Math-Net.Ru

Общероссийский математический портал

И. А. Поповян, Оптимальные логарифмические функции для подъема решения показательного сравнения, *Дискрет. матем.*, 2007, том 19, выпуск 2, 51–62

DOI: <https://doi.org/10.4213/dm19>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.27.143

26 апреля 2023 г., 12:04:52

Оптимальные логарифмические функции для подъема решения показательного сравнения

© 2007 г. И. А. Поповян

Статья посвящена изучению задачи подъема решения показательного сравнения в кольцах целых алгебраических чисел. Для подъема решения в кольцах целых рациональных чисел Г. Ризель предложил использовать аппарат частных Ферма. С их помощью задача сводится к решению линейного сравнения по модулю простого числа, при этом это сравнение оказывается несократимым. В настоящей работе построены аналоги частных Ферма в кольце целых алгебраических чисел, также приводящие к несократимым линейным сравнениям для задачи подъема решения в этом случае.

1. Введение

Настоящая статья посвящена изучению задачи дискретного логарифмирования в кольцах целых алгебраических чисел. Пусть K — конечное расширение $\mathbf{Q}$, $\mathbf{Z}_K$ — его кольцо целых, $\mathfrak{p}$ — простой идеал $\mathbf{Z}_K$. Цель данной работы — предложить алгоритм сведения задачи дискретного логарифмирования в группе $(\mathbf{Z}_K/\mathfrak{p}^N)^*$

$$\alpha^x \equiv \beta \pmod{\mathfrak{p}^N}, \quad x \in \mathbf{Z}, \quad (1)$$

где $N \in \mathbf{N} \setminus \{1\}$, $\alpha, \beta \in \mathbf{Z}_K \setminus \mathfrak{p}$, к случаю $N = 1$ (так называемая задача подъема решения), работающий быстрее известных на сегодняшний день алгоритмов. Отметим, что поскольку фактор-кольцо $\mathbf{Z}_K$ по произвольному идеалу конечно, оно может быть эффективно использовано для построения криптографических схем и протоколов.

Впервые, по всей видимости, задача подъема решения в случае $K = \mathbf{Q}$ была рассмотрена в работе Г. Ризеля [1], в которой был предложен подход с применением частных Ферма. Г. Коэн в главе 4.2 в [2] указал, что для ее решения в случае произвольного K могут быть использованы $\mathfrak{p}$ -адический логарифм и логарифм Артина–Хассе, и предложил квадратичный метод, работающий за $[\log_2 N]$ итераций. В 2003 году идея Коэна была реализована в комбинированном методе [3], дополняющем квадратичный метод использованием $\mathfrak{p}$ -адического логарифма. В статье [4] автором был предложен комбинированный метод с применением логарифма Артина–Хассе и $\mathfrak{p}$ -адического логарифма, работающий за $[\log_p N]$ итераций.

В данной работе будут вычислены общие наименьшие кратные порядков элементов некоторых специальных подгрупп фактор-группы главных единиц, что позволит сконструировать новые функции, являющиеся аналогами частных Ферма. Затем будут получены явные формулы, выражающие связь этих функций с логарифмом Артина–Хассе и $\mathfrak{p}$ -адическим логарифмом. Аналогичные вопросы о связи логарифмических функций в случае

$K = \mathbf{Q}$ были рассмотрены Ю. В. Нестеренко в работе [5], где также была предложена конструкция частного Ферма в кольце $\mathbf{Z}_K$. Наконец, будет показано, что использование введенных аналогов частных Ферма позволяет в ряде случаев упростить процедуру подъема решения. Аналогичный результат в случае $K = \mathbf{Q}$ был получен М. А. Черепневым в [6].

Автор благодарен М. А. Черепневу за помощь в работе над статьей.

2. Вычисление логарифмов

Напомним некоторые определения и факты из алгебраической теории чисел и p -адического анализа. В настоящей статье мы будем придерживаться терминологии, введенной в [7].

Пусть p — простое рациональное число, такое что $p \mid (p)$, тогда обозначим $e \in \mathbf{N}$: $p^e \parallel (p)$ индекс ветвления и $f \in \mathbf{N}$: $\#(\mathbf{Z}_K/p) = p^f$ степень расширения идеала p . Пусть $N \in \mathbf{N} \setminus \{1\}$, а $\rho = [e/(p-1)] + 1$.

Нам понадобится также следующая функция: при $y \in \mathbf{R}$, $y > 0$, обозначим $[y] \in \mathbf{N}$ минимальное число такое, что $[y] \geq y$, а при $y \leq 0$ положим $[y] = 0$.

Разложение на простые идеалы в $\mathbf{Z}_K$ однозначно, поэтому можно определить p -адический показатель v . Согласно [7] (см. §1 главы IV) показатель v единственным образом продолжается до показателя $\bar{v}$ на пополнении $K_{\bar{v}}$ поля K по показателю v . Для $M \in \mathbf{Z}$ положим

$$\mathbf{Z}_{\bar{v}}^M = \{\xi \in K_{\bar{v}} : \bar{v}(\xi) \geq M\}.$$

Обозначим кольцо показателя $\mathbf{Z}_{\bar{v}} = \mathbf{Z}_{\bar{v}}^0$, а группу его единиц $\mathbf{Z}_{\bar{v}}^* = \mathbf{Z}_{\bar{v}}^0 \setminus \mathbf{Z}_{\bar{v}}^1$.

