Андрей Бирюк
Кубанский государственный университет, Краснодар
Отчет за 2012 год.

1. Результаты, полученные в этом году. (Жюри особо отмечает, что не следуют ограничиваться только списком опубликованных и поданных в печать работ, нужно кратко сформулировать результаты, причем крайне желательно ориентировать текст на широкую математическую аудиторию, а не только на узких специалистов в области исследования.)

Подготовлена к печати работа [1] о связях решений уравнения Бюргерса и уравнения теплопроводности, с вытекающими следствиями о существовании и единственности решений уравнения Бюргерса в многомерном случае. Отметим, что теорема единственности решения уравнения Бюргеса, в отличие от теоремы единственности для уравнения теплопроводности справедлива без всяких дополнительных условий. Напомню, что в случае уравнения теплопроводности необходимо наложить некоторые ограничения, например, на рост в бесконечности по пространственным координатам (условия Тихонова). С различной степенью интенсивности я работал над этим текстом более 10 лет (в силу ряда причин). Результаты статьи мне представляются новыми либо малоизвестными. Среди новых результатов отмечу, например, доказательство теоремы Виддера в многомерном случае. Исторический обзор представляет интерес. Полный текст представлен в приложении 1.

В рамках моей работы по теории турбулентности я получил простые строгие утверждения (со строгими доказательствами) связывающие подходы Колмогорова и Обухова 1941 года к теории турбулентности. Эти факты на физическо-эвристическом уровне строгости изложены в книге «Турбулентность. Наследие Колмогорова» У. Фриш, М:ФАЗИС, 1998. Согласно моей личной корреспонденции с профессором У. Фришем, а также с другими известными учеными, например, с профессором Peter Constantin из Чикаго, строгих математических утверждений с доказательствами по этому вопросу на настоящий момент не представлено. Мои результаты обсуждены в июне 2012 с профессором Волтером Крэгом, однако, не опубликованы. (см. также пункт 4 настоящего отчета).

В рамках научной работы с сотрудниками своего университета совместно с М.И. Дроботенко и А.А. Свидловым получено небольшое расширение результатов первоначально полученных А.А. Свидловым в направлении отказа от излишней гладкости при описании планетарных волн, возникновение которых обуславливается вращением Земли, уравнением Россби. В простейшем случае, уравнение Россби выглядит следующим образом:

$$\Delta u_t + u_{x_1} = f.$$

Здесь u_t и u_{x_1} обозначают соответственно частные производные по времени и по координате x_1. Это уравнение имеет интересные свойства. Например, представляет интерес условие разрешимости начально-краевой задачи Неймана. Результаты доложены 18 июня 2012 года в McMaster University, Гамильтон, Канада.

В рамках научной работы со студентами опубликована совместная работа со студентом КубГУ [2]. В работе сформулирован и доказан ряд утверждений, имеющий определенную ценность в задаче вычисления последних ненулевых цифр десятичного представления числа $n!$ при больших значениях n. На настоящий момент, мы можем за доли секунд вычислить десятки таких цифр (текущий максимум: 27 цифр) для значений n порядка $10^{100} - 10^{200}$, что невозможно без применения математических утверждений. В связи с труднодоступностью места публикации, полный текст приложен к отчету (приложение 2).

2. Опубликованные и поданные в печать работы.

А. Научные:

[0] Biryuk, Andrei; Craig, Walter. *Bounds on Kolmogorov spectra for the Navier-Stokes equations.* Physica D, **241**, No. 4, 426-438 (2012).

Примечание. О выходе работы [0] было известно в конце прошлого года и информацию о ней, включая краткий обзор, см. в отчете за прошлый год. С другой стороны, в июне 2012 года я узнал что в 2010 году в Бразилии вышла другая моя статья. Поскольку я ни разу не отчитывался о ее выходе (в т.ч. в момент подачи заявки конкурс фонда «Династия»), приведу данные о ней в отчете за этот год:

[0′] Biryuk, Andrey; Gomes, Diogo A. *An introduction to the Aubry-Mather theory.* São Paulo J. Math. Sci. **4**, No. 1, 17-63 (2010).

[1] Бирюк А. Э. *О преобразовании уравнения Бюргерса к уравнению теплопроводности.*

Отвергнута из УМН по причине слишком маленького объема.

