с помощью формул (2.28)–(2.31), выполняются следующие сравнения:*

$$A_k C_k \equiv E \pmod{p^{2^k}} \tag{2.32}$$

и

$$\overline{R}(\overline{\delta_k}) \equiv 0 \pmod{p^{2^k}}. \tag{2.33}$$

Доказательство. Проведем доказательство индукцией по k.

При $k = 0$ теорема верна по построению C_0 и $\overline{\delta_0}$.

Пусть теперь $k > 0$, и требуемые сравнения выполнены для всех $i < k$. Таким образом,

$$A_{k-1} C_{k-1} \equiv E \pmod{p^{2^{k-1}}} \tag{2.34}$$

и

$$\overline{R}(\overline{\delta_{k-1}}) \equiv 0 \pmod{p^{2^{k-1}}}. \tag{2.35}$$

Заметим, что

$$A_{k-1} \equiv A_k \pmod{p^{2^{k-1}}}, \tag{2.36}$$

поскольку из формулы (2.30) и индуктивного предположения следует, что

$$\overline{\delta_{k-1}} \equiv \overline{\delta_k} \pmod{p^{2^{k-1}}},$$

а, значит, и

$$\frac{\partial R_t}{\partial x_l}(\overline{\delta_{k-1}}) \equiv \frac{\partial R_t}{\partial x_l}(\overline{\delta_k}) \pmod{p^{2^{k-1}}},\ 1 \leqslant t, l \leqslant n.$$

Из формул (2.34) и (2.36) непосредственно вытекает, что

$$A_k C_{k-1} \equiv E \pmod{p^{2^{k-1}}}$$

и, следовательно, $(A_k C_{k-1} - E)^2 \equiv 0 \pmod{(p^{2^{k-1}})^2 = p^{2^k}}$.

Из данного равенства, используя формулу (2.31), получаем следующую цепочку сравнений:

$$(A_k C_{k-1} - E)^2 = A_k C_{k-1} A_k C_{k-1} - 2A_k C_{k-1} + E =$$

$$= A_k(C_{k-1} A_k C_{k-1} - 2C_{k-1}) + E \equiv -A_k C_k + E \equiv 0 \pmod{p^{2^k}}.$$

Обозначим теперь через $[C_k]_1, \ldots, [C_k]_n$ строки матрицы C_k. Тогда формулу (2.30) можно переписать в виде

$$\delta_{k,j} = \delta_{k-1,j} - [C_{k-1}]_j \cdot \overline{R}(\overline{\delta_{k-1}}),\ 1 \leqslant j \leqslant n. \tag{2.37}$$

Разложим многочлены $R_i(x_1, \ldots, x_n)$, $1 \leqslant i \leqslant n$, в ряд Тейлора в окрестности точки $\overline{\delta_{k-1}}$ и рассмотрим значение $R_i(x_1, \ldots, x_n)$ в точке $\overline{\delta_k}$. Воспользовавшись формулой (2.37), получим следующее выражение:

$$R_i(\overline{\delta_k}) = \sum_{s=0}^{\deg R_i} \frac{T^s R_i(\overline{\delta_{k-1}})}{s!}, \tag{2.38}$$

где T — дифференциальный оператор вида

$$T = -\sum_{j=1}^{n} [C_{k-1}]_j \cdot \overline{R}(\overline{\delta_{k-1}}) \frac{\partial}{\partial x_j}.$$

Таким образом,

$$T^s = (-1)^s \sum_{j_1+\ldots+j_n=s} \binom{s}{j_1, \ldots, j_n} ([C_{k-1}]_1 \cdot \overline{R}(\overline{\delta_{k-1}}))^{j_1} \ldots ([C_{k-1}]_n \cdot \overline{R}(\overline{\delta_{k-1}}))^{j_n} \times$$
$$\times \frac{\partial^s}{\partial x_1^{j_1} \ldots \partial x_n^{j_n}}, \tag{2.39}$$

где $\binom{s}{j_1, \ldots, j_n} = \dfrac{s!}{j_1! \ldots j_n!}$ — мультиномиальный коэффициент.

Введем обозначение

$$B_{k,j_1,\ldots,j_n} = ([C_{k-1}]_1 \cdot \overline{R}(\overline{\delta_{k-1}}))^{j_1} \ldots ([C_{k-1}]_n \cdot \overline{R}(\overline{\delta_{k-1}}))^{j_n} \tag{2.40}$$

Заметим, что, если раскрыть скобки в формуле (2.40), то получится сумма вида

$$B_{k,j_1,\dots,j_n} = \sum_{t_1+\dots+t_n=s} b_{t_1,\dots,t_n} (R_1(\overline{\delta_{k-1}}))^{j_1} \dots (R_n(\overline{\delta_{k-1}}))^{j_n}, \tag{2.41}$$

Здесь числа $b_{t_1,\dots,t_n} \in \mathbb{Z}$, поскольку по построению все элементы матрицы C_{k-1} являются целыми числами, а многочлены R_j имеют целые коэффициенты.