Согласно [7] (см. теорему 2 в §4 главы III) в кольце $\mathbf{Z}_{\bar{v}}$ существует единственный с точностью до ассоциированности простой элемент π , характеризующийся равенством $\bar{v}(\pi) = 1$. Рассмотрим $\pi_1 \in p \setminus p^2$ (такой элемент найдется, так как $p \neq p^2$ ввиду их различного разложения на простые идеалы в кольце $\mathbf{Z}_K$), он ассоциирован с π , так как $\bar{v}(\pi/\pi_1) = \bar{v}(\pi) - v(\pi_1) = 0$. Тогда, заменив при необходимости π на π_1 , можно считать, что $\pi \in \mathbf{Z}_K$.

2.1. Вычисление логарифма Артина–Хассе

Рассмотрим многочлен

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

назовем его логарифмом Артина–Хассе. Обладающее свойствами, аналогичными свойствам логарифмов, его значение $\bmod p^N$ используется в теореме 1 в [4] для решения задачи подъема при $N \leq \rho$.

Следующее утверждение дает эффективный алгоритм вычисления логарифма Артина–Хассе $\bmod p^e$.

Предложение 1. Пусть x — переменная. Имеет место сравнение

$$L(1+x) \equiv \frac{(1+x)^p - (1+x^p)}{p} \bmod p^e. \quad (2)$$

Доказательство. Воспользуемся равенством

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

Запишем цепочку сравнений по модулю p для $0 < i < p$:

$$\begin{aligned} \frac{\binom{p}{i}}{p} &\equiv \frac{(p-1)!}{i!(p-i)!} \equiv \frac{(p-1) \dots (p-i+1)}{i!} \\ &\equiv \frac{(-1)^{i-1}(i-1)!}{i!} \equiv \frac{(-1)^{i-1}}{i} \pmod{p}. \end{aligned}$$

Но это верно и для делителя $p^e \mid p$.

В случае $p = 2$ логарифм Артина–Хассе превращается в линейный одночлен. При $p > 2$ верно неравенство $\rho \leq e$ и формула (2) имеет место также по $\text{mod } p^N$, $N \leq \rho$, то есть применима для вычисления логарифма Артина–Хассе, использованного в теореме 1 из [4].

2.2. Вычисление p -адического логарифма

Определим теперь p -адический логарифм для $x \in \mathbf{Z}_p^\rho$ как сумму ряда в $K_{\bar{v}}$

$$\text{Log}(1+x) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{x^i}{i}. \quad (3)$$

Согласно [7] этот ряд сходится и принимает значения в $\mathbf{Z}_{\bar{v}}^\rho$. Более того, для $x, y \in \mathbf{Z}_{\bar{v}}^\rho$ верны равенства

$$\bar{v}(\text{Log}(1+x)) = \bar{v}(x), \quad \text{Log}((1+x)(1+y)) = \text{Log}(1+x) + \text{Log}(1+y).$$

В записи

$$\text{Log}(1+x) \equiv \sum_{i=1}^{\infty} (-1)^{i+1} \frac{x^i}{i} \pmod{\pi^N},$$

при $x \in \mathbf{Z}_{\bar{v}}^\rho$ сумма на самом деле конечна, что следует из сходимости ряда (3). При этом для $x, y \in \mathbf{Z}_{\bar{v}}^{(\rho)}$ логарифмическое свойство p -адического логарифма, конечно, сохраняется и по $\text{mod } \pi^N$, то есть

$$\text{Log}((1+x)(1+y)) \equiv \text{Log}(1+x) + \text{Log}(1+y) \pmod{\pi^N},$$

и используется в таком виде для подъема решения при $N > \rho$ (см. теорему 1 в [4]). Следующее утверждение дает эффективный алгоритм вычисления p -адического логарифма по модулю степени π .

Предложение 2. Пусть $M \in \mathbf{N} \cup \{0\}$, $\eta \in \mathbf{Z}_{\bar{v}}^{(\rho)}$. Тогда имеет место сравнение

$$\text{Log}(1+\eta) \equiv \frac{(1+\eta)^{p^{\lceil M/e \rceil}} - 1}{p^{\lceil M/e \rceil}} \pmod{\pi^{M+1+\sigma}},$$

где

$$\sigma = \begin{cases} \rho & \text{при } M \geq \rho > 2, \\ [2(1 - \{e/(p-1)\})] & \text{в противном случае.} \end{cases}$$

Доказательство. Пусть $V = \lceil M/e \rceil$. Пусть Exp обозначает p -адическую экспоненту (см. §5 главы IV в [7]), тогда при $\eta \in \mathbf{Z}_{\bar{v}}^{(\rho)}$ рассмотрим тождество

$$\text{Exp}(p^V \text{Log}(1 + \eta)) = (1 + \eta)^{p^V},$$

верное, так как $(1 + \eta)^{p^V} - 1 \in \mathbf{Z}_{\bar{v}}(\rho)$. По определению экспоненты

$$\text{Exp}(p^V \text{Log}(1 + \eta)) = 1 + \frac{p^V \text{Log}(1 + \eta)}{1!} + \frac{(p^V \text{Log}(1 + \eta))^2}{2!} + \dots,$$

