Записки научных
семинаров ПОМИ
Том 502, 2021 г.

А. Л. Смирнов

О СЛОЖЕНИЯХ НА МУЛЬТИПЛИКАТИВНОМ МОНОИДЕ ЦЕЛЫХ ЧИСЕЛ

Введение

С каждым кольцом A связан моноид $A^\times$. Этот моноид состоит из всех элементов A, а операция умножения наследуется из A. Рассмотрим следующую задачу: перечислить все A, для которых существует изоморфизм моноидов

$$A^\times \simeq \mathbb{Z}^\times. \tag{1}$$

На первый взгляд эта задача выглядит довольно странно. Интерес к ней мотивирован ниже. Основная причина такого интереса кроется в теории обобщенных колец. Дополнительная причина интереса к таким кольцам связана с мотивными когомологиями (см. §1).

Оказалось, что удобно расширить задачу и вместо колец со свойством (1) классифицировать гауссовы кольца (см. 1.3).

Классификация факториальных колец выглядит недостижимой целью. Достаточно упомянуть двухсотлетнюю проблему Гаусса: доказать, что существует бесконечно много вещественных квадратичных полей с факториальным кольцом целых. Однако эта цель достигнута, хотя и весьма нетривиальным образом, для мнимых квадратичных полей. Заметим, что эти два случая отличаются друг от друга структурой группы единиц. Возможно, что задача классификации гауссовых колец могла бы оказаться более доступной.

Автор благодарит М. А. Цфасмана за ссылки на работы, в которых изучаются кривые, определенные над конечным полем и не имеющие рациональных точек.

§1. Мотивировки и примеры

В этом разделе обсуждаются причины интереса к рассматриваемой проблеме.

Ключевые слова: обобщенные кольца, тензорный квадрат, полиномы Вейля, Гаусс, десятый дискриминант.

Работа выполнена при поддержке РФФИ (грант 19-01-00513).

1.1. Связь с теорией обобщенных колец. Одна из проблем теории обобщенных колец (см. [1]) состоит в тривиальности тензорного квадрата $\mathbb{Z}$ над $\mathbb{F}_1$. Точнее говоря, естественная стрелка обобщенных колец

$$\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z} \to \mathbb{Z}.$$

является изоморфизмом. Можно рассмотреть некоммутативное тензорное произведение $\mathbb{Z} \boxtimes_{\mathbb{F}_1} \mathbb{Z}$, и оно, конечно, отличается от $\mathbb{Z}$. Более того, можно значительно приблизить некоммутативный тензорный квадрат $\mathbb{Z}$ к коммутативному, рассмотрев его фактор-кольцо

$$\mathbb{Z} \boxtimes_{\mathbb{Z}^\times} \mathbb{Z}.$$

Ниже увидим, что этот фактор также отличается от $\mathbb{Z}$.

Каждая пара колец A_1 и A_2 со свойством (1) позволяет построить интересный пример модуля над этим кольцом. Действительно, для $i = 1$ и $i = 2$ выберем изоморфизм моноидов $\sigma_i : \mathbb{Z}^\times \to A_i^\times$ и введем на множестве $\mathbb{Z}$ операцию

$$x +_i y = \sigma_i^{-1}(\sigma_i x + \sigma_i y).$$

Таким образом мы получаем модуль над $\mathbb{Z}\boxtimes_{\mathbb{Z}^\times}\mathbb{Z}$.

1.2. Связь с мотивами. Для гладкого многообразия X над произвольным полем определены мотивные когомологии $H^p(X, \mathbb{Z}(q))$. Индекс подкрутки q называется весом этой группы когомологий. Сложность мотивных когомологий быстро растет с весом. Однако при весе $q = 1$ все группы в некотором смысле известны. А именно (см. [2, Prop. 2.2]),

$$H^p(X, \mathbb{Z}(1)) = \begin{cases} \Gamma(X, \mathcal{O}_X^*), & p = 1; \\ \operatorname{Pic} X, & p = 2; \\ 0, & p \neq 1, 2. \end{cases}$$

Эти же две группы играют ключевую роль в теории алгебраических чисел. Именно их мы и ограничиваем в определении гауссова кольца (см. 1.3.1).

