ПРЕПРИНТЫ ПОМИ РАН

ГЛАВНЫЙ РЕДАКТОР

С.В. Кисляков

РЕДКОЛЛЕГИЯ

В.М.Бабич, Н.А.Вавилов, А.М.Вершик, М.А.Всемирнов, А.И.Генералов, И.А.Ибрагимов, Л.Ю.Колотилина, Б.Б.Лурье, Ю.В.Матиясевич, Н.Ю.Нецветаев, С.И.Репин, Г.А.Серегин

Учредитель: Федеральное государственное бюджетное учреждение науки
Санкт-Петербургское отделение Математического института
им. В. А. Стеклова Российской академии наук

Свидетельство о регистрации средства массовой информации: ЭЛ №ФС 77-33560 от 16 октября 2008 г. Выдано Федеральной службой по надзору в сфере связи и массовых коммуникаций

Контактные данные: 191023, г. Санкт-Петербург, наб. реки Фонтанки, дом 27

телефоны:(812)312-40-58; (812) 571-57-54

e-mail: admin@pdmi.ras.ru

http://www. pdmi.ras.ru /preprint/

Заведующая информационно-издательским сектором Симонова В.Н

ПРЕПРИНТ ПОМИ – 11/2016

Неклассические бирациональные модели $\operatorname{Spec}\mathbb{Q}$

А. Л. Смирнов

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
smirnov@pdmi.ras.ru

Декабрь, 2016

Аннотация

В работе изучаются такие обобщенные подкольца кольца целых чисел, спектр которых является бирациональной моделью поля рациональных чисел. Доказано однородное усиление теоремы Евдокимова. Предложен подход к вычислению гомотопических групп с помощью обобщенных подколец кольца целых.

Ключевые слова и фразы: обобщенное кольцо, обобщенная схема, арифметическая кривая, особенность, касп, нодальная точка, бирациональный, модель, поле из одного элемента, гомотопическая группа.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант RFFI-16-01-00750).

ПРЕПРИНТЫ
Санкт-Петербургского отделения
Математического института им. В. А. Стеклова
Российской академии наук

PREPRINTS
of the St. Petersburg Department of Steklov Institute of Mathematics

---

ГЛАВНЫЙ РЕДАКТОР

С. В. Кисляков

РЕДКОЛЛЕГИЯ

В. М. Бабич, Н. А. Вавилов, А. М. Вершик, М. А. Всемирнов,
А. И. Генералов, И. А. Ибрагимов, Л. Ю. Колотилина,
В. Н. Кублановская, Г. В. Кузьмина, Б. Б. Лурье,
Ю. В. Матиясевич, Н. Ю. Нецветаев, С. И. Репин, Г. А. Серегин,
В. Н. Судаков, О. М. Фоменко

Введение

Данная работа связана с программой геометризации арифметики, где в качестве образца рассматривается алгебраическая геометрия над конечным полем. В настоящее время имеется по меньшей мере два систематических подхода к построению арифметической геометрии: подход Ш. Харана [1] и подход Н. Дурова [2]. Видимо, ни один из существующих подходов не отвечает всем пожеланиям. Тем не менее в каждой из теорий появились обобщенные кольца и схемы, изучение которых интересно как само по себе, так и для прояснения общей ситуации. Данная работа связана с подходом Дурова.

Рассмотрим сначала геометрический аналог интересующих нас арифметических проблем. Пусть X – алгебраическая кривая над некоторым полем F и $K = F(X)$ – поле рациональных функций на X. Нас интересуют бирациональные модели поля K, то есть алгебраические кривые V/F с фиксированным изоморфизмом $F(V) = K$. Ситуация с такими моделями достаточно ясна. А именно, среди моделей K имеется одна особенно приятная – полная и гладкая. Все другие модели могут быть получены из полной и гладкой с помощью вырезания и стягивания конечных подсхем (см., например, [3]).

Процедура вырезания полностью применима и в чисто арифметическом случае, то есть для спектров колец целых в числовых полях. Что касается процедуры стягивания, то ее применимость весьма ограничена. А именно, можно стягивать только равнохарактеристические подсхемы, да и то не все. При этом будут получаться спектры немаксимальных порядков числовых полей. Но нельзя, например, создать касп у $\operatorname{Spec}\mathbb{Z}$ или склеить точки разных характеристик.

Ситуация со стягиванием изменилась после введения обобщенных колец и схем. Примеры возникающих при этом обобщенных колец указаны в [4] и названы конгруэнц-кольцами. В данной работе мы продолжаем изучение обобщенных бирациональных моделей числовых полей. В §1 приведены сведения об обобщенных кольцах. В частности, введено понятие конгруэнц-подкольца и сформулирована теорема Евдокимова. Основные результаты работы являются усилением этой теоремы и приведены в §2. А именно, теоремы 2.2.2 и 2.2.3. Эти теоремы в последующих работах планируется применить для классификации бирациональных моделей $\mathbb{Q}$. В §3 приведено несколько нерешенных задач. Предложен подход к вычислению гомотопических групп с помощью обобщенных подколец $\mathbb{Z}$.

