Math-Net.Ru

Общероссийский математический портал

М. Е. Зеленова, Решение полиномиальных систем в целых числах, *Матем. заметки*, 2015, том 98, выпуск 3, 356–371

DOI: <https://doi.org/10.4213/mzm10545>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.237.59.107

26 апреля 2023 г., 16:56:28

Решение полиномиальных систем в целых числах

М. Е. Зеленова

В статье описывается метод нахождения целых решений однородной полиномиальной системы с целыми коэффициентами, имеющей конечное число решений в проективном пространстве над полем комплексных чисел, обладающих определенным свойством.

Библиография: 10 названий.

DOI: 10.4213/mzm10545

1. Введение. Известна задача о нахождении корней уравнений и систем в определенных кольцах или полях.

Часть алгоритмов, решающих данную задачу в конкретных случаях, основана на классическом результате, а именно, лемме Гензеля о подъеме решения полиномиального сравнения (см. [1]). Идея данных алгоритмов состоит в том, что сначала с помощью подъема ищется решение данного уравнения или системы по модулю степени некоторого простого числа, а потом с помощью полученного результата ищется ответ к исходной задаче.

Данная идея была использована, например, в статье [2] для факторизации многочленов с рациональными коэффициентами. Также модифицированный алгоритм подъема был использован автором в статье [3] для нахождения решений полиномиальных уравнений в полях алгебраических чисел.

Известен также алгоритм нахождения рациональных решений целочисленных линейных систем (см. [4]).

В данной статье рассматривается вопрос о нахождении целых решений однородной полиномиальной системы.

Рассмотрим однородную систему уравнений

$$\begin{aligned} P_1(x_0, x_1, \dots, x_m) &= 0, \\ P_2(x_0, x_1, \dots, x_m) &= 0, \\ &\dots\dots\dots \\ P_n(x_0, x_1, \dots, x_m) &= 0, \end{aligned} \tag{1.1}$$

где $P_i \in \mathbb{Z}[x_0, x_1, \dots, x_m]$, $i = 1, \dots, n$, – однородные многочлены.

С ней можно связать неоднородную систему уравнений

$$\begin{aligned} R_1(x_1, \dots, x_m) &= 0, \\ R_2(x_1, \dots, x_m) &= 0, \\ &\dots\dots\dots \\ R_n(x_1, \dots, x_m) &= 0, \end{aligned} \tag{1.2}$$

где $R_i(x_1, \dots, x_m) = P_i(1, x_1, \dots, x_m)$, $i = 1, \dots, n$. Обратно к системе (1.1) можно вернуться, положив

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

Пусть $J = (P_1, \dots, P_n)$ – идеал, порожденный многочленами, задающими левую часть однородной системы (1.1). Тогда нули идеала J совпадают с нулями системы (1.1) в m -мерном проективном пространстве над полем $\mathbb{C}$, а если положить $x_0 = 1$, то и с нулями системы (1.2) в $\mathbb{C}^m$.

Предположим, что система (1.1) имеет конечное число решений в m -мерном проективном пространстве над $\mathbb{C}$, т.е. $\dim J = 0$. Тогда и система (1.2) имеет конечное число решений в $\mathbb{C}^m$. Предположим также, что $n = m$. Предложенный в статье алгоритм позволяет при данных предположениях найти целые решения системы (1.1), обладающие определенным свойством.

2. Основные теоретические сведения. Подробно с теорией, изложенной в данном пункте, можно ознакомиться в книге [5].

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

ОПРЕДЕЛЕНИЕ 1. Идеал I называется *примарным*, если из условий $ab \in I$ и $a \notin I$ следует, что для некоторого $n \in \mathbb{N}$ выполнено $b^n \in I$.

ОПРЕДЕЛЕНИЕ 2. *Радикалом* кольца I называется множество

$$\sqrt{I} = \{a \in \mathbb{Q}[x_0, \dots, x_m] \mid \text{найдется } n \in \mathbb{N}: a^n \in I\}.$$

ЗАМЕЧАНИЕ 1. Если I – примарный идеал, то $\sqrt{I}$ является простым идеалом кольца $\mathbb{Q}[x_0, \dots, x_m]$.

ТЕОРЕМА 1 (существование примарного разложения). *Для любого идеала $I \subset \mathbb{Q}[x_0, \dots, x_m]$ существуют примарные идеалы $I_1, \dots, I_s$ такие, что*

- 1) $I = I_1 \cap \dots \cap I_s$;
- 2) представление из пункта 1) минимально по отношению к s , т.е. ни один из идеалов I_j нельзя из него исключить;
- 3) при $j \neq k$ $\sqrt{I_j} \neq \sqrt{I_k}$.

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 1].

ТЕОРЕМА 2 (единственность примарного разложения). *Предположим, что идеал $I \subset \mathbb{Q}[x_0, \dots, x_m]$ имеет два неприводимых примарных разложения*

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

где $\sqrt{I_j} = \mathfrak{p}_j$, $\sqrt{I'_k} = \mathfrak{p}'_k$, $1 \leq j \leq s$, $1 \leq k \leq t$. Тогда $s = t$, и примарные компоненты можно менять местами таким образом, что $\mathfrak{p}_j = \mathfrak{p}'_j$, $1 \leq j \leq s$. Идеалы $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ называются простыми идеалами, ассоциированными с I .

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 1].

ОПРЕДЕЛЕНИЕ 3. Пусть $\mathfrak{p}$ – однородный простой идеал. Тогда *проективная размерность* $\mathfrak{p}$ определяется как $\dim \mathfrak{p} = \text{tr. deg}(\mathbb{Q}[x_0, \dots, x_m]/\mathfrak{p}) - 1$. Если I – однородный идеал с ассоциированными простыми идеалами $\mathfrak{p}_1, \dots, \mathfrak{p}_s$, то $\dim I$ определяется следующим образом:

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

ОПРЕДЕЛЕНИЕ 4. Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ – все простые идеалы, ассоциированные с I . Идеал I называется *несмешанным*, если $\dim \mathfrak{p}_j = \dim I$ для всех $1 \leq j \leq s$.

ОПРЕДЕЛЕНИЕ 5. Пусть $I \subset \mathbb{Q}[x_0, \dots, x_m]$ – однородный несмешанный идеал. Для произвольного целого числа r , $1 \leq r \leq m$, и переменных $u_{i,j}$, $1 \leq i \leq r$, $0 \leq j \leq m$, определим *линейные формы*

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

Обозначим через $\bar{I}(r)$ множество всех многочленов G , принадлежащих кольцу $\mathbb{Q}[u_{1,0}, \dots, u_{r,m}]$, таких, что $Gx_i^M \in (I, L_1, \dots, L_r)$ при $0 \leq i \leq m$, где M – некоторое натуральное число.

