**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА**

**МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ**

*На правах рукописи*

УДК 511.225+511.23

Поповян Илья Ардашесович

# ПОДЪЁМ РЕШЕНИЙ ПОКАЗАТЕЛЬНЫХ УРАВНЕНИЙ В КОНЕЧНЫХ КОЛЬЦАХ

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва, 2007

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

**Научный руководитель:** кандидат физико-математических наук, доцент М.А. Черепнев

**Официальные оппоненты:** доктор физико-математических наук, профессор В.Г. Чирский,
кандидат физико-математических наук, Е.В. Горбатов

**Ведущая организация:** Владимирский государственный педагогический университет

Защита диссертации состоится 18 мая 2007 г. в 16 ч. 15 мин. на заседании диссертационного совета Д.501.001.84 в Московском государственном университете им. М.В. Ломоносова по адресу: 119992, ГСП-2, Москва, Ленинские горы, МГУ, Механико-математический факультет, ауд. 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (главное здание МГУ, 14 этаж).

Автореферат разослан 18 апреля 2007 г.

Ученый секретарь
диссертационного совета
Д.501.001.84 в МГУ
профессор В.Н. Чубариков

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.**

В современной криптографии важную роль играет понятие односторонней функции. *Односторонней* называется такая вычислимая за полиномиальное время, то есть за время, равное многочлену от длины входа, функция, задача обращения которой неполиномиальна. Согласно У. Диффи[1] в середине 70-х годов Дж. Гилл предложил использовать в качестве одностороннего отображения возведение в степень по модулю простого числа. Позже оно было обобщено до возведения в степень в произвольной конечной циклической группе, то есть если $(G, \times)$ – циклическая группа, $G = < g >$, то

$$\mathbb{Z} \to G \ : \ n \mapsto g^n.$$

Задача обращения этого отображения называется *(обобщенной) задачей дискретного логарифмирования (GDLP)*, а при $G = (\mathbb{Z}/(p))^*$, где $p$ – простое рациональное число, эта задача называется просто *задачей дискретного логарифмирования (DLP)*. На ее предположительной неполиномиальности основана стойкость многих асимметричных криптосхем, таких как, например, схема распределения ключей Диффи-Хэллмэна[1] или схема электронной подписи Эль-Гамаля[2] и ее варианты, DSA[3] и ГОСТ-34.10-94.

Естественным обобщением DLP является GDLP для $G = (\mathbb{Z}/(m))^*$, где $m \in \mathbb{Z}$ – составное. Задача полиномиального сведения GDLP в $(\mathbb{Z}/m\mathbb{Z})^*$ к DLP в группах $(\mathbb{Z}/p_i\mathbb{Z})^*$, соответствующих всем простым делителям $p_i$ числа $m$, решена. Решение состоит в применении китайской теоремы об остатках для сведения задачи в $(\mathbb{Z}/m\mathbb{Z})^*$ к задаче в $(\mathbb{Z}/p^k\mathbb{Z})^*, p^k||m$, и так называемого подъёма решения.

*Подъёмом решения* в кольце целых рациональных чисел называется задача сведения GDLP в $(\mathbb{Z}/p^k\mathbb{Z})^*$ к DLP в $(\mathbb{Z}/p\mathbb{Z})^*$. Одним из первых эту задачу в более общей постановке рассмотрел Г. Ризель[4] и предложил использовать для ее решения аппарат частных Ферма. Свойства частных

---

[1] W. Diffie and M. E. Hellman, *New Directions in Cryptography.* IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, pp. 644-654.

[2] T. ElGamal , *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory, Vol. IT-31, No. 4, July 1985, pp. 469-472.

[3] FIPS 186 , *Digital signature standard.* Federal Information Processing Standards Publication 186, U.S. Department of Commerce/ N.I.S.T., National Technical Information Service, Springfield, Virginia, 1994.

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

Ферма позволили ему свести задачу подъёма решения к линейным сравнениям, и использовать решения последних для нахождения дискретных логарифмов в $(\mathbb{Z}/(m))^*$ при некоторых значениях $m$, в частности, при $m = p^k$.