[2] Зеленый А.С., Бирюк А.Э. *Алгебраические утверждения и компьютерные вычисления.* Вестник студенческого научного общества факультета математики и компьютерных наук Кубанского государственного университета: Сборник научных трудов студентов и преподавателей факультета математики и компьютерных наук Кубанского государственного университета. Выпуск.3. Краснодар: Кубанский государственный университет, 2012, С. 80 - 86.

Б. Прочие публикации:

[3] Бирюк А. Э., Сукманюк В. Н. *О подготовке учащихся к решению задач высокого уровня сложности по геометрии.* Современные образовательные технологии педагогов Кубани и соотечественников за рубежом: научно методический сборник. Краснодар: ККИДППО, 2012г. 140с. ISBN 978-5-9901702-2-8, страницы: 15-21.

3. Участие в конференциях и школах.

Я являлся со организатором студенческой конференции КубГУ в апреле 2012. Студенты математического факультета под моим руководством сделали 4 доклада по темам «Элементы математической теории радуги», «Молекулярный подход к изучению атмосферы», «Расчет высоты прилива», «Последние не нулевые цифры числа N!». На основе последнего опубликована совместная со студентом работа «Алгебраические утверждения и компьютерные вычисления».

18 июня 2012 года сделал доклад «On the Rossby equation» в рамках Aims Lab семинара на факультете математики и статистики в университете МакМастер (McMaster University), город Гамильтон, Канада.

22 июня 2012 прочитал лекцию «Comparison theorems for p-elliptic equations with laden levelsets as coefficients and some other topics» на коллоквиуме в институте математических исследований Филдса (Fields Institute for Research in Mathematical Sciences), посвященному 20-летнему юбилею института (Back2Fields Colloquium series, Fields 20th anniversary), город Торонто, Канада.

4. Работа в научных центрах и международных группах.

С 9 по 27 июня 2012 я работал в McMaster University (Hamilton, Канада). В группе под руководством профессора Walter Craig, мы работали по теме сингулярных множеств решений системы Навье-Стокса и возможных ветвление решений, если решения рассматривать как кривые в Гильбертовом пространстве. Обсуждались возможные причины ветвления, такие как возможный скачёк энергии или диссипация энергии. Осуждались возможности микролокального анализа (одновременная локализация, сингулярности, как в основном пространстве, так и в Фурье пространстве). Сформулированы условные результаты, которые хотя и имеют некоторую внутреннюю красоту, но все же далеки от желаемого из-за обилия различных предположений и допущений. Наведён относительный порядок в современном понимании той области теории турбулентности, которая называется теорией Колмогорова-Обухова 1941 года. Сформулированы математические утверждения, которые либо являются новыми либо тщательно забытыми. Надеюсь, что результаты будут опубликованы в следующем году.

В апреле 2012 года я консультировал сотрудников Bank of Montreal (Канада) о возможности применения тех или иных финансовых моделей.

Поддерживаю связи с научными сотрудниками банка Credit-Suisse, в котором я работал в 2007-2008 г.

За отчетный период, я дважды рецензировал статьи для «SIAM Journal on Mathematical Analysis (SIMA)», один раз для «Proceedings of the AMS», а так же для некоторых научных конкурсов.

Сотрудничаю с центрами проведения студенческих Интернет-олимпиад по математике и другим дисциплинам с центрами проведения этих олимпиад в г. Йошкар-Ола (Россия) и Ариэль (Израиль). Являюсь координатором проведения студенческих дисциплинарных олимпиад в Кубанском государственном университете.

5. Педагогическая деятельность (включая научное руководство).

В этом году я стал первым заместителем председателя жюри регионального этапа (Краснодарский край) Всероссийской олимпиады школьников по математике. Возглавил работу по составлению задач для муниципального этапа олимпиады школьников по математике.

Работаю в программе повышения квалификации учителей школ Краснодарского края по математике (углубленное изучение предмета в школе). Участвовал в дистанционных семинарах для учителей математики г. Симферополь (Украина).

Веду курсы математического анализа на математическом факультете КубГУ, а также курс «Математический анализ на многообразиях» в магистратуре и другие курсы. Занимаюсь кружковой работой со школьниками и студентами.

Работаю со студентами 1 и 2 курса на факультативе по олимпиадной математике. На студенческих олимпиадах по математике мои студенты показывают относительно высокие результаты. Подчеркну, что для студентов провинциального вуза это является весьма мощным стимулом для дальнейшей работы.