ТЕОРЕМА 3. Пусть I – однородный несмешанный идеал кольца $\mathbb{Q}[x_0, \dots, x_m]$ и $\dim I = r - 1$. Пусть $I = I_1 \cap \dots \cap I_t$ – неприводимое примарное разложение I , $\sqrt{I_j} = \mathfrak{p}_j$ и k_j – показатель I_j , где $1 \leq j \leq t$. Тогда $\bar{I}(r)$ – главный идеал кольца $\mathbb{Q}[u_{1,0}, \dots, u_{r,m}]$, и, если обозначить $\bar{\mathfrak{p}}_j = (F_j)$, то все F_j неприводимы, и $F = F_1^{k_1} \dots F_s^{k_s}$ – порождающий элемент идеала $\bar{I}(r)$.

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 2].

ОПРЕДЕЛЕНИЕ 6. Для любого однородного несмешанного идеала I , где $I \subset \mathbb{Q}[x_0, \dots, x_m]$, многочлен $F \in \mathbb{Q}[u_{1,0}, \dots, u_{r,m}]$ такой, что $\bar{I}(r) = (F)$, называется *ассоциированной формой идеала I* .

ОПРЕДЕЛЕНИЕ 7. Логарифмической высотой многочлена $P = \sum a_{\vec{\gamma}} T_1^{\gamma_1} \dots T_m^{\gamma_m} \in \mathbb{Q}[T_1, \dots, T_m]$ 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 $|\cdot|_v$ на поле $\mathbb{Q}$ (т.е. в данном случае $\mathcal{M}$ состоит из всех простых чисел и ∞), а $|P|_v = \max_{\vec{\gamma}} |a_{\vec{\gamma}}|_v$.

ЗАМЕЧАНИЕ 2. Если многочлен $P \in \mathbb{Z}[T_1, \dots, T_m]$ и имеет взаимно простые в совокупности коэффициенты, то $h(P) = \log |P|_{\mathbb{C}}$.

ОПРЕДЕЛЕНИЕ 8. Пусть $I \in \mathbb{Q}[x_0, \dots, x_m]$ – однородный несмешанный идеал, $r = \dim I + 1$ и $\bar{I}(r) = (F)$. Тогда *степенью и логарифмической высотой идеала I* называются величины $\deg I = \deg_{\bar{u}_1} F$ и $h(I) = h(F)$ соответственно.

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

ДОКАЗАТЕЛЬСТВО. См. [6; гл. 7 § 7].

ЛЕММА 2. Пусть $P \in \mathbb{Q}[x_0, \dots, x_m]$ – однородный многочлен и $I = (P)$. Тогда

- 1) $\deg I = \deg P$;
- 2) $h(I) \leq h(P) + m^2 \deg P$.

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 5].

ЛЕММА 3. Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ – простые однородные идеалы кольца $\mathbb{Q}[x_0, \dots, x_m]$, а $Q_1, \dots, Q_t \in \mathbb{Q}[x_0, \dots, x_m]$ – однородные многочлены, такие, что при $1 \leq j \leq t$ выполнены условия $Q_j \notin \mathfrak{p}_j$, $\deg Q_j \leq D$, $h(Q_j) \leq h$. Тогда существует однородный многочлен $Q \in \mathbb{Q}[x_0, \dots, x_m]$ такой, что $Q \notin \mathfrak{p}_j$, $1 \leq j \leq t$, и

$$\deg Q = D, \quad h(Q) \leq h + 2 \ln t.$$

ДОКАЗАТЕЛЬСТВО. Обозначим через S_i некоторый одночлен вида $x_0^{k_0} \dots x_m^{k_m}$, где $k_i \in \mathbb{Z}_+$, $\deg S_i = D - \deg Q_i$ и $S_i \notin \mathfrak{p}_i$. Докажем теперь индукцией по l , $1 \leq l \leq t$, что существуют целые числа $\lambda_1, \dots, \lambda_l$, $0 \leq \lambda_j \leq j$, такие, что

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

Докажем сначала базу индукции. Действительно, при $l = 1$ положим $\lambda_1 = 1$. Пусть теперь $l \geq 2$, и доказано существование целых чисел $\lambda_1, \dots, \lambda_{l-1}$. Пусть

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

Тогда существует не более одного λ такого, что $Q_0 + \lambda S_l Q_l \in \mathfrak{p}_l$ и не более $l - 1$ чисел λ таких, что

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

Следовательно, среди $l + 1$ чисел $0, 1, \dots, l$ найдется число λ_l такое, что

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

Положим

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

Видно, что построенный многочлен Q удовлетворяет условиям леммы 3.

ЛЕММА 4. Пусть $\mathfrak{a}$ – несмешанный однородный идеал кольца $\mathbb{Q}[x_0, \dots, x_m]$. Пусть $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_t$ – неприводимое примарное разложение идеала $\mathfrak{a}$, $\sqrt{\mathfrak{a}_i} = \mathfrak{p}_i$ и k_i – показатель $\mathfrak{a}_i$, $1 \leq i \leq t$. Тогда

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

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 4].

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

ЛЕММА 5. Пусть $\mathfrak{a}$ – это однородный несмешанный идеал кольца $\mathbb{Q}[x_0, \dots, x_m]$, $\dim \mathfrak{a} = r - 1$. Пусть $Q \in \mathbb{Q}[x_0, \dots, x_m]$ – однородный многочлен, не содержащийся ни в каком простом идеале, ассоциированном с $\mathfrak{a}$. Тогда при $r \geq 2$ существует однородный несмешанный идеал I кольца $\mathbb{Q}[x_0, \dots, x_m]$, $\dim I = r - 2$, удовлетворяющий условиям

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

ДОКАЗАТЕЛЬСТВО. См. [7; лемма 11].

