ЧЕБЫШЕВСКИЙ СБОРНИК
Том 16 Выпуск 2 (2015)

УДК 511.2

О РЕШЕНИИ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ В ПРОИЗВОЛЬНЫХ ПОРЯДКАХ

М. Е. Зеленова (г. Москва)

Аннотация

В данной статье описывается алгоритм решения полиномиальных уравнений в кольце $\mathfrak{D}[x]$, где $\mathfrak{D}$ – произвольный порядок поля $\mathbb{Q}(\omega)$, а ω – целое алгебраическое число. Предложенный алгоритм является развитием идеи Курта Гензеля, описанной им в 1904 году и впоследствии названной леммой Гензеля о подъеме решения полиномиального сравнения. Описываемый алгоритм основан на следующих теоретических результатах. Во-первых, оцениваются коэффициенты разложения по базису порядка $\mathfrak{D}$ решений уравнения, то есть выводится оценка на высоту решения полиномиального уравнения в произвольном порядке поля алгебраических чисел. Во-вторых, выписывается итерационная формула, не содержащая в себе делений, позволяющая произвести квадратичный подъем решения соответствующего сравнения по модулю степени простого числа в порядке. В-третьих, подбирается эффективная оценка на степень простого числа, до которой следует поднимать решение вышеуказанного сравнения для получения точного решения исходного уравнения.

Следует заметить, что для корректной работы алгоритма требуется выбрать простое число p, по которому будет производиться подъем, так, чтобы выполнялись определенные условия. А именно, p не должно делить норму результанта исходного многочлена и его производной и дискриминант целого алгебраического числа ω. Также вычислительная сложность алгоритма уменьшается, если удается подобрать простое число p, которое в дополнение к двум условиям, изложенным в предыдущем предложении, обладает тем свойством, что минимальный многочлен алгебраического числа ω, все коэффициенты которого редуцированы по модулю p, неприводим в конечном поле из p элементов. В этом случае вычислительная сложность алгоритма составляет $\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0\leqslant i\leqslant m} \overline{|\gamma_i|}) + m^3 \ln(\max_{0\leqslant i\leqslant m} \overline{|\gamma_i|}) \ln\ln(\max_{0\leqslant i\leqslant m} \overline{|\gamma_i|})$ арифметических операций. Здесь m – степень исходного многочлена, γ_i, $0 \leqslant i \leqslant m$ – его коэффициенты, а $\overline{|\gamma|}$ – максимум модулей всех чисел, сопряженных с γ. В том же случае, когда не удается выбрать простое число p так, чтобы минимальный многочлен ω был неприводим в конечном поле из p элементов, вычислительная сложность алгоритма составляет $\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0\leqslant i\leqslant m} \overline{|\gamma_i|}) +$

$m^3 \ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) + m^d \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil))$ арифметических операций. Здесь d – количество неприводимых сомножителей, на которые раскладывается минимальный многочлен числа ω в $\mathbb{F}_p$. Алгоритм, изложенный в статье, включает в себя стратегию выбора простого числа p для достижения меньшей вычислительной сложности.

Ключевые слова: полиномиальные уравнения, алгебраические числа, группа Галуа.

Библиография: 15 названий.

SOLUTION OF POLYNOMIAL EQUATIONS IN ARBITRARY ORDERS

M. E. Zelenova

Abstract

The article deals with an algorithm of solving polynomial equations in a ring $\mathfrak{O}[x]$, where $\mathfrak{O}$ is an arbitrary order of field $\mathbb{Q}(\omega)$ and ω is an algebraic integer. The algorithm develops Kurt Hensel's idea published in 1904 which was named Hensel's lifting lemma later. The algorithm described is based on the following theoretical results. Firstly, basis of order $\mathfrak{O}$ expansion coefficients of the equation roots are estimated, i. e. an estimate for the polynomial equation roots height in an algebraic number field arbitrary order is derived. Secondly, an iterative formula for the corresponding polynomial congruence solution quadratic lifting modulo power of prime in the order is obtained. This formula does not contain any divisions. Thirdly, an effective bound for prime power the congruence solution needs to be lifted to obtain the exact solution of the original equation is derived.