откуда

$$\text{Log}(1 + \eta) + r(\eta) = \frac{(1 + \eta)^{p^V} - 1}{p^V},$$

где

$$r(\eta) = r_2 + r_3 + \dots, \quad r_i = \frac{p^{(i-1)V} (\text{Log}(1 + \eta))^i}{i!}, \quad i = 2, 3, \dots$$

Используя определение V , при $n \geq 2$ получим оценку

$$\begin{aligned} \bar{v}(r_n) - M &= \bar{v} \left(\frac{p^{V(n-1)} (\text{Log}(1 + \eta))^n}{n!} \right) - M \\ &= eV(n-1) + \bar{v}(\eta)n - \bar{v}(n!) - M \\ &\geq M(n-2) + \bar{v}(\eta)n - v(n!). \end{aligned} \quad (4)$$

1. Пусть $\sigma = [2(1 - \{e/(p-1)\})]$, покажем, что $\bar{v}(r(\eta)) \geq M + 1 + \sigma$, откуда и будет следовать доказываемое. Из (4) получаем, что при $n \geq 2$

$$\begin{aligned} \bar{v}(r_n) - M &\geq M(n-2) + \bar{v}(\eta)n - v(n!) > M(n-2) + n(\bar{v}(\eta) - e/(p-1)) \\ &\geq 2(\rho - e/(p-1)) = 2(1 - \{e/(p-1)\}). \end{aligned}$$

Здесь мы воспользовались оценкой

$$\bar{v}(n!) = v(n!) = e \sum_{i=1}^{\infty} [n/p^i] < \frac{en}{p-1}$$

и тем, что $\bar{v}(\eta) - \rho \geq 0$. Откуда, в силу строгости неравенства при $n \geq 2$

$$\bar{v}(r_n) \geq M + 1 + [2(1 - \{e/p-1\})].$$

2. Пусть $\sigma = \rho$, покажем, что $\bar{v}(r(\eta)) \geq M + 1 + \rho$, откуда и будет следовать доказываемое. При $n = 2$ из (4) получаем, что

$$\bar{v}(r_2) - M \geq 2\bar{v}(\eta) - v(2) \geq 2\rho - v(2). \quad (5)$$

Рассмотрим два случая. Пусть сначала $p > 2$, тогда формула (5) дает неравенства

$$\bar{v}(r_2) - M \geq 2\rho \geq \rho + 1.$$

Если же $p = 2$, то по определению $\rho = e + 1$, $v(2) = e$, и из (5) следует, что

$$\bar{v}(r_2) - M \geq 2\rho - v(2) = e + 2 = \rho + 1.$$

Итак, в обоих случаях, $\bar{v}(r_2) \geq M + 1 + \rho$.

При $n \geq 3$ из (4) следует, что

$$\begin{aligned}\bar{v}(r_n) - M &\geq M(n-2) + \bar{v}(\eta)n - v(n!) \\ &\geq M(n-2) + n(\bar{v}(\eta) - \rho) + 1 \geq M + 1 \geq \rho + 1.\end{aligned}$$

Здесь мы воспользовались оценкой $\bar{v}(n!) \leq n\rho - 1$, которая верна в силу строгости неравенств

$$\bar{v}(n!) = v(n!) = e \sum_{i=1}^{\infty} [n/p^i] < \frac{en}{p-1} < n\rho,$$

и тем, что $\bar{v}(\eta) - \rho \geq 0$. Отсюда $\bar{v}(r_n) \geq M + 1 + \rho$ при $n \geq 3$.

Замечание 1. Аналогичные формулы в случае $K = \mathbf{Q}$ были получены в [5].

3. Оптимальные логарифмические функции

В настоящей разделе мы установим связь между логарифмами, p -адическим и Артина–Хассе, и новыми логарифмическими функциями, определенным в кольце $\mathbf{Z}_K$ по аналогии с классическим частным Ферма. Будут получены формулы для вычисления решения показательного сравнения, аналогичные формулам из теорем 1.2, 1.3, 2.3 в [4], однако записанные в терминах новых функций.

Введем обозначения $\mathbf{Z}_v = \mathbf{Z}_\rho \cap K$, $\mathbf{Z}_v^* = \mathbf{Z}_\rho^* \cap K$. Для $s \in \mathbf{N}$ рассмотрим множества

$$U_s = \{\eta \in \mathbf{Z}_v : v(\eta - 1) \geq s\}.$$

Отметим несколько свойств этих множеств. Во-первых, $U_s \subset \mathbf{Z}_v^*$. Во-вторых, несложно заметить, что каждое U_s с операцией умножения из $\mathbf{Z}_v$ образует группу $(U_s, \times)$. В самом деле, умножение двух элементов U_s , очевидно, не выводит за пределы U_s ; единицей является $1 \in U_s$; обратным элементом к $1 + \xi \in U_s$ является элемент $1 - \xi/(1 + \xi)$, также лежащий в U_s , так как $1 + \xi \in \mathbf{Z}_v^*$. Наконец, легко видеть, что для $s', s'' \in \mathbf{N}$, $s' < s''$ выполняется включение $U_{s''} \subseteq U_{s'}$.