Данная работа частично выполнена во время пребывания автора в Математическом Институте Макса Планка в Бонне в 2016 году. Автор благодарит Институт и его сотрудников за гостеприимство.

1 Конгруэнц-подкольца

Обычно ниже мы используем термин "кольцо" вместо термина "обобщенное кольцо" [2]. Как обычно, $R(n)$ – множество n-арных операций R. При этом $R(n) = R^n$ для классического кольца R. Все кольца предполагаются коммутативными.

1.1 Классический случай

Здесь приведены некоторые сведения о классических особенностях. Они предназначены служить образцом при изучении обобщенного случая. Особенности алгебраических кривых достаточно подробно рассмотрены в [3].

1.1.1. Стягивание подсхем в классическом случае. Опишем некоторый способ стягивания классических подсхем. Этот способ ниже будет применен к обобщенному случаю. Ограничимся аффинными схемами. Пусть $U = \operatorname{Spec} A$, I – идеал в A и $Z = \operatorname{Spec} A/I$ – замкнутая подсхема U. Предположим, что задано подкольцо $E \subset A/I$ и $W = \operatorname{Spec} E$. Рассмотрим диаграмму схем

$$\begin{tikzcd} Z \arrow[r, hook, "j"] \arrow[d, "p"'] & U \arrow[d, dashed] \\ W \arrow[r, dashed] & V \end{tikzcd} .$$

Здесь j – замкнутое вложение, соответствующее проекции $A \to A/I$, а p – проекция, соответствующая вложению $E \subset A/I$. Схема W рассматривается как результат факторизации схемы Z, а V рассматривается как результат стягивания схемы U вдоль p. В качестве V возьмем копредел части этой диаграммы, состоящей из стрелок j и p. Существование такого копредела легко увидеть из существования предела в двойственной категории колец.

$$\begin{tikzcd} A/I & A \arrow[l, "q"'] \\ E \arrow[u, hook, "i"] & A_{q,i} \arrow[l, dashed] \arrow[u, dashed] \end{tikzcd} .$$

Здесь $A_{q,i}$ – просто прообраз $q^{-1}(iE) \subset A$.

Если мы рассматриваем не просто схемы, а схемы над некоторым кольцом F, то все данные должны быть определены над F. Тогда и $A_{q,i}$ наследует структуру F-алгебры.

1.1.2. Пример. Пусть $A = \mathbb{R}[x]$, $I = ((1+x)(1-x))$, $E = \mathbb{R}$. В этом случае

$$A_{q,i} = \{f \in \mathbb{R}[x] | f(1) = f(-1)\} = \mathbb{R}[u,v]/(u^2 - v^2 + u^3).$$

Здесь $u = x^2 - 1$, $v = x - x^3$. Таким образом, точки $x = 1$ и $x = -1$ стягиваются в простую двойную точку $(u = 0, v = 0)$ с касательным конусом из двух прямых.

1.1.3. Пример. Пусть $A = \mathbb{R}[x]$, $I = (x^2)$, $E = \mathbb{R}$. В этом случае

$$A_{q,i} = \{f \in \mathbb{R}[x] | f'(0) = 0\} = \mathbb{R}[u,v]/(v^2 - u^3).$$

Здесь $u = x^2$, $v = x^3$. Таким образом, подсхема $\mathbf{A}^1$, заданная уравнением $x^2 = 0$, стягивается в касп $(u = 0, v = 0)$ с неприведенным касательным конусом.

1.1.4. Пример. Пусть $A = \mathbb{R}[x,y]/(xy - 1)$, $I = (x^2 + 1)$, $E = \mathbb{R}$. В этом случае

$$A_{q,i} = \{f \in \mathbb{R}[x, x^{-1}] | f(i) \in \mathbb{R}\} = \mathbb{R}[u,v,w]/(uv - 1, 2 + u + v - w^2) =$$

$$= \mathbb{R}[s,t,w]/(s+t-st, s+t-w^2) = \mathbb{R}[t,w]/(t^2+w^2-tw^2).$$

Здесь $u = x^2$, $v = y^2$, $w = x+y$, $s = u+1$, $t = v+1$. Таким образом, схемная точка степени 2, состоящая из двух геометрических точек $x = i$ и $x = -i$, переходит при стягивании в простую двойную точку $(t = 0, w = 0)$ с неращепимым над базовым полем $\mathbb{R}$ касательным конусом.