Notice that a prime p which is used for lifting needs to satisfy certain conditions for the algorithm correct work. In particular, p should not derive the original polynomial and its derivative resultant norm and also p should not derive discriminant of an algebraic integer ω. Also the algorithm complexity is decreased if it is possible to choose prime p which in addition to two previous conditions has the following property: the minimal polynomial of ω which coefficients are reduced modulo p is irreducible over finite field $\mathbb{F}_p$. In this case the algorithm complexity is $\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) + m^3 \ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil)$ arithmetic operations. Here m is the original polynomial degree, γ_i, $0 \leqslant i \leqslant m$ are its coefficients and $\lceil\overline{\gamma}\rceil$ is the algebraic numbers conjugated to γ absolute values maximum. If it is impossible to choose prime number p such that minimal polynomial of ω is irreducible over $\mathbb{F}_p$ then the algorithm complexity is $\mathcal{O}(m^4 + m^3 \ln m \ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) + m^3 \ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil) + m^d \ln\ln(\max_{0\leqslant i\leqslant m} \lceil\overline{\gamma_i}\rceil))$ arithmetic operations. Here d is the minimal polynomial of ω irreducible factors over $\mathbb{F}_p$ number. The algorithm includes strategy to select a prime p to achieve lower computational complexity.

Keywords: polynomial equations, algebraic numbers, Galois group.

Bibliography: 15 titles.

1. Введение

Нахождение корней уравнений и систем в определенных кольцах или полях является одной из классических задач алгебры и теории чисел.

Один из подходов к решению данной задачи основан на классическом результате, а именно, лемме Гензеля о подъеме решения полиномиального сравнения (см. [1]). Идея алгоритмов, построенных с помощью данного подхода, 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. Известен также алгоритм нахождения рациональных решений целочисленных линейных систем (см. [3]).

Также модифицированный алгоритм подъема был использован автором в статье [4] для нахождения решений полиномиальных уравнений в полях алгебраических чисел. Полученный в данной работе результат является обобщением алгоритма, описанного автором в статье [4]. Первая статья не содержала в себе оценку простого числа p, по которому требовалось производить подъем. В данной работе такая оценка имеет место быть.

Итак, пусть ω — целое алгебраическое число степени d, и

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

где $c_d = 1$, — его минимальный многочлен. Обозначим через $\mathfrak{D}$ произвольный порядок поля $K = \mathbb{Q}(\omega)$. Предлагаемый алгоритм позволяет по заданному многочлену $f(x) \in \mathfrak{D}[x]$ найти все его корни, принадлежащие $\mathfrak{D}$, а также определяет случаи, когда исходное уравнение корней не имеет.

2. Алгоритм

Предположим, что

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

— многочлен без кратных корней.

Положим $R = \gamma_m D(f)$, где $D(f)$ — дискриминант многочлена $f(x)$, $R \in \mathfrak{D}$; $N(R) \in \mathbb{Z}$ — норма R.

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

Каждый элемент $\beta \in \mathfrak{D}$ представим в виде

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

где $b_i \in \mathbb{Z}$. Здесь $\Omega = \{\omega_1, \ldots, \omega_d\}$ — базис $\mathfrak{D}$. Будем использовать обозначение

$$\|\beta\| = \max |b_i|.$$

Также обозначим через D_ω дискриминант числа ω, а через D_{spl} — дискриминант поля разложения многочлена $\mu_\omega(x)$.

Для произвольного алгебраического числа γ положим

$$\lceil\!\overline{\gamma}\!\rceil = \max_{1\leqslant k\leqslant d} |\gamma^{(k)}|,$$

где $\gamma^{(k)}$ – числа, сопряженные с γ.

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.