ТЕОРЕМА 4. Пусть D – натуральное число, h – действительное. Пусть $\mathfrak{a}, \mathfrak{b} = (P_1, \dots, P_n) \subset \mathbb{Q}[x_0, \dots, x_m]$ – однородные идеалы, причем $\mathfrak{a}$ несмешан, $\mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(\mathfrak{a})$, $p = \dim \mathfrak{a} \geq r = \dim \mathfrak{b}$, $\deg \mathfrak{a} \leq D^{m-p}$, P_i однородны и

$$\deg P_i \leq D, \quad h(P_i) \leq h.$$

Тогда существует однородный несмешанный идеал $I \subset \mathbb{Q}[x_0, \dots, x_m]$ такой, что $\dim I = \dim \mathfrak{b}$ и

- 1) $\deg I \leq \deg \mathfrak{a} \cdot D^{p-r}$;
- 2) $h(I) \leq ((p-r) \deg \mathfrak{a} \cdot h + D \cdot h(\mathfrak{a}) + 6m^2(p-1) \deg \mathfrak{a} \cdot D) D^{p-r-1}$;
- 3) $\mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(I)$.

ЗАМЕЧАНИЕ 3. При $\dim \mathfrak{a} = m$ следует считать $\deg \mathfrak{a} = 1$, $h(\mathfrak{a}) = 0$.

ДОКАЗАТЕЛЬСТВО. 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 выполняться. Следовательно, первый случай невозможен.

Рассмотрим теперь второй случай: $\dim \mathfrak{a} > \dim \mathfrak{b}$ и, в свою очередь, разобьем его на два подслучая: $\dim \mathfrak{a} = m$ и $1 \leq \dim \mathfrak{a} \leq m - 1$.

Если $\dim \mathfrak{a} = m$, то положим $I = (P)$, где P – один из ненулевых многочленов P_i . Тогда согласно лемме 1 I – несмешанный идеал, и $\dim I = m - 1 < \dim \mathfrak{a}$. По лемме 2

$$\deg I = \deg P \leq D, \quad h(I) \leq h(P) + m^2 \deg P \leq h + m^2 D;$$

следовательно, в данном случае идеал I удовлетворяет утверждениям теоремы.

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

Применим лемму 3 к многочленам $Q_1, \dots, Q_t$ и идеалам $\mathfrak{p}_1, \dots, \mathfrak{p}_t$. Они удовлетворяют условиям леммы; следовательно, существует однородный многочлен $Q \in \mathbb{Q}[x_0, \dots, x_m]$, удовлетворяющий условиям $Q \notin \mathfrak{p}_j$, $1 \leq j \leq t$, а также

$$\deg Q = D \quad \text{и} \quad h(Q) \leq h + 2 \ln t.$$

Тогда по лемме 4

$$t \leq \sum_{i=1}^t k_i \deg \mathfrak{p}_i = \deg \mathfrak{a} \leq D^{m-p}$$

и, следовательно,

$$h(Q) \leq h + 2(m-p) \ln D.$$

Применим теперь лемму 5 к идеалу $\mathfrak{a}$ и многочлену Q . Полученный в лемме 5 идеал J должен иметь размерность $\dim J = \dim \mathfrak{a} - 1$ и удовлетворять условиям

$$\begin{aligned} \deg J &\leq \deg \mathfrak{a} \deg Q \leq D^{m-p} \cdot D = D^{m+1-p}, \\ h(J) &\leq h(\mathfrak{a}) \deg Q + h(Q) \deg \mathfrak{a} + 4m^2 \deg Q \deg \mathfrak{a}. \end{aligned}$$

Предположим теперь, что $\dim \mathfrak{a} = \dim \mathfrak{b} + 1$. Тогда $\dim J = \dim \mathfrak{b}$, а для J будут выполняться все утверждения теоремы 4; 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 4 не выполняется, теорема верна для идеалов J и $\mathfrak{b}$. Следовательно, существует несмешанный однородный идеал I , $\dim I = \dim \mathfrak{b}$, такой, что

$$\begin{aligned} \deg I &\leq \deg J \cdot D^{\dim J - \dim \mathfrak{b}} \leq \deg J \cdot D^{p-1-r} \\ &\leq \deg \mathfrak{a} \deg Q \cdot D^{p-1-r} = \deg \mathfrak{a} \cdot D^{p-r}, \\ h(I) &\leq ((p-r-1) \deg J \cdot h + D \cdot h(J) + 6m^2(p-2) \deg J \cdot D) \cdot D^{p-r-2} \\ &\leq ((p-r-1) \deg \mathfrak{a} \cdot Dh + D \cdot (h(\mathfrak{a})D + (h + 2 \ln t) \deg \mathfrak{a} + 2(m-p) \ln D) \\ &\quad + 6m^2(p-2) \deg \mathfrak{a} \cdot D^2) D^{p-r-2} \\ &\leq ((p-r-1) \deg \mathfrak{a} \cdot h + D \cdot h(\mathfrak{a}) + h \cdot \deg \mathfrak{a} + 2(m-p) \deg \mathfrak{a} + 2(m-p) \ln D \\ &\quad + 6m^2(p-2) \deg \mathfrak{a} \cdot D) D^{p-r-1} \\ &\leq ((p-r) \deg \mathfrak{a} \cdot h + D \cdot h(\mathfrak{a}) + 6m^2(p-1) \deg \mathfrak{a} \cdot D) D^{p-r-1}. \end{aligned}$$

Кроме того, $\mathfrak{R}(\mathfrak{b}) \subset \mathfrak{R}(I)$. Таким образом, для идеала I выполняются все условия теоремы 4, что противоречит исходному предположению о том, что для идеала $\mathfrak{a}$ теорема 4 неверна.

3. Оценка модуля решений системы. В данном пункте оцениваются модули решений систем (1.1) и (1.2) через максимумы степеней и логарифмических высот исходных многочленов системы.

ТЕОРЕМА 5. Пусть $\mathfrak{p} \subset \mathbb{Q}[x_0, \dots, x_m]$ — это однородный простой идеал, $r = 1 + \dim \mathfrak{p} \geq 1$, $x_0 \notin \mathfrak{p}$ и $\bar{\mathfrak{p}}(r) = (F) \in \mathbb{Q}[u_{1,0}, \dots, u_{r,m}]$. Тогда

- 1) существует конечное нормальное расширение $\mathfrak{L}_1 \supset \mathbb{Q}[u_{1,0}, \dots, u_{r-1,m}]$ такое, что

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

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

- 2) каждая точка $\bar{\alpha}^{(j)} = (1 : \alpha_1^{(j)} : \dots : \alpha_m^{(j)}) \in \mathbb{P}_{\mathfrak{L}_1}^m$, $j = 1, \dots, g$ является общей точкой идеала $\mathfrak{p}$, т.е. для любого однородного многочлена $Q \in \mathbb{Q}[x_0, \dots, x_m]$ $Q \in \mathfrak{p}$ тогда и только тогда, когда $Q(\bar{\alpha}^{(j)}) = 0$.