Заметим, что, согласно формуле (2.35), при любом j, $1 \leqslant j \leqslant n$,

$$R_j(\overline{\delta_{k-1}}) \equiv 0 \pmod{p^{2^{k-1}}},$$

откуда из из формулы (2.41) следует, что

$$B_{k,j_1,\dots,j_n} \equiv 0 \pmod{p^{2^{k-1}(j_1+\dots+j_n)} = p^{2^{k-1}s}}.$$

Таким образом, при $s \geqslant 2$

$$B_{k,j_1,\dots,j_n} \equiv 0 \pmod{p^{2^k}}. \tag{2.42}$$

Перепишем теперь формулу (2.38) с учетом (2.39) и (2.40). Получим следующее выражение:

$$\begin{aligned} R_i(\overline{\delta_k}) &= \sum_{s=0}^{\deg R_i} \frac{(-1)^s}{s!} \sum_{j_1+\dots+j_n=s} \frac{s!}{j_1! \dots j_n!} B_{k,j_1,\dots,j_n} \frac{\partial^s R_i(\overline{\delta_{k-1}})}{\partial x_1^{j_1} \dots \partial x_n^{j_n}} = \\ &= \sum_{s=0}^{\deg R_i} \sum_{j_1+\dots+j_n=s} (-1)^s B_{k,j_1,\dots,j_n} \frac{1}{j_1! \dots j_n!} \cdot \frac{\partial^s R_i(\overline{\delta_{k-1}})}{\partial x_1^{j_1} \dots \partial x_n^{j_n}}. \end{aligned} \tag{2.43}$$

Запишем многочлен $R_i(x_1, \dots, x_n)$ в виде

$$R_i(x_1, \dots, x_n) = \sum_{(i_1,\dots,i_n)} \gamma_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n},$$

где $\gamma_{i_1,\dots,i_n} \in \mathbb{Z}$. Тогда частные производные данного многочлена имеют вид

$$\begin{aligned} \frac{\partial^s R_i(x_1, \dots, x_n)}{\partial x_1^{j_1} \dots \partial x_n^{j_n}} &= \sum_{(i_1,\dots,i_n)} \gamma_{i_1,\dots,i_n} i_1 \dots (i_1 - j_1 + 1) \dots i_n \dots (i_n - j_n + 1) \times \\ \times x_1^{i_1-j_1} \dots x_n^{i_n-j_n} &= \sum_{(i_1,\dots,i_n)} \gamma_{i_1,\dots,i_n} \frac{i_1!}{(i_1-j_1)!} \dots \frac{i_n!}{(i_n-j_n)!} x_1^{i_1-j_1} \dots x_n^{i_n-j_n}. \end{aligned} \tag{2.44}$$

Если в выражении (2.44) находится такой индекс t, $1 \leqslant t \leqslant n$, что $i_t < j_t$, то соответствующее слагаемое нужно положить равным нулю.

С учетом формулы (2.44) равенство (2.43) можно записать как

$$R_i(\overline{\delta_k}) = \sum_{s=0}^{\deg R_i} \sum_{j_1+\ldots+j_n=s} \sum_{(i_1,\ldots,i_n)} (-1)^s \gamma_{i_1,\ldots,i_n} B_{k,j_1,\ldots,j_s} \frac{i_1!}{j_1!(i_1-j_1)!} \ldots \times$$

$$\times \frac{i_n!}{j_n!(i_n-j_n)!} x_1^{i_1-j_1} \ldots x_n^{i_n-j_n} = \sum_{s=0}^{\deg R_i} \sum_{j_1+\ldots+j_n=s} \sum_{(i_1,\ldots,i_n)} (-1)^s \gamma_{i_1,\ldots,i_n} B_{k,j_1,\ldots,j_s} \times$$

$$\times \binom{i_1}{j_1} \ldots \binom{i_n}{j_n} x_1^{i_1-j_1} \ldots x_n^{i_n-j_n}, \tag{2.45}$$

где $\binom{i_l}{j_l}$, $1 \leqslant l \leqslant n$ — биномиальные коэффициенты.

Заметим, что все коэффициенты в разложении (2.45) являются целыми числами, следовательно, используя формулу (2.42), можно заключить, что

$$R_i(\overline{\delta_k}) \equiv R_i(\overline{\delta_{k-1}}) - \sum_{j=1}^{n} [C_{k-1}]_j \overline{R}(\overline{\delta_{k-1}}) \frac{\partial R_i(\overline{\delta_{k-1}})}{\partial x_j} \pmod{p^{2^k}},\ 1 \leqslant i \leqslant n.$$

Полученные сравнения можно переписать в векторном виде:

$$\overline{R}(\overline{\delta_k}) \equiv \overline{R}(\overline{\delta_{k-1}}) - A_{k-1} C_{k-1} \overline{R}(\overline{\delta_{k-1}}) \pmod{p^{2^k}}. \tag{2.46}$$

Применим к выражению (2.46) предположение индукции (2.34) и (2.35). Получим следующее:

$$\overline{R}(\overline{\delta_k}) \equiv (E - A_{k-1} C_{k-1}) \overline{R}(\overline{\delta_{k-1}}) \equiv 0 \pmod{(p^{2^{k-1}})^2 = p^{2^k}}.$$

Таким образом, теорема 20 доказана. □

2.5 Нахождение рациональных решений неоднородной полиномиальной системы

Рассмотрим систему уравнений (2.2). Пусть

$$\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) = (\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}) \tag{2.47}$$

