Московский Государственный Университет
имени М.В. Ломоносова
Механико-математический факультет

На правах рукописи
УДК 511.2

Маркелова Александра Викторовна

РАЗРЕШИМОСТЬ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В КОЛЬЦАХ

Специальность 01.01.06 - математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва, 2011

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

Научный руководитель:	кандидат физико-математических наук, доцент Михаил Алексеевич Черепнёв
Официальные оппоненты:	доктор физико-математических наук, профессор Владимир Григорьевич Чирский
	кандидат физико-математических наук Вадим Владиславович Назаров
Ведущая организация:	Институт информационных наук и технологий безопасности (ИИНТБ) РГГУ

Защита диссертации состоится 11 марта 2011 г. в 16 ч. 45 м.на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М.В. Ломоносова по адресу: Российская Федерация, 119991, ГСП-1, Москва, Ленинские горы, д. 1, МГУ, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета Московского государственного университета имени М.В. Ломоносова (Главное здание, 14 этаж).

Автореферат разослан 11 февраля 2011 г.

Ученый секретарь
диссертационного совета
Д.501.001.84 при МГУ
доктор физико-математических наук,
профессор

А.О.Иванов

Общая характеристика работы

Актуальность темы

Задача дискретного логарифмирования является одной из ключевых задач современной теории чисел. Вопрос дискретного логарифмирования в конечных кольцах зачастую полиномиально сводится к дискретному логарифмированию в конечных полях. Но в случае, если мультипликативная группа кольца не является циклической, возникает дополнительный вопрос: вопрос о существовании решения показательного сравнения.

Buchmann J., Jacobson M.J., Teske E.[1] приводят алгоритм для проверки разрешимости в произвольной абелевой группе. Данный алгоритм для конечной мультипликативной абелевой группы G и элементов $\alpha, \beta \in G$ за $O(\sqrt{|\langle\alpha\rangle|})$ умножений проверяет, принадлежит ли элемент β циклической группе $\langle\alpha\rangle$, порождённой элементом α, и в случае положительного ответа находит $\log_\alpha \beta$. Для проверки используется таблица, состоящая из $O(\sqrt{|\langle\alpha\rangle|})$ пар элементов.

Данный алгоритм малоинтересен, поскольку имеет слишком большую сложность. Естественно ожидать, что при рассмотрении задачи не в произвольной группе, а в мультипликативной группе некоторого конкретного конечного кольца, структура которого нам хорошо известна, сложность окажется существенно меньше.

Этой темой занимался О.Н.Василенко. Он рассматривал вопрос о разрешимости показательного сравнения в кольце вычетов по составному модулю[2] и в факторкольце многочленов над конечным полем[3]. Им были получены некоторые критерии разрешимости для частных случаев.

Прежде всего, рассмотрим задачу дискретного логарифмирования в кольце вычетов по составному модулю. О.Н.Василенко сформулировал и доказал

[1]Buchmann J., Jacobson M.J., Teske E. On some computational problems in finite abelian groups. *Mathematics of Computation*, 1997, V. 66 (220), p. 1663-1687.

[2]Василенко О.Н. О разрешимости задачи дискретного логарифмирования в кольцах вычетов. *Фунд. и прикл. матем*, 2002. 8, № 3. 647-653.

[3]Василенко О.Н. О дискретном логарифмировании в некоторых группах. *Вестник МГУ*, сер.1. Матем. Механ., 2000, №5, с. 53-55.

теорему[2], позволяющую проверять разрешимость показательного сравнения

$$a^x \equiv b \pmod{M}$$

для $M = p_1 \cdot ... \cdot p_k$, где все p_i - различные нечётные простые, имеющие специальный вид, при условии, что порядок a по модулям p_i строго равен одному из двух значений $p_i - 1$ или $\frac{p_i-1}{2}$.

Далее, интерес представляет вопрос о разрешимости показательного сравнения в факторкольце многочленов над полем. Cohen H., Dyaz y Dyaz F., Olyver M. в 1998 году[4], затем Hess F., Pauli S., Pohst M.E. в 2003 году[5] и позднее Поповян И.А. в 2006 году[6] рассматривали задачу подъёма решений показательного сравнения в кольце целых алгебраических чисел. Было доказано, что решение сравнения

$$\alpha^x \equiv \beta \pmod{\pi^\nu}$$

для некоторых $\alpha, \beta \in \mathbb{Z}_{\mathbb{K}}$ и простого идеала π полиномиально сводится к нахождению решения сравнения

$$\alpha^x \equiv \beta \pmod{\pi}.$$

Такое сведение осуществлялось при помощи различных логарифмических функций, а именно частных Ферма специального вида, p-адических логарифмов и логарифмов Артина-Хассе.

Частным случаем рассматриваемой задачи является сравнение вида

$$a^n(x) \equiv b(x) \pmod{p^\nu, f(x)},$$

где многочлен $f(x)$ со старшим коэффициентом 1 неприводим по модулю простого p.

При этом решение задачи сводится к нахождению решения сравнения

$$a^n(x) \equiv b(x) \pmod{p, f(x)}.$$

---

[4]Cohen H., Diaz y Diaz F., Oliver M. Computing ray class groups, conductors and discriminants. *Math. Comp.*, Vol. 67:222, 1998, pp. 773-795.

[5]Hess F., Pauli S. , Pohst M.E. Computing the multiplicative group of residue class rings. *Math. Comp.*, Vol. 72:243, 2003, pp. 1531-1548.