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 6].

ТЕОРЕМА 6. Пусть $P_1, \dots, P_s \in \mathbb{Q}[T_1, \dots, T_m]$ и $P = P_1 \cdots P_s$. Тогда

- 1) $h(P) \leq h(P_1) + \dots + h(P_s) + m \deg P$;
- 2) $h(P_1) + \dots + h(P_s) \leq h(P) + \sum_{i=1}^m \deg_{T_i} P$.

ДОКАЗАТЕЛЬСТВО. См. [5; гл. 5 § 4].

ТЕОРЕМА 7. Верны следующие оценки:

$$\ln \max_{0 \leq k \leq m} |\alpha_k^{(j)}| \leq (mh + 6m^2(m-1)D)D^{m-1} + mD^m \quad \text{и} \quad g \leq D^m,$$

где $\bar{\alpha}^{(1)}, \dots, \bar{\alpha}^{(g)}$ – все решения системы (1.1) и $\bar{\alpha}^{(j)} = (\alpha_0^{(j)}, \dots, \alpha_m^{(j)})$.

Если $\bar{\alpha} = (a_1/b_1, \dots, a_m/b_m)$ – рациональное решение системы (1.2), то верна оценка

$$\max \left\{ \ln \max_{1 \leq k \leq m} |a_k|, \ln \max_{1 \leq k \leq m} |b| \right\} \leq (mh + 6m^2(m-1)D)D^{m-1} + mD^m,$$

где $b = \text{НОК}(b_1, \dots, b_m)$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим систему (1.1) и идеал $J = (P_1, \dots, P_n)$. Напомним, что согласно предположению $\dim J = 0$.

Предположим, что

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

Применим теорему 4 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) $\deg I \leq D^m$;
- 2) $h(I) \leq (mh + 6m^2(m-1)D)D^{m-1}$;
- 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 выбрать с точностью до константы, будем считать, что $F \in \mathbb{Z}[u_0, \dots, u_m]$ и имеет взаимно простые в совокупности коэффициенты.

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

$$h(F) \leq (mh + 6m^2(m-1)D)D^{m-1}.$$

По теореме 3 $I = I_1 \cap \dots \cap I_t$, где все I_i – примарные идеалы, $\mathfrak{p}_i$ – соответствующие радикалы, k_i – показатели I_i и $\bar{\mathfrak{p}}_i = (F_i)$. Тогда $F = F_1^{k_1} \dots F_t^{k_t}$. При этом $\dim I_i = 0$ при $i = 1, \dots, t$, поскольку $\dim I = 0$.

Применим к идеалу $\mathfrak{p}_i$ для каждого $i = 1, \dots, t$ теорему 5. Многочлен F имеет целые коэффициенты; следовательно, $F_i \in \mathbb{Z}[u_0, \dots, u_m]$, и согласно теореме 5 можно выбрать F_i следующим образом:

$$F_i = a_i \prod_{j=g_{i-1}}^{g_i} (\alpha_0^{(j)} u_0 + \dots + \alpha_m^{(j)} u_m) = L_{g_{i-1}} \dots L_{g_i}, \quad a_i \in \mathbb{Z}, \quad g_0 = 1, \quad g_t = g. \quad (3.1)$$

Таким образом,

$$F = (L_1 \dots L_{g_1})^{k_1} \dots (L_{g_{t-1}} \dots L_g)^{k_t} = W_1 \dots W_w,$$

где каждый из многочленов W_j , $j = 1, \dots, w$ совпадает с одним из многочленов $L_1, \dots, L_g$. Тогда, по теореме 6, учитывая, что $\alpha_0^{(j)} = 1$, получим

$$\begin{aligned} \max_{0 \leq k \leq m} |\alpha_k^{(j)}| &\leq \prod_{j=1}^g \max_{0 \leq k \leq m} |\alpha_k^{(j)}| \leq \prod_{j=1}^g \max |\text{коэф. } L_j| \\ &\leq \prod_{j=1}^w \max |\text{коэф. } W_j| \leq e^{h(F) + m \deg F}. \end{aligned} \quad (3.2)$$

Таким образом,

$$\ln \max_{0 \leq k \leq m} |\alpha_k^{(j)}| \leq (mh + 6m^2(m-1)D)D^{m-1} + mD^m,$$

а само количество корней не превосходит D^m .

Докажем теперь второе утверждение теоремы. Пусть у системы (1.2) существует рациональное решение $\bar{\alpha} = (a_1/b_1, \dots, a_m/b_m)$, где $(a_k, b_k) = 1$, $1 \leq k \leq m$. Отсюда следует, что у системы (1.1) есть решение $\bar{\alpha}^{(l)} = (1, \alpha_1^{(l)}, \dots, \alpha_m^{(l)})$, где $\alpha_j^{(l)} = a_j/b_j$, $1 \leq j \leq m$, или, что то же самое,

$$\bar{\alpha}^{(l)} = \left(b, \frac{b}{b_1} a_1, \dots, \frac{b}{b_m} a_m \right), \quad \text{где} \quad \frac{b}{b_k} a_k \in \mathbb{Z}, \quad \left(b, \frac{b}{b_1} a_1, \dots, \frac{b}{b_m} a_m \right) = 1.$$

Согласно теореме 5 $\bar{\alpha}^{(l)}$ является корнем многочлена F_i для некоторого $1 \leq i \leq t$. Напомним, что $F_i \in \mathbb{Z}[u_0, \dots, u_m]$ и имеет взаимно простые в совокупности коэффициенты, а также, согласно формуле (3.1)

$$F_i = L_{g_{i-1}} \dots L_{g_i},$$

где для любого j , $g_{i-1} \leq j \leq g_i$, $L_j \in \mathbb{Z}[u_0, \dots, u_m]$, имеет взаимно простые в совокупности коэффициенты, и L_j имеет вид $L_j = qu_0 + p_1 u_1 + \dots + p_m u_m$, где $(q, p_1, \dots, p_m)$ – решение системы (1.1) и $(q, p_1, \dots, p_m) = 1$. Следовательно, существует индекс r , $g_{i-1} \leq r \leq g_i$, для которого верно следующее:

$$L_r = bu_0 + \frac{b}{b_1} a_1 u_1 + \dots + \frac{b}{b_m} a_m u_m.$$

Согласно формуле (3.2)

$$\begin{aligned} \max |\text{коэф. } L_r| &\leq \prod_{j=1}^g \max |\text{коэф. } L_j| \leq \prod_{j=1}^w \max |\text{коэф. } W_j| \\ &\leq e^{h(F)+m \deg F} \leq e^{(mh+6m^2(m-1)D)D^{m-1}+mD^m}. \end{aligned} \quad (3.3)$$