Осуществляю научное руководство студентами 3, 4 и 5 курсов (формально у меня всего 4 студента, но фактически я работаю с 10 студентами) и один магистрант (формально за мной числится один, фактически их три). В прошлом году, но уже после отчета за 2011 год, руководимая мною магистрант второго (выпускного) года обучения Ирина Шаповалова успешно защитила магистерскую диссертацию по теме «Метод комплексного потенциала и задачи со свободной границей» 20 декабря 2011 г. Тем не менее, необходимо вернутся к теме и исправить имеющиеся недочеты работы и развить идеи.

Приложение 1.

О преобразовании уравнения Бюргерса к уравнению теплопроводности

А. Э. Бирюк[1]

Аннотация. Преобразование уравнения Бюргерса к уравнению теплопроводности, опубликованное в работах Флорина 1948, Хопфа 1950 и Коула 1951, имеет интересное приложение к вопросу единственности решения уравнения Бюргерса. Оказывается, что теорема единственности классического решения задачи Коши для нелинейного уравнения Бюргерса справедлива без каких-либо дополнительных условий, в отличие от линейного уравнения теплопроводности, где необходимы, например, Тихоновские ограничения на рост решений. В §1 мы обсуждаем это преобразование и доказываем с его помощью теорему существования и теорему единственности задачи Коши для уравнения Бюргерса. В последней теореме ключевым образом используется результат Виддера о единственности решения уравнения теплопроводности в классе неотрицательных функций. Поскольку мы не смогли найти доказательства теоремы единственности Виддера для многомерного случая в математической литературе, мы приводим своё в дополнении. В §2 мы делаем краткий обзор работы Флорина, который, решая трехмерную задачу консолидации влажной почвы, выполнил преобразование в наибольшей степени общности, включая случай переменных коэффициентов. В §3 мы делаем краткий обзор работы Форсайта опубликованной в 1906 содержащей формулы похожие на преобразование уравнения Бюргерса к уравнению теплопроводности.

§1. Преобразование. Многомерное уравнение Бюргерса можно записать в одной из следующих двух различных форм:

$$\frac{\partial \boldsymbol{v}}{\partial t} + \nabla \frac{(\boldsymbol{v},\boldsymbol{v})}{2} = \nu \Delta \boldsymbol{v} \qquad \text{или} \qquad \frac{\partial \boldsymbol{v}}{\partial t} + (\boldsymbol{v},\nabla)\boldsymbol{v} = \nu \Delta \boldsymbol{v}\,. \tag{1}$$

Здесь $\boldsymbol{v} = \boldsymbol{v}(t,\boldsymbol{x}) \in \mathbb{R}^n$, $t \geqslant 0$, $\boldsymbol{x} \in \mathbb{R}^n$, а ν — положительная константа. Напомним, что $(\boldsymbol{v},\nabla)$ — это оператор дифференцирования вдоль векторного поля $\boldsymbol{v}$. Символы ∇ и Δ обозначают операторы набла (градиент) и Лапласа, действующие только по переменным $\boldsymbol{x}$. В общем случае $\nabla \frac{(\boldsymbol{v},\boldsymbol{v})}{2} \neq (\boldsymbol{v},\nabla)\boldsymbol{v}$. Однако, мы будем рассматривать лишь потенциальный случай ($\boldsymbol{v} = \nabla H$), для которого указанные выражения совпадают.

Пусть $T > 0$, либо $T = +\infty$. Классическим решением уравнения (1) в полосе $[0,T) \times \mathbb{R}^n$ будем называть непрерывное векторное поле

$$\boldsymbol{v} : [0,T) \times \mathbb{R}^n \to \mathbb{R}^n\,,$$

которое при $t > 0$ является дважды непрерывно дифференцируемым по переменным $\boldsymbol{x}$, один раз по переменной t, при каждом фиксированном $t \geqslant 0$ является потенциальным (т.е. градиентом скалярной функции) и удовлетворяет уравнению (1).

Поскольку мы рассматриваем потенциальный случай, начальные данные тоже должны быть потенциальными:

$$\boldsymbol{v}(0,\boldsymbol{x}) = \boldsymbol{v}_0(\boldsymbol{x}) = \nabla H_0(\boldsymbol{x})\,. \tag{2}$$

Функция $H_0 : \mathbb{R}^n \to \mathbb{R}$ предполагается непрырывно дифференцируемой.