[6]Поповян И.А. Подъём решений показательного сравнения. *Математические заметки*, 2006, 80:1, с.76-86

Однако, решение последнего сравнения можно "поднимать" не только по степеням p, но и по степеням $f(x)$. Вопрос о подъёме решений сравнения

$$a^n(x) \equiv b(x) \pmod{p, f^\nu(x)} \tag{1}$$

рассматривался О.Н.Василенко[3], и им были получены некоторые результаты для случая $p/2 < \nu \leq p$, $\mathrm{ord}a(x) = p\delta_1$, $\mathrm{ord}b(x) = p\delta_2$, $\delta_2|\delta_1|p^d - 1$ ($d = \deg f(x)$) при условии, что $\frac{a^{p^d-1}(x)-1}{f(x)} \not\equiv 0 \pmod{p, f(x)}$. А именно, при данных ограничениях и в случае разрешимости сравнения (1) были получены формулы для подъёма решений этого сравнения.

Цель работы

Цель диссертации - получение конструктивных критериев разрешимости задачи дискретного логарифмирования в кольцах вычетов по произвольному составному модулю и в факторкольцах многочленов над конечными полями, подъём решений показательного сравнения в факторкольцах многочленов над конечными полями по степени неприводимого многочлена, оптимизация вычислительной сложности полученных алгоритмов.

Научная новизна

Результаты диссертации являются новыми и состоят в следующем:

• Получен критерий разрешимости показательного сравнения в кольце вычетов по модулю составного числа. Доказано, что вопрос о разрешимости показательного сравнения по модулю произвольного составного числа полиномиально сводится к вычислению символов степенного вычета с некоторыми простыми индексами, являющимися делителями $p-1$, где $p|M$. Приведён конструктивный полиномиальный алгоритм такого сведения. Итоговая теорема обобщает полученные О.Н.Василенко критерии.

• Решена задача подъёма решений по модулю степени неприводимого многочлена над конечным полем. Приведён алгоритм её полиномиального сведения к аналогичной задаче по модулю самого неприводимого многочлена. Итоговая теорема обобщает критерии О.Н.Василенко.

• Решена задача подъёма решений показательного сравнения в цепных кольцах. Описаны возможные оптимизации алгоритма подъёма решений по модулю степени неприводимого многочлена над конечным полем при помощи построения конструктивных изоморфизмов в цепные кольца. Получены оценки сложности предлагаемых модификаций.

• Получен критерий разрешимости показательного сравнения по модулю произвольного многочлена над конечным полем. Доказано, что вопрос о разрешимости полиномиально сводится к вычислению символов степенного вычета.

• Получены формулы для "подъёма" символа степенного вычета в ряде случаев, используемых в доказанных выше критериях разрешимости. А именно, показано, что в случае, когда $r^k||p-1$, вычисление символа степени r^k полиномиально сводится к вычислению символов степени r, где r - простое.

Основные методы исследования

В диссертации используются методы алгебраической теории чисел, теории конечных колец, теории сложности вычислений.

Теоретическая и практическая ценность

В диссертации доказываются теоремы и выводятся формулы, которые могут найти применение в алгебраической теории чисел. Построенные алгоритмы с оценками сложности могут использоваться в вычислительной теории чисел.

Апробация работы

Результаты диссертации докладывались автором на следующих научных семинарах и конференциях:

• на научно-исследовательском семинаре по теории чисел под руководством проф. Ю.В.Нестеренко, проф. Н.Г.Мощевитина (2008 г., 2010 г.);

• на семинаре "Теоретико-числовые вопросы криптографии" под руководством доц. М.А.Черепнёва (2008 г., 2009 г., 2010 г.);

• на конференции “Ломоносовские чтения” (Москва, 2009 г.);

• на конференции “Математика и безопасность информационных технологий” (Москва, 2004 г., 2009 г., 2010 г.).

Публикации

Результаты автора по теме диссертации опубликованы в 3 работах, список которых приводится в конце автореферата [1-3].

Структура и объём диссертации

Диссертация состоит из введения, четырёх глав, заключения и библиографии (37 наименований). Общий объём диссертации составляет 89 страниц.

Содержание работы

Во введении, являющемся первой главой, описывается структура диссертации, обосновывается актуальность темы и научная новизна полученных результатов, излагаются основные результаты диссертации.

Во второй главе сформулирован и доказан критерий разрешимости сравнения

$$a^x \equiv b \pmod{M}, \tag{2}$$

где $M = p_1^{\nu_1} \cdot \ldots \cdot p_k^{\nu_k}$, p_i - различные простые, $\nu_i \in \mathbb{N}$, $a, b \in (\mathbb{Z}/M\mathbb{Z})^*$.

Для случая $k = 1$ разрешимость проверяется с использованием частных Ферма $Q(a, r) = \frac{a^{\lambda(r)}-1}{r} \pmod{r}$ по следующим теоремам.

Теорема 1. *Для $M = p^\nu$, где p - простое, нечётное, $\nu > 1$, сравнение (2) равносильно системе*

$$\begin{cases} Q(a, p^{\nu-1})x \equiv Q(b, p^{\nu-1}) \pmod{p^{\nu-1}}, \\ a^x \equiv b \pmod{p}. \end{cases}$$

Теорема 2. *Для $M = 2^\nu, \nu \geq 5$ сравнение (2) равносильно системе*

$$\begin{cases} Q(a, 2^{\nu-2})x \equiv Q(b, 2^{\nu-2}) \pmod{2^{\nu-2}}, \\ a^x \equiv b \pmod{4}. \end{cases}$$

Данные теоремы широко[7,8,9] известны для случая, когда a - первообразный по модулю простого нечётного p или $a = 5$ при $p = 2$. Однако, они верны и для произвольного a. Эти теоремы полезны не только для проверки разрешимости, но и для подъёма решений показательного сравнения. Решения линейных сравнений приведённых выше систем будут использоваться в следующей теореме.

