Записки научных
семинаров ПОМИ
Том 365, 2009 г.

С. В. Востоков, М. А. Иванов, Г. К. Пак

К ОДНОЙ РАБОТЕ ХАССЕ О ЗАКОНЕ ВЗАИМНОСТИ ЭЙЗЕНШТЕЙНА

1. Введение

G. Eisenstein в работе [1] изучает равенство степенных вычетов $\left(\frac{\alpha}{\beta}\right)$ и $\left(\frac{\beta}{\alpha}\right)$ в круговом поле $\mathbb{Q}(\zeta)$, где ζ – первообразный корень простой степени p из 1, а α и β – числа из кольца $\mathbb{Z}[\zeta]$. Он рассматривает отдельно частные случаи:

1. $\beta = 1 - \zeta$.
2. $\beta = a$, где a – целое рациональное число, взаимно простое с p.

Именно во втором случае он получает элегантный закон взаимности:

$$\left(\frac{\alpha}{a}\right) = \left(\frac{a}{\alpha}\right), \quad \text{если} \quad \alpha \equiv b \mod (1-\zeta)^2, \quad \text{где} \quad b \in \mathbb{Z}, \quad (b,p) = 1.$$

H. Hasse обобщает закон взаимности Эйзенштейна на произвольное круговое поле и получает следующий результат (см. [2]).

Пусть $K = \mathbb{Q}(\zeta)$, $\zeta := \zeta_n$, $n = \prod_{i=1}^{r} p_i^{m_i}$, $m_i > 0$. Пусть q – простое число такое, что $q^{p_i - 1} \equiv 1 \mod p_i^{m_i}$, $i = 1, 2, \ldots, r$; $\mathfrak{p}_i$ – простой идеал над (p_i) в круговом поле $\mathbb{Q}(\zeta_{p_i^{m_i}})$, α – число из кольца $\mathbb{Z}[\zeta]$ со свойством $(\alpha, nq) = 1$, $a \equiv \xi_i^{p_i} \mod \mathfrak{p}_i^2$ при некоторых ξ_i из K, $i = 1, \ldots, r$.

Теорема (Hasse)**.** *Для символов n-ых (соответственно $n/4$) степенных вычетов в K имеет место закон взаимности*

$$\left(\frac{\alpha}{q}\right)_n = \left(\frac{q}{\alpha}\right)_n, \qquad \textit{если} \quad n \not\equiv 0 \mod 4$$
$$\left(\frac{\alpha}{q}\right)_{n/4} = \left(\frac{q}{\alpha}\right)_{n/4}, \quad \textit{если} \quad n \equiv 0 \mod 4.$$

Работа выполнена при поддержке гранта ИНТАС, а также гранта РФФИ 08-01-00777-а, и SFB 478 Münster, “Geometrische Strukturen” .

В частности, для $n = p^m$ *имеем условие* $\alpha \equiv \xi^p \mod \mathfrak{p}^2$, $\xi \in K$, *и при* $p \neq 2$: $\left(\frac{\alpha}{q}\right) = \left(\frac{q}{\alpha}\right)$, *если* $q^{p-1} \equiv 1 \mod p^m$.

В настоящей работе мы находим необходимые и достаточные условия равенства степенных вычетов $\left(\frac{\alpha}{a}\right)_n$ и $\left(\frac{a}{\alpha}\right)_n$ в круговом поле $\mathbb{Q}(\zeta_n)$, $2 \nmid n$, для целых рациональных a, $(a, n) = 1$.

Основная теорема доказывается в §2 (см. теорема 1). В §3 доказываются также дополнительные теоремы (Ergänzungssätze).