1.3. Гауссовы кольца. Оказалось, что удобно изменить задачу и вместо колец со свойством (1) классифицировать гауссовы кольца. В некотором отношении исходная задача сужается. Например, не все

кольца со свойством (1) конечнопорождены как $\mathbb{Z}$-алгебры. В частности, не является конечнопорожденной алгебра $\mathbb{Z}$-полиномов от счетного числа переменных. С другой стороны, мы расширяем задачу. Например, конечные поля не обладают свойством (1), а кольцо $\mathbb{F}_q[x]$ обладает свойством (1) только при $q = 3$.

1.3.1. Определение. *Коммутативное кольцо A назовем гауссовым, если*

(1) *A конечнопорожденная $\mathbb{Z}$-алгебра;*
(2) *A факториально;*
(3) *группа обратимых элементов A^* конечна.*

Отметим несколько свойств гауссовых колец.

1.3.2. Гауссово кольцо не имеет ненулевых делителей нуля, то есть является областью целостности. Это часть свойства факториальности. Поэтому можно говорить о характеристике гауссова кольца. А именно,

$$\operatorname{char} A = \operatorname{char} K, \text{ где } K \text{ поле частных } A.$$

1.3.3. Гауссово кольцо нетерово. Это свойство вытекает из первого условия гауссовости. Таким образом, при изучении гауссовых колец мы избегаем различных тонкостей, связанных с понятием факториальности (см. [3]). Факториальное кольцо по определению является областью целостности.

1.3.4. Гауссово кольцо нормально, то есть целозамкнуто в своем поле частных K. Это следует из факториальности A (см. [3, гл. VII, §1, теор. 2]).

1.3.5. Гауссово кольцо конечномерно, где размерность определена по Круллю. Это вытекает из конечнопорожденности A как $\mathbb{Z}$-алгебры. Более того (см. [4, Предл. 14]),

$$\dim A = \begin{cases} \operatorname{tr.deg}(K/\mathbb{Q}) + 1, & \text{если } \operatorname{char} K = 0; \\ \operatorname{tr.deg}(K/\mathbb{F}_p), & \text{если } \operatorname{char} K = p. \end{cases} \tag{2}$$

1.3.6. Предложение. *Пусть A гауссово кольцо. Если* $\dim A = 0$*, то* $A \simeq \mathbb{F}_q$.

Доказательство. Нулевой идеал прост в A, так как A область целостности. Пусть μ произвольный максимальный идеал A. В силу нульмерности цепочка $(0) \subset \mu$ вырождается. Поэтому (0) максимальный

идеал, то есть A поле. Из (2) вытекает, что расширение $A/\mathbb{F}_p$ алгебраично. Из конечнопорожденности A вытекает, что A конечное расширение $\mathbb{F}_p$. □

1.3.7. Предложение. *Пусть A гауссово кольцо характеристики 0. Если $\dim A = 1$, то A изоморфно кольцу целых в одном из полей $\mathbb{Q}$ или $\mathbb{Q}(\sqrt{-d})$ для $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$.*

Доказательство. По условию на характеристику $K \supset \mathbb{Q}$, где K – поле частных A. Из (2) вытекает, что расширение $K/\mathbb{Q}$ алгебраично. Из конечнопорожденности A вытекает, что K конечно над $\mathbb{Q}$. Из нормальности A вытекает, что A кольцо целых K. Из теоремы Дирихле о единицах и конечности A^* для гауссовых колец вытекает, что либо $K = \mathbb{Q}$, либо K – мнимое квадратичное поле. Таким образом, предложение вытекает из решения проблемы Гаусса о десятом дискриминанте (см. [5]). □

В мнимых квадратичных полях имеется три немаксимальных числовых порядка $R_f = fR + \mathbb{Z}$ с тривиальной группой Пикара. А именно, R_2 для $\mathbb{Q}[\sqrt{-1}], \mathbb{Q}[\sqrt{-3}]$ и R_3 для $\mathbb{Q}[\sqrt{-3}]$ (см. [6]). Однако эти кольца не факториальны, не будучи нормальными.

1.4. Серии гауссовых колец. Все инварианты интересующих нас в данной работе колец являются гомотопическими инвариантами.