1.1.5. Особенности кривых. В 1.1.1 представлена процедура создания особенностей. Отметим и кратко обсудим несколько вопросов, которые возникают при изучении особых кривых. В классике эти вопросы обычно не вызывают серьезных затруднений, но в обобщенном случае мы оказываемся в зоне неизвестности и каждый шаг может привести к значительным трудностям.

1. Естественным образом особые кривые возникают при изучении кривых вложенных, например, в $\mathbf{A}^2$. Желательно уметь переходить от описания искусственно созданной особенности к естественно возникшей особенности и наоборот.

2. Желательно иметь набор численных инвариантов локальной особенности, таких, например, как кратность и кондуктор (см. [3, Ch. IV, §2]). А именно, $\delta_Q = \dim_k \mathcal{O}_Q/\mathcal{O}'_Q$ и $n_Q = \dim_k \operatorname{Ann}(\mathcal{O}_Q/\mathcal{O}'_Q)$. Здесь $\mathcal{O}'_Q$ – кольцо функций локальной особенности, $\mathcal{O}'_Q$-Mod – категория $\mathcal{O}'_Q$-модулей, а $\mathcal{O}_Q$ – кольцо функций ростка кривой, полученного разрешением локальной особенности.

3. Среди бирациональных моделей K имеется одна особенно приятная, а именно – полная и гладкая. Будем считать, что именно такова кривая X. Все модели V поля K могут быть получены с помощью "домиков" вида

$$\begin{tikzcd} U \arrow[r, hook, "i"] \arrow[d, "p"'] & X \\ V & \end{tikzcd},$$

где i – открытое вложение, а p – конечный морфизм степени один. Альтернативно, все модели V поля K могут быть получены с помощью "домиков" вида

$$\begin{tikzcd} & X \arrow[d, "q"] \\ V \arrow[r, hook, "j"'] & Y \end{tikzcd},$$

где j – открытое вложение, а q – конечный морфизм степени один.

4. Помимо процедуры создания особенностей имеется и процедура рарешения особенностей. В случае кривых имеются даже две такие процедуры: нормализация и более конструктивная процедура раздутия.

1.2 Обобщенный случай

Понятие обобщенного конгруэнц-кольца введено в [4]. Ниже мы слегка обобщим его по аналогии с классическим случаем (см. 1.1.1).

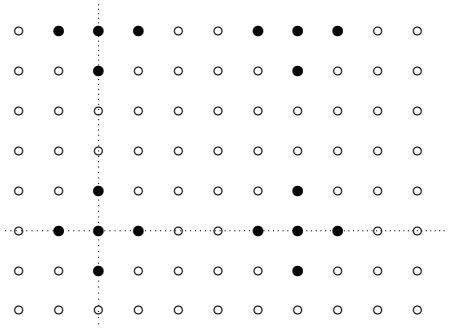
1.2.1 Определение. *Рассмотрим классическое кольцо A, идеал $I \subset A$ и обобщенное подкольцо $E \subset A/I$. Конгруэнц-кольцо $A_{q,i}$, по определению, – предел диаграммы*

$$\begin{tikzcd} A/I & A \arrow[l, "q"'] \\ E \arrow[u, hook, "i"] & A_{q,i} \arrow[l, dashed] \arrow[u, dashed] \end{tikzcd},$$

где q – проекция, а i – вложение. Иными словами, $A_{q,i}$ – прообраз $q^{-1}(iE) \subset A$.

Если мы рассматриваем не просто кольца, а алгебры над некоторым кольцом L, то и $A_{q,i}$ наследует структуру L-алгебры.

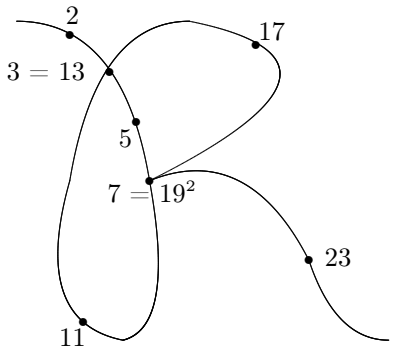
1.2.2. Пример. Пусть $A = \mathbb{Z}$, $I = (5)$, $E = \mathrm{F}$. Среди бинарных операций $\mathbb{Z}$, т. е. $\mathbb{Z}(2) = \mathbb{Z}^2$, на картинке



элементы $A_{q,i}(2)$ закрашены черным цветом.

2 Неклассические бирациональные модели

Мы собираемся изучать неклассические бирациональные модели полей алгебраических чисел. Среди таких моделей имеются, например, сингулярные модели для $\operatorname{Spec}\mathbb{Z}$. Один из примеров такой модели представлен рисунком



Здесь склееены простые 3 и 13, а также имеется касп в простом числе 19. Более того, этот касп склеен с простым числом 7. В классической теории нет ничего подобного, так как все классические схемы "живут" над $\operatorname{Spec}\mathbb{Z}$. Изображенная же на картинке обобщенная схема "живет" ниже $\operatorname{Spec}\mathbb{Z}$.