Положим $\varphi_0(\boldsymbol{x}) = \exp\left(\frac{H_0(\boldsymbol{x})}{-2\nu}\right)$. Пусть функция $\varphi(t,\boldsymbol{x})$ является (положительным) решением задачи Коши для уравнения теплопроводности:

$$\varphi_t = \nu \Delta \varphi\,, \qquad \varphi(0,\boldsymbol{x}) = \varphi_0(\boldsymbol{x})\,. \tag{3}$$

Иными словами, при $t > 0$ полагаем:

$$\varphi(t,\boldsymbol{x}) = \frac{1}{(4\pi t\nu)^{n/2}} \int_{\mathbb{R}^n} \varphi_0(\boldsymbol{z}) \exp\left(\frac{-(\boldsymbol{x}-\boldsymbol{z})^2}{4t\nu}\right) d\boldsymbol{z}\,. \tag{4}$$

Необходимым и достаточным условием существования указанной функции φ в полосе $[0,T)\times\mathbb{R}^n$ является сходимость интеграла (4) для каждых $t \in (0,T)$ и $\boldsymbol{x} \in \mathbb{R}^n$. Из него следует простое достаточное условие:

$$\liminf_{|\boldsymbol{x}|\to\infty} \frac{H_0(\boldsymbol{x})}{|\boldsymbol{x}|^2} \geqslant \frac{-1}{2T}\,. \tag{5}$$

[1]Работа выполнена при частичной поддержке фонда «Династия».

Здесь в случае $T = +\infty$ мы полагаем, что $\frac{-1}{2T} = 0$.

Сформулируем теорему разрешимости уравнения Бюргерса.

Теорема 1. *В используемых обозначениях, при условии* (5), *векторное поле*

$$\boldsymbol{v} = -2\nu\nabla \ln \varphi = -2\nu\frac{\nabla\varphi}{\varphi}$$

является классическим решением задачи Коши (1), (2) в полосе $[0,T)\times\mathbb{R}^n$.

Доказательство. Действительно:

$$\tfrac{\partial \boldsymbol{v}}{\partial t} + \nabla\tfrac{(\boldsymbol{v},\boldsymbol{v})}{2} - \nu\Delta\boldsymbol{v} = -2\nu\nabla\left(\tfrac{\varphi_t - \nu\Delta\varphi}{\varphi}\right).$$

Теорема доказана, так как φ определена и положительна в полосе $[0,T)\times\mathbb{R}^n$. □

Таким образом, условие (5) является достаточным условием разрешимости задачи Коши (1), (2) в полосе $[0,T)\times\mathbb{R}^n$. Оно является в определенном смысле точным в силу следующего примера. Рассмотрим случай начальных данных $\boldsymbol{v}_0(\boldsymbol{x}) = -\boldsymbol{x}/T$, т.е. $H_0(\boldsymbol{x}) = -\frac{1}{2T}|\boldsymbol{x}|^2$. Тогда решение принимает следующий вид: $\boldsymbol{v}(t,\boldsymbol{x}) = \frac{-\boldsymbol{x}}{T-t}$. Это решение перестает существовать при $t \geqslant T$.

Перейдем к вопросу единственности решения для уравнения Бюргерса. Справедлива следующая теорема:

Теорема 2. *Задача Коши (1), (2) допускает не более одного классического решения в полосе* $[0,T)\times\mathbb{R}^n$.

Ключевым моментом в доказательстве этой теоремы является то, что задача Коши для уравнения теплопроводности (3) обладает не более чем единственным решением в классе положительных функций. В работе Виддера [5, гл. 8, §2] этот факт доказан в одномерном случае ($n = 1$). Доказательство этой теоремы в многомерном случае приводится ниже в качестве дополнения к данной статье.

