УДК 512.741 Вестник СПбГУ. Сер. 1. Т. 3 (61). 2016. Вып. 3

# АРИФМЕТИКА ГИПЕРБОЛИЧЕСКИХ ФОРМАЛЬНЫХ МОДУЛЕЙ

*Р. П. Востокова*[1], *П. Н. Питаль*[2]

[1] Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова, Российская федерация, 190005, Санкт-Петербург, ул. 1-я Красноармейская, 1
[2] Санкт-Петербургский государственный университет, Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7–9

В работе рассмотрены гиперболические формальные группы, происходящие из теории эллиптических кривых, с точки зрения теории формальных модулей. В первой части работы изучены свойства гиперболических формальных групп: даны явные формулы для формальных логарифма и экспоненты, изучена их сходимость. Во второй части найдена изогения, ее ядро и высота, построен $p$-типический логарифм. Далее построены экспонента Артина—Хассе и функция Востокова, проверена корректность их построения и основные свойства. Библиогр. 4 назв.

*Ключевые слова*: гиперболические формальные модули, формальные модули, формальные группы.

**Введение.** В теории эллиптических кривых есть особый класс так называемых гиперболических кривых. Уравнение Вейерштрасса в проективной плоскости для таких кривых имеет вид

$$Y^2Z + \mu_1 XYZ = X^3 + \mu_2 X^2 Z.$$

В настоящей работе мы изучаем формальные группы, соответствующие этим кривым. Мы строим основные арифметические характеристики этих формальных групп — логарифм и экспоненту (см. п. 1), исследуем их сходимость в полных дискретно нормированных полях (см. п. 1.3). Далее мы находим изогению и ее ядро для гиперболических формальных групповых законов (см. п. 2). Наконец, в целях нахождения явных формул спаривания Гильберта для гиперболических формальных модулей, построенных на максимальном идеале кольца целых локального поля, строим $p$-типический логарифм, функцию Артина—Хассе и обратную к ней функцию Востокова (см. п. 3).

## 1. Логарифм и экспонента гиперболического группового закона.

***1.1. Инвариантный дифференциал.*** Для формальной группы $F(X,Y)$ над кольцом $A$ *инвариантным формальным дифференциалом* называется дифференциальная формальная форма вида $\omega(X) = P(X)dX \in A[[X]]dX$ такая, что выполняется $\omega \circ F(X,Y) = \omega(X)$ (подробнее см. в [1, с. 125]).

Для любого формального ряда $P[X] \in A[[X]]$, удовлетворяющего равенству $P(F(X,Y))F(X,Y)_x = P(X)$, дифференциальная форма $\omega(X) = P(X)dX$ будет формальным дифференциалом (здесь под $F_x$ мы понимаем формальную производную $F(X,Y)$ по первой переменной). Если справедливо $P(0) = 1$, дифференциальная форма $\omega$ называется *нормализованным инвариантным дифференциалом* и обозначается $\Omega$.

Известно, что для любой формальной группы $F$ над кольцом $A$ существует единственный нормализованный инвариантный дифференциал вида $\Omega = F_x(0,X)^{-1}dX$, а все остальные инвариантные дифференциалы имеют вид $a\Omega$, где $a \in A$ (см., например, [1, с. 125]).



 DOI: 10.21638/11701/spbu01.2016.305

**_1.2. Логарифм и экспонента формальной гиперболической группы._** Для гиперболических эллиптических кривых соответствующая формальная группа имеет вид (см. [2])

$$F_{\mu 1,\mu 2}(X,Y)=\frac{X+Y-\mu_1 XY}{1+\mu_2 XY}.$$

**Замечание.** В дальнейшем будем предполагать, что уравнение $T^2-\mu_1 T-\mu_2=0_{\mathcal{O}}$ (где $\mathcal{O}$ — кольцо, над которым мы рассматриваем $F_{\mu 1,\mu 2}$) разрешимо в $\mathcal{O}$ и $a,b\in\mathcal{O}$ — корни этого уравнения. Тогда будем иметь $\mu_1=a+b$, $\mu_2=-ab$, и, следовательно

$$F_{a,b}(X,Y)=\frac{X+Y-\mu_1 XY}{1+\mu_2 XY}=\frac{X+Y-(a+b)XY}{1-abXY}.$$

Логарифм формальной группы $F_{a,b}$, который является изоморфизмом из $F_{a,b}$ в аддитивную формальную группу $G_a=X+Y$, задается с помощью нормализованного инвариантного дифференциала $\Omega$, как формальный интеграл: $\lambda_{F_{a,b}}=\int\Omega$ (см. [3, с. 1058]).