— одно из рациональных решений системы (2.2), удовлетворяющее условию

$$p \nmid b = \text{НОК}(b_1, \ldots, b_n). \tag{2.48}$$

Поскольку выполняется формула (2.48), то найдется вектор $\overline{\delta}_0$, такой, что

$$\overline{R}(\overline{\delta}_0) \equiv 0 \pmod{p} \tag{2.49}$$

и

$$\overline{\delta}_0 \equiv \overline{\alpha} \pmod{p}. \tag{2.50}$$

Поскольку $\overline{\alpha}$ — вектор, состоящий из рациональных чисел, что формулу (2.50) следует понимать как $\nu_p(\alpha_i - \delta_{0,i}) > 0$, где $1 \leqslant i \leqslant n$. Здесь $\nu_p(\cdot)$ — степень вхождения простого числа p в произвольное рациональное число.

Теорема 21. *Для векторов $\overline{\alpha}$ и $\overline{\delta}_0$, определенных формулами* (2.47)–(2.50)*, и для любого числа $K \in \mathbb{N}$ выполняется следующее сравнение:*

$$\overline{\alpha} \equiv \overline{\delta_K} \pmod{p^{2^K}}, \tag{2.51}$$

где $\overline{\delta_K}$ — вектор, полученный из $\overline{\delta}_0$ по формуле (2.30).

Доказательство. Введем следующее обозначение:

$$r = \min_{1 \leqslant i \leqslant n} \nu_p(\alpha_i - \delta_{K,i}).$$

Заметим, что, согласно формуле (2.50), выполняется неравенство $r > 0$.

Разложим в ряд Тейлора функции R_i, $1 \leqslant i \leqslant n$, в окрестности точки $\overline{\delta_K}$. Аналогично формуле, полученной в доказательстве теоремы 20, будет иметь место равенство

$$-R_i(\overline{\delta_K}) = R_i(\overline{\alpha}) - R_i(\overline{\delta_K}) = \sum_{j=1}^{n} \frac{\partial R_i(\overline{\delta_K})}{\partial x_j}(\alpha_j - \delta_{K,j}) + R_i', \tag{2.52}$$

где

$$R_i' = \sum_{j,k=1}^{n} \frac{1}{2} \frac{\partial R_i}{\partial x_j \partial x_k}(\overline{\delta_K})(\alpha_j - \delta_{K,j})(\alpha_k - \delta_{K,k}) + \ldots,$$

При этом по формуле, аналогичной (2.45), выполняются условия

$$R_i' \in \mathbb{Z}[x_1, \ldots, x_n]$$

и

$$\nu_p(R_i') \geqslant 2r. \tag{2.53}$$

Запишем формулу (2.52) в векторном виде. Получим следующее выражение

$$\overline{R}(\overline{\delta_K}) = A_K(\overline{\delta_K} - \overline{\alpha}) + \overline{R'}, \tag{2.54}$$

где

$$\nu_p(\overline{R'}) \geqslant 2r. \tag{2.55}$$

Умножим теперь равенство (2.54) на матрицу C_K и воспользуемся формулами (2.32) и (2.33). Получим, что выполняется цепочка сравнений по модулю p^{2^K}:

$$C_V \cdot \overline{R}(\overline{\delta_K}) \equiv (\overline{\delta_K} - \overline{\alpha}) + C_K \cdot \overline{R'} \equiv 0 \pmod{p^{2^K}},$$

то есть

$$\overline{\alpha} - \overline{\delta_K} \equiv C_K \cdot \overline{R'} \pmod{p^{2^K}}, \tag{2.56}$$

Согласно формулам (2.50) и (2.55), левая часть сравнения (2.56) должна делиться в точности на p^r, правая часть должна делиться на p^{2r}, а разность — на p^{2^K}. Отсюда можно заключить, что

$$r \geqslant \min(2r, 2^K).$$

Поскольку $r > 0$, то из предыдущей формулы следует, что

$$r \geqslant 2^K$$

и, таким образом,

$$\overline{\alpha} \equiv \overline{\delta_K} \pmod{p^{2^K}}.$$

□

Положим

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

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

Тогда согласно результатам, полученным в теореме 19, для вектора $\overline{\alpha}$ верны оценки

$$\max_{1 \leqslant k \leqslant n} |a_k| \leqslant C \text{ и } |b| \leqslant C. \tag{2.57}$$

Замечание 13. *Если требуется найти* $\overline{\alpha'}$ *— целое решение системы (2.2), удовлетворяющее условию*

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

то либо $\overline{\alpha'} = \overline{\delta_V}$*, где*

$$V = \lfloor \log_2(\log_p(2C)) \rfloor + 1, \tag{2.58}$$

либо такого решения не существует.