Теорема 3. *Пусть $k \geq 2$ и $\mathrm{ord}_{p_i^{\nu_i}} a = \delta_i = p_j^{\mu_{ij}} \delta_{ij}$, $(p_j, \delta_{ij}) = 1$ для всех пар (i, j). Обозначим через c_i решение сравнения $a^x \equiv b \pmod{p_i^{\nu_i}}$ по модулю δ_i, а через $\widetilde{c_i}$ - его вычет по модулю $p_i^{\mu_{ii}}$. Сравнение (2) разрешимо тогда и только тогда, когда выполнены следующие условия:*

1) при $\nu_i > 1$ сравнение $a^x \equiv b \pmod{p_i^{\nu_i}}$ разрешимо;

2) при любых $i \neq j$ сравнение $a^x \equiv b \pmod{p_i p_j}$ разрешимо;

3) если $\nu_j > 1$ и $\mu_{ij} > 0$, то $(ba^{-\widetilde{c_j}})^{\delta_{ij} p_j^{\max\{\mu_{ij} - \mu_{jj}, 0\}}} \equiv 1 \pmod{p_i}$.

В результате исходная задача редуцируется к случаю, когда $k = 2$, p_1, p_2 - нечётные, $\nu_1 = \nu_2 = 1$.

Далее в главе 2 сформулирован следующий критерий разрешимости показательного сравнения по модулю pq для некоторых частных случаев.

Лемма 3. *Пусть $p = 2r + 1$, $q = 2s + 1$, где $(r, s) = 1$, r и s - нечётные. Сравнение*

$$a^x \equiv b \pmod{pq}$$

разрешимо тогда и только тогда, когда:

1) $a^x \equiv b$ разрешимо по модулям p и q;

2) $\left(\left(\frac{a}{p}\right) - 1\right)\left(\left(\frac{a}{q}\right) - 1\right)\left(\left(\frac{b}{p}\right) - \left(\frac{b}{q}\right)\right) = 0$.

Совокупность данной леммы и теоремы 3 даёт обобщение результатов О.Н.Василенко[2]. В частности, можно отказаться от условия $\nu_i = 1$, снять ограничения на чётность M и на значения $\mathrm{ord}_{p_i} a$.

В лемме 3 для проверки разрешимости используется символ Лежандра. Для обобщения результатов на случай произвольных p и q нам потребуется

[7] Riesel H. Some soluble cases of the discrete logarithm problem. *BIT*, v28, no4, 1988.

[8] Нестеренко Ю.В., Частные Ферма и p-адические логарифмы. *Труды по дискретной математике*, т. 5, М. "Физматлит", 2002, с. 173-188.

[9] Василенко О.Н. *Теоретико-числовые алгоритмы в криптографии.* М.: МЦНМО, 2003.

обобщение символа Лежандра - символ степенного вычета.

Здесь приводится определение в соответствии с Artin E., Tate J.[10].

Пусть задано поле $\mathbb{K}$, являющееся конечным расширением $\mathbb{Q}$, простой идеал π в его кольце целых $\mathbb{Z}_{\mathbb{K}}$, целое число $m \notin \pi$, и пусть $\mathbb{K}$ содержит m-ый корень из единицы ξ_m. При этом $m \mid N\pi - 1$. Для целого алгебраического α определим *символ степенного вычета* следующим образом:

$$\left(\frac{\alpha}{\pi}\right)_m = \xi_m^s \equiv \alpha^{\frac{N\pi-1}{m}} \pmod{\pi}, \text{ если } \alpha \notin \pi;$$

$$\left(\frac{a}{\pi}\right)_m = 0, \text{ если } \alpha \in \pi.$$

Данный символ является обобщением символа Лежандра и обладает аналогичными свойствами: периодичностью и мультипликативностью.

Пусть далее $p - 1 = r_1^{\alpha_1} r_2^{\alpha_2} \cdot \ldots \cdot r_s^{\alpha_s} \cdot p'$, $q - 1 = r_1^{\beta_1} r_2^{\beta_2} \cdot \ldots \cdot r_s^{\beta_s} \cdot q'$, где все r_i - различные простые и $(p', r_i) = (q', r_i) = (p', q') = 1$. Пусть заданы разложения на простые идеалы в кольцах целых алгебраических:

$$(p) = \pi_{j1}\pi_{j2}\cdots \text{ в } \mathbb{Z}[\xi_{r_j^{\alpha_j}}],$$

$$(q) = \rho_{j1}\rho_{j2}\cdots \text{ в } \mathbb{Z}[\xi_{r_j^{\beta_j}}].$$

Обозначим $\pi_j = \pi_{j1}$ и $\rho_j = \rho_{j1}$.

Пусть $\mathrm{ord}_p a = \prod_{j=1}^{s} r_j^{\gamma_{1j}} \delta_1$, $\mathrm{ord}_q a = \prod_{j=1}^{s} r_j^{\gamma_{2j}} \delta_2$, где $0 \le \gamma_{1j} \le \alpha_j$, $0 \le \gamma_{2j} \le \beta_j$, $\delta_1 | p'$, $\delta_2 | q'$. При этом

$$a \equiv g_1^{\frac{p-1}{\mathrm{ord}_p a} s_1} \equiv g_1^{r_j^{\alpha_j - \gamma_{1j}} s_{1j}} \pmod{p},$$

$$a \equiv g_2^{\frac{q-1}{\mathrm{ord}_q a} s_2} \equiv g_2^{r_j^{\beta_j - \gamma_{2j}} s_{2j}} \pmod{q}$$

для некоторых первообразных g_1, g_2. Причём $(r_j, s_{1j}) = (r_j, s_{2j}) = 1$.

Тогда для любого j при $\gamma_{1j} \neq 0$ и $\gamma_{2j} \neq 0$ однозначно определяются такие e_{1j} и e_{2j}, что $0 < e_{1j} < r_j^{\gamma_{1j}}$, $0 < e_{2j} < r_j^{\gamma_{2j}}$, что $(e_{1j}, r_j) = (e_{2j}, r_j) = 1$ и

$$\left(\frac{a}{\pi_j}\right)_{r_j^{\alpha_j}} = \xi_{r_j^{\alpha_j}}^{r_j^{\alpha_j - \gamma_{1j}} e_{1j}}, \quad \left(\frac{a}{\rho_j}\right)_{r_j^{\beta_j}} = \xi_{r_j^{\beta_j}}^{r_j^{\beta_j - \gamma_{2j}} e_{2j}}.$$

[10] Artin E., Tate J. *Class Field Theory.* 1968, W.A.Benjamin, Inc.