1.4.1. Предложение. *Пусть A коммутативное кольцо. Тогда*

(1) *Конечнопорожденность $\mathbb{Z}$-алгебры A равносильна конечнопорожденности $\mathbb{Z}$-алгебры $A[x]$.*
(2) *Факториальность A равносильна факториальности $A[x]$.*
(3) *Если $\mathrm{Rad}(A) = 0$, то структурное вложение $A \subset A[x]$ индуцирует изоморфизм $A^* \simeq A[x]^*$. Кроме того, $\mathrm{Rad}(A) = 0$ тогда и только тогда, когда $\mathrm{Rad}(A[x]) = 0$.*

Доказательство. Первое утверждение очевидно. Второе утверждение доказано в [3, гл. VII, §5, теор. 2 и ниже]. Третье утверждение доказано в [7, гл. I, упр. 2]. □

Таким образом, гауссовы кольца встречаются бесконечными сериями: если A гауссово кольцо, то и кольца $A[x_1], A[x_1, x_2]$ и т.д. гауссовы. То же самое можно сказать и для колец со свойством (1).

1.4.2. Определение. *Кольцо A назовем несократимым, если не существует такого кольца A_0, что A изоморфно $A_0[x]$.*

Конечно, особенно интересны несократимые гауссовы кольца. Например, $\mathbb{F}_q$ и $\mathbb{Z}$ именно таковы.

С сериями колец связано одно интересное явление. Оно состоит в том, что кольца полиномов над неизоморфными кольцами могут быть изоморфны (см., например, [8]). Однако, в данной работе это явление не изучается.

1.5. Геометрические гауссовы кольца размерности 1. Предположим, что A гауссово кольцо характеристики p и $\mathbb{F}_q$ целое замыкание $\mathbb{F}_p$ в A. Предположим также, что

$$\dim A = 1.$$

1.5.1. Предложение. *Пусть $U = \operatorname{Spec} A$. Тогда существует единственная гладкая проективная кривая X над $\mathbb{F}_q$, содержащая U в качестве открытого подмножества.*

Доказательство. В размерности 1 нормальность равносильна регулярности. Поэтому U – гладкая кривая. Хорошо известно, что всякая гладкая кривая имеет единственную гладкую проективную модель. □

Таким образом, геометрическому гауссову кольцу размерности 1 соответствует следующий набор данных:

$$A \mapsto (p, q, X, U).$$

Здесь $p = \operatorname{char} A$, q – число элементов целого замыкания $\mathbb{F}_p$ в A, X – гладкая проективная кривая над $\mathbb{F}_q$, U – непустое открытое подмножество X. При этом

$$A \simeq \Gamma(U, \mathcal{O}_X).$$

Мы собираемся понять, какие же наборы получаются из гауссовых колец. Введем обозначения. Пусть g – род X,

$$J \text{ – якобиан } X,$$

$$N_r(X) \text{ – число рациональных точек } X \text{ над полем } \mathbb{F}_{q^r},$$

$$N_r(J) \text{ – число рациональных точек } J \text{ над полем } \mathbb{F}_{q^r}.$$

Ниже нам потребуется следующий факт.

1.5.2. Теорема. *Пусть X – гладкая проективная кривая над полем $\mathbb{F}_q$. Тогда стандартный гомоморфизм*

$$\deg : \operatorname{Pic} X \to \mathbb{Z}$$

является эпиморфизмом. Иными словами, степени всех замкнутых точек X в совокупности взаимно просты.

Доказательство. Пусть a и b два достаточно больших взаимно простых числа. Из оценки Вейля следует, что $N_a(X) > 0$ и $N_b(X) > 0$. Поэтому на X имеются точки степеней a_1 и b_1, где a_1 делит a, а b_1 делит b. Так как a и b взаимно просты, то a_1 и b_1 также взаимно просты. □

1.5.3. Предложение. *Кольцо A гауссово тогда, и только тогда, когда $U = X - P$, где P рациональная точка на X, а $N_1(J) = 1$.*

Доказательство. Предположим сначала, что кольцо A гауссово. Пусть $X - U = P_1 \cup \cdots \cup P_r$, где P_i – замкнутая точка X. Из конечности A^* и теоремы Дирихле о единицах вытекает, что $r \leqslant 1$. Из аффинности U вытекает, что $r > 0$. Поэтому $r = 1$ и $X - U = P$.