Доказательство. Из формулы (2.58) следует, что

$$C < \frac{p^{2^V}}{2}. \tag{2.59}$$

Оценим норму вектора разности $\overline{\alpha'}$ и $\overline{\delta_V}$ с учетом формул (2.57) и (2.59) и того факта, что по условию $\|\delta_V\| \leqslant \frac{p^{2^V}}{2}$:

$$\max_{1 \leqslant i \leqslant n} |\alpha_i - \delta_{V,i}| \leqslant \max_{1 \leqslant i \leqslant n} |\alpha_i| + \max_{1 \leqslant i \leqslant n} |\delta_{V,i}| \leqslant C + \frac{p^{2^V}}{2} < p^{2^V}.$$

Но разность $\overline{\alpha'} - \overline{\delta_V}$ — целочисленный вектор, каждая координата которого, согласно формуле (2.51), делится на p^{2^V}. Значит, все координаты вектора $\overline{\alpha'} - \overline{\delta_V}$ равны нулю, и, следовательно,

$$\overline{\alpha} = \overline{\delta_V}.$$

□

Теорема 22. *Пусть* s, h *— целые числа. Предположим, что существуют целые числа* f *и* g*, такие, что*

$$gs \equiv f \pmod{h} \text{ и } |f|, |g| \leqslant \lambda\sqrt{h}, \tag{2.60}$$

где λ *— положительный корень уравнения*

$$\lambda^2 + \lambda - 1 = 0. \tag{2.61}$$

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

$$u_i = v_i s - w_i h. \tag{2.62}$$

Тогда

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

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

Замечание 14. *Доказательство теоремы 22 можно найти в статье [19]. В данной статье оно приводится в более полном виде.*

Для доказательства данной теоремы потребуются некоторые утверждения, касающиеся свойств цепных дробей, доказательства которых можно найти в книгах [12] и [14].

Утверждение 13. *Все подходящие дроби несократимы.*

Доказательство. См. [14, теор. 11]. □

Утверждение 14. *Знаменатели подходящих дробей образуют строго возрастающую последовательность.*

Доказательство. См. [14, гл. 1 §4]. □

Утверждение 15. *Пусть*

$$\gamma = [c_0; c_1, c_2, \ldots]$$

— конечная или бесконечная цепная дробь с целыми элементами, причем для $n \geqslant 1$ выполняется неравенство $c_n \geqslant 1$, а для конечной дроби ее последнее неполное частное больше 1. Тогда для любых двух соседних подходящих дробей к γ имеем

$$|q_{n-1}\gamma - p_{n-1}| > |q_n\gamma - p_n|, n \geqslant 0.$$

Доказательство. См. [12, теор. 8.3]. □

Утверждение 16. *Всякая несократимая рациональная дробь $\frac{f}{g}$, удовлетворяющая неравенству*

$$|\gamma - \frac{f}{g}| < \frac{1}{2g^2},$$

есть подходящая дробь числа γ.

Доказательство. См. [14, теор. 19]. □

Доказательство. (теор. 22).

Поскольку

$$gs \equiv f \pmod{h},$$

то по определению для некоторого $t \in \mathbb{Z}$ выполняется равенство

$$f = gs - th. \tag{2.63}$$

Тогда разность $\left|\frac{s}{h} - \frac{t}{g}\right|$ можно оценить с помощью формул (2.60), (2.61) и (2.63) следующим образом:

$$\left|\frac{s}{h} - \frac{t}{g}\right| = \left|\frac{f}{hg}\right| = \left|\frac{fg}{hg^2}\right| \leqslant \left|\frac{\lambda^2 h}{hg^2}\right| < \frac{1}{2g^2}.$$

То есть для чисел $\frac{s}{h}$ и $\frac{t}{g}$ выполняются условия утверждения 16, и, таким образом, $\frac{t}{g}$ является некоторой подходящей дробью числа $\frac{s}{h}$.

Введем обозначение

$$\frac{t}{g} = \frac{w_j}{v_j}. \tag{2.64}$$

Докажем, что $j = k$, где k — число, определенное в условии теоремы 22.

Из утверждения 13 следует, что $(w_j, v_j) = 1$. Но $\frac{w_j}{v_j} = \frac{t}{g}$, следовательно,

$$t = zw_j,\ g = zv_j, \tag{2.65}$$

где $z \in \mathbb{N}$.

Перепишем формулу 2.63 с учетом равенств (2.64) и (2.65). Получим следующее выражение:

$$|f| = |gs - th| = z|v_j s - w_j h| = z|u_j| \geqslant |u_j|. \tag{2.66}$$

Таким образом, из формул (2.60) и (2.66) следует, что

$$|u_j| \leqslant \lambda\sqrt{h} < \sqrt{h}.$$

Согласно утверждению 15, последовательность $\{u_i\}$ убывает, а k — наименьший индекс, обладающий свойством $|u_k| < \sqrt{h}$, следовательно, $j \geqslant k$.

С другой стороны, по формуле (2.62) верны равенства

$$u_j = v_j s - w_j h \text{ и } u_k = v_k s - w_k h,$$

откуда следует, что

$$u_j v_k - u_k v_j = (w_k v_j - w_j v_k)h \equiv 0 \pmod{h}. \tag{2.67}$$

При этом, согласно утверждению 14,

$$v_k \leqslant v_j. \tag{2.68}$$

Также из формул (2.60) и (2.65) следует, что

$$|v_j| \leqslant z|v_j| = |g| \leqslant \lambda\sqrt{h}. \tag{2.69}$$

Пользуясь неравенствами (2.60), (2.61), (2.68) и (2.69), получаем следующую цепочку неравенств:

$$|u_j v_k - u_k v_j| \leqslant (|u_j| + |u_k|)|v_j| < (\lambda\sqrt{h} + \sqrt{h})\lambda\sqrt{h} = \lambda(\lambda+1)h = h. \tag{2.70}$$