При $\gamma_{1j} = 0$ ($\gamma_{2j} = 0$) считаем $e_{1j} = 1$ ($e_{2j} = 1$).

Для вычисления чисел e_{1j}, e_{2j} необходимо и достаточно вычислить символы степенного вычета для a.

В этих обозначениях можно сформулировать следующую теорему, дающую критерий разрешимости показательного сравнения по модулю pq.

Теорема 6. *Сравнение*

$$a^x \equiv b \pmod{pq}$$

разрешимо в том и только том случае, когда $a^x \equiv b$ разрешимо по модулям p и q, и для всех j выполнено:

- если $\gamma_{2j} \geq \gamma_{1j}$, то

$$\left(\left(\frac{a}{\pi_j}\right)_{r_j^{\alpha_j}} - 1\right) \cdot \left(\left(\frac{b}{\pi_j}\right)_{r_j^{\alpha_j}}^{e_{1j}^{-1} \pmod{r_j^{\gamma_{1j}}}} - \left(\frac{b}{\rho_j}\right)_{r_j^{\beta_j}}^{r_j^{\gamma_{2j}-\gamma_{1j}} \cdot e_{2j}^{-1} \pmod{r_j^{\gamma_{2j}}}}\right) = 0;$$

- иначе

$$\left(\left(\frac{a}{\rho_j}\right)_{r_j^{\beta_j}} - 1\right) \cdot \left(\left(\frac{b}{\pi_j}\right)_{r_j^{\alpha_j}}^{r_j^{\gamma_{1j}-\gamma_{2j}} \cdot e_{1j}^{-1} \pmod{r_j^{\gamma_{1j}}}} - \left(\frac{b}{\rho_j}\right)_{r_j^{\beta_j}}^{e_{2j}^{-1} \pmod{r_j^{\gamma_{2j}}}}\right) = 0.$$

Совокупность теорем 3 и 6 даёт общий критерий разрешимости показательного сравнения в кольце вычетов.

В третьей главе диссертации рассматривается показательное сравнение в кольце $R = GF(q)[x]/(f^\nu(x))$, где $q = p^l$, p - простое число, $l \in N$, $\nu \in N \backslash \{1\}$, а многочлен $f(x)$ неприводим над $GF(q)[x]$, имеет старший коэффициент 1 и $\deg f(x) = d$.

R является кольцом с однозначным разложением на простые множители[11], и каждый элемент кольца R можно однозначно представить в виде:

$$a(x) \equiv a^{(0)}(x) + a^{(1)}(x)f(x) + ... + a^{(\nu-1)}(x)f^{\nu-1}(x) \pmod{f^\nu(x)},$$
$$\deg a^{(i)}(x) < d.$$

Обозначим $K_s(a(x)) = a^{(s)}(x)$ - s-ый коэффициент в этом разложении. Положим по определению $K_\nu(a(x)) = 0$.

[11] Ван дер Варден Б. Л. *Алгебра.* Наука, Москва, 1976.

Если $\mathrm{ord}_R u(x) = p^\mu$, то $u(x) \equiv 1 \pmod{f(x)}$. Таким образом, корректно определить следующую функцию:

$$D_\nu(u(x)) = \begin{cases} D : f^D(x) || u(x) - 1, & \text{при } u(x) \not\equiv 1 \pmod{f^\nu(x)}; \\ \nu, & \text{при } u(x) \equiv 1 \pmod{f^\nu(x)}. \end{cases}$$

Функция $K_{D_\nu(a^{q^d-1}(x))}(a^{q^d-1}(x))$ фактически является аналогом частного Ферма в рассматриваемом факторкольце многочленов. С её помощью сформулирована и доказана теорема о подъёме решений в факторкольце по степени неприводимого многочлена над произвольным конечным полем.

Теорема 9 (о подъёме решений). *Сравнение*

$$a^n(x) \equiv b(x) \pmod{f^\nu(x)}$$

над полем $GF(q)$ *равносильно системе:*

$$\begin{cases} a^n(x) \equiv b(x) \pmod{f(x)}; \\ \textit{при } i \in \{0, ..., \mu - 1\} \\ \quad s(i) = D_\nu(a^{(q^d-1)p^i}(x)); \\ \quad n_i K_{s(i)}(a^{(q^d-1)p^i}(x)) \equiv \\ \qquad K_{s(i)}(b^{q^d-1}(x) a^{-(q^d-1)(n_0+n_1 p+...+n_{i-1}p^{i-1})}(x)) \pmod{f(x)}; \\ n \equiv n_0 + n_1 p + ... + n_{\mu-1} p^{\mu-1} \pmod{p^\mu}; \\ a^{n(q^d-1)}(x) \equiv b^{q^d-1}(x) \pmod{f^\nu(x)}. \end{cases}$$

где $\mathrm{ord}_R a(x) = p^\mu \delta$, $\delta | q^d - 1$.

Используя теорему 9, нетрудно построить конструктивный полиномиальный алгоритм подъёма решений и проверки разрешимости в кольце R, сложность которого при $l = 1$ составляет $O(d\nu \log(d\nu)(d + \log \nu) \log p)$ арифметических операций в поле $GF(p)$, а при $l > 1$ равна $O(ld\nu \log l \log(d\nu)(dl + \log \nu) \log p)$ арифметических операций в поле $GF(p)$. Кроме того, поскольку кольцо R является цепным, то можно построить конструктивный изоморфизм из R в $\overline{R} \cong GF(p^r)[x]/(x^t)$ (при $r = ld$, $t = \nu$), что позволяет в некоторых случаях оптимизировать алгоритм проверки разрешимости и подъёма решений.