Если векторное поле $\boldsymbol{v}$ является классическим решением задачи Коши (1), (2) в полосе $[0,T)\times\mathbb{R}^n$, то в этой полосе найдется потенциал H (т.е. $\boldsymbol{v} = \nabla H$) такой, что $H(0,\boldsymbol{x}) = H_0(\boldsymbol{x})$ и который, удовлетворяет уравнению

$$\tfrac{\partial H}{\partial t} + \tfrac{1}{2}(\nabla H, \nabla H) - \nu\Delta H = 0\,. \tag{6}$$

В самом деле, пусть $\widetilde{H} = \widetilde{H}(t,\boldsymbol{x})$ — произвольный потенциал, который существует по условию. Без ограничения общности, можем считать, что $\widetilde{H}(t,\boldsymbol{0}) = H_0(\boldsymbol{0})$. Подставим тождество $\boldsymbol{v} = \nabla\widetilde{H}$ в уравнение (1) и, перенеся все в левую часть, получим:

$$\nabla\left(\tfrac{\partial\widetilde{H}}{\partial t} + \tfrac{1}{2}(\nabla\widetilde{H},\nabla\widetilde{H}) - \nu\Delta\widetilde{H}\right) = 0 \quad \text{или} \quad \tfrac{\partial\widetilde{H}}{\partial t} + \tfrac{1}{2}(\nabla\widetilde{H},\nabla\widetilde{H}) - \nu\Delta\widetilde{H} = F(t)\,.$$

Тогда функция $H(t,\boldsymbol{x}) = \widetilde{H}(t,\boldsymbol{x}) - \int_0^t F(\tau)d\tau$ удовлетворяет уравнению (6).

Лемма. *Пусть векторное поле* $\boldsymbol{v}$ *является классическим решением задачи Коши (1), (2) в полосе* $[0,T)\times\mathbb{R}^n$. *Тогда существует положительная функция* φ *такая, что*

$$\varphi_t = \nu\Delta\varphi\,, \qquad \varphi(0,\boldsymbol{x}) = \exp\left(\tfrac{H_0(\boldsymbol{x})}{-2\nu}\right) \quad \text{и} \quad \boldsymbol{v} = -2\nu\nabla\ln\varphi\,.$$

Доказательство. Возьмем потенциал H, такой, что $H(0,\boldsymbol{x}) = H_0(\boldsymbol{x})$ и который удовлетворяет (6). Положив $\varphi(t,\boldsymbol{x}) = e^{-H(t,\boldsymbol{x})/(2\nu)}$, мы получим доказательство леммы. □

Теорема 2 следует из этой леммы и теоремы единственности решения задачи Коши для уравнения теплопроводности в классе положительных функций.

Из теоремы 2 следует, что сходимость интеграла (4) при всех $t \in (0,T)$ и $\boldsymbol{x} \in \mathbb{R}^n$ является не только достаточным условием разрешимости задачи Коши (1), (2) в полосе $[0,T)\times\mathbb{R}^n$, но и необходимым.

Интересно отметить, что теорема единственности решения для нелинейного уравнения Бюргерса справедлива без каких-либо дополнительных условий, в то время, как для линейного уравнения теплопроводности необходимы дополнительные условия, например, условия Тихонова [9], ограничивающие рост решений на бесконечности.

§2. Обзор работы Флорина [1] (1948).

Долгое время считалось, что задача преобразования уравнения Бюргерса к уравнению теплопроводности впервые была решена в начале 50-х годов XX века независимо друг от друга Хопфом

и Коулом. Однако, в последнее время появились исследования, утверждающие, что это преобразование удалось осуществить раньше: русским механиком Флориным в 1948 году и шотладским математиком Форсайтом в 1906 году. В связи с отсутствием единого мнения математиков, мы исследовали вопрос когда впервые в математической литературе уравнение Бюргерса было сведено к линейному параболическому уравнению второго порядка (уравнению теплопроводности). Анализ первоисточников показывает, что работа Флорина действительно содержит в себе преобразование уравнения Бюргерса к уравнению теплопроводности, причем выполненное в большей степени общности, чем у самих Хопфа и Коула. Так как это преобразование в работах Флорина носит в себе характер одной из подзадач в решении проблемы консолидации влажной почвы, то широкой известности среди математиков этот факт не мог получить по понятным причинам.

Приведем фрагмент работы [1].