Проверим теперь, что $\deg P = 1$. Рассмотрим точную последовательность

$$\mathbb{Z} \xrightarrow{\delta} \mathrm{Cl}(X) \xrightarrow{j^*} \mathrm{Cl}(U) \to 0, \tag{3}$$

где j – вложение $U \subset X$, а $\delta(1) = [P]$ (см. [9, II, Предл. 6.5]). Из точности этой последовательности и факториальности A вытекает сюръективность δ. Кроме того, так как X– гладкая кривая, то имеется изоморфизм $\mathrm{Cl}(X) \to \mathrm{Pic}(X)$, при котором $P \mapsto [\mathcal{O}(P)]$ (см. [9, гл. II, §6, следствие 6.16]). Таким образом, получили диаграмму

$$\mathbb{Z} \xrightarrow{\delta} \mathrm{Pic}\, X \xrightarrow{\deg} \mathbb{Z}, \tag{4}$$

где обе стрелки эпиморфизмы (относительно deg см. 1.5.2), а их композиция переводит P в $\deg P$. Отсюда вытекает, что $\deg P = 1$.

Проверим теперь, что $N_1(J) = 1$. Хорошо известно, что

$$\mathrm{Pic}_0(X) = J(\mathbb{F}_q).$$

Таким образом, равенство $N_1(J) = 1$ равносильно тривиальности группы $\mathrm{Pic}_0(X)$. По определению, $\mathrm{Pic}_0(X)$ – ядро стрелки $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$. Однако, как мы видели выше, композиция стрелок $\deg \circ \delta$ из диаграммы (4) является эпиморфизмом $\mathbb{Z} \to \mathbb{Z}$. Но всякий такой эпиморфизм является и мономорфизмом. Поэтому δ мономорфизм и изоморфизм. Отсюда вытекает и мономорфность deg. Таким образом, одна из импликаций предложения проверена.

Предположим теперь, что $U = X - P$, где P – рациональная точка X, а $N_1(J) = 1$. Надо проверить, что A – гауссово кольцо. Иными словами, надо проверить, что группа A^* конечна и что A факториально. Конечность A^* вытекает из теоремы Дирихле. Осталось проверить тривиальность $\mathrm{Cl}(U)$ или сюръективность δ из (3). Для этого заметим, что стрелка deg из (4) изоморфизм. Это вытекает из точности последовательности

$$0 \to \mathrm{Pic}_0(X) \to \mathrm{Pic}\, X \xrightarrow{\deg} \mathbb{Z} \to 0 \tag{5}$$

и тривиальности $\mathrm{Pic}_0(X) = J(\mathbb{F}_q)$. Последовательность (5) точна по определению Pic_0 и по теореме 1.5.2.

Кроме того, $\deg \delta(1) = \deg P = 1$. Поэтому $\delta(1)$ образующая $\mathrm{Pic}(X) = \mathbb{Z}$ и δ эпиморфизм. □

1.5.4. Предложение. *Пусть $g = 0$. Тогда $X = \mathbf{P}^1$, $U = \mathbf{A}^1$.*

Доказательство. Хорошо известно, что над конечным полем каждая коника имет рациональную точку (см., например, [10]). □

1.5.5. Предложение. *Пусть $g > 0$. Кольцо A гауссово тогда, и только тогда, когда $N_1(X) = 1$, $N_1(J) = 1$ и $U = X - P$, где P единственная рациональная точка на X.*

Доказательство. Ввиду предложения 1.5.3 достаточно доказать, что $N_1(X) = 1$. Для $g > 0$ отображение $X \to J$, $Q \mapsto [Q] - [P]$ – вложение. Поэтому $N_1(X) \leqslant N_1(J)$. □

§2. Гауссовы кривые

Мы пришли к задаче перечисления таких кривых X над $\mathbb{F}_q$, что

$$N_1(X) = 1, \quad N_1(J) = 1. \tag{6}$$

Будем называть такие кривые гауссовыми.

Мы собираемся искать гауссовы кривые с малыми q и g.

2.1. Полиномы Гаусса–Вейля. С каждой кривой X над конечным полем связан полином f_X, а именно характеристический полином оператора Фробениуса φ на $H^1(X)$, где H^* когомологии Вейля. Более традиционно сопоставлять X слегка другой полином, а именно

$$P_X(t) = \det(1 - \varphi t).$$

Таким образом, $P_X(t) = t^{2g} f_X(1/t)$. Тогда $\deg P = 2g$ и

$$P_X = 1 - s_1 t + \cdots - s_{2g-1} t^{2g-1} + s_{2g} t^{2g}, \tag{7}$$

где s_i – элементарная симметрическая функция собственных чисел оператора φ. Известно, что $s_i \in \mathbb{Z}$.