В четвёртой главе сформулирован и доказан критерий разрешимости задачи дискретного логарифмирования в факторкольце по произвольному составному многочлену над полем $GF(q)$, $q = p^l$.

Как и в случае кольца вычетов, вначале получена теорема, сводящая проверку разрешимости по модулю произвольного приводимого многочлена к аналогичной задаче по модулю произведения двух различных неприводимых многочленов.

Теорема 11. *Пусть* $F(x) = f_1^{\nu_1}(x) \cdot ... \cdot f_k^{\nu_k}(x)$, *где все* f_i - *различные неприводимые над полем* $GF(q)$, *со старшими коэффициентами 1,* $k > 1$, $\mathrm{ord}_{f_i^{\nu_i}(x)} a(x) = \delta_i = p^{\mu_i}\delta_i'$, *где* $(p, \delta_i') = 1$. *Обозначим через* n_i *решение сравнения* $a^n(x) \equiv b(x) \pmod{f_i^{\nu_i}(x)}$, *а через* $\widetilde{n}_i$ *его вычет по модулю* p^{μ_i}. *Сравнение*

$$a^n(x) \equiv b(x) \pmod{F(x)}$$

разрешимо тогда и только тогда, когда выполнены следующие условия:

1) $\forall i$ *сравнение* $a^n(x) \equiv b(x) \pmod{f_i^{\nu_i}(x)}$ *разрешимо;*

2) $\forall i \neq j$ *сравнение* $a^n(x) \equiv b(x) \pmod{f_i(x) f_j(x)}$ *разрешимо;*

3) $\widetilde{n}_i \equiv \widetilde{n}_j \pmod{p^{\min(\mu_i, \mu_j)}}$.

Отдельно в главе 4 рассмотрен частный случай задачи, использующий обобщение символа Якоби для многочленов, поскольку этот случай является наиболее простым с вычислительной точки зрения.

Если $f(x)$ - неприводимый многочлен со старшим коэффициентом 1, то *обобщённый символ Якоби* определяется следующим образом[12]:

$$\left(\frac{g(x)}{f(x)}\right) = \begin{cases} 1, & \text{если } (f(x), g(x)) = 1 \text{ и} \\ & g(x) \text{ - квадрат по модулю } f(x); \\ -1, & \text{если } (f(x), g(x)) = 1 \text{ и} \\ & g(x) \text{ - не квадрат по модулю } f(x); \\ 0, & \text{иначе.} \end{cases}$$

Если $f(x) = f_1(x) \cdot \ldots \cdot f_r(x)$, где $f_i(x)$ - неприводимые, со старшими коэффициентами 1, то обобщённый символ Якоби определяется по мультипликативности:

$$\left(\frac{g(x)}{f(x)}\right) = \prod_{i=0}^{r} \left(\frac{g(x)}{f_i(x)}\right).$$

Обобщённый символ Якоби обладает стандартными свойствами: мультипликативностью и периодичностью. Полиномиальный алгоритм вычисления

[12] Bach E., Shallit J. *Algorithmic number theory.* V. 1. MIT Press, Massachusetts, 1996.

обобщённого символа Якоби[12] для произвольных многочленов $f(x)$ и $g(x)$ использует закон взаимности, а также квадратичный характер в поле $GF(q)$ $(\chi(c) = c^{\frac{q-1}{2}})$.

Лемма 9. *Пусть p - нечётное простое, $\deg f_1(x) = d_1$, $\deg f_2(x) = d_2$, $p^{ld_1} = 2r+1$, $p^{ld_2} = 2s+1$, где $(r,s) = 1$, r и s - нечётные. Сравнение*

$$a^n(x) \equiv b(x) \pmod{f_1(x)f_2(x)}$$

разрешимо тогда и только тогда, когда

1) $a^n(x) \equiv b(x)$ разрешимо по модулям $f_1(x)$ и $f_2(x)$;
2) $\left(\left(\frac{a(x)}{f_1(x)}\right) - 1\right)\left(\left(\frac{a(x)}{f_2(x)}\right) - 1\right)\left(\left(\frac{b(x)}{f_1(x)}\right) - \left(\frac{b(x)}{f_2(x)}\right)\right) = 0.$

Например, данная лемма применима для произвольного $a(x)$ в случае, если $p = 3$, $l = 1$, $(d_1, d_2) = 1$, d_i - нечётные.

Далее будем рассматривать задачу только над простым полем и обобщим лемму 9 на произвольный случай.

Пусть $\deg f_1(x) = d_1, \deg f_2(x) = d_2, p^{d_1}-1 = r_1^{\alpha_1}...r_s^{\alpha_s}p_1', p^{d_2}-1 = r_1^{\beta_1}...r_s^{\beta_s}p_2'$, где r_i - различные простые и $(p_1', r_i) = (p_2', r_i) = (p_1', p_2') = 1$.

Для всех j $(1 \le j \le s)$ и $i = 1, 2$ введём следующие обозначения: σ_i - корень $f_i(x)$, $\mathbb{Q}(\sigma_1, \xi_{r_j^{\alpha_j}}) = \mathbb{K}_{1j}$, $\mathbb{Q}(\sigma_2, \xi_{r_j^{\beta_j}}) = \mathbb{K}_{2j}$, $\mathbb{Z}_{\mathbb{K}_{ij}}$ - кольцо целых в $\mathbb{K}_{ij}$, $(p) = \pi_{j1}\pi_{j2}...$ - разложение на простые в $\mathbb{Z}_{\mathbb{K}_{1j}}$, $\pi_j = \pi_{j1}$, $(p) = \rho_{j1}\rho_{j2}...$ - разложение на простые в $\mathbb{Z}_{\mathbb{K}_{2j}}$, $\rho_j = \rho_{j1}$.