Для вычисления нормализованного инвариантного дифференциала $\Omega$ найдем

$$F_{a,b}(X,Y)_x=\frac{abY^2-(a+b)Y+1}{(1-abXY)^2}.$$

Тогда дифференциал будет равен

$$\Omega_{F_{a,b}}(X)=F_{a,b}(0,X)_x^{-1}dX=\left(abX^2-(a+b)X+1\right)^{-1}dX=\frac{dX}{(1-aX)(1-bX)}.$$

Пусть выполняется $a\neq b$, тогда будем иметь

$$\frac{dX}{(1-aX)(1-bX)}=\frac{1}{(a-b)X}\cdot\left(\frac{1}{1-aX}-\frac{1}{1-bX}\right)dX=\frac{dX}{a-b}\sum_{n\geqslant 0}\left(a^{n+1}-b^{n+1}\right)\cdot X^n.$$

Формально проинтегрировав последний ряд, получим

$$\lambda_{F_{a,b}}(X)=(a-b)^{-1}\cdot\sum_{n\geqslant 0}\frac{(a^{n+1}-b^{n+1})}{n+1}\cdot X^{n+1},\quad a\neq b$$

или

$$\lambda_{F_{a,b}}(X)=(a-b)^{-1}\cdot\left(\log\left(\frac{1-bX}{1-aX}\right)\right),\quad a\neq b.$$

Вычислим теперь формальную экспоненту для формальной группы $F_{a,b}$, которая является обратной по суперпозиции к ряду $\lambda_{F_{a,b}}$:

$$e_{F_{a,b}}(X)=\frac{\exp(aX)-\exp(bX)}{a\cdot\exp(aX)-b\cdot\exp(bX)},\quad a\neq b.$$

**Замечание.** Несложно проверить, что при $a=b$ логарифм формальной группы $F_{a,a}$ будет равен $\lambda_{F_{a,a}}=a^{-1}\sum_{n\geqslant 1}a^nX^n$, что в точности соответствует общему случаю, если записать $\lambda_{F_{a,b}}$ в виде

$$\lambda_{F_{a,b}}(X)=(a-b)^{-1}\cdot\sum_{n\geqslant 0}\frac{a^{n+1}-b^{n+1}}{n+1}\cdot X^{n+1}=\sum_{n\geqslant 0}\left(\sum_{k\geqslant 0}^{n}\frac{(a^kb^{n-k})}{n+1}\right)\cdot X^{n+1}.$$

Аналогичное замечание верно и для экспоненты $e_{F_{a,a}}(X)$.

***1.3. Области сходимости формальных экспоненты и логарифма.*** Пусть $\mathcal{O}$ — полное дискретно нормированное кольцо нулевой характеристики и $\nu$ — нормирование в $\mathcal{O}$. Пусть $\mathfrak{M}$ — максимальный идеал $\mathcal{O}$, а $p = \mathrm{Char}(\mathcal{O}/\mathfrak{M})$ — характеристика его поля вычетов (мы будем предполагать, что это не ноль).