Определим на U_s функции Q_{s,π^M} , $M \in \mathbf{N}$, по формуле

$$Q_{s,\pi^M}: U_s \rightarrow \mathbf{Z}_v, \quad \eta \mapsto \frac{\eta^{\lambda_s(\pi^M)} - 1}{\pi^M},$$

где $\lambda_s(\pi^M)$ — общее наименьшее кратное порядков образов элементов $\eta \in U_s$ в $(\mathbf{Z}_v/\pi^M)^*$.

Важнейшее свойство этих функций содержится в следующем утверждении.

Предложение 3. Пусть $\eta, \xi \in U_s$, тогда

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

то есть отображение

$$Q_{s,\pi^M}: (U_s, \times) \rightarrow (\mathbf{Z}_v/\pi^M, +)$$

является гомоморфизмом.

Доказательство. По определению

$$\begin{aligned} Q_{s,\pi^M}(\eta\xi) - Q_{s,\pi^M}(\eta) - Q_{s,\pi^M}(\xi) &\equiv \frac{(\eta\xi)^{\lambda_s(\pi^M)} - \eta^{\lambda_s(\pi^M)} - \xi^{\lambda_s(\pi^M)} + 1}{\pi^M} \\ &\equiv \frac{\eta^{\lambda_s(\pi^M)} - 1}{\pi^M} (\xi^{\lambda_s(\pi^M)} - 1) \equiv Q_{s,\pi^M}(\eta)(\xi^{\lambda_s(\pi^M)} - 1) \equiv 0 \pmod{\pi^M}, \end{aligned}$$

так как $Q_{s,\pi^M}(\eta) \in \mathbf{Z}_v$, а $\xi^{\lambda_s(\pi^M)} \equiv 1 \pmod{\pi^M}$ по определению $\lambda_s(\pi^M)$.

Для $\eta \in U_{s'} \setminus U_{s'+1}$, $s' \in \mathbf{N}$, положим

$$\tau(\eta) = \min\{t \in \mathbf{N} \cup \{0\} : s'p^t \geq e/(p-1)\} = \left\lceil \log_p \left(\frac{e}{(p-1)s'} \right) \right\rceil.$$

Далее нам понадобится следующая лемма.

Лемма 1. Пусть $\eta \in U_{s'} \setminus U_{s'+1}$, $s' \in \mathbf{N}$.

Тогда

$$v(\eta^p - 1) \geq \min\{e + s', s'p\},$$

где равенство имеет место при $e + s' \neq s'p$.

Пусть к тому же $\tau = \tau(\eta)$ и $t \in \mathbf{N} \cup \{0\}$, тогда

$$v(\eta^{p^t} - 1) = \begin{cases} s'p^t & \text{при } 0 \leq t \leq \tau, \\ s'p^\tau + e(t - \tau) + r & \text{при } 0 \leq \tau < t, \end{cases}$$

где $r \in \mathbf{N} \cup \{0\}$ — постоянная, зависящая только от η , и $r = 0$ при $s'p^\tau \neq e/(p-1)$.

Доказательство. Докажем первое утверждение. По условию $v(\eta - 1) = s'$, поэтому в силу теоремы 1 из §1 главы IV в [7] η может быть представлена в виде $\eta = 1 + \pi^{s'}\eta_1$, где $\eta_1 \in \mathbf{Z}_v^*$. Тогда по формуле бинома

$$\eta^p = (1 + \pi^{s'}\eta_1)^p = 1 + p\pi^{s'} \sum_{n=1}^{p-1} \frac{\binom{p}{n}}{p} \pi^{s'(n-1)} \eta_1^n + \pi^{s'p} \eta_1^p.$$

Заметим, что $\eta_1^p \in \mathbf{Z}_v^*$ и

$$\sum_{n=1}^{p-1} \frac{\binom{p}{n}}{p} \pi^{s'(n-1)} \eta_1^n \in \mathbf{Z}_v^*,$$

так как

$$0 = v\left(\frac{\binom{p}{1}}{p} \eta_1\right) < s' = v\left(\frac{\binom{p}{2}}{p} \pi^{s'} \eta_1^2\right) < 2s' = v\left(\frac{\binom{p}{3}}{p} \pi^{2s'} \eta_1^3\right) < \dots$$

Тогда по известной формуле

$$v(\eta^p - 1) \geq \min\{v(p\pi^{s'}), v(\pi^{s'p})\} = \min\{e + s', s'p\}, \quad (6)$$

где равенство имеет место при $e + s' = v(p\pi^{s'}) \neq v(\pi^{s'p}) = s'p$.

Доказательство второго утверждения почти дословно повторяет доказательство леммы 3 в [4], поэтому здесь мы приведем лишь его схему.