Но из сравнения (2.67) вытекает, что разность $|u_j v_k - u_k v_j|$ должна делиться на h, откуда вкупе с формулой (2.70), вытекает, что

$$u_j v_k = u_k v_j,$$

и, таким образом, $w_j v_k = w_k v_j$. То есть

$$\frac{w_j}{v_j} = \frac{w_k}{v_k},$$

и, следовательно,

$$\frac{f}{g} = \frac{s v_k - h w_k}{v_k} = \frac{u_k}{v_k}.$$

□

Из доказанного выше вытекает следующая теорема:

Теорема 23. *Если требуется найти*

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

— рациональное решение системы (2.2), удовлетворяющее условию

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

и $p \nmid b$, *где* p *задается 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 теоремы* 22, *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.

Доказательство. По теореме 21, при условии $\overline{\alpha} \equiv \overline{\delta_0} \pmod{p}$ и $p \nmid b$ выполняется сравнение

$$\overline{\alpha} \equiv \overline{\delta_V} \pmod{p^{2^V}}.$$

Кроме того, при выборе $V = \lfloor \log_2 \log_p \left(\frac{C^2}{\lambda^2} \right) \rfloor + 1$ верно неравенство

$$h = p^{2^V} \geqslant \left(\frac{C^2}{\lambda^2} \right),$$

то есть $C \leqslant \lambda \sqrt{h}$, а из теоремы 19 известно, что

$$\max_{1 \leqslant i \leqslant n} |a_i| \leqslant C \text{ и } \max_{1 \leqslant i \leqslant n} |b_i| \leqslant C.$$

То есть выполняются все условия теоремы 22. □

2.6 Алгоритм решения неоднородной полиномиальной системы в рациональных числах

Алгоритм 2.1.

Дано: система уравнений

$$\begin{cases} R_1(x_1, \ldots, x_n) &= 0 \\ R_2(x_1, \ldots, x_n) &= 0 \\ \ldots \\ R_n(x_1, \ldots, x_n) &= 0, \end{cases} \tag{2.71}$$

где $R_i \in \mathbb{Z}[x_1, \ldots, x_n]$, $i = 1, \ldots, n$ и $\dim(P_1, \ldots, P_n) = 0$
($\overline{P}(x_0, \ldots, x_m) = 0$ *— соответствующая однородная система*);

числа D и h, такие, что

$$\max_{1\leqslant i\leqslant n}\deg R_i\leqslant D,\ \ \max_{1\leqslant i\leqslant n}h(R_i)\leqslant h;$$

простое число p.

Найти: множество решений $\overline{\alpha}=(\frac{a_1}{b_1},\ldots,\frac{a_n}{b_n})$ данной системы в $\mathbb{Q}^n$, удовлетворяющих условиям

$$p\nmid b=\text{НОК}(b_1,\ldots,b_n) \tag{2.72}$$

и

$$\nu_p(\det J|_{\overline{\alpha}})=0,\ \text{где}\ J=\begin{pmatrix}\frac{\partial R_1}{\partial x_1} & \cdots & \frac{\partial R_1}{\partial x_n}\\ \cdots & & \\ \frac{\partial R_n}{\partial x_1} & \cdots & \frac{\partial R_n}{\partial x_n}\end{pmatrix}, \tag{2.73}$$

или доказать, что таких решений не существует.

1. Положить $S'=\emptyset$.

2. Найти все решения системы сравнений

$$\overline{R}(x_1,\ldots,x_n)\equiv 0\pmod p$$

в $\mathbb{Z}^n$.

Если она неразрешима, то исходная система уравнений не имеет решений в $\mathbb{Q}^n$, удовлетворяющих условиям алгоритма.

Если система сравнений разрешима, то обозначим через S множество векторов $\overline{\delta}\in\mathbb{Z}^n$, таких, что

$$\overline{R}(\overline{\delta})\equiv 0\pmod p$$

для каждого $\overline{\delta}\in S$. Выбрать $\overline{\delta}$ так, чтобы выполнялось неравенство

$$\|\delta_{\|}\leqslant\frac{p}{2}.$$

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

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

5. Для каждого $\overline{\delta}\in S$ выполнять следующие действия:

5.1. Положить $\overline{\delta_0} = \overline{\delta}$.

5.2. Вычислить матрицу $A_0 = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\overline{\delta_0}) & \dots & \frac{\partial R_1}{\partial x_n}(\overline{\delta_0}) \\ \dots & & \\ \frac{\partial R_n}{\partial x_1}(\overline{\delta_0}) & \dots & \frac{\partial R_n}{\partial x_n}(\overline{\delta_0}) \end{pmatrix}$.

5.3. Вычислить $\det A_0$. Если $p | \det A_0$, то перейти к шагу 5.

5.4. Найти матрицу C_0, удовлетворяющую условию

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

5.5. Для каждого $k = 1, \dots, V$ вычислить:

5.5.1. $\overline{\delta_k} \equiv \overline{\delta_{k-1}} - C_{k-1} \cdot \overline{R}(\overline{\delta_{k-1}}) \mod p^{2^k}$, где $\|\delta_k\| \leqslant \frac{p^{2^k}}{2}$.