Положим

$$\mathrm{F} = \mathbb{F}_{1^2}. \tag{1}$$

Здесь $\mathbb{F}_{1^2}(n)$ состоит из всех $a = (a_1, \ldots, a_n)$, где $a_i \in \{-1, 0, +1\}$ и почти все $a_i = 0$, самое большее с одним исключением. Иными словами, для каждого a должен найтись индекс j такой, что $a_i = 0$ при $i \neq j$.

Мы рассматриваем любое классическое кольцо A как F-алгебру с помощью гомоморфизма, переводящего (-1) в (-1).

2.1 Сингулярные модели $\operatorname{Spec}\mathbb{Z}$

Сначала напомним понятие конечности в обобщенном контексте.

2.1.1 Определение. *Пусть $\rho : A \to B$ – морфизм обобщенных колец. Кольцо B называется конечным над A, если функтор ограничения скаляров $\rho_* : B\text{-Mod} \to A\text{-Mod}$ переводит конечнопорожденные модули в конечнопорожденные.*

Некоторые общие свойства конечных алгебр обсуждаются в [4, 2.1].

Будем говорить, что $\operatorname{Spec} R$ – конечный фактор $\operatorname{Spec}\mathbb{Z}$, если $R \subset \mathbb{Z}$ и $\mathbb{Z}$ конечно над R. Будем говорить, что $\operatorname{Spec} R$ представляет сингулярную модель $\operatorname{Spec}\mathbb{Z}$, если $\operatorname{Spec} R$ – конечный фактор $\operatorname{Spec}\mathbb{Z}$ и локализация R по всем ненулевым элементам $R(1)$ совпадает с $\mathbb{Q}$.

Следующая теорема описывает строение конечных факторов $\operatorname{Spec}\mathbb{Z}$, определенных над $\mathrm{F} = \mathbb{F}_{1^2} \subset \mathbb{Q}$ (например, $\operatorname{Spec}\mathbb{N}$ не такой).

2.1.2 Теорема. *Предположим, что $\mathrm{F} \subset R \subset \mathbb{Z}$. Тогда*

1. *Если $\operatorname{Spec} R$ – конечный фактор $\operatorname{Spec}\mathbb{Z}$, то $\operatorname{Spec} R$ – сингулярная модель $\operatorname{Spec}\mathbb{Z}$;*
2. *$\operatorname{Spec} R$ – сингулярная модель $\operatorname{Spec}\mathbb{Z}$ тогда и только тогда, когда $R \supset R_N$ (см. [4]) для некоторого N.*

Это утверждение было сформулировано в [4] в качестве гипотезы. Эта гипотеза была сведена с помощью приема Н. Дурова к утверждению теоремы 2.1.3. Таким образом, весьма существенную роль в доказательстве теоремы 2.1.2 играет следующая теорема С. Евдокимова.

2.1.3 Теорема ([5])**.** *Пусть W – некоторая F-подалгебра $\mathbb{Z}$, $(a, b) \in W(2)$ и $\gcd(a, b) = 1$. Тогда $(1, N) \in W(2)$, где $N = ab$.*

2.2 Однородные представления

Для классификации бирациональных моделей $\operatorname{Spec}\mathbb{Q}$, которую мы планируем провести в последующих работах, потребуется однородное усиление теоремы Евдокимова.

2.2.1. Однородные комбинации степени d. Пусть $(x, y) \mapsto x * y$ – свободная бинарная коммутативная операция. Имеется естественный гомоморфизм

$$\mathrm{F}[*] \to \mathbb{Q}[A, B], \quad * \mapsto (A, B).$$

Положим $\deg(*) = 1$, $\deg A = \deg B = 1$. Тогда вышеуказанный гомоморфизм становится гомоморфизмом градуированных колец.

Пусть $a, b \in \mathbb{Q}$. Говорим, что существует однородное представление $c \in \mathbb{Q}$ степени d с помощью бинарной операции $(a, b) \in \mathbb{Q}(2)$, если для некоторого n существует операция $f \in \mathrm{F}[*]_d(n)$, так что $c = f(x_1, \dots, x_n)$, где $x_i \in \mathrm{F}(1)$. Множество всех таких c обозначим X_d.

Иными словами, X_d состоит из целых чисел, представимых полным бинарным деревом высоты d, на листьях которого расположены элементы $\mathrm{F}(1)$. Для вычисления числа, представленного таким деревом, идем от листьев к корню и ко входам x, y вершины применяем операцию $ax + by$, а ее результат подаем на выход из вершины.