Зададим кольцо $\tilde{\mathcal{O}}$ как $\tilde{\mathcal{O}} = \mathcal{O} \otimes \mathbb{Q}$ и продолжим $\nu$ на тензорное произведение естественным образом:

$$\nu(a \otimes b) = \nu(a) + \mathrm{ord}_p(b) \cdot \nu(p), \quad a \in \mathcal{O}, \quad b \in \mathbb{Q}.$$

Пусть $\|x\|_\rho = \rho^{\nu(x)}$ — норма на $\mathcal{O}$, где $\rho \in R$, $0 < \rho < 1$. Изучим сходимость формальных степенных рядов $f(X) = \sum_{n\geqslant 0} a_n X^n$ с коэффициентами из $\mathcal{O}$ по норме $\| \ \|_\rho$. Известно (см., например, [1]), что

DV1) для всех натуральных чисел $n$ справедливо неравенство $\nu(n!) \leqslant \nu(p) \cdot \frac{n-1}{p-1}$;

DV2) ряд $f = \sum_{n\geq 0} a_n$ сходится тогда и только тогда, когда имеет место равенство $\lim\limits_{n\to\infty} \nu(a_n) = \infty$;

DV3) пусть ряд $f(x) = \sum_{n\geq 0} a_n x^n$ сходится на множестве $A$, и при этом существует $N \in \mathbb{N}$ такое, что для всех натуральных чисел $n \neq N$ и для всех элементов $x$ из множества $A$ верно $\nu(a_n x^n) \geqslant \nu(a_N x^N)$; тогда для всех $x$ из $A$ также верно $\nu(f(x)) = \nu(a_N x^N)$.

Пусть имеем $a, b, c, a_i, b_i \in \mathcal{O}$. Введем следующие обозначения:

- $D_r = \{x \in \tilde{\mathcal{O}} | \nu(x) > r\}$;
- $B_{f(x)} = D_{\log_\rho(r_{f(x)})}$ — экспоненциальный круг сходимости ряда $f(x)$, если $\{x \in \tilde{\mathcal{O}}| \ \|x\|_\rho < r_{f(x)}\}$ — круг сходимости ряда $f(x)$;
- $PL(x) = \sum\limits_{n\geqslant 1} \frac{a_n}{n} x^n$;
- $PE(x) = \sum\limits_{n\geqslant 1} \frac{b_n}{n!} x^n$;
- $ME(x) = \sum\limits_{n\geqslant 1} \frac{c^n}{n!} x^n$;
- $ME_{a,b}(x) = ME((a-b)x) - 1$;
- $MHL_a(x) = \sum\limits_{n\geqslant 1} (a)^{n-1} x^n$;
- $ML_a(x) = \sum\limits_{n\geqslant 1} \frac{(a)^{n-1}}{n} x^n$;
- $HL_{a,b}(x) = (b-a)^{-1} \sum\limits_{n\geqslant 1} \frac{a^n - b^n}{n} x^n$;
- для последних четырех рядов можно рассматривать $AC_{f(x)}$ — множество значений параметров $(a, b)$, при которых ряд $f(x)$ сходится на границе круга сходимости;
- $\phi = \nu(p)/(p-1)$;
- $(f(X))_n$ — $n$-й член ряда $f(x) = \sum\limits_{n\geq 0} a_n x^n$.

**Предложение 1.1.** *Справедливы утверждения:*

*a)* $B_{PL(x)} = \{x \in \tilde{\mathcal{O}} | \nu(x) > 0\}$;
*ряд PE сходится в каждой точке области* $D_{\frac{\nu(p)}{p-1}}$, *причем если выполняется* $b_1 \in \mathcal{O}^*$, *справедливо* $\nu(PE(x)) = \nu(x)$ *при* $x \in B_{PE(x)}$;

*b)* $B_{ME(x)} = D_{\frac{\nu(p)}{p-1}}$, *ряд ME расходится на границе круга.*

Доказательство. *a)* Воспользуемся $DV2$ и изучим предел нормирования общего члена ряда на бесконечности, учитывая $a_n \in \mathcal{O}$: $\nu(PL(x))_n = \nu\left(\frac{a^n}{n}x^n\right) \geqslant n \cdot \nu(x) - \nu(n) \geqslant n \cdot \nu(x) - (\log_p(n))\nu(p) \to \infty$ при $n \to \infty$.