5.5.2. $A_k = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\overline{\delta_k}) & \dots & \frac{\partial R_1}{\partial x_n}(\overline{\delta_k}) \\ \dots & & \\ \frac{\partial R_n}{\partial x_1}(\overline{\delta_k}) & \dots & \frac{\partial R_n}{\partial x_n}(\overline{\delta_k}) \end{pmatrix}$.

5.5.3. $C_k \equiv 2C_{k-1} - C_{k-1} A_k C_{k-1} \pmod{p^{2^k}}$, где $\|C_k\| \leqslant \frac{p^{2^k}}{2}$.

5.6. Для каждого $k = 1, \dots, n$:

5.6.1. Положить $u_1 = v_1 \delta_{V,k} - w_1 p^{2^V}$, где $\frac{w_1}{v_1}$ — первая подходящая дробь к $\frac{\delta_{V,k}}{p^{2^V}}$.

5.6.2. Положить $u = u_1$, $t = 1$.

5.6.3. Выполнять, пока $|u| \geqslant p^{2^{V-1}}$:

5.6.3.1. Положить $t = t + 1$.

5.6.3.2. Вычислить $\frac{w}{v}$ — t-ую подходящую дробь к $\frac{\delta_{V,k}}{p^{2^V}}$.

5.6.3.3. Вычислить $u = v\delta_{V,k} - w p^{2^V}$.

5.6.4. Положить $\frac{a_k}{b_k} = \frac{u}{v}$.

5.7. Вычислить $\overline{R}(\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n})$. Если $\overline{R}(\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}) = 0$, то

$$S' = S' \cup \{(\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n})\}.$$

6. Если $S' = \emptyset$, то дать ответ, что система

$$\overline{R}(x_1, \dots, x_n) = 0$$

не имеет решений в $\mathbb{Q}^n$, удовлетворяющих условию (2.73).

Замечание 15. *Соответствующие подходящие дроби на шаге 5.6.3.2 можно вычислять с помощью рекуррентных формул (см. [12]).*

Теорема 24. *Алгоритм 2.1 находит все решения системы* (2.71)*, принадлежащие* $\mathbb{Q}^n$ *и удовлетворяющие условиям* (2.72) *и* (2.73)*, если они есть, а также выдает ответ, что таких решений нет, если их не существует.*

Доказательство. Если система (2.71) обладает рациональным решением

$$\overline{\alpha} = (\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}) \in \mathbb{Q}^n,$$

таким, что $p \nmid \text{НОК}(b_1, \ldots, b_n)$, то на шаге 2 алгоритма найдется вектор $\overline{\delta_0}$, такой, что

$$\overline{R}(\overline{\delta}_0) \equiv 0 \pmod{p}$$

и

$$\overline{\delta}_0 \equiv \overline{\alpha} \pmod{p},$$

поскольку $\overline{\alpha} \pmod{p}$ удовлетворяет условию

$$\overline{R}(\overline{\alpha} \pmod{p}) \equiv 0 \pmod{p},$$

и, следовательно, $\overline{\alpha} \pmod{p} \in S'$.

Так как $\overline{\delta}_0 \equiv \overline{\alpha} \pmod{p}$, то из свойства сравнений следует, что

$$\det A_0 \equiv \det J(\overline{\alpha}) \pmod{p}, \tag{2.74}$$

поэтому из условия

$$\nu_p(\det J|_{\overline{\alpha}}) = 0$$

следует, что $\nu_p(\det A_0) = 0$, и на шаге 5.4 к матрице A_0 найдется обратная по модулю p.

Если же $\nu_p(\det A_0) > 0$, то из формулы (2.74) следует, что

$$\nu_p(\det J|_{\overline{\alpha}}) > 0,$$

то есть такое решение не удовлетворяет условию (2.73), и можно переходить к следующему $\overline{\delta}$ на шаге 5.

Согласно результатам, полученным в теореме 20, на шаге 5.5 строится вектор $\overline{\delta}_V$, удовлетворяющий условию $\overline{R}(\overline{\delta}_V) \equiv 0 \pmod{p^{2^V}}$, а из теоремы 21 следует, что

$$\overline{\alpha} \equiv \overline{\delta}_V \pmod{p^{2^V}}.$$

Далее, из теорем 19, 22 и 23 следует, что на шаге 5.6 решение $\overline{\alpha}$ однозначно восстанавливается из вектора $\overline{\delta}_V$.

Таким образом, доказано, что каждое целое решение системы (2.71), удовлетворяющее (2.72) и (2.73), содержится среди векторов, найденных на шаге 5.6 алгоритма.

В то же время, на шаге 5.7 выполняется подстановка в исходную систему всех полученных на шаге 5.6 "кандидатов" на решение, поэтому лишних ответов алгоритм выдать не может.

Если же не существует элементов $\overline{\delta} \in \mathbb{Z}^n$, таких, что

$$\overline{R}(\overline{\delta}) \equiv 0 \pmod{p},$$

то это значит, что система (2.71) заведомо не имеет решений, удовлетворяющих требованиям алгоритма 2.1. В этом случае алгоритм остановится на шаге 2. □

2.7 Алгоритм решения однородной полиномиальной системы в целых числах

Алгоритм 2.2.