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 $R = \gamma_m D(f)$, $N(R)$ и $R' \in \mathfrak{D}$, такое, что $N(R) = R \cdot R'$. *[см. лемму 1]*
3. Вычислить $A(x), B(x) \in \mathfrak{D}[x]$, такие, что
$$R = A(x)f(x) + B(x)f'(x).$$
[см. лемму 2]
4. Вычислить D_ω, D_{spl}.
5. Положить $W = [(4\log|D_{spl}| + 2,5d + 5)^2]$.
6. Для каждого i, удовлетворяющего $p_i \leqslant W$, выполнять следующие действия:

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

   6.2. Проверить, выполняются ли условия
   $$(p_i, N(R)) = 1 \text{ и } (p_i, D_\omega) = 1.$$
   Если нет, то перейти на начало шага 6.

   6.3. 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 8.

   6.4. Если $\mathcal{M} = \emptyset$ или $\#\mathcal{M} > r_i$, то положить
   $$\mathcal{M} = \{\mu_{i,1}(\omega), \ldots, \mu_{i,r_i}(\omega)\}, K = r_i, P = p_i.$$

7. Если $\mathcal{M} = \emptyset$, то найти простое число $p > p_W$, 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 $\mathcal{M} = \{\mu_1(\omega), \ldots, \mu_r(\omega)\}$, $K = r$, $P = p$.

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

   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 $x \equiv a_k \pmod{\mathfrak{p}_k}$, $1 \leqslant k \leqslant K$.

9. 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. [5], гл. II §2]*

10. 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 8, а при $K > 1$ — на шаге 9]

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

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

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

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

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

12. Найти решение N_0 сравнения

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

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

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

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

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

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

 14.1. Положить $\delta_0 = \delta$.

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

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

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

 14.3. Проверить, удовлетворяет ли число δ_V равенству

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

 Если равенство выполняется, то

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

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

Замечание 1. *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 [6], гл. 3.*

3. Обоснование шагов 5–7

Более подробно с теорией, изложенной в данном параграфе, можно ознакомиться в книгах [7] и [8]; определение символа Артина и формулировка теоремы 1 в более общем виде содержится в работе [9].

Теорема 1. *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, $p \nmid \Delta$, удовлетворяющее условиям $\left(\frac{L/\mathbb{Q}}{p}\right) = \sigma$ и $p \leqslant (4\log|D| + 2{,}5n + 5)^2$.*

Доказательство. См. [9], §8.8. □

Следствие 1. *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. $p \leqslant (4\log|D_{spl}| + 2{,}5d + 5)^2$.

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 2. *Справедлива оценка*

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

Доказательство. См. [10]. □

Замечание 2. *Заметим, что доля унитарных многочленов с целыми коэффициентами степени l, группа Галуа которых меньше, чем S_l, а коэффициенты ограничены B, составляет $\mathcal{O}\left(\frac{\log B}{\sqrt{B}}\right)$, 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 следствия 1. Тогда в алгоритме появляется возможность сократить количество вычислений, перепрыгнув с шага 6 сразу на шаг 8, а потом на шаг 10.*

4. Обоснование подъема решений

Лемма 1. *Существует $R' \in \mathfrak{D}$ такое, что $N(R) = R \cdot R'$.*

Доказательство. См. [11], гл. 2 §2. □

Лемма 2. *Существуют $A(x), B(x) \in \mathfrak{D}[x]$ такие, что $R = A(x)f(x) + B(x)f'(x)$. При этом многочлены $A(x)$ и $B(x)$ можно выписать в явном виде.*

Доказательство. См. [12], гл. 5 §34. □

Лемма 3. *При любом $k \geqslant 0$ для чисел N_k, определенных на шагах 12 и 13 алгоритма, выполняется сравнение*

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

Доказательство. Проведем доказательство индукцией по k. При $k = 0$ теорема верна по построению N_0. Пусть теперь $k \geqslant 1$, 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,

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

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

□

Теорема 3. *При любом $k \geqslant 0$ для чисел δ_k, определенных на шагах 14.1 и 14.2 алгоритма, выполняется следующее сравнение:*

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

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 3 алгоритма.