*b)* Воспользовавшись $DV1$ и $b_n \in \mathcal{O}$, получим $\nu(PE(x))_n = \nu\left(\frac{b_n}{n!}x^n\right) \geqslant n\nu(x) - \nu(n!) \geqslant n\nu(x) - (n-1) \cdot \frac{\nu(p)}{p-1} = \nu(x) + (n-1) \cdot \left(\nu(x) - \frac{\nu(p)}{p-1}\right)$. Очевидно, что при $\nu(x) > \frac{\nu(p)}{p-1}$ выполняется $\nu(PE(x))_n \geqslant \nu(x) + (n-1) \cdot (\nu(x) - \frac{\nu(p)}{p-1}) \to \infty$ при $n \to \infty$. Более того, имеем $\nu\left(PE(x)_n\right) > \nu(x)$ $\forall n \geqslant 2$, поэтому, учитывая $\nu(PE(x))_1 = \nu(b_1 \cdot x) = \nu(x)$, в соответствии с $DV3$, получаем $\nu(PE(x)) = \nu(x)$ при $\nu(x) > \frac{\nu(p)}{p-1}$.

*c)* В предыдущем пункте мы доказали $D_{\frac{\nu(p)}{p-1}} \subset B_{ME}$. Предположим, что обратное неверно, тогда в $B_{ME}$ должна по меньшей мере содержаться граница $D_{\frac{\nu(p)}{p-1}}$, т. е. для любого $\tau \in \{\theta \in \tilde{\mathcal{O}} |\ \nu(\theta) = \frac{\nu(p)}{p-1}\}$ ряд $ME(\tau)$ сходится. Это эквивалентно $\nu(ME(\tau))_n \to \infty$ при $n \to \infty$. Выделив подпоследовательность, окончательно получим $\nu(ME(\tau))_{p^m} \to \infty$ при $m \to \infty$. Проверим, что это не так:

$$\lim_{m\to\infty} \nu(ME(\tau))_{p^m} = \lim_{m\to\infty}\left(p^m \frac{\nu(p)}{p-1} - \nu(p)\sum_{n=1}^{m} p^{m-1}\right) = \\ = \lim_{m\to\infty}\left(\nu(p)\left(\frac{p^m}{p-1} - \frac{p^m-1}{p-1}\right)\right) = \frac{\nu(p)}{p-1}.$$

Таким образом, мы нашли явное противоречие, заодно изучив поведение ряда на границе.

□

Из предложения 1.1 непосредственно вытекает следствие.

**Следствие 1.2.** *Пусть имеем* $a, b \in \mathcal{O}$. *Тогда справедливы следующие утверждения:*
$B_{MHL_a(x)} = D_0$, $AC_{MHL_a(x)} = \{a \in \mathcal{O} | \nu(a) > 0\}$;
$B_{ML_a(x)} = D_0$, $AC_{ML_a(x)} = \{a \in \mathcal{O} | \nu(a) > 0\}$;
$B_{HL_{a,b}(x)} = D_0$, $AC_{HL_{a,b}(x)} = \mathcal{O} \times \mathcal{O} \setminus \{(a,b) |\ a, b \in \mathcal{O}, \nu(a) + \nu(b) \neq 0\}$;
$B_{ME_{a,b}(x)} = D_{\phi - \nu(a-b)}, AC_{ME_{a,b}(x)}$ *пусто.*

**Теорема 1.3 (Сходимость формальных логарифма и экспоненты).** *Пусть* $F_{a,b}(X,Y) = (X + Y - (a+b)XY)/(1 - abXY)$ — *гиперболический формальный групповой закон над* $\mathcal{O}$, *тогда справедливы утверждения:*

*1) логарифм* $\lambda_{F_{a,b}}(x) = (a-b)^{-1} \cdot \sum\limits_{n\geqslant 0} \frac{(a^{n+1} - b^{n+1})}{n+1} \cdot x^{n+1}$ *расходится, только если выполняется* $\nu(abx) = 0$, *и сходится во всех остальных случаях.*

*2) экспонента $e_{F_{a,b}}(x) = \frac{\exp(ax)-\exp(bx)}{a\cdot\exp(ax)-b\cdot\exp(bx)}$ в случае $a \neq b$ сходится при $\nu(x) > \frac{\nu(p)}{p} - \nu(a-b)$ и расходится в остальных точках, в случае $a = b \neq 0$ расходится только лишь в точке 0, и, наконец, если $a = b = 0$, сходится во всех точках.*

Доказательство. Формальный логарифм $\lambda_{F_{a,b}}$ совпадает с $HL_{a,b}$, для которого мы уже доказали требуемое в следствии 1.2.