Таким образом, мы показали, что

$$\begin{aligned} |b| &\leq e^{(mh+6m^2(m-1)D)D^{m-1}+mD^m}, \\ |a_j| &\leq \left| \frac{b}{b_j} a_j \right| \leq e^{(mh+6m^2(m-1)D)D^{m-1}+mD^m}, \quad 1 \leq j \leq m. \end{aligned}$$

4. Нахождение решения неоднородной системы по модулю степени простого числа. Положим $m = n$. Введем следующие обозначения:

$$\bar{R} = \begin{pmatrix} R_1 \\ R_2 \\ \dots \\ R_n \end{pmatrix}, \quad \bar{\delta}_k = \begin{pmatrix} \delta_{k,1} \\ \delta_{k,2} \\ \dots \\ \delta_{k,n} \end{pmatrix}, \quad A_k = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\bar{\delta}_k) & \dots & \frac{\partial R_1}{\partial x_n}(\bar{\delta}_k) \\ \dots & \dots & \dots \\ \frac{\partial R_n}{\partial x_1}(\bar{\delta}_k) & \dots & \frac{\partial R_n}{\partial x_n}(\bar{\delta}_k) \end{pmatrix},$$

где $k = 0, 1, 2, \dots$.

Пусть p – простое число, не делящее $\det A_0$. Пусть также $\bar{\delta}_0$ – вектор, удовлетворяющий условию $\bar{R}(\bar{\delta}_0) \equiv 0 \pmod{p}$, а C_0 – матрица, такая, что $A_0 C_0 \equiv E \pmod{p}$. Зададим $\bar{\delta}_k$ и C_k , где $k \in \mathbb{N}$, следующими формулами:

$$\bar{\delta}_k \equiv \bar{\delta}_{k-1} - C_{k-1} \cdot \bar{R}(\bar{\delta}_{k-1}) \pmod{p^{2^k}}, \quad \text{где} \quad \max_{1 \leq i \leq n} |\delta_{k,i}| \leq \frac{p^{2^k}}{2}, \quad (4.1)$$

$$C_k \equiv 2C_{k-1} - C_{k-1} A_k C_{k-1} \pmod{p^{2^k}}, \quad \text{где} \quad \max |\text{элементы } C_k| \leq \frac{p^{2^k}}{2}. \quad (4.2)$$

ТЕОРЕМА 8. При любом $k \in \mathbb{Z}$, $k \geq 0$ выполняются следующие сравнения:

$$A_k C_k \equiv E \pmod{p^{2^k}}, \quad \bar{R}(\bar{\delta}_k) \equiv 0 \pmod{p^{2^k}}.$$

ДОКАЗАТЕЛЬСТВО. Проведем доказательство индукцией по k . При $k = 0$ теорема верна по построению C_0 и $\bar{\delta}_0$. Пусть теперь $k > 0$ и требуемые сравнения выполнены для всех $i < k$. Таким образом,

$$A_{k-1} C_{k-1} \equiv E \pmod{p^{2^{k-1}}}, \quad \bar{R}(\bar{\delta}_{k-1}) \equiv 0 \pmod{p^{2^{k-1}}}.$$

Заметим, что $A_{k-1} \equiv A_k \pmod{p^{2^{k-1}}}$, поскольку из формулы (4.1) и индуктивного предположения следует, что $\bar{\delta}_{k-1} \equiv \bar{\delta}_k \pmod{p^{2^{k-1}}}$, а значит, и

$$\frac{\partial R_m}{\partial x_l}(\bar{\delta}_{k-1}) \equiv \frac{\partial R_m}{\partial x_l}(\bar{\delta}_k) \pmod{p^{2^{k-1}}}.$$

Следовательно, $A_k C_{k-1} \equiv E \pmod{p^{2^{k-1}}}$ и $(A_k C_{k-1} - E)^2 \equiv 0 \pmod{p^{2^k}}$.

Из данного равенства, используя формулу (4.2), предположение индукции, вытекает, что

$$\begin{aligned}(A_k C_{k-1} - E)^2 &= A_k C_{k-1} A_k C_{k-1} - 2A_k C_{k-1} + E \\ &= A_k (C_{k-1} A_k C_{k-1} - 2C_{k-1}) + E \equiv -A_k C_k + E \equiv 0 \pmod{p^{2^k}}.\end{aligned}$$

Также выполняется следующая цепочка сравнений по модулю p^{2^k} :

$$\begin{aligned}\bar{R}(\bar{\delta}_k) &\equiv \bar{R}(\bar{\delta}_{k-1} - C_{k-1} \cdot \bar{R}(\bar{\delta}_{k-1})) \equiv \bar{R}(\bar{\delta}_{k-1}) - A_{k-1} C_{k-1} \bar{R}(\bar{\delta}_{k-1}) \\ &\equiv (E - A_{k-1} C_{k-1}) \bar{R}(\bar{\delta}_{k-1}) \equiv 0 \pmod{p^{2^k}},\end{aligned}$$

так как по предположению индукции для любых $1 \leq j, l \leq n$

$$R_j(\bar{\delta}_{k-1}) \cdot R_l(\bar{\delta}_{k-1}) \equiv 0 \pmod{(p^{2^{k-1}})^2 = p^{2^k}}.$$

5. Нахождение рационального решения неоднородной системы. Положим

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

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

Пусть $\bar{\alpha} = (\alpha_1, \dots, \alpha_n) = (a_1/b_1, \dots, a_n/b_n)$ – одно из рациональных решений системы (1.2), удовлетворяющее условию $p \nmid b = \text{НОК}(b_1, \dots, b_n)$. Согласно результатам, полученным в п. 3,

$$\max_{1 \leq k \leq n} |a_k| \leq C, \quad |b| \leq C. \quad (5.1)$$

Пусть V – некоторая константа, определенная ниже.