Пусть далее $\mathrm{ord}_{f_1(x)}a(x) = r_j^{\gamma_{1j}}\delta_{1j}$, $\mathrm{ord}_{f_2(x)}a(x) = r_j^{\gamma_{2j}}\delta_{2j}$, где $0 \le \gamma_{1j} \le \alpha_j$, $0 \le \gamma_{2j} \le \beta_j$, $(r_j, \delta_{1j}) = (r_j, \delta_{2j}) = 1$. При этом для некоторых порождающих элементов $g_1(x) \pmod{f_1(x)}$ и $g_2(x) \pmod{f_2(x)}$ выполнено

$$a(x) \equiv g_1(x)^{\frac{p^{d_1}-1}{\mathrm{ord}_{f_1(x)}a(x)}s_1} \equiv g_1(x)^{r_j^{\alpha_j-\gamma_{1j}}s_{1j}} \pmod{p,\ f_1(x)},$$

$$a(x) \equiv g_2(x)^{\frac{p^{d_2}-1}{\mathrm{ord}_{f_2(x)}a(x)}s_2} \equiv g_2(x)^{r_j^{\beta_j-\gamma_{2j}}s_{2j}} \pmod{p,\ f_2(x)},$$

где $(r_j, s_{1j}) = (r_j, s_{2j}) = 1$ для всех j $(1 \le j \le s)$.

Тогда для любого j при $\gamma_{1j} \ne 0$ и $\gamma_{2j} \ne 0$ однозначно определяются такие $0 < e_{1j} < r_j^{\gamma_{1j}}$, $0 < e_{2j} < r_j^{\gamma_{2j}}$, что $(e_{1j}, r_j) = (e_{2j}, r_j) = 1$ и

$$\left(\frac{a(\sigma_1)}{\pi_j}\right)_{r_j^{\alpha_j}} = \xi_{r_j^{\alpha_j}}^{r_j^{\alpha_j-\gamma_{1j}}e_{1j}}, \quad \left(\frac{a(\sigma_2)}{\rho_j}\right)_{r_j^{\beta_j}} = \xi_{r_j^{\beta_j}}^{r_j^{\beta_j-\gamma_{2j}}e_{2j}}.$$

При $\gamma_{1j} = 0$ ($\gamma_{2j} = 0$) считаем $e_{1j} = 1$ ($e_{2j} = 1$).

Для нахождения чисел e_{ij} необходимо и достаточно вычислить символы степенного вычета для $a(\sigma_i)$.

Теорема 14. *Сравнение*

$$a^n(x) \equiv b(x) \pmod{p,\ f_1(x)f_2(x)}$$

разрешимо тогда и только тогда, когда разрешимы аналогичные сравнения по модулям $f_1(x)$ и $f_2(x)$ и для всех j ($1 \le j \le s$) выполнено:

- если $\gamma_{2j} \ge \gamma_{1j}$, то

$$\left(\left(\frac{a(\sigma_1)}{\pi_j}\right)_{r_j^{\alpha_j}} - 1\right) \cdot \left(\left(\frac{b(\sigma_1)}{\pi_j}\right)_{r_j^{\alpha_j}}^{e_{1j}^{-1} \pmod{r_j^{\gamma_{1j}}}} - \left(\frac{b(\sigma_2)}{\rho_j}\right)_{r_j^{\beta_j}}^{r_j^{\gamma_{2j}-\gamma_{1j}} \cdot e_{2j}^{-1} \pmod{r_j^{\gamma_{2j}}}}\right) = 0;$$

- иначе

$$\left(\left(\frac{a(\sigma_2)}{\rho_j}\right)_{r_j^{\beta_j}} - 1\right) \cdot \left(\left(\frac{b(\sigma_1)}{\pi_j}\right)_{r_j^{\alpha_j}}^{r_j^{\gamma_{1j}-\gamma_{2j}} \cdot e_{1j}^{-1} \pmod{r_j^{\gamma_{1j}}}} - \left(\frac{b(\sigma_2)}{\rho_j}\right)_{r_j^{\beta_j}}^{e_{2j}^{-1} \pmod{r_j^{\gamma_{2j}}}}\right) = 0.$$

Таким образом, совокупность теорем 11 и 14 даёт критерий разрешимости показательного сравнения в произвольном факторкольце многочленов над конечным полем.

Вопрос о разрешимости показательного сравнения, как в случае кольца вычетов по составному модулю, так и в случае факторкольца многочленов, свёлся к вычислению символов степенного вычета. Полученные критерии являются конструктивными, только если вычисление соответствующих символов можно выполнить за полиномиальное время. Изучению этого вопроса посвящена **пятая глава диссертации**.

На данный момент вопрос о быстром вычислении r-степенного символа (для простого r) в общем случае остаётся открытым. Хорошо известен способ вычисления символа Лежандра (т.е. при $r = 2$). Scheidler R.[13] (глава 7) описывает алгоритмы вычисления символов степенного вычета для $r = 3,\ 5$. В 2009 году аналогичный алгоритм, использующий обобщённый закон взаимности и

[13]Scheidler R. Applications of Algebraic Number Theory to Cryptography. PhD Dissertation, University of Manitoba (Canada), 1993. (http://math.ucalgary.ca/ rscheidl/Papers/my-thesis.pdf)

алгоритм евклидового нормирования Ленстры, был приведён для $r = 7$.[14] Там же были, например, приведены явные формулы для $\left(\frac{7}{\pi}\right)_7$, $\left(\frac{\xi_7+\xi_7^6}{\pi}\right)_7$, $\left(\frac{\xi_7^2+\xi_7^5}{\pi}\right)_7$, $\left(\frac{\xi_7^3+\xi_7^4}{\pi}\right)_7$. Методы, используемые в данных работах, можно обобщить для других r-степенных символов при небольших значениях r, однако это выходило за рамки нашего исследования.