В 2002 году вышла статья Ю.В. Нестеренко[5], в которой он показал возможность использования $p$-адических логарифмов вместо частных Ферма для подъёма решения в кольце $\mathbb{Z}$, а также установил связь между этими функциями.

Частные Ферма обладают следующим свойством: их значения на первообразных корнях по модулю $p$ не делятся на $p$. Это свойство обеспечивает несократимость линейных сравнений, возникающих в процессе подъёма решения, что, в свою очередь, позволяет эффективно их решать. В работе М.А. Черепнева[6] предложен способ модификации частного Ферма таким образом, чтобы указанное свойство выполнялось и для произвольного элемента $g \in (\mathbb{Z}/p\mathbb{Z})^*$.

Естественным теоретико-числовым обобщением задачи подъёма решения показательного сравнения в $\mathbb{Z}$ является аналогичная задача с заменой кольца целых $\mathbb{Z}$ на кольцо целых $\mathbb{Z}_K$ какого-либо конечного расширения $K$ поля $\mathbb{Q}$.

В 1979 году Н. Накагоши[7] получил полное, хотя и не всегда конструктивное, описание мультипликативной группы $\left(\mathbb{Z}_K/\mathfrak{p}^N\right)^*$, однако результат был малопригоден для практического применения. Почти 20 лет спустя, в 1998 году, Г. Коэн, Ф. Диаз-и-Диаз и М. Оливер[8], работая над алгоритмами вычислений в теории полей классов, впервые дали конструктивное описание мультипликативного базиса группы $(\mathbb{Z}_K/\mathfrak{m})^*$ по произвольному идеалу $\mathfrak{m}$ кольца $\mathbb{Z}_K$. Рассматривая задачу нахождения представления произвольного элемента в заданном мультипликативном базисе группы $(\mathbb{Z}_K/\mathfrak{m})^*$, они свели ее к аналогичной задаче в $\left(\mathbb{Z}_K/\mathfrak{p}^N\right)^*$, где $\mathfrak{p}$ – простой идеал, такой что $\mathfrak{p}^N||\mathfrak{m}$. Далее они заметили, что для решения последней, являющейся родственной задаче подъёма решения, вполне естественно попытаться воспользоваться $\mathfrak{p}$-адическим логарифмом, и указали, что такой подход действительно срабатывает почти для

---

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

[6]Черепнев М. А., *О некотором свойстве дискретного логарифма.* Тез. докл. XII межд. конф. "Проблемы теоретической кибернетики". Н. Новгород, 1999.

[7]Nakagoshi N., *The structure of the multiplicative group of residue classes modulo $\mathfrak{p}^{N+1}$.* Nagoya Math. J., Vol. 73 (1979), 41-60.

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

всех идеалов. Однако при большом значении параметра $\frac{e}{p-1}$, где $e$ – индекс ветвления идеала $\mathfrak{p}$, а $p$ – простое рациональное, такое что $\mathfrak{p}|(p)$, применить $\mathfrak{p}$-адический логарифм не удается. Поэтому вместо использования $\mathfrak{p}$-адического логарифма они предложили *индуктивный метод*, названный *квадратичным*, позволяющий за $[\log_2 N]$ итераций получить представление произвольного элемента в заданном мультипликативном базисе уже для произвольного простого идеала $\mathfrak{p}$.

Продолжая тематику, в 1999 году в своей книге[9] Г. Коэн предложил обобщить квадратичный метод при помощи так называемого логарифма Артина-Хассе. Также он заметил, что для решения задачи нахождения представления произвольного элемента в заданном мультипликативном базисе группы $\left(\mathbb{Z}_K/\mathfrak{p}^N\right)^*$ можно использовать *комбинированный метод*, совмещающий квадратичный метод и подход с $\mathfrak{p}$-адическим логарифмом, однако подробных решений не привел. В 2003 году вышла статья Ф. Гесса, Ч. Паули и М. Поста[10], в которой указанный комбинированный метод был реализован, при этом были также получены оценки его сложности в терминах операций с матрицами и арифметических операций с алгебраическими числами в соответствующих факторах.