2. Теорема о глобальном законе взаимности в круговом поле

Обозначения

- $2 \nmid n = \prod_{i=1}^r p_i^{m_i}$, $n_i = n/p_i^{m_i}$;
- $\sum_{i=1}^r a_i n_i \equiv 1 \pmod n$ (например, $\sum_{i=1}^r a_i n_i = 1$, или $a_i n_i + b_i p_i^{m_i} = 1$);
- $\mathrm{Tr}_i : \mathbb{Q}(\zeta_{n_i}) \to \mathbb{Q}$;
- $\zeta_i := \zeta_{p_i^{m_i}}$, $\pi_i = \zeta_i - 1$, $1 \leqslant i \leqslant r$;
- $\zeta_i' = \zeta_{p_1 \ldots p_{i-1} p_{i+1} \ldots p_r}$;
- $\{\pi_1^{\alpha_1} \ldots \pi_r^{\alpha_r},\ 0 \leqslant \alpha_i < \varphi(p_i^{m_i})\}$ – базис $\mathbb{Z}[\zeta]$ над $\mathbb{Z}$, где $\zeta := \zeta_n$;
- $\underline{\alpha}(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$ такой, что $\underline{\alpha}(\pi_1, \ldots, \pi_r) = \alpha \in \mathbb{Z}[\zeta]$ и $(\underline{\alpha}(0, \ldots, 0), n) = 1$;
- $\mathrm{res}_i := \mathrm{res}_{X_i}$;
- $\partial_i = \frac{\partial}{\partial X_i}$.

Определение ряда Φ_i

1.1. Операторы на $\mathbb{Z}[X_1, \ldots, X_r]$:

$$X_k^{\triangle_i} = \triangle_i(X_k) = \begin{cases} X_i^{p_i}, & k = i, \\ (1 + X_k)^{p_i} - 1, & k \neq i, \end{cases} \qquad 1 \leqslant i \leqslant r.$$

1.2. $\ell_i(f) = \frac{1}{p_i} \log(f^{p_i}/f^{\triangle_i})$ для $f \in \mathbb{Z}[X_1, ..., X_r]$, $(f(0, ..., 0), n) = 1$; $\Phi_i(\underline{\alpha}, \underline{\beta}) = \ell_i(\underline{\beta})\partial_i \ell_i(\underline{\alpha}) - \ell_i(\underline{\beta})\partial_i \log \underline{\alpha} + \ell_i(\underline{\alpha})\partial_i \log \underline{\beta}$.

Теорема (Востоков, [3]). *Для* $\alpha, \beta \in \mathbb{Z}[\zeta_n]$, $(\alpha\beta, n) = 1$, $(\alpha, \beta) = 1$ *имеем*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \zeta_n^S,$$

$$S = \sum_{i=1}^{r} a_i n_i \mathrm{Tr}_i \left(\mathrm{res}_i \frac{\Phi_i(\underline{\alpha}, \underline{\beta})}{\left(\underline{\zeta}_i^{p_i^{m_i}} - 1\right)} \bigg|_{X_k = \pi_k, k \neq i} \right). \tag{1}$$

3. Основная теорема

Вслед за Хассе будем обозначать $\{\alpha, \beta\}_n := \left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1}$.

Имеют место следующие свойства символа $\{,\}$.

1. $\{\alpha_1\alpha_2, \beta\}_n = \{\alpha_1, \beta\}_n \{\alpha_2, \beta\}_n$,
   $\{\alpha, \beta_1\beta_2\}_n = \{\alpha, \beta_1\}_n \{\alpha, \beta_2\}_n$.
2. Если $n' \mid n$, то $\{\alpha, \beta\}_{n/n'} = \{\alpha, \beta\}_n^{n'}$.
3. $\{\alpha, \beta\}_n = \prod_{i=1}^{r} \{\alpha, \beta\}_{p_i^{m_i}}^{a_i}$.
4. Если $\sigma_r : \zeta_n \to \zeta_n^{r^{-1}}$ в $\mathbb{Q}(\zeta_n)$, то $\{\alpha^{\sigma_r}, \beta^{\sigma_r}\}_n = \{\alpha, \beta\}_n^{r^{-1}}$.