Помимо r-степенных символов нас интересовал вопрос о вычислении символов степени r^k. Именно этому посвящена **пятая глава** диссертации. В ней доказано, что для символов специального вида данный вопрос можно полиномиально свести к символам r-ой степени, а именно, получены формулы «подъёма» символа степенного вычета для некоторых частных случаев, используемых в теоремах 6 и 14.

Пусть $m = r^k$ для некоторого простого r, σ - корень $f(x)$ в его поле разложения, $\mathbb{K} = \mathbb{Q}(\sigma, \xi_m)$, $\mathbb{K}_1 = \mathbb{Q}(\sigma, \xi_r)$. Рассмотрим разложения идеала (p) в кольцах целых алгебраических:

$$(p) = \pi_1\pi_2 \cdot ... \cdot \pi_n \text{ в } \mathbb{Z}_{\mathbb{K}}, \tag{3}$$

$$(p) = \pi'_1\pi'_2 \cdot ... \cdot \pi'_l \text{ в } \mathbb{Z}_{\mathbb{K}_1}. \tag{4}$$

Обозначим за $\widetilde{\pi_i}'$ продолжение идеала π'_i в $\mathbb{Z}_{\mathbb{K}}$.

В пятой главе диссертации сформулированы и доказаны две следующие теоремы.

Теорема 15. *Пусть π - идеал из разложения (3), π' - идеал из разложения (4) и $\pi \mid \widetilde{\pi}'$. Пусть $g(x)$ - образующий в поле $GF(p)[x]/(f(x))$, для которого известно, что $\left(\frac{g(\sigma)}{\pi}\right)_{r^k} = \xi_{r^k}^s$. Пусть для некоторого $a(x)$ требуется определить такое $c \in \mathbb{N}$, что $\left(\frac{a(\sigma)}{\pi}\right)_{r^k} = \xi_{r^k}^c$, $0 \le c < r^k$. Обозначим $a_0(x) = a(x)$. Тогда c является решением системы:*

$$\begin{cases} \left(\frac{g(\sigma)}{\pi'}\right)_r^{c_0} = \left(\frac{a(\sigma)}{\pi'}\right)_r, \text{ где } 0 \le c_0 < r; \\ \text{при } i \in \{1, ..., k-1\}: \\ \quad a_i^r(x) \equiv a_{i-1}(x)g^{-c_{i-1}}(x) \pmod{p, f(x)}; \\ \quad \left(\frac{g(\sigma)}{\pi'}\right)_r^{c_i} = \left(\frac{a_i(\sigma)}{\pi'}\right)_r, \text{ где } 0 \le c_i < r; \\ c \equiv s(c_0 + c_1 r + c_2 r^2 + ... + c_{k-1}r^{k-1}) \pmod{r^k}. \end{cases}$$

[14] Caranay P.C., Scheidler R. An efficient seventh power residue symbol algorithm. *International Journal of Number Theory*, 2009 (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.158.2501)

Следующая теорема во многом повторяет теорему 15, однако она позволяет существенно упростить вычисления. При возведении произвольного $a(x) \in (GF(p)[x]/(f(x)))^*$ в степень $\frac{p^d-1}{p-1}$ мы получаем элемент порядка $p-1$, т.е. просто целое число по модулю p. Этот факт позволяет нам для случая $r^k||p-1$ перейти к вычислениям в простом подполе (т.е. просто по модулю p).

Теорема 16. *Пусть $m = r^k$ - такое, что $r^k||p-1$ (т.е. $r \nmid \frac{p^d-1}{p-1}$). Пусть π - идеал из разложения (3), π' - идеал из разложения (4) и $\pi \mid \widetilde{\pi}'$. Пусть g - образующий в поле $GF(p)$, для которого $\left(\frac{g}{\pi}\right)_{r^k} = \xi_{r^k}^s$. Пусть для некоторого $a(x)$ требуется найти такое $c \in \mathbb{N}$, что $\left(\frac{a(\sigma)}{\pi}\right)_{r^k} = \xi_{r^k}^c$, $0 \le c < r^k$. Обозначим $a_0 \equiv a^{\frac{p^d-1}{p-1}}(x) \pmod{p,\ f(x)}$. Тогда c является решением системы:*

$$\begin{cases} \left(\frac{g}{\pi'}\right)_r^{c_0} = \left(\frac{a_0}{\pi'}\right)_r, \ \text{где } 0 \le c_0 < r; \\ \text{при } i \in \{1, ..., k-1\}: \\ \qquad a_i^r \equiv a_{i-1} g^{-c_{i-1}} \pmod{p}; \\ \qquad \left(\frac{g}{\pi'}\right)_r^{c_i} = \left(\frac{a_i}{\pi'}\right)_r, \ \text{где } 0 \le c_i < r; \\ c \equiv s \cdot \left(\frac{p^d-1}{p-1}\right)^{-1} \cdot (c_0 + c_1 r + c_2 r^2 + ... + c_{k-1} r^{k-1}) \pmod{r^k}. \end{cases}$$

В теоремах 15 и 16 для нахождения a_i требуется извлечение корня r-ой степени. Это выполняется при помощи алгоритма Адлемана, Мандерса, Миллера[12] (гл. 7.3), являющегося обобщением алгоритма Шенкса. В данном алгоритме требуется решать задачу дискретного логарифмирования в подгруппе порядка r, что равносильно вычислению символа r-степенного вычета[15].

Недостатком данных теорем является необходимость вычисления символа степенного вычета степени r^k для некоторого элемента поля. Однако, в некоторых случаях мы можем выбрать идеалы π и π' таким образом, что значение s, используемое в теоремах, будет известно.

В пятой главе диссертации рассмотрены три случая для $r^k||p-1$, в которых мы можем получить число s, требуемое в теореме 16.

[15] Adleman L.M., Pomerance C., Rumely R.S. On Distinguishing Prime Numbers from Composite Number. *Ann. Math.* 117, 173-206, 1983.