При $t = 0$ первое равенство при $0 \leq t \leq \tau$ очевидно. Пусть $t = 1, \tau \geq 1$, тогда по определению $s' \leq s'p^{\tau-1} < e/(p-1)$ и $e + s' > s'p$, откуда с учетом (6) получаем, что

$$v(\eta^{p^t} - 1) = v(\eta^p - 1) = s'p = s'p^t.$$

Проведя индукцию по s' , получим, что $v(\eta^{p^t} - 1) = s'p^t$ при $0 \leq t \leq \tau$, чем и докажем первое равенство.

Пусть теперь $t = 1, \tau = 0$, тогда по определению $s' = s'p^\tau \geq e/(p-1)$ и $e + s' \leq s'p$, откуда с учетом (6) получаем, что

$$v(\eta^{p^t} - 1) = v(\eta^p - 1) = s' + e + r = s'p^\tau + e(t - \tau) + r,$$

где $r \geq 0$. Причем, если $s' = s'p^\tau \neq e/(p-1)$, то $e + s' < s'p$, и из того же (6) следует, что

$$v(\eta^{p^t} - 1) = v(\eta^p - 1) = s' + e = s'p^\tau + e(t - \tau).$$

Проведя индукцию по s' , получим, что $v(\eta^{p^t} - 1) = s'p^\tau + e(t - \tau) + r$ при $0 \leq \tau < t$, чем и докажем второе равенство.

Вычислим теперь значения $\lambda_s(\pi^M)$ для некоторых $s, M \in \mathbb{N}$.

Следствие 1. Пусть $s, N \in \mathbb{N}$.

1. Если $s \geq p$, то $\lambda_s(\pi^N) = p^{\lceil (N-s)/e \rceil}$.
2. Если $s < p$, то $\lambda_s(\pi^{sp}) = p$.

Доказательство. Пусть $\eta \in U_{s'} \setminus U_{s'+1}, s' \in \mathbb{N}, s' \geq s$.

Докажем первое утверждение. Пусть $V = \lceil (N-s')/e \rceil$. Заметим сразу, что $V = 0 \iff N \leq s'$, тогда, как легко видеть,

$$\text{ord}_{\pi^N}(\eta) = 1 = p^V.$$

Пусть теперь $V \geq 1$. Заметим, что при $s' \geq s \geq p$, справедливы соотношения $\tau(\eta) = 0$ и $s'p^{\tau(\eta)} \neq e/(p-1)$, тогда по лемме 1 и определению V

$$\begin{aligned} v(\eta^{p^{V-1}} - 1) &= e(V-1) + s' < N, \\ v(\eta^{p^V} - 1) &= eV + s' \geq N. \end{aligned}$$

Это и означает, что $\text{ord}_{\pi^N}(\eta) = p^V$, а общее наименьшее кратное достигается при $s' = s$ и равно $p^{\lceil (N-s)/e \rceil}$. Тогда по определению

$$\lambda_s(\pi^N) = p^{\lceil (N-s)/e \rceil}.$$

Докажем второе утверждение. Очевидно, что $s' \geq sp$ тогда и только тогда, когда порядок η по модулю π^{sp} равен 1. Пусть теперь $s \leq s' < sp$. Рассмотрим два подслучая. Пусть сначала $s' < e/(p-1)$, тогда $\tau(\eta) \geq 1$, и по лемме 1 $\eta^p \in U_{s'p} \subseteq U_{sp}$, так как $sp \leq s'p$. Отсюда

$$\text{ord}_{\pi^{sp}}(\eta) = p.$$

Если же $s' \geq e/(p-1)$, то $\tau(\eta) = 0$ и по лемме 1

$$v(\eta^p - 1) = e + s' + r \geq s'p + r,$$

то есть $\eta^p \in U_{s'p+r} \subseteq U_{sp}$, так как $sp \leq s'p + r$.

Таким образом, в любом случае при $\eta \notin U_{sp}$ порядок $\text{ord}_{\pi^{sp}}(\eta) = p$, откуда по определению $\lambda_s(\pi^{sp}) = p$.

Следствие 1 дает формулы, позволяющие для $\eta \in U_s$ эффективно вычислять значения $Q_{s,\pi^N}(\eta)$ при $s \geq \rho$ и $Q_{s,\pi^{sp}}(\eta)$ при $s < \rho$.

Покажем теперь, что функции Q_{s,π^M} , рассматриваемые по модулю некоторой степени π , периодичны.

Следствие 2. Пусть $s, N \in \mathbf{N}$.

1. Пусть $N \geq s \geq \rho$, тогда при $\Delta \in U_N$

$$Q_{s,\pi^N}(\Delta) \equiv 0 \pmod{\pi}.$$

2. Пусть $s < \rho$, тогда при $\Delta \in U_{sp}$

$$Q_{s,\pi^{sp}}(\Delta) \equiv 0 \pmod{\pi^{\min\{e, sp\}}}.$$

Доказательство. Докажем первое утверждение. Положим $V = e[(N-s)/e]$. Согласно пункту 1 следствия 1, $\lambda_s(\pi^N) = p^V$. Так как $v(\Delta-1) \geq \rho > e/(p-1)$, справедливы соотношения $\tau(\Delta) = 0$ и $v(\Delta-1)p^{\tau(\Delta)} \neq e/(p-1)$. Поэтому из леммы 1 следует, что

$$v(Q_{s,\pi^N}(\Delta)) = v((\Delta^{\lambda_s(\pi^N)} - 1)/\pi^N) = eV + v(\Delta-1) - N \geq eV,$$

так как $N \geq \rho$, а $v(\Delta-1) \geq N$.