Заметим, что, поскольку $\bar{\alpha}$ – рациональное решение системы (1.2) и $p \nmid b$, найдется вектор $\bar{\delta}_0$ такой, что $\bar{R}(\bar{\delta}_0) \equiv 0 \pmod{p}$ и $\bar{\delta}_0 \equiv \bar{\alpha} \pmod{p}$. Для данного $\bar{\delta}_0$ вычислим $\bar{\delta}_V$ по формуле (4.1).

Введем следующее обозначение:

$$r = \min_{1 \leq i \leq n} \nu_p(\alpha_i - \delta_{V,i}).$$

Заметим, что согласно вышеизложенному $r > 0$.

Разложим в ряд Тейлора функции R_i , $1 \leq i \leq n$, в окрестности точки $\bar{\delta}_V$. Получим следующее выражение:

$$-R_i(\bar{\delta}_V) = R_i(\bar{\alpha}) - R_i(\bar{\delta}_V) = \sum_{j=1}^n \frac{\partial R_i}{\partial x_j}(\bar{\delta}_V)(\alpha_j - \delta_{V,j}) + R'_i, \quad (5.2)$$

где

$$R'_i = \sum_{j,k=1}^n \frac{\partial R_i}{\partial x_j} \frac{\partial R_i}{\partial x_k}(\bar{\delta}_V)(\alpha_j - \delta_{V,j})(\alpha_k - \delta_{V,k}) + \dots,$$

$R'_i \in \mathbb{Z}[x_1, \dots, x_n]$ и $\nu_p(R'_i) \geq 2r$.

Из формулы (5.2) следует, что

$$\bar{R}(\bar{\delta}_V) = A_V(\bar{\delta}_V - \bar{\alpha}) + \bar{R}', \quad \text{где } \nu_p(\bar{R}') \geq 2r.$$

Следовательно,

$$C_V \cdot \bar{R}(\bar{\delta}_V) \equiv (\bar{\delta}_V - \bar{\alpha}) + C_V \cdot \bar{R}' \equiv 0 \pmod{p^{2^V}}.$$

Значит, $r \geq \min(2r, 2^V)$. Таким образом,

$$r \geq 2^V, \quad \bar{\alpha} \equiv \bar{\delta}_V \pmod{p^{2^V}}.$$

ЗАМЕЧАНИЕ 4. Если требуется найти $\bar{\alpha}'$ – целое решение системы (1.2), удовлетворяющее условию $\bar{\alpha}' \equiv \bar{\delta}_0 \pmod{p}$, то либо $\bar{\alpha}' = \bar{\delta}_V$, где $V = \lfloor \log_2(\log_p(2C)) \rfloor + 1$, либо такого решения не существует.

ДОКАЗАТЕЛЬСТВО. Оценим норму вектора разности $\bar{\alpha}'$ и $\bar{\delta}_V$:

$$\max_{1 \leq i \leq n} |\alpha_i - \delta_{V,i}| \leq \max_{1 \leq i \leq n} |\alpha_i| + \max_{1 \leq i \leq n} |\delta_{V,i}| \leq C + \frac{p^{2^V}}{2} < p^{2^V}.$$

Но разность $\bar{\alpha}' - \bar{\delta}_V$ – целочисленный вектор, делящийся на p^{2^V} . Следовательно, $\bar{\alpha} = \bar{\delta}_V$.

ТЕОРЕМА 9. Пусть s, h – целые числа. Предположим, что существуют целые числа f и g такие, что

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

где λ – положительный корень уравнения $\lambda^2 + \lambda - 1 = 0$. Пусть $w_i/v_i, i = 1, 2, \dots$, – подходящие дроби к s/h . Положим $u_i = v_i s - w_i h$. Тогда $f/g = u_k/v_k$, где k – наименьшее целое число, для которого выполняется неравенство $|u_k| < \sqrt{h}$.

ЗАМЕЧАНИЕ 5. Доказательство теоремы 9 можно найти в статье [4]. 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 [1] и [8].

УТВЕРЖДЕНИЕ 1. Все подходящие дроби несократимы.

ДОКАЗАТЕЛЬСТВО. См. [8; теорема 11].

УТВЕРЖДЕНИЕ 2. Знаменатели подходящих дробей образуют строго возрастающую последовательность.

ДОКАЗАТЕЛЬСТВО. См. [8; гл. 1 § 4].

УТВЕРЖДЕНИЕ 3. Пусть $\gamma = [c_0; c_1, c_2, \dots]$ – конечная или бесконечная цепная дробь с целыми элементами, причем для $n \geq 1$ выполняется неравенство $c_n \geq 1$, а для конечной дроби ее последнее неполное частное больше 1. Тогда для любых двух соседних подходящих дробей к γ имеем

$$|q_{n-1}\gamma - p_{n-1}| > |q_n\gamma - p_n|, \quad n \geq 0.$$

ДОКАЗАТЕЛЬСТВО. См. [1; теорема 8.3].

УТВЕРЖДЕНИЕ 4. Всякая несократимая рациональная дробь f/g , удовлетворяющая неравенству

$$\left| \gamma - \frac{f}{g} \right| < \frac{1}{2g^2},$$

есть подходящая дробь числа γ .

ДОКАЗАТЕЛЬСТВО. См. [8; теорема 19].

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 9. Поскольку $gs \equiv f \pmod{h}$, для некоторого $t \in \mathbb{Z}$ выполняется равенство $f = gs - th$. Тогда разность $|s/h - t/g|$ можно оценить следующим образом:

$$\left| \frac{s}{h} - \frac{t}{g} \right| = \left| \frac{f}{hg} \right| = \left| \frac{fg}{hg^2} \right| \leq \left| \frac{\lambda^2 h}{hg^2} \right| < \frac{1}{2g^2}.$$

То есть для чисел s/h и t/g выполняются условия утверждения 4, и, таким образом, t/g является некоторой подходящей дробью числа s/h . Обозначим $t/g = w_j/v_j$. Докажем, что $j = k$, где k – число, определенное в условии теоремы 9.

Из утверждения 1 следует, что $(w_j, v_j) = 1$. Но $w_j/v_j = t/g$; следовательно, $t = zw_j$, $g = zv_j$, где $z \in \mathbb{N}$. Следовательно,

$$|f| = |gs - th| = z|v_j s - w_j h| = z|u_j| \geq |u_j|.$$

Таким образом, $|u_j| \leq \lambda\sqrt{h} < \sqrt{h}$. Согласно утверждению 3 последовательность $\{u_i\}$ убывает, а k – наименьший индекс, обладающий свойством $|u_k| < \sqrt{h}$; следовательно, $j \geq k$.