Дано: система уравнений

$$\begin{cases} P_1(x_0, x_1, \ldots, x_n) &= 0 \\ P_2(x_0, x_1, \ldots, x_n) &= 0 \\ \ldots & \\ P_n(x_0, x_1, \ldots, x_n) &= 0, \end{cases} \tag{2.75}$$

где $P_i \in \mathbb{Z}[x_0, x_1, \ldots, x_n]$, $i = 1, \ldots, n$ — однородные многочлены и $\dim(P_1, \ldots, P_n) = 0$;

числа D и h, такие, что

$$\max_{1 \leqslant i \leqslant n} \deg P_i \leqslant D, \quad \max_{1 \leqslant i \leqslant n} h(P_i) \leqslant h;$$

простое число p.

Найти: множество целых решений $\overline{\alpha}$ данной системы, имеющих взаимно простые в совокупности координаты и удовлетворяющих условию

$$\exists j \in \overline{0, n} : \nu_p(M_j|_{\overline{\alpha}}) = 0, \tag{2.76}$$

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

или доказать, что таких решений не существует.

1. Положить $S = \emptyset$, $S' = \emptyset$.

2. Для каждого $l = 0, \dots, n$ выполнять следующие действия:

   2.1. Для каждого $i = 1, \dots, n$ положить
   $T_i(y_0, \dots, y_{l-1}, y_{l+1}, y_n) = P_i(\frac{x_0}{x_l}, \dots, \frac{x_{l-1}}{x_l}, 1, \frac{x_{l+1}}{x_l}, \frac{x_n}{x_l})$.

   2.2. Применить алгоритм 1 к системе

   $$\overline{T}(x_0, \dots, x_n) = 0$$

   и числам D, h, p.

   Обозначить результат работы алгоритма 1 через S.

   2.3. Если $S \neq \emptyset$, то для каждого

   $$\overline{\alpha'} = (\frac{a_0}{b_0}, \dots, \frac{a_n}{b_n}) \in S :$$

   2.3.1. Вычислить $b = \text{НОК}(b_0, \dots, b_n)$.
   2.3.2. Положить $\overline{\alpha} = (b\frac{a_0}{b_0}, \dots, b\frac{a_{l-1}}{b_{l-1}}, b, \dots, b\frac{a_{l+1}}{b_{l+1}}, \dots, b\frac{a_n}{b_n})$.
   2.3.3. Положить $S' = S' \cup \{\overline{\alpha}\}$.

3. Если $S' = \emptyset$, то дать ответ, что система

   $$\overline{P}(x_0, \dots, x_n) = 0$$

   не имеет целых решений, удовлетворяющих условию (2.76).

Лемма 21. *Если дифференцируемая функция $F : G \to \mathbb{R}$ локально однородна степени m в области $G \subset \mathbb{R}^n$, то в G выполняется тождество Эйлера:*

$$x_1 \frac{\partial F(x_1, \dots, x_n)}{\partial x_1} + \dots + x_n \frac{\partial F(x_1, \dots, x_n)}{\partial x_n} = mF(x_1, \dots, x_n). \qquad (2.77)$$

Доказательство. См. [8, гл. 8]. □

Теорема 25. *Алгоритм 2.2 находит все решения системы* (2.75)*, принадлежащие* $\mathbb{Z}^n$ *и удовлетворяющие условию* (2.76)*, если они есть, а также выдает ответ, что таких решений нет, если их не существует.*

Доказательство. Выберем произвольный индекс r, такой, что $0 \leqslant r \leqslant n$. Докажем, что на 2-ом шаге алгоритма 2.2 при фиксированном индексе $l = r$ найдутся все целые решения

$$\overline{\alpha} = (t_0, \ldots, t_n)$$

системы (2.75), удовлетворяющие условиям (2.76) и $p \nmid t_r$. Для этого докажем, что из условия (2.76) следует (2.73).

Покажем сначала, что из условия (2.76) следует равенство

$$\nu_p(M_r|_{\overline{\alpha}}) = 0.$$

Заметим, что для любого i, $1 \leqslant i \leqslant n$, многочлены $P_i(x_1, \ldots, x_n)$ является однородными функциями степени $\deg R_i$. Следовательно, к ним можно применить тождество Эйлера для однородных функций. Из формулы (2.77) следует, что для произвольного $1 \leqslant i \leqslant n$

$$x_0 \frac{\partial P_i}{\partial x_0} + \ldots + x_n \frac{\partial P_i}{\partial x_n} = \deg P_i \cdot P_i. \tag{2.78}$$

Подставив в равенство (2.78) вектор α, получим следующее соотношение:

$$t_0 \frac{\partial P_i}{\partial x_0}(\overline{\alpha}) + \ldots + t_n \frac{\partial P_i}{\partial x_n}(\overline{\alpha}) = 0. \tag{2.79}$$

Выразим из равенства (2.79) для каждого i, $1 \leqslant i \leqslant n$, $\dfrac{\partial P_i}{\partial x_j}(\overline{\alpha})$, подставим в матрицу $M'_j|_{\overline{\alpha}}$ и воспользуемся простейшими свойствами определителя матрицы. Получим следующую формулу:

$$t_j M_r|_{\overline{\alpha}} = \pm t_r M_j|_{\overline{\alpha}}. \tag{2.80}$$

По условию, $\nu_p(M_j|_{\overline{\alpha}}) = 0$ и $p \nmid t_r$, таким образом, из формулы (2.80) непосредственно следует, что

$$\nu_p(M_r|_{\overline{\alpha}}) = 0.$$

Докажем теперь от противного, что из условия $\nu_p(M_r|_{\overline{\alpha}}) = 0$ следует выполнение условия (2.73).