Лемма. *Пусть* $n = \prod_{i=1}^{r} p_i^{m_i}$, $n' = n/p_1 \dots p_r$, $\zeta := \zeta_n$, $\zeta' = \zeta_{n/n'}$ – *первообразные корни степени* n *и* n/n' *соответственно.* $\mathrm{Tr} := \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$. *Тогда* $\mathrm{Tr}\,(\zeta') = (-1)^r n'$.

Доказательство. 1. $r = 1$, $n = p^m$, $n' = p^{m-1}$. Тогда ζ' – корень степени $n/n' = p$ из 1, то есть удовлетворяющий неприводимому над $\mathbb{Q}$ многочлену $1 + X + \dots + X^{p-1}$, поэтому $\mathrm{Tr}_{\mathbb{Q}(\zeta')/\mathbb{Q}}(\zeta') = -1$, и значит, $\mathrm{Tr}\,(\zeta') = -p^{m-1} = -n'$.

2. $r = 2$, $n = p^m q^k$, $n' = p^{m-1} q^{k-1}$. Пусть $\zeta' = \zeta_{pq} = \zeta_p \zeta_q$. Имеем башню полей:

$$\mathbb{Q} - \mathbb{Q}(\zeta_{p^m}) - \mathbb{Q}(\zeta_{p^m})(\zeta_{q^k}) = \mathbb{Q}(\zeta_n).$$

Из п. 1 получаем

$$\begin{aligned} \mathrm{Tr}\,(\zeta') &= \mathrm{Tr}\,(\zeta_p \zeta_q) = \mathrm{Tr}_{\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}}(\zeta_p \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{p^m})}(\zeta_q)) \\ &= \mathrm{Tr}_{\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}}(-q^{k-1}\zeta_p) = p^{m-1} q^{k-1}. \end{aligned}$$

3. Общий случай – индукция по r. □

Пусть a — фиксированное целое рациональное число, взаимно простое с n.

Теорема 1. *Следующие условия эквивалентны*

1. $\{a,\alpha\}_n = 1$ *для всех* $\alpha \in \mathbb{Z}[\zeta_n]$, $(\alpha, n) = 1$.
2. $\{a, 1-\zeta_i'(\zeta_i - 1)\}_n = 1$, $1 \leqslant i \leqslant r$ *(относительно обозначений см.* §1*).*
3. $\frac{a^{p_i-1}-1}{p_i} \equiv 0 \mod p_i^{m_i}$, $1 \leqslant i \leqslant r$.

Доказательство. Прежде всего рассмотрим i-тое слагаемое s_i в формуле (1) теоремы §1:

$$s_i = a_i n_i \mathrm{Tr}_i \left(\mathrm{res}_i \frac{\Phi_i(a, \underline{\alpha})}{\left(\underline{\zeta}_i^{p_i^{m_i}} - 1\right)} \bigg|_{X_k = \pi_k, k \neq i} \right),$$

и проверим, что

$$s_i = a_i n_i \frac{a^{p_i-1}-1}{p_i} c_i \mathrm{Tr}_i \left(\mathrm{res}_i \frac{\partial_i \log \underline{\alpha}}{\underline{\zeta}_i^{p_i^{m_i}} - 1} \bigg|_{X_k = \pi_k, k \neq i} \right), \tag{2}$$

$c_i \in \mathbb{Z}_p^*$.

Действительно, по определению $\ell_i(a)$ имеем

$$\begin{aligned} \ell_i(a) &= \frac{1}{p_i} \log a^{p_i-1} = \frac{1}{p_i} \log \left(1 + \frac{a^{p_i-1}-1}{p_i} p_i\right) \\ &= \frac{a^{p_i-1}-1}{p_i} \left(1 - \frac{1}{2} \frac{a^{p_{i-1}}-1}{p_i} p_i + \frac{1}{3} \left(\frac{a^{p_{i-1}}-1}{p_i} p_i\right)^2 - \cdots\right). \end{aligned}$$

Откуда

$$\ell_i(a) = \frac{a^{p_i-1}-1}{p_i} c_i, \tag{3}$$

где $c_i \in \mathbb{Z}_p^*$. Кроме того, т.к. $\ell_i(a) \in \mathbb{Z}_p$, то

$$\partial_i \ell_i(a) = 0$$

и, очевидно,

$$\partial_i \log a = a^{-1} \partial_i a = 0,$$

т.к. $a \in \mathbb{Z}$. Значит,

$$\Phi_i(a, \alpha) = \ell_i(a) \partial_i \log \underline{\alpha}.$$

Отсюда и из (3) следует (2).