Формальная экспонента определяется равенством $e_{F_{a,b}} = \frac{\exp(a-b)X-1}{a\exp(a-b)X-b} = b^{-1}\frac{ME_{a,b}}{a\cdot ME_{a,b}-b}$. В случае $x \in D_{\phi-\nu(a-b)}$ ряд $ME_{a,b}$ сходится, согласно следствию 1.2, а значит, если выполняется $aME_{a,b} \neq b$ (что, очевидно, возможно только при $a = b$), экспонента сходится как отношение сходящегося и ненулевого сходящегося. Проверим теперь сходимость на границе круга, т. е. предположим $x = \frac{\nu(p)}{p-1} - \nu(a-b)$. Представим экспоненту в следующем виде:

$$e_{F_{a,b}} = \left(\frac{b-a}{a\cdot a\exp((a-b)x) - ba}\right) + a^{-1} = G(x) + a^{-1}.$$

Заметим, что если $G$ сходится не к $a^{-1}$, сходится и ряд $1/G$, который равен $(a\cdot a\exp((a-b)x) - ba)/(b-a)$ и, очевидно, расходится на границе $D_{\phi-\nu(a-b)}$.

Остается случай $a = b$ (предположим пока, что выполняется $a \neq 0$). В этом случае будем иметь

$$\lambda_{F_{a,b}} = a^{-1}\sum_{n\geqslant 1} a^n x^n,$$

а значит экспонента представляется как

$$e_{F_{a,b}} = \frac{1}{a} - \frac{1}{x}$$

и, очевидно, расходится только при $x = 0$. В случае $a = b = 0$ мы получаем аддитивный групповой закон с линейной экспонентой. □

**2. Изогения, ее ядро и высота, $p$-типический логарифм.** Пусть $F_{a,b}$ — гиперболическая формальная группа, заданная на кольце $A$. Вычислим ее изогению $[n]_{a,b}(X) = e_{F_{a,b}}(n\lambda_{F_{a,b}}(X))$. После подстановки будем иметь

$$[n]_{a,b}(X) = \frac{\exp\left((a-b)n(a-b)^{-1}\cdot\left(\log\left(\frac{1-bX}{1-aX}\right)\right)\right) - 1}{a\exp\left((a-b)n(a-b)^{-1}\cdot\left(\log\left(\frac{1-bX}{1-aX}\right)\right)\right) - b}.$$

Упростив, получим

$$[n]_{a,b}(X) = \frac{\left(\frac{1-bX}{1-aX}\right)^n - 1}{a\left(\frac{1-bX}{1-aX}\right)^n - b}.$$

Найдем ее ядро:

$$\frac{\left(\frac{1-bX}{1-aX}\right)^n - 1}{a\left(\frac{1-bX}{1-aX}\right)^n - b} = 0 \Leftrightarrow \left(\frac{1-bX}{1-aX}\right)^n - 1 = 0 \Leftrightarrow (a\zeta - b)X = \zeta - 1 \Leftrightarrow X = \frac{\zeta-1}{a\zeta-b},$$

где $\zeta$ — корень $n$-й степени из 1.