Первый случай. $d = 1$, $\mathbb{K} = \mathbb{Q}(\xi_m)$. В данном случае получаем, что $\pi = (p,\ \xi_{r^k} - g^{\frac{p-1}{r^k}})$ и $\pi' = (p,\ \xi_r - g^{\frac{p-1}{r}})$ (при этом выполнено, что $\pi \mid \widetilde{\pi}'$). Тогда $\frac{p^d-1}{p-1} = 1$ и $s = 1$, т.е. последнее сравнение системы перепишется как

$$c \equiv c_0 + c_1 r + c_2 r^2 + ... + c_{k-1} r^{k-1} \pmod{r^k}.$$

Второй случай. Пусть $d > 1$, $\sigma \in \mathbb{Q}(\xi_{r^k})$, т.е. $\mathbb{K} = \mathbb{Q}(\xi_{r^k})$. Тогда получим, что разложение на множители идеала (p) имеет вид:

$$(p) = \prod_{(s_i, r^k)=1} (p,\ \xi_{r^k} - g^{\frac{p-1}{r^k} s_i}). \tag{5}$$

Пусть $\pi_i = (p,\ \xi_{r^k} - g^{\frac{p-1}{m} s_i})$, тогда $N(\pi_i) = p$ для всех i. Выберем $\pi = (p,\ \xi_{r^k} - g^{\frac{p-1}{r^k}})$. При этом получим, что $s = 1$, т.е. последнее сравнение системы перепишется как

$$c \equiv \left(\frac{p^d - 1}{p-1}\right)^{-1} \cdot (c_0 + c_1 r + c_2 r^2 + ... + c_{k-1} r^{k-1}) \pmod{r^k}.$$

Заметим, что если $\sigma \in \mathbb{Q}(\xi_r)$, то в $\mathbb{K}_1 = \mathbb{Q}(\xi_r)$ имеет место разложение (p), аналогичное (5). Тогда в качестве π' можно выбрать $(p,\ \xi_r - g^{\frac{p-1}{r}})$.

Третий случай. Пусть $\sigma \notin \mathbb{Q}(\xi_m)$ и $\sigma + \xi_m - \xi_m^i ((i, m) = 1)$ не являются корнями $f(x)$. Тогда $\mathbb{Q}(\sigma,\ \xi_m) = \mathbb{Q}(\theta)$, где $\theta = \sigma + \xi_m$.

Найдём $Q(x)$ - минимальный многочлен элемента θ и рассмотрим его разложение на множители по модулю p. Обозначим за $\sigma_1 = \sigma,\ \sigma_2,\ ...,\ \sigma_d$ - все корни $f(x)$.

Рассмотрим многочлен:

$$P(x) = \prod_{(s_i, m)=1} \prod_{j=1}^{d} (x - (\sigma_j + \xi_m^{s_i})).$$

Лемма 12. *Пусть g - произвольный первообразный корень по модулю p. Тогда*

$$P(x) \equiv \prod_{(s_i, m)=1} f(x - g^{\frac{p-1}{m} s_i}) \pmod{p}.$$

Поскольку θ - корень $P(x)$, то для его минимального многочлена $Q(x)$ и некоторого набора индексов I выполнено:

$$Q(x) \equiv \prod_{i \in I} f(x - g^{\frac{p-1}{m} s_i}) \pmod{p}.$$

Предположим, что $p^2 \nmid d(Q)$. Тогда

$$(p) = \prod_{i \in I} (p,\ f(\xi_m + \sigma - g^{\frac{p-1}{m} s_i})).$$

Обозначим $\pi_i = (p,\ f(\xi_m + \sigma - g^{\frac{p-1}{m} s_i}))$. При этом $N(\pi_i) = p^d$. Таким образом, для данного случая мы также можем найти s, требуемое в теореме. А именно, $s \equiv s_i^{-1} \cdot \frac{p^d-1}{p-1} \pmod{m}$, то есть последнее сравнение системы перепишется как

$$c \equiv s_i^{-1} \cdot (c_0 + c_1 r + c_2 r^2 + ... + c_{k-1} r^{k-1}) \pmod{r^k}.$$

Таким образом, в рассмотренных случаях вычисление r^k-степенного вычета полиномиально сводится к вычислению символов r-степенного вычета для некоторых элементов.

В **заключении диссертации** подводятся основные итоги работы, а также указаны возможные дальнейшие темы для исследования. Вопросы, рассмотренные в диссертации, могут получить дальнейшее развитие в следующих направлениях:

• вычисление символов r-степенного вычета для некоторых простых r;

• получение явного вида простых делителей идеала (p), для которых можно явно выписать значение $\left(\frac{g(\sigma)}{\pi}\right)_m$ в случае $m \nmid p - 1$;

• исследование вопроса эквивалентности вычисления символов степенного вычета и проверки разрешимости задачи дискретного логарифмирования.

Автор выражает благодарность научному руководителю, кандидату физико-математических наук, доценту Михаилу Алексеевичу Черепнёву за постановку задач и помощь в работе.

Автор благодарит кандидата физико-математических наук, доцента Антона Александровича Клячко за ценные советы.

Автор благодарит коллектив кафедры теории чисел и отделения аспирантуры механико-математического факультета за поддержку.

Публикации автора по теме диссертации

1. Маркелова А.В. О разрешимости задачи дискретного логарифмирования. *Вестник МГУ*, сер.1. Матем. Механ., 2008, №6, с. 6-9.

2. Маркелова А.В. Дискретное логарифмирование в произвольных факторкольцах многочленов от одной переменной над конечным полем. *Дискретная математика*, 2010г., том 22, выпуск 2, стр. 120-132.

3. Маркелова А.В. О разрешимости задачи дискретного логарифмирования в кольце вычетов по составному модулю. *Математика и безопасность информационных технологий*. Материалы конференции в МГУ 28-29 октября 2004 г. С.185-191. М.: МЦМНО, 2005