В диссертации исследуется задача подъёма решений показательных сравнений в кольцах целых произвольных конечных расширений поля рациональных чисел.

**Научная новизна работы.**

Основные результаты диссертации являются новыми и состоят в следующем:

1. Доказаны теоремы о подъёме решений показательных сравнений в кольцах целых алгебраических чисел, дающие новые явные формулы для вычисления решений с использованием логарифма Артина-Хассе и $\mathfrak{p}$-адического логарифма. Получены формулы для эффективного вычисления логарифма Артина-Хассе и $\mathfrak{p}$-адического логарифма. На основе этих результатов построен полиномиальный алгоритм подъёма решений показательных сравнений в кольцах целых алгебраических чисел.

2. Подсчитана функция Кармайкла для некоторых специальных групп, связанных с группой главных единиц кольца целых $\mathfrak{p}$-адического пополнения произвольного поля алгебраических чисел.

3. Построены аналоги частных Ферма на подгруппах группы главных

[9]Cohen H., *Advanced Topics in Computational Number Theory.* GTM 193, Springer-NY, 1999.

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

единиц кольца целых $\mathfrak{p}$-адического пополнения произвольного поля алгебраических чисел, которые позволяют упростить процедуру подъёма решений показательных сравнений в кольцах целых алгебраических чисел. Получены формулы, связывающие построенные аналоги частных Ферма с логарифмом Артина-Хассе и $\mathfrak{p}$-адическим логарифмом, обобщающие полученные ранее формулы для целых рациональных аргументов.

**Цель работы.**

1. Построить новый алгоритм подъёма решений показательных сравнений в кольцах целых полей алгебраических чисел, оценить его эффективность.

2. Оптимизировать выбор логарифмических функций, используемых для решения указанной задачи.

**Методы исследования.**

Работа опирается на исследования в теории алгебраических чисел и $\mathfrak{p}$-адическом анализе, а также на теоретико-числовые алгоритмы. Для исследования свойств $\mathfrak{p}$-адического логарифма, логарифма Артина-Хассе и оптимальных логарифмических функций, а также для вычисления порядков элементов применяются методы теории алгебраических чисел и $\mathfrak{p}$-адического анализа. Для оценки сложностей предложенных алгоритмов – результаты теории сложности вычислений.

**Теоретическая и практическая ценность.**

Работа носит теоретический характер. Результаты диссертации могут найти применение в теории алгебраических чисел, $\mathfrak{p}$-адическом анализе и вычислительной теории чисел.

**Апробация работы.**

Результаты диссертации докладывались на следующих семинарах и конференциях:

1. Научно-исследовательский семинар по теории чисел под руководством Ю.В. Нестеренко и Н.Г. Мощевитина, механико-математический факультет МГУ (2003 г.);

2. Семинар „Теоретико-числовые вопросы криптографии“ под руководством М.А. Черепнева и Ю.В. Нестеренко, механико-математический факультет МГУ (2004-2006 гг.).

3. Конференция „Математика и безопасность информационных технологий“, МГУ (2003 г.)

4. Конференция „Ломоносовские чтения“, МГУ (2006 г.)

5. Международная конференция „Диофантовы и аналитические проблемы теории чисел“, МГУ (2007 г.).

**Публикации.**

Результаты диссертации опубликованы в двух работах автора [1-2], список которых приводится в конце автореферата. Работ, написанных в соавторстве, нет.

**Структура и объем работы.**

Диссертация изложена на 83 страницах. Она состоит из введения, трех глав и списка литературы, включающего 36 наименований.

## КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Пусть $K$ – конечное расширение $\mathbb{Q}$, $\mathbb{Z}_K$ – его кольцо целых. Пусть также $\mathfrak{p}$ – простой идеал $\mathbb{Z}_K$. Рассмотрим показательное сравнение

$$\alpha^x \equiv \beta \bmod \mathfrak{p}^N,\ x \in \mathbb{Z}, \tag{1}$$

где $N \in \mathbb{N}\backslash\{1\}$, $\alpha, \beta \in \mathbb{Z}_K\backslash\mathfrak{p}$. Задача сведения нахождения решения сравнения (1) к нахождению решения сравнения

$$\alpha^x \equiv \beta \bmod \mathfrak{p},\ x \in \mathbb{Z}$$

называется *задачей подъёма решения показательного сравнения (1) в кольце* $\mathbb{Z}_K$. Решению этой задачи посвящена **вторая глава** диссертации. В ней предложен алгоритм комбинированного типа с использованием логарифма Артина-Хассе и $\mathfrak{p}$-адического логарифма.

Пусть идеал $\mathfrak{p}$ лежит над $p \in \mathbb{Z}$ и имеет индекс ветвления $e$ и степень расширения $f$, то есть $e \in \mathbb{N} : \mathfrak{p}^e || (p)$ и $f \in \mathbb{N} : \#(\mathbb{Z}_K/\mathfrak{p}) = p^f$. Обозначим $\rho = \left[\frac{e}{p-1}\right] + 1$ и пусть $\nu$ обозначает $\mathfrak{p}$-адический показатель в $\mathbb{Z}_K$. Зафиксируем также какой-либо элемент $\pi \in \mathbb{Z}_K$, такой что $\nu(\pi) = 1$.

Основной результат о подъёме решения разбивается на три случая и формулируется соответственно в одном утверждении и двух теоремах. Первый, „вырожденный“, случай состоит в том, что

$$\nu(\alpha^{p^f-1} - 1) \geq N.$$

**Утверждение 2.1.** *Пусть* $\alpha, \beta \in \mathbb{Z}_K \backslash \mathfrak{p}$, $N \in \mathbb{N} \backslash \{1\}$ *и* $a = \nu(\alpha^{p^f-1} - 1) \geq N$ *(допустимо* $a = \infty$*).*

*Тогда*

$$\alpha^x \equiv \beta \bmod \mathfrak{p}^N, x \in \mathbb{Z} \Leftrightarrow \begin{cases} \beta^{p^f-1} \equiv 1 \bmod \mathfrak{p}^N, \\ \alpha^x \equiv \beta \bmod \mathfrak{p}, x \in \mathbb{Z}. \end{cases}$$

В следующей теореме рассматривается "низкий" случай, то есть

$$\nu(\alpha^{p^f-1} - 1) < N \leq \rho,$$

возникающий из-за того, что в $\mathbb{Z}_K$ индекс ветвления $e$ идеала $\mathfrak{p}$ может быть больше $p$. Для решения задачи подъёма в этом случае используется специальная функция, *логарифм Артина-Хассе*, задаваемая многочленом

$$L(1+x) = \sum_{i=1}^{p-1} (-1)^{i-1} \frac{x^i}{i}.$$

Обладающий свойствами, аналогичными свойствам обычных логарифмов, логарифм Артина-Хассе позволяет в несколько этапов провести подъём решения сравнения (1).

**Лемма 2.1.** *Пусть* $x, y, z \in \mathbb{Z}_K, x \in \mathfrak{p}, 1 \leq \nu(y) \leq \nu(z)$, *тогда*

*I)*

$$\nu(L(1+x)) = \nu(x).$$

*II)*

$$L((1+y)(1+z)) \equiv L(1+y) + L(1+z) \bmod \mathfrak{p}^{p\nu(y)}.$$

Далее для $y \in \mathbb{R}$ скобки $\lceil y \rceil$ обозначают *верхнюю положительную целую часть*, то есть при $y \in \mathbb{R}, y > 0$ обозначим $\lceil y \rceil \in \mathbb{N}$ – минимальное, такое что $\lceil y \rceil \geq y$, а при $y \leq 0$ положим $\lceil y \rceil := 0$.

**Теорема 2.1.** *Пусть* $\alpha, \beta \in \mathbb{Z}_K \backslash \mathfrak{p}$, $N \in \{2, \ldots, \rho\}$, $a = \nu(\alpha^{p^f-1} - 1) < N$ *и* $t = \lceil \log_p \frac{N}{a} \rceil$.