Приведем рекурсивное описание X_d. Для этого рекурсивно определим множества $X_0, X_1, \dots \subset \mathbb{Z}$. Положим

$$X_0 = \mathrm{F}(1) = \{-1, 0, +1\}.$$

Для $d = 1, 2, \dots$, по определению,

$$X_d = \{au + bv \in \mathbb{Z}(1) | u, v \in X_{d-1}\}.$$

Легко видеть, что X_d инвариантно относительно умножения на (-1).

Нам потребуется также понятие однородной представимости бинарной операции. Говорим, что существует однородное представление $(c_1, c_2) \in \mathbb{Q}(2)$ степени d с помощью бинарной операции $(a, b) \in \mathbb{Q}(2)$, если для некоторого n существует операция $f \in \mathrm{F}[*]_d(n)$, так что $c = f(x_1, \dots, x_n)$, где $x_i \in \mathrm{F}(2)$.

Зафиксируем $a, b \in \mathbb{Z}$. Ниже будем предполагать, что

$$\gcd(a, b) = 1. \tag{2}$$

Пусть

$$N = ab. \tag{3}$$

Следующая теорема – основной качественный результат данной работы.

2.2.2 Теорема. *Существует $d > 0$ такое, что $1 \in X_d$.*

Теорема 2.2.2 будет выведена ниже из теоремы 2.2.3. Доказательство этой теремы, наряду с леммой 2.2.5, представляют собой конструктивную версию теоремы 2.2.2.

2.2.3 Теорема. *Предположим, что для $d \in \{1, 2, \dots\}$ выполнены условия*

$$a^d + b^d \equiv 1 \ (mod\ N), \tag{4}$$

$$d \text{ – четно}, \tag{5}$$

$$d \geq N. \tag{6}$$

Тогда $1 \in X_d$.

2.2.4. Доказательство теоремы 2.2.2. Выберем и зафиксируем $e > 0$ и $f > 0$, такие, что $a^e \equiv 1 \pmod b$ and $b^f \equiv 1 \pmod a$. Для всякого кратного e и f выполнено (4). Среди таких кратных много чисел, для которых выполнены (5) и (6). На этом вывод теоремы 2.2.2 из теоремы 2.2.3 завершен.

Ключевой шаг в доказательстве теоремы 2.2.3 – ее частный случай, сформулированный и доказанный в следующей лемме.

2.2.5 Лемма. *Предположим, что для $d \in \{1, 2, \dots\}$ выполнены условия (4), (5) и (6) теоремы 2.2.3 и, кроме того,*

$$|a| \le 2|b| \text{ и } |b| \le 2|a|. \tag{7}$$

Тогда $1 \in X_d$.

Доказательство. В описании X_d (см. 2.2.1) можно заменить (a) на $(-a)$ (и аналогично для b). Поэтому без потери общности считаем, что $a \ge 0$ и $b \ge 0$. Кроме того, из (2) и (7) вытекает, что ни a, ни b не равны 0. Итак, ниже

$$a > 0, \qquad b > 0. \tag{8}$$

Нам потребуется слегка более точная нижняя оценка на a и b. А именно, если $a = 1$ или $b = 1$, то лемма очевидна. Поэтому без потери общности считаем, что

$$\min(a, b) \ge 2, \quad \max(a, b) \ge 3, \quad N \ge 6. \tag{9}$$

Рекурсивно определим последовательность целых $q_0, q_1, \dots, q_{d/2}$ (в обозначении уже использована четность d – см. (5)). А именно, пусть

$$q_0 = 1.$$

Предположим, что $0 \le i < d/2$ и q_i уже определено. Выберем $u_i, v_i \in \mathbb{Z}$ так, что

$$0 \le u_i < b, \qquad q_i \equiv u_i a^{d-2i} \pmod b, \tag{10}$$

$$0 \le v_i < a, \qquad q_i \equiv v_i b^{d-2i} \pmod a. \tag{11}$$

и положим

$$q_{i+1} = \left| \frac{q_i - u_i a^{d-2i} - v_i b^{d-2i}}{N} \right|. \tag{12}$$

Например, из (4) вытекает, что $u_0 = 1$, $v_0 = 1$. Поэтому $q_1 = \left|(1 - a^d - b^d)/N\right|$.