Согласно предположению индукции, $f(\delta_{k-1}) \equiv 0 \pmod{p^{2^{k-1}}}$.

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

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

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

$$= \frac{(f(\delta_{k-1}))^2 R'}{N(R)} A(\delta_{k-1}) \equiv 0 \pmod{p^{2^k}},$$

так как по предположению индукции $(f(\delta_{k-1}))^2 \equiv 0 \pmod{(p^{2^{k-1}})^2 = p^{2^k}}$. □

5. Оценка коэффициентов решения уравнения

Пусть $\alpha \in \mathfrak{D}$ – корень уравнения $f(x) = 0$. 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 известные величины.

Лемма 4. *Имеет место равенство $|\alpha| \leqslant \frac{\max_{0 \leqslant i < m} |\gamma_i|}{|\gamma_m|} + 1$, где γ_i – коэффициенты многочлена $f(x)$.*

Доказательство. См. [13], гл. 9 §39. □

Теорема 4. *Имеет место неравенство*

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

где

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

Доказательство. Обозначим через $\Omega' = \{\omega'_1, \ldots, \omega'_d\}$ базис, взаимный к Ω. Тогда

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

Следовательно,

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

Здесь $(\omega_i')^{(j)}$, $1 \leqslant i,j \leqslant d$ – числа, сопряженные с ω_i', а $\alpha^{(j)}$, $1 \leqslant j \leqslant d$ – числа, сопряженные к α. Они 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.

Так как $\gamma_m^{(j)}$ – целое алгебраическое число и $\gamma_m^{(j)} \neq 0$, то $N\left(\gamma_m^{(j)}\right) \in \mathbb{Z}\backslash\{0\}$. Следовательно,

$$1 \leqslant |N(\gamma_m^{(j)})| = |\gamma_m \gamma_m^{(2)} \ldots \gamma_m^{(d)}| \leqslant |\gamma_m^{(j)}| \overline{|\gamma_m|}^{d-1}.$$

Таким образом, $|\gamma_m^{(j)}| \geqslant \overline{|\gamma_m|}^{1-d}$.
По лемме 4,

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

Следовательно,

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

□

6. Обоснование корректности работы алгоритма

Теорема 5. *Алгоритм находит все решения уравнения $f(x) = 0$ в $\mathfrak{D}$ и возвращает пустое множество, если данное уравнение неразрешимо.*

Если $\alpha \in \mathfrak{D}$ – корень многочлена $f(x)$, то на шаге 6 найдется такое число δ_0, что $f(\delta_0) \equiv 0 \pmod p$, $\delta_0 \equiv \alpha \pmod p$ и $\|\delta_0\| \leqslant \frac{p}{2}$. Поскольку

$$\delta_k \equiv \delta_{k-1} - f(\delta_{k-1}) B(\delta_{k-1}) R' N_k \pmod{p^{2^k}} \text{ и } f(\delta_{k-1}) \equiv 0 \pmod{p^{2^{k-1}}}$$

при любом $k \geqslant 1$, то $\delta_V \equiv \delta_0 \equiv \alpha \pmod p$.

По теореме 3,

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

Левую часть сравнения можно представить в виде

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

Таким образом, выполняется сравнение

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

Разложим (p) в произведение простых идеалов:

$$(p) = \mathcal{P}_1 \ldots \mathcal{P}_r.$$

Заметим также, что все $\mathcal{P}_i$ различны, поскольку $p \nmid D_\omega$.

Из формулы (1) следует, что

$$(\alpha - \delta_V)\sum_{i=1}^{m}\gamma_i(\alpha^{i-1} + \alpha^{i-2}\delta_V + \cdots + (\delta_V)^{i-1}) \equiv 0 \pmod{\mathcal{P}_i^{2^V}}, \tag{2}$$

где $1 \leqslant i \leqslant r$.