*Тогда*

$$\alpha^x \equiv \beta \bmod \mathfrak{p}^N, x \in \mathbb{Z}$$
$$\Updownarrow$$
$$\begin{cases} x \equiv \sum_{i=0}^{t-1} y_i p^i \bmod p^t, y_i \in \{0,1,\ldots,p-1\}, & (T1.1) \\ y_i L\left(\alpha^{p^i(p^f-1)}\right) \equiv L\left(\left(\beta\alpha^{-\sum_{j=0}^{i-1} y_j p^j}\right)^{(p^f-1)}\right) \bmod \mathfrak{p}^{ap^{i+1}}, & (T1.2) \\ \qquad i = 0,\ldots,t-2 \ npu \ t \geq 2, & \\ y_{t-1} L\left(\alpha^{p^{t-1}(p^f-1)}\right) \equiv L\left(\left(\beta\alpha^{-\sum_{j=0}^{t-2} y_j p^j}\right)^{(p^f-1)}\right) \bmod \mathfrak{p}^N, & (T1.3) \\ \alpha^x \equiv \beta \bmod \mathfrak{p}, x \in \mathbb{Z}. & (T1.4) \end{cases}$$

В следующей теореме рассматривается "высокий" случай, то есть

$$\nu(\alpha^{p^f-1} - 1) < N, \ N > \rho.$$

Процедура подъёма в этом случае состоит в использовании теоремы 2.1 при $N = \rho$ для нахождения части решения и дополнительном однократном применении $\mathfrak{p}$-*адического логарифма*, определяемого на $\mathfrak{p}$-адическом пополнении $K_\nu$ рядом

$$Log_{\mathfrak{p}}(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}.$$

Для $0 \neq \eta - 1 \in \mathfrak{p}$ обозначим

$$R(\eta) := \lceil \frac{N - \nu(\eta-1)p^{\lceil \log_p \frac{\rho}{\nu(\eta-1)} \rceil} - r(\eta)}{e} \rceil,$$

где

$$r(\eta) := \nu(\eta^{p^{\lceil \log_p \frac{e}{(p-1)\nu(\eta-1)} \rceil + 1}} - 1) - \nu(\eta^{p^{\lceil \log_p \frac{e}{(p-1)\nu(\eta-1)} \rceil}} - 1) - e.$$

Эти функции определяют мультипликативный порядок числа $\eta$ в факторе $\left(\mathbb{Z}_K/\mathfrak{p}^N\right)^*$.

**Теорема 2.2.** *Пусть* $\alpha, \beta \in \mathbb{Z}_K \backslash \mathfrak{p}$, $N \in \mathbb{N}, N > \rho$, $a = \nu(\alpha^{p^f-1} - 1) < N, t = \lceil \log_p \frac{\rho}{a} \rceil$ *и* $R = R(\alpha^{p^f-1})$.

*Тогда*

$$\alpha^x \equiv \beta \bmod \mathfrak{p}^N, x \in \mathbb{Z}$$
$$\Updownarrow$$
$$\begin{cases} x \equiv y_0 + y_1 p^t \bmod p^{t+R}, y_0, y_1 \in \mathbb{Z} : 0 \le y_0 < p^t, 0 \le y_1 < p^R, & (T2.1) \\ \alpha^{y_0(p^f-1)} \equiv \beta^{(p^f-1)} \bmod \mathfrak{p}^\rho, & (T2.2) \\ y_1 Log_{\mathfrak{p}} \left(\alpha^{p^t(p^f-1)}\right) \equiv Log_{\mathfrak{p}} \left((\beta\alpha^{-y_0})^{(p^f-1)}\right) \bmod \pi^N, & (T2.3) \\ \alpha^x \equiv \beta \bmod \mathfrak{p}, x \in \mathbb{Z}. & (T2.4) \end{cases}$$

**Третья глава** диссертации посвящена формальному построению алгоритма подъёма решения и другим вспомогательным вопросам, возникающим в связи с его вычислительной частью. В частности, даются эффективные формулы для вычисления логарифма Артина-Хассе и $\mathfrak{p}$-адического логарифма. Также приводится алгоритм решения линейного сравнения

$$x\gamma \equiv \delta \bmod \mathfrak{p}^M,\ x \in \mathbb{Z},$$

возникающего в формулах (T1.2),(T1.3),(T2.3).