Из (2), (10) и (11) вытекает, что $q_i \in \mathbb{Z}$. В частности,

$$q_{d/2} \in \mathbb{Z}. \tag{13}$$

Утверждается, что

$$q_{d/2} \le \binom{d}{d/2}. \tag{14}$$

Отсюда вытекает заключение леммы 2.2.5. Действительно, из (12) последовательно находим: $1 = a^d + b^d \pm q_1 N = a^d + b^d \pm N(u_1 a^{d-2} + v_1 b^{d-2} \pm N q_2)$ и т. д. Поэтому

$$1 = \sum_{i=0}^{d} w_i a^{d-i} b^i, \tag{15}$$

где $w_i = \pm u_i$ при $1 \le i < d/2$, $w_{d/2} = \pm q_{d/2}$ и $w_i = \pm v_i$ при $d/2 < i \le d$. В частности, все $w_i \in \mathbb{Z}$. Кроме того, $|u_i| \le N$ и $|v_i| \le N$ (см. (10), (11)). Поэтому $|u_i| \le d$ и $|v_i| \le d$ (см. (6)). Следовательно,

$$|u_i| \le \binom{d}{i}, \qquad |v_i| \le \binom{d}{d-i}. \tag{16}$$

Учитывая (14) и (16), заключаем, что

$$|w_i| \le \binom{d}{i}. \tag{17}$$

Биномиальный коэффициент в (17) равен числу листков бинарного дерева высоты d, соответствующих моному $a^i b^{d-i}$. На них расположим $|w_i|$ элементов $\operatorname{sign}(w_i)$, а на незаполненных листках поместим нули. Такое дерево вычисляет элемент $t \in X_d$ (см. 2.2.1). Из (15) вытекает, что $t = 1$. Поэтому $1 \in X_d$.

Осталось доказать (14). Для этого докажем по индукции, что

$$q_i \le \frac{2^i}{4}[a^{d-2i-1} + b^{d-2i-1}]. \tag{18}$$

База индукции $i = 0$. В этом случае (18) сводится к тому, что

$$4 \le [a^{d-1} + b^{d-1}]. \tag{19}$$

Это вытекает из (9) и того, что $d \ge N$ (см. (6)).

Рассмотрим индукционный переход $i \to i+1$. Так как, по определению,

$$q_{i+1} = \left| \frac{q_i}{N} - \frac{u_i a^{d-2i} + v_i b^{d-2i}}{N} \right|$$

и $|x - y| \le \max(x, y)$ для $x, y > 0$, то достаточно из индукционного предположения вывести неравенства

$$\frac{q_i}{N} \le \frac{2^{i+1}}{4}[a^{d-2(i+1)-1} + b^{d-2(i+1)-1}] \tag{20}$$

и

$$\frac{u_i a^{d-2i} + v_i b^{d-2i}}{N} \le \frac{2^{i+1}}{4}[a^{d-2(i+1)-1} + b^{d-2(i+1)-1}]. \tag{21}$$

Для проверки (20) достаточно ввиду индукционного предположения показать, что

$$2^i[a^{d-2i-1} + b^{d-2i-1}] \le 2^{i+1}[a^{d-2i-3} + b^{d-2i-3}]N.$$

Упрощая, получаем $a^{d-2i-1} + b^{d-2i-1} \le 2ab \cdot a^{d-2i-3} + 2ab \cdot b^{d-2i-3}$. Для этого достаточно проверить неравенства $a^{d-2i-1} \le 2ab \cdot a^{d-2i-3}$ и $b^{d-2i-1} \le 2ab \cdot b^{d-2i-3}$. Или $a \le 2b$ и $b \le 2a$. Это верно по предположению (7).

Для проверки (18) осталось проверить (21), то есть проверить неравенство

$$u_i a^{d-2i} + v_i b^{d-2i} \le \frac{2^{i+1}}{4}[ba^{d-2i} + ab^{d-2i}]. \tag{22}$$

Это верно при $i \geq 1$, так как $u_i < b$, $v_i < a$. Это верно и при $i = 0$, так как $u_0 = v_0 = 1$.

Для завершения доказательства леммы 2.2.5 осталось из (18) вывести (14). Применим (18) к $n = d/2$. Получим

$$q_n \leq \frac{2^n}{4}[a^{-1} + b^{-1}] \leq \frac{2^n}{2\min(a,b)}. \tag{23}$$

Из формулы Стирлинга вытекает неравенство

$$\binom{2n}{n} \geq \frac{2^{2n}}{\sqrt{\pi n}\sqrt[6]{e}}. \tag{24}$$

Действительно, формула Стирлинга утверждает, что

$$\Gamma(s) = s^{s-\frac{1}{2}} \cdot e^{-s} \cdot \sqrt{2\pi} \cdot e^{\frac{\theta}{12s}} \qquad (0 < \theta < 1).$$

Нас интересует оценка снизу для биномиального коэффициента

$$\binom{2n}{n}, \text{ где } n = 1, 2, \ldots$$

Пользуясь формулой Стирлинга, получаем

$$\binom{2n}{n} = \frac{2n\Gamma(2n)}{n^2\Gamma(n)^2} = \frac{2n}{n^2}\frac{(2n)^{2n-\frac{1}{2}} \cdot e^{-2n} \cdot \sqrt{2\pi} \cdot e^{\frac{\theta}{24n}}}{\left(n^{n-\frac{1}{2}} \cdot e^{-n} \cdot \sqrt{2\pi} \cdot e^{\frac{\eta}{12n}}\right)^2} = \frac{2^{2n}}{\sqrt{\pi n}} e^{\frac{\theta - 4\eta}{24n}} \geq \frac{2^{2n}}{\sqrt{\pi n}\sqrt[6]{e}}.$$