2.1.1. Определение. *Пусть $P(t)$ целочисленный полином, а q – степень простого числа. Назовем P полиномом Вейля для q, если*

(1) $\deg P$ *– четное число (обозначим его $2g$);*
(2) $P(0) = 1$*;*
(3) *верно функциональное уравнение $P(1/qt) = P(t)$;*
(4) *если $1/\lambda$ комплексный корень P, то $|\lambda| = \sqrt{q}$.*

Известно, что P_X – полином Вейля. В частности, из функционального уравнения вытекает, что

$$s_{2g} = q^g s_0, \;\; s_{2g-1} = q^{g-1} s_1, \;\; \ldots, \;\; s_{g+1} = q s_{g-1}. \tag{8}$$

Известное соотношение $H^*(J) = \Lambda^* H^1(X)$ показывает, что

$$s_i \text{ – след оператора Фробениуса на } H^i(J). \tag{9}$$

Кроме того, по теореме Лефшеца

$$N_1(X) = 1 - s_1 + q$$

и

$$N_1(J) = P(1).$$

Поэтому условия (6) из определения гауссовых кривых равносильны условиям

$$s_1 = q \tag{10}$$

и

$$P(1) = 1. \tag{11}$$

2.1.2. Определение. *Пусть $P(t)$ целочисленный полином, а q – степень простого числа. Назовем P полиномом Гаусса–Вейля для q, если*

(1) P *– полином Вейля для q;*
(2) $P(1) = 1$*;*
(3) $s_1 = q$*.*

Для полинома Вейля

$$|s_i| \leqslant \binom{2g}{i} q^{i/2}. \tag{12}$$

2.1.3. Предложение. *Пусть P – полином Гаусса–Вейля над полем $\mathbb{F}_q$. Тогда*

$$q \leqslant (\deg P)^2.$$

Доказательство. В самом деле, $s_1 \leqslant 2g\sqrt{q}$ в силу вейлевости P. С учетом (10) получаем отсюда, что $q \leqslant 2g\sqrt{q}$. □

Заметим, что бывают полиномы Гаусса–Вейля, не соответствующие никакой кривой. Пример такого полинома встретится ниже (см. 2.4) при описании полиномов Гаусса–Вейля для $g = 3$.

Приведем некоторые необходимые критерии представимости полинома кривой. С кривой X наряду с коэффициентами $s_0 = 1, s_1, \ldots$ связан набор моментов $p_0 = 1$, p_1, …, где

$$p_1 = \sum \lambda_i, \quad p_2 = \sum \lambda_i^2, \ldots$$

Моменты и элементарные симметрические функции связаны между собой известными формулами Ньютона.

2.1.4. Предложение. *Пусть P_X – полином, соответствующий гауссовой кривой $X/\mathbb{F}_q$. Тогда*

$$s_2 \geqslant 0.$$

Доказательство. В самом деле, $N_2(X) \geqslant 1$, так как $N_2(X) \geqslant N_1(X)$. С другой стороны, по формуле Лефшеца $N_2 = 1 - p_2 + q^2 = 1 - (p_1 s_1 - 2s_2) + q^2 = 1 + 2s_2$. □

2.1.5. Предложение. *Пусть P_X – полином, соответствующий гауссовой кривой $X/\mathbb{F}_q$. Тогда*

$$s_3 \leqslant q s_2.$$

Доказательство. В самом деле, $N_3(X) \geqslant 1$, так как $N_3(X) \geqslant N_1(X)$. С другой стороны, по формуле Лефшеца

$$\begin{aligned} N_3 &= 1 - p_3 + q^3 = 1 - (p_2 s_1 - p_1 s_2 + 3s_3) + q^3 = 1 + 2s_2 \\ &= 1 - (q^2 - 2s_2)q + q s_2 - 3s_3 + q^3 = 1 + 3q s_2 - 3s_3. \end{aligned}$$ □

2.2. Гауссовы кривые рода 1. Имеется в точности три такие кривые $X/\mathbb{F}_q$. А именно,

$$X/\mathbb{F}_2 : y^2 + y = x^3 + x + 1,$$
$$X/\mathbb{F}_3 : y^2 = x^3 - x - 1,$$

$$X/\mathbb{F}_4 : y^2 + y = x^3 + \alpha \quad (\alpha^2 = \alpha + 1).$$

Неравенство $q \leqslant 4$ (см. 2.1.3) сводит вопрос к небольшому перебору. Такой перебор удобно производить с помощью явных форм эллиптических кривых и их эндоморфизмов в произвольной характеристике (см. [11]).