В теоремах 2.1 и 2.2 используются логарифмические функции, вычисление значений которых по определениям представляется непрактичным. В следущих двух утверждениях приводятся формулы, позволяющие вычислить эти функции за полиномиальное по $p$ число умножений в кольце $\mathbb{Z}_K$.

Следущее утверждение дает простое тождество для логарифма Артина-Хассе.

**Утверждение 3.1.** *Пусть $x$ – переменная, имеет место сравнение*

$$L(1+x) \equiv \frac{(1+x)^p - (1+x^p)}{p} \bmod \mathfrak{p}^e.$$

Утверждение 3.2 дает полиномиально вычислимое $\mathfrak{p}$-адическое приближение для $\mathfrak{p}$-адического логарифма.

**Утверждение 3.2.** *Пусть $M \in \mathbb{N} \cup \{0\}, \eta \in K_\nu, \nu(\eta) \ge \rho$. Тогда имеет место сравнение*

$$Log_{\mathfrak{p}}(1+\eta) \equiv \frac{(1+\eta)^{p^{\left\lceil \frac{M}{e} \right\rceil}} - 1}{p^{\left\lceil \frac{M}{e} \right\rceil}} \bmod \pi^{M+1+\sigma},$$

*где*

$$\sigma = \begin{cases} \rho & \text{при } M \geq \rho, \\ \left[2\left(1 - \left\{\frac{e}{p-1}\right\}\right)\right] & \text{иначе.} \end{cases}$$

Наконец, проводится рассчет вычислительной сложности предлагаемого алгоритма подъёма решения. При получении оценок растущими параметрами считались лишь $p$ и $N$.

**Теорема 3.5.** *Сложность алгоритма подъёма решения равна*

$$T = O(\log^3(p^N) \log\log(p^N)).$$

В последней, **четвертой, главе** диссертации строятся новые логарифмические функции, применение которых приводит к нескратимости сравнений вида (T1.2), (T1.3) и (T2.3).

Предложенные в первой главе функции, логарифм Артина-Хассе и $\mathfrak{p}$-адический логарифм, обладают неприятным свойством. А именно, сравнения (T1.2), (T1.3) и (T2.3) для любого элемента $\alpha$ являются сократимыми, то есть их левая часть содержится в идеале $\mathfrak{p}$. В случае с частными Ферма этого эффекта можно было избежать используя их модификацию, предложенную М.А. Черепневым. В связи с этим возникла задача: построить логарифмические функции, пригодные к использованию для подъёма решения вместо логарифма Артина-Хассе и $\mathfrak{p}$-адического логарифма, но не обладающие упомянутым свойством. Такие функции были названы *оптимальными логарифмическими функциями.*

Новые логарифмические функции строятся по аналогии с частными Ферма. Для всех $s \in \mathbb{N}$ рассмотрим множества

$$U_s := \{\eta \in \mathbb{Z}_\nu : \nu(\eta - 1) \geq s\},$$

и для $M \in \mathbb{N}, \eta \in U_s$ определим функции

$$Q_{s,\pi^M}(\eta) = \frac{\eta^{\lambda_s(\pi^M)} - 1}{\pi^M} \tag{2}$$

где $\lambda_s(\pi^M)$ – функция Кармайкла фактор-группы $U_s/U_M$, равная по определению НОК порядков образов элементов $\eta \equiv 1 \bmod \mathfrak{p}^s$ в $(\mathbb{Z}_\nu/\pi^M)^*$.

Затем доказываются утверждения об их свойствах. Во-первых, показывается, что эти функции обладают логарифмическим свойством.