Так как $\delta_V \equiv \alpha \pmod p$, то верно, что $\delta_V \equiv \alpha \pmod{\mathcal{P}_i}$, $1 \leqslant i \leqslant r$, и, таким образом,

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

По лемме 2, $B(\delta_V)f'(\delta_V) \equiv R \pmod p$, и, следовательно,

$$B(\delta_V)f'(\delta_V) \equiv R \pmod{\mathcal{P}_i}, 1 \leqslant i \leqslant r. \tag{3}$$

Докажем от противного, что $R \not\equiv 0 \pmod{\mathcal{P}_i}$, $1 \leqslant i \leqslant r$. Предположим, что это не так, и $R \in \mathcal{P}_i$. Но тогда и

$$N(R) \in \mathcal{P}_i. \tag{4}$$

Однако $N(R)$ — целое число, откуда и из условия (4) следует, что $p \mid N(R)$. Но это противоречит выбору p. Таким образом, доказано, что $R \not\equiv 0 \pmod{\mathcal{P}_i}$, $1 \leqslant i \leqslant r$.

Теперь из выражения (3) следует, что $f'(\delta_V) \not\equiv 0 \pmod{\mathcal{P}_i}$, $1 \leqslant i \leqslant r$.

Итак, $\mathcal{P}_i$ – простой идеал в $\mathfrak{D}$. При этом

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

и

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

Следовательно, $\alpha \equiv \delta_V \pmod{\mathcal{P}_i^{2^V}}$ для любого индекса $1 \leqslant i \leqslant r$, и, таким образом, $\alpha \equiv \delta_V \pmod{p^{2^V}}$.

Оценим модуль коэффициентов разности α и δ_V:

$$\|\alpha - \delta_V\| \leqslant \|\alpha\| + \|\delta_V\| \leqslant CU + \frac{p^{2^V}}{2} < p^{2^V}, \text{ так как } V > \log_2(\log_p(2CU)).$$

Но каждый коэффициент $\alpha - \delta_V$ – 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 14.2 алгоритма. □

7. Оценка сложности работы алгоритма

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

Теорема 6. *Существует хотя бы одно простое число $p > 2$, удовлетворяющее условию*

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

Для которого верно, что $(p, N(R)) = 1$. Здесь A — константа, удовлетворяющая условию

$$\prod_{q<p} q > e^{Ap}, \tag{5}$$

где произведение берется по всем простым числам q, меньшим p (см. [14, §22.2]).

Доказательство. Выполняется следующее равенство:

$$N(R) = R \cdot R^{(2)} \cdot \ldots \cdot R^{(d)}, \tag{6}$$

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

Заметим, что R можно записать в виде

$$R = (-1)^{\frac{m(m-1)}{2}} R(f, f'), \tag{7}$$

где $R(f, f')$ — 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 неравенству Адамара (см. [15, гл. 8 §7]) и формуле (7), получаем неравенство

$$|R| = |(R(f, f'))| \leqslant (m \cdot \max_{0\leqslant i\leqslant m} |\gamma_i|)^{2m-1}(2m-1)^{m-\frac{1}{2}}. \tag{8}$$

Аналогично можно показать, что верны соотношения

$$|R^{(j)}| \leqslant (m \cdot \max_{0\leqslant i\leqslant m} |\gamma_i^{(j)}|)^{2m-1}(2m-1)^{m-\frac{1}{2}},\ 2 \leqslant j \leqslant d, \tag{9}$$

где $\gamma_i^{(j)}$ — числа, сопряженные с γ_i. Теперь из формул (6), (8) и (9) следует, что

$$|N(R)| \leqslant (m^2(2m-1))^{d(m-\frac{1}{2})} \max_{0\leqslant i\leqslant m} \overline{|\gamma_i|}^{(2m-1)d}. \tag{10}$$

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 формулы (10) и (5). Получим следующую цепочку неравенств:

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

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 7. *Наихудшая сложность 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 равна

$$\mathcal{O}(m^3). \tag{11}$$

Для шага 3 требуется вычислить m и $m-1$ определителей такого же вида, откуда сложность шага 3 получается равной

$$\mathcal{O}(m^4). \tag{12}$$

На шаге 6 требуется для каждого $p_i < W$, где W — граница, зависящая только от исходного порядка, раскладывать на множители многочлены степени d. Следовательно, временная сложность шага 6 не зависит от многочлена $f(x)$.