Докажем второе утверждение. Согласно пункту 2 следствия 1, справедливо равенство $\lambda_s(\pi^{sp}) = p$, поэтому из леммы 1 для $s' = v(\Delta-1) \geq sp$ следует, что

$$\begin{aligned} v(Q_{s,\pi^{sp}}(\Delta)) &= v((\Delta^{\lambda_s(\pi^{sp})} - 1)/\pi^{sp}) \\ &\geq \min\{e + s', s'p\} - sp = \min\{e + s' - sp, s'p - sp\} \\ &\geq \min\{e + sp - sp, sp^2 - sp\} \geq \min\{e, sp\}. \end{aligned}$$

Следствие 3. Пусть $s, N \in \mathbf{N}$, $\eta \in U_{s'} \setminus U_{s'+1}$, $s' \in \mathbf{N}$, $s' \geq s$.

1. Пусть $s' \geq \rho$, тогда $v(Q_{s,\pi^N}(\eta)) = e[(N-s)/e] + s' - N$.

2. Пусть $s' < \rho$, тогда $s' \leq e/(p-1)$ и

- (а) если $s' < e/(p-1)$, то $v(Q_{s,\pi^{sp}}(\eta)) = (s' - s)p$,
- (б) если $s' = e/(p-1)$, то $v(Q_{s,\pi^{sp}}(\eta)) \geq (s' - s)p$.

Утверждения следуют из определения функции Q_{s,π^M} , следствия 1 и леммы 1.

3.1. Функции $Q_{s,\pi^{sp}}$ и логарифм Артина–Хассе

Рассмотрим случай $N \leq \rho$ и получим формулы, выражающие значения логарифма Артина–Хассе, используемого в [4], через значения функций $Q_{s,\pi^{sp}}$.

Далее в этом параграфе будем считать, что

$$\eta \in U_s \setminus U_{s+1}, \quad s \in \mathbf{N}, \quad s < e/(p-1). \quad (7)$$

Заметим, что тогда согласно пункту 2 (а) следствия 3

$$v(Q_{s,\pi^{sp}}(\eta)) = (s - s)p = 0. \quad (8)$$

Рассмотрим отображение

$$Q'_{s,\pi^{sp}}: U_s \rightarrow \mathbf{Z}_v / \pi^{\min\{e, sp\}}, \quad \xi \mapsto Q_{s,\pi^{sp}}(\xi) \bmod \pi^{\min\{e, sp\}}.$$

Согласно пункту 2 следствия 2 справедливо включение $U_{sp} \subseteq \text{Ker } Q'_{s,\pi^{sp}}$.

Так как L — многочлен, отображение

$$L': U_s / U_{sp} \rightarrow \mathbf{Z}_v / \pi^{\min\{e, sp\}}, \quad \xi \mapsto L(\xi) \bmod \pi^{\min\{e, sp\}}$$

определено корректно и является гомоморфизмом, переводящим умножение в сложение, поскольку обладает логарифмическим свойством согласно лемме 1 в [4]. Рассмотрим ограничения $Q_{s,\pi^{sp}}$ и L на мультипликативную циклическую подгруппу $\langle \eta \rangle \subset U_s / U_{sp}$, порожденную элементом η вида (7).

Введем обозначение

$$l_{s,\pi^{sp}}(\eta) = \frac{L(\eta)}{Q_{s,\pi^{sp}}(\eta)}.$$

Легко видеть, что ввиду (8)

$$v(l_{s,\pi^{sp}}(\eta)) = v(L(\eta)) - v(Q_{s,\pi^{sp}}(\eta)) = s, \quad (9)$$

так как из определения видно, что $v(L(\eta)) = s$.

Для $\xi \equiv \eta^m \bmod \pi^{sp}$, $m \in \mathbf{N}$, из логарифмического свойства L и $Q_{s,\pi^{sp}}$ следует, что

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

Отсюда, применяя (8), находим, что

$$L(\xi) \equiv Q_{s,\pi^{sp}}(\xi)l_{s,\pi^{sp}}(\eta) \bmod \pi^{\min\{e, sp\}}. \quad (10)$$

Применим теперь полученные результаты к элементам кольца $\mathbf{Z}_K \subset \mathbf{Z}_v$ и покажем, как функция $Q_{s,\pi^{sp}}$ может быть использована вместо логарифма Артина–Хассе для подъема решения показательных сравнений в случае $N < e/(p-1) + 1$.

Теорема 1. Пусть $\alpha \in \mathbf{Z}_K \setminus \mathfrak{p}$, $\beta \in \langle \alpha \rangle \subset \mathbf{Z}_K / \mathfrak{p}^N$, $N \in \mathbf{N}$: $1 < N < e/(p-1) + 1$. Пусть также $a = v(\alpha^{p^f-1} - 1) < N$, $t = \lceil \log_p(N/a) \rceil$.