Действительно, предположим, что $\nu_p(\det J|_{\overline{\alpha'}}) > 0$, где

$$\overline{\alpha'} = (\frac{a_0}{b_0}, \ldots, \frac{a_n}{b_n}),$$

$$p \nmid b = \text{НОК}(b_0, \ldots, b_r),$$
$$t_0 = \frac{a_0}{b_0}b, \ldots, t_r = b, \ldots, t_n = \frac{a_n}{b_n}b.$$

Но для произвольных $0 \leqslant k \leqslant n$ и $1 \leqslant i \leqslant n$

$$\left.\frac{\partial T_i}{\partial y_k}\right|_{\overline{\alpha'}} = \left.\frac{\partial P_i}{\partial x_k}\right|_{(\frac{a_0}{b_0},\ldots,1,\ldots,\frac{a_n}{b_n})} = b^{\deg P_i} \left.\frac{\partial P_i}{\partial x_k}\right|_{\overline{\alpha}}.$$

Следовательно,

$$\det J|_{\overline{\alpha'}} = b^{\deg P_i} \cdot M_r|_{\overline{\alpha}}.$$

Отсюда, так как по условию $p \nmid b$, получаем $\nu_p(M_r|_{\overline{\alpha}}) > 0$. Получили противоречие с тем, что $\nu_p(M_j|_{\overline{\alpha}}) = 0$ по условию. Таким образом, доказано, что из условия (2.76) следует (2.73), то есть на шаге 2 алгоритма 2.2 корректно применять алгоритм 2.1.

Далее, поскольку в алгоритме 2.2 требуется найти решения с взаимно простыми в совокупности координатами, то все координаты решения не могут делиться на одно и то же простое число p.

То есть, на шаге 2 алгоритма действительно находятся все решения, поскольку последовательно перебираются все возможные случаи:

$$p \nmid t_0;\ p|t_0, p \nmid t_1;\ \ldots;\ p|t_0, \ldots, p|t_{n-1}, p \nmid t_n.$$

Теорема 25 доказана.

□

Список литературы

[1] Бахвалов Н. С., Жидков Н. П., Кобельков Г. М. Численные методы. М: ФМЛ, 2001. 630 с.

[2] Боревич З. И., Шафаревич И. Р. Теория чисел. М: Наука, 1972. 496 с.

[3] ван дер Варден Б. Л. Алгебра. М: Наука, 1976. 649 с.

[4] Василенко О. Н. Теоретико–числовые алгоритмы в криптографии. М: МЦНМО, 2003. 328 с.

[5] Герман О. Н., Нестеренко Ю. В. Теоретико-числовые методы в криптографии. М: Академия, 2012. 272 с.

[6] Зарисский О., Самюэль П., Коммутативная алгебра, т. 1. М: Иностранная литература, 1963. 379 с.

[7] Зарисский О., Самюэль П., Коммутативная алгебра, т. 2. М: Иностранная литература, 1963. 439 с.

[8] Зорич В. А. Математический анализ, т. 1. М: ФАЗИС, 1997. 554 с.

[9] Курош А. Г. Курс высшей алгебры. М: Наука, 1965. 431 с.

[10] Ленг С. Алгебра. М: Мир, 1968. 564 с.

[11] Нестеренко Ю. В. О мере алгебраической независимости значений некоторых функций // Матем. сб. 1985, т. 128, № 170, с. 545–568.

[12] Нестеренко Ю. В. Теория чисел. М: Академия, 2008. 272 с.

[13] Постников М. М. Теория Галуа. М: ГИФМЛ, 1963. 220 с.

[14] Хинчин А. Я. Цепные дроби. М: ГИТТЛ, 1986. 115 с.

[15] Bach E., Shallit J. Algorithmic Number Theory, vol. I: Efficient Algorithms. Cambridge, London: The MIT Press, 1996. 496 p.

[16] Bach E., Sorenson J. Explicit bounds for primes in residue classes // Proceedings of Symposia in Applied Mathematics. 1994, vol. 48, p. 535–539.

[17] Cohen H. A Course in Computational Algebraic Number Theory. — 3., corr. print. Berlin, Heidelberg, New York: Springer, 1996. 545 p.

[18] Cox D. A. Galois Theory. Hoboken: Wiley, 2012. 602 p.

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

[20] Gallagher P. X. The Large Sieve and Probabilistic Galois Theory // Proceedings of Symposia in Pure Mathematics. 1973, vol. 24, p. 91–101.

[21] Hardy G. H., Wright E. M. An Introduction to the Theory of Numbers. Oxford: Oxford University Press, 1985. 438 p.

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

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

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

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

[26] Nesterenko Yu. V. Algebraic Independence. New Delhi, Chennai, Mumbai, Kolkata: Narosa Publishing House, 2009. 165 p.

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

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

Публикации автора

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

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

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