С другой стороны, $u_j = v_j s - w_j h$, а $u_k = v_k s - w_k h$, откуда следует, что

$$u_j v_k - u_k v_j = (w_k v_j - w_j v_k) h \equiv 0 \pmod{h}.$$

При этом, согласно утверждению 2 $v_k \leq v_j$. Также, по доказанному ранее, $|v_j| \leq z|v_j| = |g| \leq \lambda\sqrt{h}$. Следовательно,

$$|u_j v_k - u_k v_j| \leq (|u_j| + |u_k|)|v_j| < (\lambda\sqrt{h} + \sqrt{h})\lambda\sqrt{h} = \lambda(\lambda + 1)h = h.$$

Таким образом, $u_j v_k = u_k v_j$, и $w_j v_k = w_k v_j$. Т.е.

$$\frac{w_j}{v_j} = \frac{w_k}{v_k}, \quad \frac{f}{g} = \frac{sv_k - hw_k}{v_k} = \frac{u_k}{v_k}.$$

ЗАМЕЧАНИЕ 6. Если требуется найти $\bar{\alpha} = (a_1/b_1, \dots, a_n/b_n)$ – рациональное решение системы (1.2), удовлетворяющее условию $\bar{\alpha} \equiv \bar{\delta}_0 \pmod{p}$ и $p \nmid b$, то либо $a_i/b_i = f_k/g_k$, где f_k и g_k выбираются согласно условиям теоремы 9, а $h = p^{2^V}$, где $V = \lfloor \log_2 \log_p(C^2/\lambda^2) \rfloor + 1$, либо такого решения не существует.

ДОКАЗАТЕЛЬСТВО. Согласно результатам, полученным в п. 3, при условии $\bar{\alpha} \equiv \bar{\delta}_0 \pmod{p}$ и $p \nmid b$ выполняется сравнение $\bar{\alpha} \equiv \bar{\delta}_V \pmod{p^{2^V}}$. Кроме того, при выборе $V = \lfloor \log_2 \log_p(C^2/\lambda^2) \rfloor + 1$ верно неравенство $h = p^{2^V} \geq (C^2/\lambda^2)$, т.е. $C \leq \lambda\sqrt{h}$, а из результатов, полученных в п. 3, известно, что $\max_{1 \leq i \leq n} |a_i| \leq C$ и $\max_{1 \leq i \leq n} |b_i| \leq C$. То есть выполняются все условия теоремы 9.

6. Алгоритм. Алгоритм 1. Дано:
система уравнений

$$\begin{aligned} R_1(x_1, \dots, x_n) &= 0, \\ R_2(x_1, \dots, x_n) &= 0, \\ &\dots\dots\dots \\ R_n(x_1, \dots, x_n) &= 0, \end{aligned} \quad (6.1)$$

где $R_i \in \mathbb{Z}[x_1, \dots, x_n]$, $i = 1, \dots, n$ и $\dim(P_1, \dots, P_n) = 0$ ($\bar{P}(x_0, \dots, x_m) = 0$ – соответствующая однородная система);
числа D и h , такие, что $\max_{1 \leq i \leq n} \deg R_i \leq D$, $\max_{1 \leq i \leq n} h(R_i) \leq h$;
простое число p .

Найти: множество решений $\bar{\alpha} = (a_1/b_1, \dots, a_n/b_n)$ данной системы в $\mathbb{Q}^n$, удовлетворяющих условиям $p \nmid b = \text{НОК}(b_1, \dots, b_n)$ и

$$\nu_p(\det J|_{\bar{\alpha}}) = 0, \quad \text{где} \quad J = \begin{pmatrix} \frac{\partial R_1}{\partial x_1} & \dots & \frac{\partial R_1}{\partial x_n} \\ \dots\dots\dots \\ \frac{\partial R_n}{\partial x_1} & \dots & \frac{\partial R_n}{\partial x_n} \end{pmatrix}, \quad (6.2)$$

или доказать, что таких решений не существует.

1. Положить $S' = \emptyset$.
2. Найти все решения системы сравнений $\bar{R}(x_1, \dots, x_n) \equiv 0 \pmod{p}$ 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 $\bar{\delta} \in \mathbb{Z}^n$ таких, что $\bar{R}(\bar{\delta}) \equiv 0 \pmod{p}$ для каждого $\bar{\delta} \in S$. Выбрать $\bar{\delta}$ так, чтобы выполнялось неравенство $\max_{1 \leq i \leq n} |\delta_{0,i}| \leq p/2$.
3. Вычислить $C = \exp((nh + 6n^2(n-1)D)D^{n-1} + 2nD^n)$.
4. Вычислить $V = \lfloor \log_2 \log_p(C^2/\lambda^2) \rfloor + 1$.
5. Для каждого $\bar{\delta} \in S$ выполнять следующие действия:
 - 5.1. положить $\bar{\delta}_0 = \bar{\delta}$;
 - 5.2. вычислить матрицу

$$A_0 = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\bar{\delta}_0) & \dots & \frac{\partial R_1}{\partial x_n}(\bar{\delta}_0) \\ \dots\dots\dots \\ \frac{\partial R_n}{\partial x_1}(\bar{\delta}_0) & \dots & \frac{\partial R_n}{\partial x_n}(\bar{\delta}_0) \end{pmatrix};$$

- 5.3. вычислить $\det A_0$; если $p \mid \det A_0$, 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. $\bar{\delta}_k \equiv \bar{\delta}_{k-1} - C_{k-1} \cdot \bar{R}(\bar{\delta}_{k-1}) \pmod{p^{2^k}}$, где $\max_{1 \leq i \leq n} |\delta_{k,i}| \leq p^{2^k}/2$;
 - 5.5.2. имеем

$$A_k = \begin{pmatrix} \frac{\partial R_1}{\partial x_1}(\bar{\delta}_k) & \dots & \frac{\partial R_1}{\partial x_n}(\bar{\delta}_k) \\ \dots\dots\dots \\ \frac{\partial R_n}{\partial x_1}(\bar{\delta}_k) & \dots & \frac{\partial R_n}{\partial x_n}(\bar{\delta}_k) \end{pmatrix};$$

2.3. если $S \neq \emptyset$, то для каждого $\overline{\alpha}' = (a_0/b_0, \dots, a_n/b_n) \in S$:

2.3.1. вычислить $b = \text{НОК}(b_0, \dots, b_n)$;

2.3.2. положить $\overline{\alpha} = (ba_0/b_0, \dots, ba_{l-1}/b_{l-1}, b, \dots, ba_{l+1}/b_{l+1}, \dots, ba_n/b_n)$;

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 (6.4).