Теперь изучим ряд $[p]_{a,b}$ по модулю $p$, считая $p$ нечетным простым числом:

$$[p]_{a,b}(X) = \frac{\left(\frac{1-bX}{1-aX}\right)^p - 1}{a\left(\frac{1-bX}{1-aX}\right)^p - b} = \frac{X^p(a-b)^p}{a - ab^pX^p - b + ba^pX^p} =$$

$$= \frac{(a^p - b^p)(ab)^{-1}}{a-b} \frac{X^p}{1 + X^p \cdot \frac{a^{p-1}-b^{p-1}}{a-b}} = \Sigma_1 \cdot (ab)^{-1} \frac{X^p}{1 + X^p \cdot \Sigma_2},$$

где использованы обозначения $\Sigma_k = \frac{a^{p-k+1}-b^{p-k+1}}{a-b} = \sum\limits_{i=0}^{p-k} a^i b^{p-k-i}$, $k = 1, 2$. Далее раскроем ряд

$$\Sigma_1 \cdot (ab)^{-1} \frac{X^p}{1 + X^p \cdot \Sigma_2} = \Sigma_1 \cdot (ab)^{-1} \sum_{n \geqslant 1} X^{pn} \cdot (\Sigma_2)^n.$$

Таким образом, имеем $[p]_{a,b}(X) \equiv g(X^p) \mod p$, и следовательно высота $F_{a,b}$ равна 1, т. е. мы доказали следующую теорему.

**Теорема 2.1.** *Гиперболическая формальная группа имеет высоту* 1 *и изогению*

$$[n]_{a,b}(X) = \frac{\left(\frac{1-bX}{1-aX}\right)^n - 1}{a\left(\frac{1-bX}{1-aX}\right)^n - b}$$

*с ядром* $\ker[n]_{a,b}(X) = \{\xi_n | \xi_n = \frac{\zeta-1}{a\zeta-b}\}$.

**Следствие 2.2.** *Универсальный p-типический закон, соответствующий* $F_{a,b}$, *имеет логарифм вида*

$$\lambda_{a,b,p}(X) = (a-b)^{-1} \cdot \sum_{n \geq 0} \frac{a^{p^n} - b^{p^n}}{p^n} \cdot X^{p^n}.$$

Теперь будем рассматривать $a$ и $b$, как переменные. Определим операторы $\Lambda$, $\Lambda^{-1}$, $\Delta$ следующим образом:

$\Delta(t^m) = t^{pm}$, где $t \in \{a, b, X\}$ — переменная (оператор Фробениуса),

$\Lambda(\Delta) = \left(1 - \frac{\Delta}{p}\right)^{-1}$,

$\Lambda^{-1}(\Delta) = \left(1 - \frac{\Delta}{p}\right)$.

**Предложение 2.3.** *Универсальный p-типический закон, соответствующий* $F_{a,b}$, *имеет логарифм вида*

$$\lambda_{a,b,p}(X) = (a-b)^{-1}\Lambda(\Delta)\left((a-b)X\right).$$

Доказательство. Это проверяется простой подстановкой:

$$(a-b)^{-1}\Lambda(\Delta)\left((a-b)X\right) = (a-b)^{-1}\left(\Lambda(\Delta)(aX) - \Lambda(\Delta)(bX)\right) =$$

$$= (a-b)^{-1}\left(\sum_{n \geq 0} \frac{a^{p^n}}{p^n} \cdot X^{p^n} - \sum_{n \geq 0} \frac{b^{p^n}}{p^n} \cdot X^{p^n}\right) =$$

$$= (a-b)^{-1} \cdot \sum_{n \geq 0} \frac{a^{p^n} - b^{p^n}}{p^n} \cdot X^{p^n} = \lambda_{a,b,p}(X). \quad \square$$

В дальнейшем нам понадобится и обратный к $p$-типическому логарифму ряд $e_{a,b,p}$, который мы будем называть $p$-типической экспонентой. Его удобно записать на языке операторов.