На шаге 7 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 6 и оценок Чебышева следует, что на поиск числа p нужно не больше, чем

$$\mathcal{O}\left(\frac{C_3}{\ln C_3}\right),\ C_3 = \frac{d(2m-1)(\ln m + \frac{1}{2}\ln(2m-1) + \ln(\max_{0\leqslant i\leqslant m}\lceil\gamma_i\rceil))}{A} \tag{13}$$

арифметических выражений. Выражение (13) можно преобразовать с учетом того, что, по предположению, порядок $\mathfrak{D}$ фиксирован. Получим следующее:

$$\mathcal{O}\left(\frac{C_3}{\ln C_3}\right) = \mathcal{O}\left(\frac{m\ln m + m\ln(\max_{o\leqslant i\leqslant m}\lceil\gamma_i\rceil)}{\ln m + \ln\ln(\max_{o\leqslant i\leqslant m}\lceil\gamma_i\rceil)}\right). \tag{14}$$

Во-вторых, на шаге 7 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 $p < C_3$. Если пользоваться алгоритмом Берлекэмпа, для этого требуется не более, чем

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

арифметических операций. Из теоремы 6 теперь можно получить, что на вторую часть шага 7 нужно не более

$$\mathcal{O}(m \ln m + m \ln(\max_{o \leqslant i \leqslant m} \lceil \gamma_i \rceil)) \tag{15}$$

операций.

На шаге 8 требуется K раз ($K \leqslant d$) решить уравнение $f(x) = 0$ в полях вида $\mathbb{F}_{p^l}$, где $l \leqslant d$. На выполнение вышеуказаннх действий требуется

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

арифметических операций (см. [6, гл. 3 §3]). С учетом формулы (13) можно заключить, что сложность шага 12 составляет

$$\mathcal{O}(m^3 (\ln m)^2 + m^3 \ln m \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) + m^3 \ln(\max_{o \leqslant i \leqslant m} \lceil \gamma_i \rceil) \ln \ln(\max_{o \leqslant i \leqslant m} \lceil \gamma_i \rceil)). \tag{16}$$

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 9 потребуется фиксированное время. Поскольку количество решений каждого уравнения на шаге 8 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 9 составляет

$$\mathcal{O}(m^d) \tag{17}$$

арифметических операций.

Для оценки числа V, выбираемого на шаге 11, заметим, что из того, что $p > 2$, следует, что

$$V \leqslant 1 + \lfloor \log_2 \log_3 (2CU) \rfloor. \tag{18}$$

Для выполнения шага 12 требуется применить обобщенный алгоритм Евклида для чисел $N(R)$ и p. Таким образом, сложность шага 12 составляет

$$\mathcal{O}(\ln p) = \mathcal{O}(\ln m + \ln \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil) \tag{19}$$

арифметических операций.

Шаги 13 и 14 выполняются за $\mathcal{O}(V m^d)$ операций. Из формулы (18) получаем, что

$$\mathcal{O}(V m^d) = \mathcal{O}(m^d \ln \ln(\max_{0 \leqslant i \leqslant m} \lceil \gamma_i \rceil)) \tag{20}$$

операций.

Объединим выражения (11), (12), (14), (15), (16), (17), (19), (20). 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. □

8. Заключение

Заметим, что если алгоритм попал в случай, описанный в замечании 2, то 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.