ТЕОРЕМА 10. Алгоритм 1 работает корректно.

ДОКАЗАТЕЛЬСТВО. Если система (6.1) обладает рациональным решением $\overline{\alpha} = (a_1/b_1, \dots, a_n/b_n) \in \mathbb{Q}^n$ таким, что $p \nmid \text{НОК}(b_1, \dots, b_n)$, 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 имеем $\det A_0 \equiv \det J(\overline{\alpha}) \pmod{p}$, 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 $\nu_p(\det J|_{\overline{\alpha}}) > 0$, т.е. такое решение не удовлетворяет условию (6.2), и можно переходить к следующему $\overline{\delta}$ на шаге 5.

Согласно результатам, полученным в теореме 8, на шаге 5.5 строится вектор $\overline{\delta}_V$, удовлетворяющий условию $\overline{R}(\overline{\delta}_V) \equiv 0 \pmod{p^{2^V}}$, а из результатов п. 5 следует, что $\overline{\alpha} \equiv \overline{\delta}_V \pmod{p^{2^V}}$.

Далее, из теорем 7, 9 и замечания 6 следует, что на шаге 5.6 решение $\overline{\alpha}$ однозначно восстанавливается из вектора $\overline{\delta}_V$.

ТЕОРЕМА 11. Алгоритм 2 работает корректно.

ДОКАЗАТЕЛЬСТВО. Выберем произвольный индекс r такой, что $0 \leq r \leq n$. Докажем, что на 2-м шаге алгоритма 2 при фиксированном индексе $l = r$ найдутся все целые решения $\overline{\alpha} = (t_0, \dots, t_n)$ системы (6.3), удовлетворяющие условиям (6.4) и $p \nmid t_r$. Для этого докажем, что из условия (6.4) следует условие (6.2).

Покажем сначала, что из условия (6.4) следует условие $\nu_p(M_r|_{\overline{\alpha}}) = 0$. Действительно, из тождества Эйлера для однородных функций (см. [9; гл. 8]) следует, что для произвольного $1 \leq i \leq n$

$$x_0 \frac{\partial P_i}{\partial x_0} + \dots + x_n \frac{\partial P_i}{\partial x_n} = \deg P_i \cdot P_i.$$

Отсюда получаем следующее равенство:

$$t_0 \frac{\partial P_i}{\partial x_0}(\overline{\alpha}) + \dots + t_n \frac{\partial P_i}{\partial x_n}(\overline{\alpha}) = 0. \quad (6.5)$$

Из равенства (6.5) и свойств определителей следует, что $t_j M_r = \pm t_r M_j$. По условию $\nu_p(M_j|_{\overline{\alpha}}) = 0$ и $p \nmid t_r$; таким образом, $\nu_p(M_r|_{\overline{\alpha}}) = 0$.

Докажем теперь от противного, что из условия $\nu_p(M_r|_{\overline{\alpha}}) = 0$ следует выполнение условия (6.2).

Действительно, предположим, что $\nu_p(\det J|_{\overline{\alpha}'}) > 0$, где $\overline{\alpha}' = (a_0/b_0, \dots, a_n/b_n)$, $p \nmid b = \text{НОК}(b_0, \dots, b_r)$, $t_0 = a_0 b/b_0, \dots, t_r = b, t_n = a_n b/b_n$. Но для произвольных $0 \leq k \leq n$ и $1 \leq i \leq n$

$$\left. \frac{\partial T_i}{\partial y_k} \right|_{\overline{\alpha}'} = \left. \frac{\partial P_i}{\partial x_k} \right|_{(a_0/b_0, \dots, 1, \dots, a_n/b_n)} = b^{\deg P_i} \left. \frac{\partial P_i}{\partial x_k} \right|_{\overline{\alpha}}.$$

Следовательно, $\det J|_{\overline{\alpha}} = b^{\deg P_i} \cdot M_r|_{\overline{\alpha}}$. Отсюда, так как $p \nmid b$, 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 на шаге 2 алгоритма 2 корректно применять алгоритм 1.

Далее, поскольку в алгоритме 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:

$$p \nmid t_0, \quad p \mid t_0, \quad p \nmid t_1, \quad \dots, \quad p \mid t_0, \quad \dots, \quad p \mid t_{n-1}, \quad p \nmid t_n.$$

ЗАМЕЧАНИЕ 8. Самым трудоемким шагом алгоритма 1 является решение системы сравнений $\overline{R}(x_1, \dots, x_n) \equiv 0 \pmod{p}$. Подробнее о решении таких систем можно прочитать в статье [10].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Ю. В. Нестеренко, *Теория чисел*, Высшее профессиональное образование, Академия, М., 2008.
- [2] A. K. Lenstra, H. W. Lenstra, Jr., L. Lovász, “Factoring polynomials with rational coefficients”, *Math. Ann.*, **261**:4 (1982), 515–534.
- [3] М. Е. Зеленова, “Решение полиномиальных уравнений в поле алгебраических чисел”, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 2014, № 1, 25–29.
- [4] J. D. Dixon, “Exact solution of linear equations using p -adic expansions”, *Numer. Math.*, **40**:1 (1982), 137–141.
- [5] Yu. V. Nesterenko, *Algebraic Independence*, Narosa Publ. House, New Delhi, 2009.
- [6] О. Зарисский, П. Самюэль, *Коммутативная алгебра*, Т. 2, ИЛ, М., 1963.
- [7] Ю. В. Нестеренко, “О мере алгебраической независимости значений некоторых функций”, *Матем. сб.*, **128**:4 (1985), 545–568.
- [8] А. Я. Хинчин, *Цепные дроби*, ГИФМЛ, М., 1960.
- [9] В. А. Зорич, *Математический анализ*, Ч. 1, ФАЗИС, М., 1997.
- [10] L. Bettale, J.-C. Faugère, L. Perret, “Solving polynomial systems over finite fields: improved analysis of the hybrid approach”, *Proc. of the 37th International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2012, 67–74.

М. Е. Зеленова

Московский государственный университет

имени М. В. Ломоносова

E-mail: mezelenova@gmail.com

Поступило

17.07.2014

Исправленный вариант

07.04.2015