**Предложение 2.4.** *Универсальный $p$-типический закон, соответствующий $F_{a,b}$, имеет экспоненту ($p$-типическую экспоненту) вида*

$$e_{a,b,p}(X) = (a-b)^{-1}\Lambda^{-1}\left((a-b)X\right).$$

Доказательство. Убедимся, что ряды действительно взаимно обратны:

$$e_{a,b,p}\left(\lambda_{a,b,p}(X)\right) = (a-b)^{-1}\Lambda^{-1}\Big((a-b)\Big((a-b)^{-1}\Lambda(\Delta)\left((a-b)X\right)\Big)\Big) =$$
$$= (a-b)^{-1}\Lambda^{-1}\left(\Lambda(\Delta)((a-b)X)\right) = (a-b)^{-1}(a-b)X = X. \quad \square$$

**3. Гиперболические формальные модули.** ***3.1. Экспонента Артина—Хассе.*** Пусть $\mathcal{O}$ — полное дискретно нормированное кольцо нулевой характеристики с совершенным полем вычетов, неразветвленное над $\mathbb{Z}_p$ (тут под $p$ мы, как и ранее, подразумеваем нечетное простое число), и $\sigma$ — автоморфизм Фробениуса на $\mathcal{O}$. Определим оператор Фробениуса $\Delta$ на кольце $X\mathcal{O}[[X]]$:

$$\Delta(aX^m) = \sigma(a)X^{pm}, \quad a \in \mathcal{O}.$$

Пусть $F$ — формальная группа над $\mathcal{O}$ высоты $h$ с логарифмом $\lambda$ и экспонентой $e$. Зададим на $X\mathcal{O}[[X]]$ структуру кольца рядов Картье:

$$f +_F g = F(f,g), \quad f,g \in X\mathcal{O}[[X]].$$

Пусть $F_p$ — $p$-типическая формальная группа изоморфная $F$ с логарифмом $\lambda_{F_p}$. Рассмотрим формальный ряд $\overline{\Lambda} \in \mathcal{O}[\Delta]$ такой, что выполняется $\lambda_{F_p} = \overline{\Lambda}(\Delta)(X)$. Экспонентой Артина—Хассе и $l$-функцией Востокова формальной группы $F$ над $\mathcal{O}$ будем называть, соответственно, следующие формальные степенные ряды:

1. $E_F(f) = e(\overline{\Lambda}(\Delta))(f)$;
2. $l_F(f) = \overline{\Lambda}^{-1}(\Delta)(\lambda(f))$,

где $f \in X\mathcal{O}[[X]]$, а под $\overline{\Lambda}^{-1}$ мы подразумеваем обратный по композиции ряд.

***3.2. Гиперболическая формальная группа.*** Пусть $F_{a,b}$ — формальная гиперболическая группа. Согласно предложениям 2.3 и 2.4 соответствующие ей $p$-типические логарифм и экспонента имеют вид

$$\lambda_{a,b,p}(X) = (a-b)^{-1}\Lambda(\Delta)((a-b)X);$$
$$e_{a,b,p}(X) = (a-b)^{-1}\Lambda^{-1}\left((a-b)X\right),$$

где обозначено

$$\Lambda(\Delta) = \left(1 - \frac{\Delta}{p}\right)^{-1}.$$

Формальные экспонента и логарифм имеют вид

$$e_{F_{a,b}}(X) = \frac{\exp\left((a-b)X\right) - 1}{a \cdot \exp\left((a-b)X\right) - b}, \quad \lambda_{F_{a,b}}(X) = (a-b)^{-1} \cdot \left(\log\left(\frac{1-bX}{1-aX}\right)\right).$$

Основываясь на этом, мы можем доказать следующую теорему.

**Теорема 3.1.** *Экспонента Артина—Хассе и $l$-функция Востокова формального гиперболического закона имеют, соответственно, вид*

$$E_{F_{a,b}}(X) = \frac{\exp\left(\left(1-\frac{\Delta}{p}\right)^{-1}(a-b)X\right)-1}{a\cdot\exp\left(1-\frac{\Delta}{p}^{-1}(a-b)X\right)-b},$$

$$l_{F_{a,b}}(X) = (a-b)^{-1}\left(\left(1-\frac{\Delta}{p}\right)^{-1}\log\left(\frac{1-bX}{1-aX}\right)\right).$$

Доказательство. Простая подстановка легко дает нам заявленное. □

Доказательство следующего утверждения следует непосредственно из лемм 2–4 работы [4].