Приступим теперь к доказательству теоремы. Ясно, что 2) – частный случай 1).

Докажем, что из 2)⇒3). Для этого в качестве α в формуле (2) возьмем число

$$\alpha := 1 - \zeta_i'(\zeta_i - 1)$$

и подсчитаем

$$d_i = \mathrm{Tr}_i\left(\mathrm{res}_i \frac{\partial_i \log \underline{\alpha}}{\underline{\zeta}^{p_i^{m_i}} - 1}\bigg|_{X_k=\pi_k, k\neq i}\right) \mod p_i.$$

В этом случае ряд

$$1/\left(\underline{\zeta}^{p_i^{m_i}} - 1\right) = 1/((1+X_i)^{p_i^{m_i}} - 1) \equiv X_i^{-p_i^{m_i}} \mod p_i.$$

Далее,

$$-\log \underline{\alpha} = -\log(1 - \underline{\zeta}_i' X_i) = \underline{\zeta}_i' X_i + \frac{1}{2}(\underline{\zeta}_i' X_i)^2 + \cdots + \frac{1}{p_i^{m_i}}(\underline{\zeta}_i' X_i)^{p_i^{m_i}} + \cdots$$

$$-\partial_i \log \underline{\alpha} = \underline{\zeta}_i' + (\underline{\zeta}_i')^2 X_i + \cdots + (\underline{\zeta}_i')^{p_i^{m_i}} (X_i)^{p_i^{m_i}-1} + \cdots .$$

Значит,

$$\mathrm{res}_i\left((\partial_i \log_i \underline{\alpha}) X_i^{-p_i^{m_i}}\right) = -(\zeta_i')^{p_i^{m_i}}.$$

Заметим, что $(\zeta_1')^{p_i^{m_i}}$ – первообразный корень степени

$$p_1 \dots p_{i-1} p_{i+1} \dots p_r$$

из 1, и, значит, по лемме

$$\mathrm{Tr}_i(\zeta_i')^{p_i^{m_i}} = (-1)^{r-1} n_i',$$

где $n_i' = p_1^{m_1-1} \dots p_{i-1}^{m_{i-1}-1} p_{i+1}^{m_{i+1}-1} \dots p_r^{m_r-1}$ – число, взаимно простое с $p_i^{m_i}$. Отсюда следует, что $(d_i, p_i) = 1$ и, значит, $s \equiv 0 \pmod n \Rightarrow s_i \equiv 0 \mod p_i^{m_i} \Rightarrow a_i n_i \frac{a^{p_i-1}-1}{p_i} c_i \equiv 0 \mod p_i^{m_i} \Rightarrow \frac{a^{p_i-1}-1}{p_i} \equiv 0 \mod p_i^{m_i}$ и мы доказали 2)⇒3).

Из условия 3) теоремы и равенства (2) следует, что i-ое слагаемое s_i, удовлетворяет сравнению $s_i \equiv 0 \mod p_i^{m_i} n_i$, то есть $s_i \equiv 0 \mod n$, и значит $\zeta_n^{s_i} = 1$, $1 \leqslant i \leqslant r$, что дает нам условие 1) теоремы. □

4. Ergänzungssätze

Как и в общем законе взаимности докажем сопутствующие результаты.