2.3. Гауссовы кривые рода 2. Покажем, что таких кривых нет. В самом деле, пусть $X/\mathbb{F}_q$ гауссова кривая и $g = 2$. Из 2.1.3 вытекает, что $q \leqslant 16$. Несложно перебрать все такие кривые, пользуясь тем, что все кривые рода 2 гиперэллиптичны. Попробуем, однако, сделать рассуждение менее зависимым от компьютера. Пусть P_X – полином гауссовой кривой X рода 2 (см. 2.1). С учетом (10) и (11) видим, что

$$P_X = 1 - qt + qt^2 - q^2t^3 + q^2t^4.$$

2.3.1. $q \geqslant 3$. Пусть $L(s) = P_X(q^{-s})$. Заметим, что $L(1/2) = 3 - 2\sqrt{q} < 0$ при $q \geqslant 9/4$. Таким образом, у $L(s)$ есть вещественный ноль между 0 и $1/2$. Но гипотеза Римана в нашей ситуации верна и никаких зигелевых нулей у $L(s)$ нет. Поэтому P_X не может быть полиномом Вейля при $q \geqslant 9/4$.

2.3.2. $q = 2$. В этом случае $P_X = 1 - 2t + 2t^2 - 4t^3 + 4t^4$ полином Гаусса–Вейля. Тем не менее, он не соответствует никакой кривой. Чтобы убедиться в этом, достаточно перебрать все кривые $X/\mathbb{F}_2$, заданные уравнением

$$y^2 + a_1x^2y + a_3xy = x^5 + a_2x^4 + a_4x^3 + a_6x^2 + a_8x + a_{10}.$$

Кривая X заведомо имеет такой вид. Это можно увидеть с помощью теоремы Римана–Роха, применяя ее к дивизорам вида nP, где P – рациональная точка на X. Вычисления показали, что всегда $N_1(X) \geqslant 2$.

2.4. Гауссовы кривые рода 3. Утверждается, что таких кривых нет. Предположим, что $X/\mathbb{F}_q$ такова. Пусть

$$P_X = 1 - qt + s_2t^2 - s_3t^3 + s_2qt^4 - q^3t^5 + q^3t^6$$

полином, связанный с X (см. 2.1). При этом s_3 определено s_2 и условием $P_X(1) = 1$. Кроме того, $q \leqslant 36$ (см. (2.1.3)), $0 \leqslant s_2 \leqslant 15q$ (см. (12) и 2.1.4). Все такие полиномы можно перебрать. Полиномов Гаусса–Вейля среди них нет.

2.5. Гауссовы кривые рода 4. Утверждается, что таких кривых нет. Предположим, что $X/\mathbb{F}_q$ такова. Пусть

$$P_X = 1 - qt + s_2t^2 - s_3t^3 + s_4t^4 - qs_3t^5 + q^2s_2t^6 - q^4t^7 + q^4t^8.$$

полином, связанный с X (см. 2.1). Заметим, что s_4 определено s_2, s_3 и условием $P_X(1) = 1$. Из 2.1.3 вытекает, что $q \leqslant 64$. Кроме того, $0 \leqslant s_2 \leqslant 28q$, $|s_3| \leqslant 56q^{3/2}$ (см. (12)). Все полиномы с такими ограничениями можно перебрать. Полиномов Гаусса–Вейля среди них нет.

2.5.1. При поиске полиномов Гаусса–Вейля был обнаружен полином с интересными свойствами. Это полином

$$f = x^8 - qx^7 + qx^4 - q^4x + q^4.$$

Он почти является полиномом Гаусса–Вейля для каждого $q \leqslant 64$. Оказалось, что для каждого такого q это единственный полином с указанными выше ограничениями на коэффициенты, все корни которого, кроме двух, вейлевские. При этом два вещественных корня $\lambda_0(q)$ и $\lambda_1(q)$ с ростом q быстро приближаются к 0 и 1. Например, $\lambda_1(q) \approx 1 + q^{-4}$. Это напоминает зигелевские нули L-рядов (см. [12]).