**Теорема 3.2 (Свойства экспоненты Артина—Хассе).** *1. $E_{F_{a,b}}, l_{Fa,b}$ корректно определены, т. е. если справедливо $f \in X\mathcal{O}[[X]]$, выполняется $E_{F_{a,b}}(f), l_{Fa,b}(f) \in X\mathcal{O}[[X]]$, и являются взаимно обратными. 2. $E_{F_{a,b}}(f+g) = E_{F_{a,b}}(f) +_F E_{F_{a,b}}(g)$.*

**Литература**

1. *Silverman J. H.* The Arithmetic of Elliptic Curves // Graduate Texts in Mathematics. Springer-Verlag. 2009. Vol. 106.

2. *Buchstaber V. M., Bunkova E. Yu.* Elliptic formal group laws, integral Hirzebruch genera and Krichever genera. 2010. *arXiv: 1010.0944*.

3. *Колывагин В. А.* Символ норменного вычета в локальных полях // УМН. 1978. Т. 33, вып. 6(204). С. 217–218.

4. *Востоков С. В.* Явная форма закона взаимности // Изв. АН СССР. Сер. матем. 1978. Т. 42, вып. 6. С. 1288–1321.

Статья поступила в редколлегию 7 октября 2015 г.

Сведения об авторах

*Востокова Регина Петровна* — доцент; rvostokova@yandex.ru

*Питаль Петр Николаевич* — аспирант; pital.petya@yandex.ru

**ARITHMETIC OF HYPERBOLIC FORMAL MODULES**

*Regina P. Vostokova*[1], *Petr N. Pital'*[2]

[1] Baltic State Technical University,
ul. 1-ya Krasnoarmeyskaya, 1, St. Petersburg, 190005, Russian Federation; rvostokova@yandex.ru

[2] St. Petersburg State University, Universitetskaya nab., 7–9, St. Petersburg, 199034, Russian Federation; pital.petya@yandex.ru

The paper considers hyperbolic formal groups which come out from the elliptic curve theory from the point of view of the theory of formal modules. The first part of the paper considers characteristics of hyperbolic formal groups, certain formulas for the formal logarithm and exponent are given, and convergence is scrutinized. Part two gives us the definition for $p$-typical logarithm; isogeny, its height and kernel are found. Further on Artin—Hasse function and Vostokov function were constructed, both correctness and their main features were checked.

Using these constructions primary elements in this kind of formal modules can be easily built, which are useful for constructing the Shafarevich basis. As a natural way of evolution, pairing on the hyperbolic formal modules can be explored. To sum up, this is the very first step of deriving explicit formula for Hilbert pairing on these kind of formal modules. The research is to be continued in this particular direction. Refs 4.

*Keywords*: hyperbolic formal modules, formal modules, formal groups.

## References

1. Silverman J. H., “The Arithmetic of Elliptic Curves”, *Graduate Texts in Mathematics* **106** (Springer-Verlag, 2009).

2. Buchstaber V. M., Bunkova E. Yu., *Elliptic formal group laws, integral Hirzebruch genera and Krichever genera* (2010), *arXiv: 1010.0944*.

3. Kolyvagin V. A., “The norm residue symbol in local fields”, *Russian Mathematics Surveys* **33**, Issue 6(204), 239–240 (1978).

4. Vostokov S. V., “Explicit form of the law of reciprocity”, *Mathematics of the USSR-Izvestiya* **13**, Issue 3, 557–588 (1978).

**Для цитирования:** Востокова Р. П., Питаль П. Н. Арифметика гиперболических формальных модулей // Вестник Санкт-Петербургского университета. Серия 1. Математика. Механика. Астрономия. 2016. Т. 3 (61). Вып. 3. С. 384–392. DOI: 10.21638/11701/spbu01.2016.305

**For citation:** Vostokova R. P., Pital' P. N. Arithmetic of hyperbolic formal modules. *Vestnik of Saint Petersburg University. Series 1. Mathematics. Mechanics. Astronomy*, 2016, vol. 3 (61), issue 3, pp. 384–392. DOI: 10.21638/11701/spbu01.2016.305