Теорема 2. *Пусть* $\zeta := \zeta_n$. *Тогда*

1. $\left(\frac{\zeta}{a}\right)_n = 1 \Leftrightarrow \frac{a^{p_i-1}}{p_i}\varphi(n_i) \equiv 0 \mod p_i^{m_i}$, *где* $n = \prod\limits_{i=1}^{r} p_i^{m_i}$.
2. $\left(\frac{a}{b}\right)_n = 1$ *для любых целых рациональных* a *и* b, *взаимно простых с* n *и друг с другом.*
3. $\{a, \zeta - 1\}_n = 1 \Leftrightarrow \frac{a^{p_i-1}}{p_i}\varphi(n_i) \equiv 0 \mod p_i^{m_i}$.

Доказательство. 1. Нам надо проверить, что при выполнении условий п. 1) имеет место равенство $\{a, \zeta\}_n = 1$, так как, очевидно, тогда $\left(\frac{\zeta}{a}\right)_n = \left(\frac{a}{\zeta}\right)_n = 1$, так как $\zeta \in \mathbb{Z}[\zeta]^*$.

Запишем корень ζ в виде $\zeta = \zeta_{n_i} \cdot \zeta_i$, где ζ_{n_i} (соответственно ζ_i) – корень степени n_i (соответственно $p_i^{m_i}$) из 1, и возьмем в формуле (2) в качестве α число $\zeta_{n_i} \cdot \zeta_i$. При этом $\zeta_i \in \mathbb{Z}[X_i]$, а $\zeta_{n_i} \in \mathbb{Z}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

Подсчитаем, как и в доказательстве теоремы 1,

$$d_i = \mathrm{Tr}\left(\mathrm{res}_i \frac{\partial_i \log \underline{\zeta}}{\underline{\zeta}_i^{p_i^{m_i}-1}}\bigg|_{X_k=\pi_k, k\neq i}\right).$$

Сперва вычислим

$$c_i = \mathrm{res}_i \frac{\partial_i \log \underline{\zeta}}{\underline{\zeta}_i^{p_i^{m_i}} - 1} \mod p_i.$$

В этом случае, как было показано,

$$1/(\underline{\zeta}_i^{p_i^{m_i}}) \equiv X_i^{-p_i^{m_i}} \mod p_i$$

и, кроме того,

$$\partial_i \log \underline{\zeta} = \underline{\zeta}^{-1}\partial_i \underline{\zeta} = \underline{\zeta}_i^{-1}\partial_i \underline{\zeta}_i = (1 + X_i)^{-1}\partial_i(1 + X_i) = (1 + X_i)^{-1},$$

и значит, c_i – целое число, удовлетворяющее сравнению $c_i \equiv \mathrm{res}_i(1 + X_i)^{-1}X_i^{-p^{m_i}} \equiv 1 \mod p_i$, откуда $(c_i, p_i) = 1$.

В итоге получаем $d_i = \mathrm{Tr}_i c_i = \varphi(n_i)c_i$.

Поэтому i-ое слагаемое s_i в формуле (1) будет равно согласно (2)

$$s_i = a_i n_i \frac{a^{p_i-1}-1}{p_i}\varphi(n_i)c_i, \quad (c_i, p_i) = 1,$$

и, значит,

$$s_i \equiv 0 \mod p_i^{m_i} \Leftrightarrow \frac{a^{p_i-1}-1}{p_i}\varphi(n_i) \equiv 0 \mod p_i^{m_i}.$$

2. Проверим второе утверждение теоремы. Заметим, что a и b – целые рациональные числа, поэтому ряд $\Phi_i(a,b) = 0$, и, значит, $s_i = 0$, $1 \leqslant i \leqslant r$, откуда $\{a,b\}_n = 1$, то есть $\left(\frac{a}{b}\right)_n = \left(\frac{b}{a}\right)_n$. Учитывая взаимную простоту чисел a и b, получаем наше утверждение.