Тогда система сравнений

$$x_i L(\alpha^{p^i(p^f-1)}) \equiv L((\beta \alpha^{-\sum_{j=0}^{i-1} x_j p^j})^{(p^f-1)}) \bmod \mathfrak{p}^{\min\{ap^{i+1}, N\}}, \\ x_i \in \mathbf{Z}, \quad 0 \leq x_i < p, \quad i = 0, 1, \dots, t-1, \quad (11)$$

эквивалентна системе сравнений

$$x_i Q_{ap^i, \pi^{ap^{i+1}}}(\alpha^{p^i(p^f-1)}) \equiv Q_{ap^i, \pi^{ap^{i+1}}}((\beta \alpha^{-\sum_{j=0}^{i-1} x_j p^j})^{(p^f-1)}) \bmod \pi^{\min\{ap^{i+1}, N\} - ap^i}, \\ x_i \in \mathbf{Z}, \quad 0 \leq x_i < p, \quad i = 0, 1, \dots, t-1. \quad (12)$$

Утверждение теоремы легко следует из леммы 1, сравнения (10) и равенства (9).

Замечание 2. В работе [4] показано, что решение сравнения

$$\alpha^x \equiv \beta \pmod{p^N}, \quad x \in \mathbb{Z},$$

может быть найдено из системы

$$\begin{aligned} x &\equiv \sum_{i=0}^{t-1} x_i p^i \pmod{p^t}, \\ \alpha^x &\equiv \beta \pmod{p}, x \in \mathbb{Z}, \end{aligned}$$

где $x_i, i = 1, \dots, t-1$, — решение системы (11).

Замечание 3. Оптимальность функций $Q_{ap^i, \pi^{ap^{i+1}}}$ состоит в том, что линейные сравнения (12) представлены в несократимом виде, т.е. $v(Q_{ap^i, \pi^{ap^{i+1}}}(\alpha^{p^i(p^f-1)})) = 0$ согласно (8), в отличие от сравнений (11), где $v(L(\alpha^{p^i(p^f-1)})) = ap^i > 0$.

3.2. Функции Q_{s, π^M} и p -адический логарифм

Докажем теперь формулу, устанавливающую связь p -адического логарифма и введенных нами функций Q_{s, π^M} в случае $N > \rho$, в котором p -адический логарифм используется в [4] для получения решения показательного сравнения.

Предложение 4. Пусть $M \in \mathbb{N} \cup \{0\}$, $\eta \in U_s$, $s \in \mathbb{N}$, $s \geq \rho$. Тогда

$$\text{Log}(\eta) \equiv \frac{\pi^{s+e[M/e]}}{p^{[M/e]}} Q_{s, \pi^{s+e[M/e]}}(\eta) \pmod{\pi^{M+1+\sigma}},$$

где

$$\sigma = \begin{cases} \rho & \text{при } M \geq \rho > 2, \\ [2(1 - \{e/(p-1)\})] & \text{в противном случае.} \end{cases}$$

Доказательство. Согласно предложению 2 имеет место формула

$$\text{Log}(\eta) \equiv \frac{\eta^{p^{[M/e]}} - 1}{p^{[M/e]}} \pmod{\pi^{M+1+\sigma}}.$$

С другой стороны, по определению $Q_{s, \pi^{s+e[M/e]}}$,

$$Q_{s, \pi^{s+e[M/e]}}(\eta) = \frac{\eta^{\lambda_s(\pi^{s+e[M/e]})} - 1}{\pi^{s+e[M/e]}},$$

где, согласно пункту 1 следствия 1,

$$\lambda_s(\pi^{s+e[M/e]}) = p^{[(s+e[M/e]-s)/e]},$$

а по определению

$$[(s+e[M/e]-s)/e] = [M/e].$$

Поэтому

$$\begin{aligned} \frac{\pi^{s+e[M/e]}}{p^{[M/e]}} Q_{s, \pi^{s+e[M/e]}}(\eta) &= \frac{\pi^{s+e[M/e]}}{p^{[M/e]}} \cdot \frac{\eta^{p^{[M/e]}} - 1}{\pi^{s+e[M/e]}} \\ &= \frac{\eta^{p^{[M/e]}} - 1}{\pi^{s+e[M/e]} p^{[M/e]}} \equiv \text{Log}(\eta) \pmod{\pi^{M+1+\sigma}}. \end{aligned}$$

Замечание 4. Аналогичная формула в случае $K = \mathbf{Q}$ была также получена в [5].

Применим теперь полученные результаты к элементам кольца $\mathbf{Z}_K \subset \mathbf{Z}_v$ и покажем, как функция Q_{s,π^M} может использоваться вместо p -адического логарифма для подъема решения показательных сравнений в случае $N > \rho$.

Заметим предварительно, что если $\eta - 1 \in \mathfrak{p}$, $q = \text{ord}_{\mathfrak{p}^0}(\eta)$, то из леммы 1 и определений $\tau(\eta)$ и ρ следует, что либо $q = p^{\tau(\eta)}$, либо $q = p^{\tau(\eta)+1}$.