Ввиду (24) для завершения доказательства леммы 2.2.5 осталось понять, что $2\min(a,b) \cdot 2^n \geq \sqrt{\pi n}\sqrt[6]{e}$. Это так при $a, b \geq 1$ и $n \geq 1$. □

2.2.6. Вывод теоремы 2.2.3 из леммы 2.2.5. Для вывода используем процедуру сближения a и b. Для пары взаимно простых положительных целых (a, b) введем высоту

$$ht(a,b) = \max(a/b, b/a).$$

Из определения ясно, что всегда $ht(a,b) \geq 1$. Если

$$ht(a,b) \leq 2,$$

то пару назовем подходящей. Для подходящей пары теорема 2.2.3 совпадает с доказанной леммой 2.2.5 и, следовательно, верна. Если пара (a, b) не подходящая, то построим по ней новую пару (a', b') со следующими свойствами:

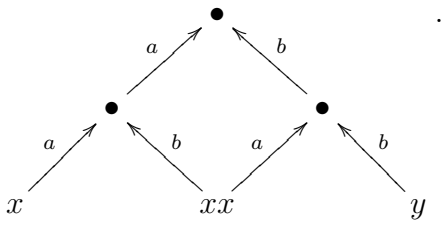
1. новая пара (a', b') допускает однородное представление с помощью исходной пары (a, b) (см. (2.2.1));
2. $ht(a', b') \leq \max(2, ht(a,b)/2)$.

Этого достаточно для доказательства теоремы 2.2.3. Действительно, из первого свойства вытекает, что любое число, которое можно однородным образом представить с помощью пары (a', b'), можно однородным образом представить и с помощью пары (a, b). Из второго свойства вытекает, что достаточно конечного числа модификаций.

Предположим, что пара (a, b) не подходящая. Без ограничения общности считаем, что

$$2a < b. \tag{25}$$

Положим $a' = a^2 + 2ab$, $b' = b^2$. Ясно, что a' и b' взаимно просты. Вот однородное представление операции для новой пары с помощью исходной: $a'x + b'y = a(ax + bx) + b(ax + by)$



Вот оценка высоты:

$$\frac{a'}{b'} = \frac{a^2 + 2ab}{b^2} \leq \frac{ab/2 + 2ab}{b^2} = \frac{5}{2}\frac{a}{b} < \frac{5}{4} \leq 2 \leq \max(2, ht(a, b)/2),$$
$$\frac{b'}{a'} = \left(\frac{a^2 + 2ab}{b^2}\right)^{-1} \leq \left(\frac{2ab}{b^2}\right)^{-1} = \frac{b}{2a} = \frac{ht(a, b)}{2} \leq \max(2, ht(a, b)/2).$$

В первом неравенстве использовано то, что $a < b/2$. Это вытекает из (25) и того, что пара (a, b) – не подходящая. Таким образом, теорема 2.2.3 доказана.

3 Заключение

Кратко обсудим некоторые проблемы и возможности, связанные с сингулярными моделями $\operatorname{Spec} \mathbb{Z}$.

Начнем с некоторой задачи перечисления деревьев. Эта задача происходит из проблемы вычислимости для обобщенной аффинной плоскости $\mathbf{A}^2_{\mathbb{F}} = \operatorname{Spec} \mathbb{F}[*]$, где $*$ – свободная коммутативная бинарная переменная, а $\mathbb{F}$ – начальный объект в категории обобщенных колец (в [2] это кольцо обозначено $\mathbb{F}_0$). По определению, имеется естественный эпиморфизм $\mathbb{F}\langle\circ\rangle \to \mathbb{F}[*]$, $\circ \mapsto *$, где $\circ$ – свободная некоммутативная бинарная переменная. Таким образом, множество $\mathbb{F}\langle\circ\rangle(n)$ представлено множеством (классов изоморфизма) пар (T, m), где T – бинарное дерево с упорядоченным множеством листьев $F(T)$, а $m : F(T) \to \{x_1, \ldots, x_n\}$ – маркировка. По определению множество $\mathbb{F}[*](n)$ является фактор-множеством $\mathbb{F}\langle\circ\rangle(n)/\sim$, где $\sim$ – отношение эквивалентности, порожденное соотношением коммутирования операции $*$ с собой: $(x*y)*(z*w) = (x * z) * (y * w)$. Требуется найти алгоритм для распознавания этого отношения эквивалентности. Отметим, что естественный гомоморфизм $\mathbb{F}[*] \to \mathbb{Z}[A, B]$, $* \mapsto$