**Лемма 4.2.** *Пусть* $\eta, \xi \in U_s$, *тогда*

$$Q_{s,\pi^M}(\eta\xi) \equiv Q_{s,\pi^M}(\eta) + Q_{s,\pi^M}(\xi) \bmod \pi^M,$$

*то есть отображение*

$$Q_{s,\pi^M} : (U_s, \times) \to (\mathbb{Z}_\nu/\pi^M, +)$$

*является гомоморфизмом.*

В лемме 4.3 вычисляются значения $\lambda_s(\pi^M)$ для некоторых $s, M \in \mathbb{N}$.

**Лемма 4.3.** *Пусть* $s, N \in \mathbb{N}$.

1. *Если* $s \geq \rho$, *то*
$$\lambda_s(\pi^N) = p^{\lceil \frac{N-s}{e} \rceil}.$$

2. *Если* $s < \rho$, *то*
$$\lambda_s(\pi^{sp}) = p.$$

В лемме 4.4 вычисляется период функций (2), что позволяет применять их к сравнениям.

**Лемма 4.4.** *Пусть* $s, N \in \mathbb{N}$.

1. *Пусть* $N \geq s \geq \rho$, *тогда при* $\Delta \in U_N$
$$Q_{s,\pi^N}(\Delta) \equiv 0 \bmod \pi^{e\lceil \frac{N-s}{e} \rceil}.$$

2. *Пусть* $s < \rho$, *тогда при* $\Delta \in U_{sp}$
$$Q_{s,\pi^{sp}}(\Delta) \equiv 0 \bmod \pi^{\min\{e, sp\}}.$$

Лемма 4.5 позволяет подобрать параметры таким образом, чтобы добиться оптимальности построенных функций.

**Лемма 4.5.** *Пусть* $s, N \in \mathbb{N}$, *а* $\eta \in U_{s'} \backslash U_{s'+1}, s' \in \mathbb{N}, s' \geq s$.

1. *Пусть* $s' \geq \rho$, *тогда*
$$\nu\left(Q_{s,\pi^N}(\eta)\right) = e\left\lceil \frac{N-s}{e} \right\rceil + s' - N.$$

*2. Пусть* $s' < \rho$, *тогда* $s' \le \frac{e}{p-1}$ *и*

*(a) Если* $s' < \frac{e}{p-1}$, *то* $\nu\left(Q_{s,\pi^{sp}}(\eta)\right) = (s'-s)p$.

*(b) Если* $s' = \frac{e}{p-1}$, *то* $\nu\left(Q_{s,\pi^{sp}}(\eta)\right) \ge (s'-s)p$.

В конце четвертой главы доказываются формулы, выражающие логарифм Артина-Хассе и $\mathfrak{p}$-адический логарифм через оптимальные логарифмические функции (2).

**Утверждение 4.3.** *Пусть* $s \in \mathbb{N}, s < \frac{e}{p-1}$ *и* $\eta \in U_s \backslash U_{s+1}$, *а*

$$\xi \in <\eta> \subset U_s/U_{sp},$$

*тогда найдется* $l_{s,\pi^{sp}}(\eta) \in \mathbb{Z}_\nu$, *такое что*

$$\nu\left(l_{s,\pi^{sp}}(\eta)\right) = s,$$

*и верна формула*

$$L(\xi) \equiv Q_{s,\pi^{sp}}(\xi)\ l_{s,\pi^{sp}}(\eta) \bmod \pi^{\min\{e,sp\}}.$$

**Утверждение 4.4.** *Пусть* $M \in \mathbb{N} \cup \{0\}$, $a\ \eta \in U_s, s \in \mathbb{N}, s \ge \rho$. *Тогда*

$$Log_{\mathfrak{p}}(\eta) \equiv \frac{\pi^{s+e\left\lceil \frac{M}{e} \right\rceil}}{p^{\left\lceil \frac{M}{e} \right\rceil}} Q_{s,\pi^{s+e\left\lceil \frac{M}{e} \right\rceil}}(\eta) \bmod \pi^{M+1+\sigma},$$

*где*

$$\sigma = \begin{cases} \rho & \text{при } M \ge \rho > 2, \\ \left\lceil 2\left(1 - \left\{\frac{e}{p-1}\right\}\right)\right\rceil & \text{иначе.} \end{cases}$$

И наконец, формулируются теоремы 4.1 и 4.2, демонстрирующие возможность использования новых логарифмических функций для подъёма решения.