3. Аналогично первому пункту: запишем корень ζ в виде $\zeta = \zeta_{n_i} \cdot \zeta_i$, где ζ_{n_i} (соответственно ζ_i) – корень степени n_i (соответственно $p_i^{m_i}$) из 1, и возьмем в формуле (2) в качестве α число $\zeta_{n_i} \cdot \zeta_i - 1$. Подсчитаем, как и в доказательстве теоремы 1,

$$d_i = \mathrm{Tr}\left(\mathrm{res}_i \frac{\partial_i \log(\underline{\zeta}-1)}{\underline{\zeta}_i^{p_i^{m_i}-1}}\bigg|_{X_k=\pi_k, k\neq i}\right).$$

Сперва вычислим

$$c_i = \mathrm{res}_i \frac{\partial_i \log(\underline{\zeta}-1)}{\underline{\zeta}_i^{p_i^{m_i}}-1} \quad \text{по} \quad \mod p_i.$$

В этом случае, как было показано,

$$1/(\underline{\zeta}_i^{p_i^{m_i}}-1) \equiv X_i^{-p_i^{m_i}} \mod p_i$$

и, кроме того,

$$\partial_i \log(\underline{\zeta}-1) = \frac{\partial_i(\underline{\zeta}-1)}{\underline{\zeta}-1} = \frac{\underline{\zeta}_{n_i}}{\underline{\zeta}-1} = \frac{\underline{\zeta}_{n_i}}{\underline{\zeta}_{n_i}(1+X_i)-1}$$
$$= \left(\frac{\underline{\zeta}_{n_i}}{\underline{\zeta}_{n_i}-1}\right)\frac{1}{1+X_i\left(\frac{\underline{\zeta}_{n_i}}{\underline{\zeta}_{n_i}-1}\right)}.$$

Тогда

$$c_i = \left(\frac{\zeta_{n_i}}{\zeta_{n_i} - 1}\right)^{p_i^{m_i}} (-1)^{p_i^{m_1}-1}(1+kp), \quad k \in \mathbb{Z}[\zeta_{n_i}].$$

Тогда $s_i \equiv 0 \mod n \Leftrightarrow d_i \equiv 0 \mod p_i^{m_i} \Leftrightarrow \frac{a^{p_i-1}-1}{p_i}$

$$\mathrm{Tr}_i \left(\frac{\zeta_{n_i}}{\zeta_{n_i} - 1}\right)^{p_i^{m_i}} (-1)^{p_i^{m_1}-1} \equiv 0 \mod p_i^{m_i}.$$

Но $\mathrm{Tr}_i \left(\frac{\zeta_{n_i}}{\zeta_{n_i}-1}\right)^{p_i^{m_i}} \equiv \varphi(n_i)/2 \pmod{p_i^{m_i}}$, поэтому получаем,

$$\frac{a^{p_i-1}-1}{p_i}\varphi(n_i) \equiv 0 \mod p_i^{m_i},$$

так как $(2, n) = 1$. □

Литература

1. G. Eisenstein, *Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze.* — J. für die reine u. ang. Mathematik **39** (1850), 351–364.
2. H. Hasse, *Das Eisensteinsche Reziprozitätsgesetz der n-ten Potenzreste.* — Math. Ann. **97** (1927), 599–623.
3. С. В. Востоков, *Классический закон взаимности степенных вычетов, как аналог теоремы об абелевом интеграле.* — Алгебра и анализ **20** (2008), No. 6, 1–10.

Vostokov S. V., Ivanov M. A., Pak G. K. On a paper by Hasse concerning Eisenstein reciprocity law.

In the present paper we give necessary and sufficient conditions equality power rezidue symbols $\left(\frac{\alpha}{a}\right)_n$ and $\left(\frac{a}{\alpha}\right)_n$ in the cyclotomic field $\mathbb{Q}(\zeta_n)$, $2 \nmid n$, for $a \in \mathbb{Z}$, $(a, n) = 1$. This result is generalization of classical Eisenstein reciprocity law and its continuation in Hasse paper.

С.-Петербургский
государственный университет
E-mail: sergei.vostokov@gmail.com

Поступило 2 февраля 2009 г.