Теорема 2. Пусть $\alpha, \beta \in \mathbf{Z}_K \setminus \mathfrak{p}$, $N \in \mathbf{N}$, $N > \rho$, $a = v(\alpha^{p^t(p^f-1)} - 1)$, где $t \in \mathbf{N} \cup \{0\}$, $\text{ord}_{\mathfrak{p}^0}(\alpha^{p^f-1}) = p^t$, и пусть $a < \infty$.

Предположим, что $x_0 \in \mathbf{Z}$, $0 \leq x_0 < p^t$, таково, что

$$\alpha^{x_0(p^f-1)} \equiv \beta^{(p^f-1)} \pmod{\mathfrak{p}^a}, \quad (13)$$

тогда сравнение

$$x \text{Log}(\alpha^{p^t(p^f-1)}) \equiv \text{Log}((\beta \alpha^{-x_0})^{(p^f-1)}) \pmod{\pi^N}, \quad x \in \mathbf{Z}, \quad (14)$$

эквивалентно сравнению

$$x Q_{a,\pi^{a+e\lceil N/e \rceil}}(\alpha^{p^t(p^f-1)}) \equiv Q_{a,\pi^{a+e\lceil N/e \rceil}}(((\beta \alpha^{-x_0})^{(p^f-1)})) \pmod{\pi^{N-a}}, \quad x \in \mathbf{Z}. \quad (15)$$

Доказательство. По определению $\alpha^{p^t(p^f-1)} \in U_a \subseteq U_\rho$, так как по определению $a \geq \rho$. Далее, в силу условия (13) справедливы включения $(\beta \alpha^{-x_0})^{(p^f-1)} \in U_a \subseteq U_\rho$, а значит, условия предложения 4 выполнены. Применим его при $M = N$, занизив степень модуля до π^N , для замены p -адического логарифма в (14) и получим, что

$$\frac{\pi^{a+e\lceil N/e \rceil}}{p^{\lceil N/e \rceil}} Q_{a,\pi^{a+e\lceil N/e \rceil}}(\alpha^{p^t(p^f-1)}) \equiv \frac{\pi^{a+e\lceil N/e \rceil}}{p^{\lceil N/e \rceil}} Q_{a,\pi^{a+e\lceil N/e \rceil}}(((\beta \alpha^{-x_0})^{(p^f-1)})) \pmod{\pi^N}.$$

Отсюда, разделив на константу $\pi^{a+e\lceil N/e \rceil}/p^{\lceil N/e \rceil}$ обе части и учитывая, что

$$v(\pi^{a+e\lceil N/e \rceil}/p^{\lceil N/e \rceil}) = a + e\lceil N/e \rceil - e\lceil N/e \rceil = a,$$

получим искомую формулу.

Замечание 5. Как и в предыдущем параграфе, функции $Q_{a,\pi^{a+e\lceil N/e \rceil}}$ оптимальны, так как линейные сравнения (15) также представлены в несократимом виде (согласно пункту 1 следствия 3):

$$v(Q_{a,\pi^{a+e\lceil N/e \rceil}}(\alpha^{p^t(p^f-1)})) = e\lceil (a + e\lceil N \rceil - a)/e \rceil + v(\alpha^{p^t(p^f-1)} - 1) - a - e\lceil N/e \rceil = 0,$$

в отличие от сравнений (14), где $v(\text{Log}(\alpha^{p^t(p^f-1)})) = a > 0$.

Замечание 6. Теорему 2 можно переформулировать и без ограничения $a < \infty$. Для этого достаточно в (15) заменить a на ρ , при этом доказательство теоремы не изменится, но несократимый вид линейных сравнений (15), вообще говоря, уже не будет иметь места. Однако на самом деле случай $a = \infty$ не представляет интереса, так как тогда сравнение (14) и модифицированное указанным образом сравнение (15) превращаются в тривиальные тождества $0 \equiv 0 \pmod{\pi^N}$ и $0 \equiv 0 \pmod{\pi^{N-\rho}}$ соответственно.

Список литературы

1. Riesel H., Some soluble cases of the discrete logarithm problem. *BIT* (1988) **28**, №4, 839–851.
2. Cohen H., *Advanced topics in computational number theory*. Springer, New York, 1999.
3. Hess F., Pauli S., Pohst M. E., Computing the multiplicative group of residue class rings. *Math. Comp.* (2003) **72**, 1531–1548.
4. Поповян И. А., Подъем решения показательного сравнения. *Матем. заметки* (2006) **80**, №1, 76–86.
5. Нестеренко Ю. В., Частные Ферма и p -адические логарифмы. *Труды по дискретной математике* (2002) **5**, 173–188.
6. Черепнев М. А., О некотором свойстве дискретного логарифма. В сб.: *Тезисы докл. XII международной конф. «Проблемы теоретической кибернетики»*. Нижний Новгород, 1999.
7. Борович З. И., Шафаревич И. Р., *Теория чисел*. Наука, Москва, 1964.

Статья поступила 12.06.2006.