§3. Заключение

В работе изучаются кривые с условиями $N_1(X) = 1$ и $N_1(J) = 1$. При этом условие $N_1(J) = 1$ экстремально жесткое, так как на абелевом многообразии всегда есть рациональные точки. Однако условие $N_1(X) = 1$ можно ужесточить и потребовать, чтобы $N_1(X) = 0$. Такие бесточечные кривые изучались несколькими авторами [13]. По-видимому, общая тенденция состоит в том, что таких кривых бесконечно много. Конечно, добавление условия $N_1(J) = 1$ сужает число возможностей. Но насколько сильно? Верно ли, что число таких кривых конечно? Более общо, конечно ли множество кривых с фиксированными значениями $N_1(X)$ и $N_1(J)$. Не меньший интерес вызывает и изучение гауссовых колец в размерности 2 и выше.

Отметим, что компактификацию поверхности $\operatorname{Spec}\mathbb{Z} \times \operatorname{Spec}\mathbb{Z}$ можно было бы попробовать использовать для имитации в арифметическом случае рассуждений Маттука–Тейта (см. [14]). Однако в теории обобщенных колец Дурова эта ожидаемая поверхность выродилась в кривую. Числовые гауссовы кольца служат мерой нетривиальности некоммутативного произведения. С этой точки зрения можно попробовать взглянуть на знаменитую работу Дейринга [15]. В этой работе

Дейринг вывел гипотезу Римана из предположения, что имеется бесконечно много числовых гауссовых колец. Это предположение не верно. Нельзя ли интерпретировать подобные рассуждения следующим образом: если кольцо $\mathbb{Z} \boxtimes_{\mathbb{Z}^\times} \mathbb{Z}$ достаточно сложное, то верна гипотеза Римана?

Литература

1. *N. Durov*, New Approach to Arakelov Geometry. `arXiv: 0704.2030 v1 [math AG] 16 Apr 2007.`
2. *A. Suslin, V. Voevodsky*, *Bloch–Kato conjecture and motivic cohomology with finite coefficients, The arithmetic and geometry of algebraic cycles*, Kluwer Acad. Publ., Dordrecht, Vol. 548, p.117–189 (2000).
3. *Н. Бурбаки*, *Коммутативная алгебра*, Москва, Мир, 1971.
4. *Ж.-П. Серр*, *Локальная алгебра и теория кратностей*, Математика, 1963, том 7, вып. 5, 3–94.
5. *H.M. Stark*, *On the gap in the theorem of Heegner.* — J. Number Theory, **1**, 16–27.
6. *Ж.-П. Серр*, *Комплексное умножение.* – В кн.: Алгебраическая теория чисел, под редакцией Дж. Касселса и А. Фрёлиха, Москва, Мир, 1969.
7. *М. Атья, И. Макдональд*, *Введение в коммутативную алгебру*, Москва, Мир, 1972.
8. *M. Hochster*, *Nonuniqueness of coefficient rings in a polynomial ring.* — Proc. AMS, **34**, No 1, 81–82 (1972).
9. *Р. Хартсхорн*, *Алгебраическая геометрия*, Мир, Москва, 1981.
10. *Ж.-П. Серр*, *Курс арифметики*, Мир, Москва, 1972.
11. *J. Tate*, *The Arithmetic of Elliptic Curves.* — Invent. Math., **23**, 179–206 (1974).
12. *D. Goldfeld*, *Gauss' class number problem for imaginary quadratic fields.* — Bull. Amer. Math. Soc., **13**, 23–37 (1985).
13. *E. W. Howe, K.E. Lauter, J. Top*, *Pointless curves of genus three and four.* `arXiv:math/0403178v1 [math.NT] 10 Mar 2004`.
14. *A. Mattuck, J. Tate*, *On the Inequality of Castelnuovo–Severi.* — Hamb. Abh., **22**, 295–299 (1958).
15. *M. Deuring*, *Imaginary quadratische Zahlkorper mit der Klassenzahl 1.* — Math. Z. **37**, 405–415 (1933).

Smirnov A. L. On additions on the multiplicative monoid of integers.

We study modules over a certain generalized ring. This ring is a noncommutative tensor square of the ring of integers. The modules in the question are related to some interesting arithmetic problems. In particular they are

related to solved Gauss' class number problem for imaginary quadratic fields.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
E-mail: smirnov@pdmi.ras.ru

Поступило 14 сентября 2021 г.