(A, B) не решает эту проблему, так как не является вложением. Это видно на картинке

$$\begin{tikzcd}
 & & \bullet & & \\
 & \bullet \arrow[ur] & & \bullet \arrow[ul] & \\
 & & \bullet\bullet \arrow[ul] \arrow[ur] & & \\
x \arrow[uur] & y \arrow[ur] & & z \arrow[ul] & w \arrow[uul]
\end{tikzcd} \quad . \tag{26}$$

Действительно, можно переставить x и y, не меняя выхода в $\mathbb{Z}[A, B]$ (при этом z и w могут быть переставлены независимо). Однако автокоммутативность для $*$ позволяет переставлять только целиком пары (x, z) и (y, w). Решение этой задачи позволит, в частности, изучать особые арифметические кривые на аффинной плоскости и соответствующей проективной плоскости. Пока же для изучения доступны лишь кривые на более грубой модели $\mathbf{P}^2$ (см. [6]).

Следующий круг вопросов связан с геометрической формулировкой теории полей классов по образцу [3]. Начать можно с вычисления групп Пикара новых особых моделей. Разумеется, должна появиться особая версия теоремы Римана–Роха и обобщение всего этого на числовые поля. Отметим, что среди особых бирациональных моделей таких полей есть и классические схемы.

Несложно определить гомологии топологических пространств с коэффициентами в обобщенном кольце R. А именно,

$$H_n(X, R) = \pi_n(R(\operatorname{Sing} X)),$$

где Sing – симплициальное множество сингулярных симплексов X. Тогда $H_n(X, \mathbb{Z})$ – обычные гомологии, а $H_n(X, \mathbb{F}_1)$ – гомотопические группы X. Рассмотренные особые модели $\mathbb{Z}$ занимают промежуточное положение между $\mathbb{Z}$ и $\mathbb{F}_1$. Интересно было бы вычислить, хотя бы частично, гомологии с коэффициентами в конгруэнц-кольце $Q_N = \mathbb{Z}_{q,i}$ (см. 1.2.1), где q – проекция $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, а $E = \mathbb{F}_1$. Если ответ окажется нетривиальным, то можно попробовать перейти к пределу по N и учесть, что $\bigcap Q_N = \mathbb{F}_1$. Конечно, прежде всего стоило бы вычислить $H_n(S^m, Q_N)$ при $n > m$ для небольших m (например, для $m = 2$).

Мы начали изучение неклассических бирациональных моделей с $\mathbb{Z}$ и $\mathbb{Q}$. Можно было бы изучать подобные вопросы для обобщенных колец $\mathbb{Z}_{\geq 0}$ и $\mathbb{Q}_{\geq 0}$ (или даже $\mathbb{Z}_{>0}$ и $\mathbb{Q}_{>0}$). В этом случае пришлось бы взять $\mathrm{F} = \mathbb{F}_1$ или $\mathbb{F}_0$. Отметим близость возникающих при этом вопросов к вопросам, рассматриваемым в [7], [8], [9]. Более того, некоторые из таких вопросов могут оказаться алгоритмически неразрешимыми [10]. Весьма детальный обзор работ по этой тематике содержится в [11].

Список литературы

[1] *Sh. Haran.* Non-additive geometry, Composition Math. 143, (2007) 618-688.

[2] *N. Durov.* New Approach to Arakelov Geometry. arXiv: 0704.2030 v1 [math AG] 16 Apr 2007.

[3] *J.-P. Serre.* Algebraic Groups and Class Fields, Springer-Verlag, 1988.

[4] *A. L. Smirnov.* Generalized subrings of arithmetic rings, J. Math. Sci. (N. Y.) 151 (2008), no. 3, 3052-3068

[5] *S. A. Evdokimov.* Proof of a congruence conjecture for generalized rings, Записки научных семинаров ПОМИ, т. 443, 2016, с. 91-94.

[6] *A. L. Smirnov.* Binary projective spaces, J. Math. Sci. (N. Y.) 161 (2009), no. 4, 572-580.

[7] *D.A. Klarner, R. Rado.* Arithmetic properties of certaine recurcively defined sets, Pacific J. of Math., Vol. 53, no 2, 1974, 445–463.

[8] *J. Lagarias.* The $3x + 1$ problem and its generalizations. The American Mathematical Monthly, Vol. 92, No. 1 (Jan., 1985), pp. 3-23

[9] *S. Burckel.* Functional equations associated with congruential functions, Theoretical Computer Science 123 (1994), 397-406.

[10] *J. H. Conway.* Unpredictable iterations, Proc. 1972 Number Theory 1972, 49-52.

[11] *J. Lagarias.* The $3x+1$ Problem: An Annotated Bibliography (1963–1999) (Sorted by Author), arXiv:math/0309224 v13 [math.NT] 11 Jan 2011.