Таким образом, описанный алгоритм имеет полиномиальную сложность и может представлять практическую значимость.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Hensel K. Neue Grundlagen der Arithmetik // J. Reine Angew. Math. 1904. Vol. 127. P. 51–84.
2. Lenstra A. K., Lenstra H. W., Lovász L. Factoring Polynomials with Rational Coefficients // Mathematische Annalen. 1982. Vol. 261. P. 515–534.
3. Dixon J. D. Exact Solution of Linear Equations Using P-Adic Expansions // Numerische Mathematik. 1982. Vol. 40. P. 137–141.
4. Зеленова М. Е. Решение полиномиальных уравнений в поле алгебраических чисел // Вестн. Моск. ун-та. Сер. 1. Матем., мех. 2014. № 1. С. 25–29.
5. Ленг С. Алгебра. М.: Мир, 1968. 564 с.
6. Герман О. Н., Нестеренко Ю. В. Теоретико-числовые методы в криптографии. М.: Академия, 2012. 272 с.
7. Постников М. М. Теория Галуа. М.: ГИФМЛ, 1963. 220 с.
8. Cox D. A. Galois Theory. Hoboken: Wiley, 2012. 602 p.
9. Bach E., Shallit J. Algorithmic Number Theory, vol. I: Efficient Algorithms. Cambridge, London: The MIT Press, 1996. 496 p.
10. Gallagher P. X. The Large Sieve and Probabilistic Galois Theory // Proceedings of Symposia in Pure Mathematics. 1973. Vol. 24. P. 91–101.

11. Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1972. 496 с.

12. ван дер Варден Б. Л. Алгебра. М.: Наука, 1976. 649 с.

13. Курош А. Г. Курс высшей алгебры. М.: Наука, 1965. 431 с.

14. Hardy G. H., Wright E. M. An Introduction to the Theory of Numbers. Oxford: Oxford University Press, 1985. 438 p.

15. Зорич В. А. Математический анализ, т. 1. М: ФАЗИС, 1997. 554 с.

REFERENCES

1. Hensel K. 1904, "Neue Grundlagen der Arithmetik" , *J. Reine Angew. Math.*, vol. 127, pp. 51–84.

2. Lenstra A. K., Lenstra H. W. & Lovász L. 1982, "Factoring Polynomials with Rational Coefficients" , *Mathematische Annalen*, vol. 261, pp. 515–534.

3. Dixon J. D. 1982, "Exact Solution of Linear Equations Using P-Adic Expansions" , *Numerische Mathematik*, vol. 40, pp. 137–141.

4. Zelenova M. E. 2014, "Solution of Polynomial Equations in the Field of Algebraic Numbers" , *Moscow University Mathematics Bulletin*, no. 1, pp. 25–29.

5. Lang S. 1968, "Algebra" [Algebra], *Mir, Moscow,* 564 p.

6. German O. N. & Nesterenko Yu. V. 2012, "Teoretiko–chislovye metody v kriptografii" [Number Theoretic Algorithms in Cryptography], *Akademia, Moscow,* 272 p.

7. Postnikov M. M. 1963, "Teoriya Galua" [Galois Theory], *GIFML, Moscow,* 220 p.

8. Cox D. A. 2012, "Galois Theory" , *Wiley, Hoboken,* 602 p.

9. Bach E. & Shallit J. 1996, "Algorithmic Number Theory, vol. I: Efficient Algorithms" , *The MIT Press, Cambridge, London.* 496 p.

10. Gallagher P. X. 1973, "The Large Sieve and Probabilistic Galois Theory" , *Proc. Symp. Pure Math.*, vol. 24, pp. 91–101.

11. Borevich Z. I. & Shafarevich I. R. 1972, "Teoriya chisel" [Number Theory], *Nauka, Moscow,* 496 p.

12. van der Waerden B. L. 1976, "Algebra" [Algebra], *Nauka, Moscow,* 649 p.

13. Kurosh A G. 1965, "Kurs vyshej algebry" [Course of Higher Algebra], *Nauka, Moscow,* 431 p.

14. Hardy G. H. & Wright E. M. 1985, "An Introduction to the Theory of Numbers" , *Oxford University Press, Oxford,* 438 p.

15. Zorich V. A. 1997, "Matematicheskij analiz, t. 1" [Mathematical Analysis I], *FAZIS, Moscow,* 554 p.

Московский государственный университет им. М. В. Ломоносова.
Получено 20.04.2015