**Теорема 4.1** *Пусть* $\alpha \in \mathbb{Z}_K \backslash \mathfrak{p}, \beta \in \langle\alpha\rangle \subset \mathbb{Z}_K/\mathfrak{p}^N$, $N \in \mathbb{N} : 1 < N < \frac{e}{p-1} + 1$. *Пусть также* $a = \nu(\alpha^{p^f-1} - 1) < N$, *а* $t = \lceil \log_p(\frac{N}{a}) \rceil$.
*Тогда система сравнений*

$$x_i L(\alpha^{p^i(p^f-1)}) \equiv L((\beta\alpha^{-\sum_{j=0}^{i-1} x_j p^j})^{(p^f-1)}) \bmod \mathfrak{p}^{\min\{ap^{i+1},N\}},$$
$$x_i \in \mathbb{Z} : 0 \le x_i < p,$$
$$i = 0, \ldots, t-1,$$

*эквивалентна системе сравнений*

$$x_i Q_{ap^i,\pi^{ap^{i+1}}}(\alpha^{p^i(p^f-1)}) \equiv$$
$$\equiv Q_{ap^i,\pi^{ap^{i+1}}}((\beta\alpha^{-\sum_{j=0}^{i-1}x_j p^j})^{(p^f-1)}) \bmod \pi^{\min\{ap^{i+1},N\}-ap^i},$$
$$x_i \in \mathbb{Z} : 0 \le x_i < p,$$
$$i = 0, \ldots, t-1.$$

**Теорема 4.2** *Пусть* $\alpha, \beta \in \mathbb{Z}_K \backslash \mathfrak{p}$, $N \in \mathbb{N}, N > \rho$. *Обозначим* $a := \nu(\alpha^{p^t(p^f-1)} - 1)$, *где* $t = \left\lceil \log_p \left( \frac{\rho}{\nu(\alpha^{p^f-1}-1)} \right) \right\rceil$, *и пусть* $a < \infty$.

*Предположим теперь, что* $x_0 \in \mathbb{Z} : 0 \le x_0 < p^t$ *таково, что выполнено*

$$\alpha^{x_0(p^f-1)} \equiv \beta^{(p^f-1)} \bmod \mathfrak{p}^a,$$

*тогда сравнение*

$$x\ Log_{\mathfrak{p}}(\alpha^{p^t(p^f-1)}) \equiv Log_{\mathfrak{p}}((\beta\alpha^{-x_0})^{(p^f-1)}) \bmod \pi^N,\ x \in \mathbb{Z}$$

*эквивалентно сравнению*

$$x\ Q_{a,\pi^{a+e\left\lceil \frac{N}{e} \right\rceil}}(\alpha^{p^t(p^f-1)}) \equiv$$
$$\equiv Q_{a,\pi^{a+e\left\lceil \frac{N}{e} \right\rceil}}(((\beta\alpha^{-x_0})^{(p^f-1)})) \bmod \pi^{N-a},\ x \in \mathbb{Z}.$$

Автор выражает глубокую благодарность своему научному руководителю, кандидату физико-математических наук, доценту Михаилу Алексеевичу Черепневу, за постановку задачи и постоянное внимание к работе.

Автор благодарен заведующему кафедрой, члену-корреспонденту РАН, профессору Ю.В. Нестеренко, и всем сотрудникам кафедры теории чисел Механико-математического факультета МГУ за творческую обстановку и доброжелательное отношение.

# РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

[1] Поповян И.А. *Подъём решения показательного сравнения.* Матем. заметки, т. 80 (2006), № 1, с. 76-86.

[2] Поповян И.А. *Оптимальные логарифмические функции для подъёма решения показательного сравнения.* Диск. матем., т. 19 (2007), № 2, с. 53-66.