Если потенциальное векторное поле $\boldsymbol{v}$ удовлетворяет уравнению (1), то существует потенциал H (т.е. $\boldsymbol{v} = \operatorname{grad} H$), который удовлетворяет уравнению:

$$\tfrac{\partial H}{\partial t} + \tfrac{1}{2}(\operatorname{grad} H, \operatorname{grad} H) = \nu \Delta H.$$

В.А.Флорин, рассматривая проблему консолидации влажной почвы, получил следующее уравнение (случай трехмерной пространственной переменной):

$$\tfrac{\partial H}{\partial t} + \alpha(\operatorname{grad} H)^2 + \beta(\operatorname{grad} H, \operatorname{grad} \psi) + \delta \nabla^2 H + \tfrac{\partial F}{\partial t} = 0, \qquad [1, \text{ур. } (17)]$$

где H — гидростатическое давление, $\alpha, \beta, \delta, \psi$, и $\partial F/\partial t$ — некоторые функции, зависящие от $\boldsymbol{x}$ и времени t.

В работе [1] на странице 1392, при предположении $\alpha/\delta = const$, Флорин делает подстановку

$$H = \tfrac{\delta}{\alpha} \ln(\varphi + C) + D, \qquad [1, \text{ур. } (18)]$$

где C и D — некоторые постоянные, и сводит уравнение [1, ур. (17)] к следующему линейному уравнению:

$$\tfrac{\partial \varphi}{\partial t} + \beta(\operatorname{grad} \varphi, \operatorname{grad} \psi) + \delta \nabla^2 \varphi + \tfrac{\alpha}{\delta}(\varphi + C)\tfrac{\partial F}{\partial t} = 0. \qquad [1, \text{ур. } (19)]$$

Позже, это преобразование, но лишь для случая постоянных коэффициентов независимо было переоткрыто Е. Хопфом [3] и Дж. Коулом [4]. В работе [4] имеется формулировка преобразования для многомерного случая.

§3. Обзор подразделов 206 и 207 из книги Форсайта [2] (1906).

В истории вопроса о перевенстве открытия преобразования уравнения Бюргерса к уравнению теплопроводности некоторые специалисты необоснованно ссылаются (напр, [10]) на том 6 монографии Форсайта [2], а именно на подразделы 206 и 207.

Следует особо подчеркнуть, что шести-томный труд Форсайта, заслуживает самой высокой оценки. Его и сейчас, спустя более чем столетие, можно смело рекомендовать для изучения как начинающим, так и состоявшимся математикам. Однако, уравнение Бюргерса к уравнению теплопроводности там не сведено. Сделаем обзор результатов Форсайта указанных подразделов.

Рассмотрим *линейное* уравнение второго порядка на неизвестную функцию $u = u(t, x)$:

$$\nu(t,x)\tfrac{\partial^2 u}{\partial x^2} - \alpha(t,x)\tfrac{\partial u}{\partial x} - \tfrac{\partial u}{\partial t} + \gamma(t,x)u = 0. \qquad (7)$$

Здесь $x \in \mathbb{R}$, t>0. Посредством *линейной* замены

$$u = \lambda(t,x)v, \qquad (8)$$

где $\lambda = \lambda(t,x)$ — некоторая фиксированная (известная) функция (параметр замены), а $v = v(t,x)$ — новая неизвестная функция, мы преобразуем уравнение (7) в новое, но снова *линейное* уравнение

$$\tilde{\nu}(t,x)\tfrac{\partial^2 v}{\partial x^2} - \tilde{\alpha}(t,x)\tfrac{\partial v}{\partial x} - \tfrac{\partial v}{\partial t} + \tilde{\gamma}(t,x)v = 0,$$

где новые коэффицинетны $\tilde{\nu}(t,x)$, $\tilde{\alpha}(t,x)$ и $\tilde{\gamma}(t,x)$ выражаются следующим образом:

$$\begin{aligned} \tilde{\nu} &= \nu\,, \\ \tilde{\alpha} &= \alpha - \tfrac{2\nu\lambda_x}{\lambda}, \\ \tilde{\gamma} &= \gamma - \tfrac{\alpha\lambda_x}{\lambda} - \tfrac{\lambda_t}{\lambda} + \tfrac{\nu\lambda_{xx}}{\lambda}. \end{aligned}$$

Следовательно, становится очевидным, что функция $I(t,x)=\nu(t,x)$ является инвариантом относительно линейных подстановок типа (8). Форсайт нашел еще один инвариант:

$$J(t,x)=\frac{\partial}{\partial x}\left(2\gamma+\nu\left(\frac{\alpha}{\nu}\right)_x-\frac{1}{2}\frac{\alpha^2}{\nu}\right)-\frac{\partial}{\partial t}\left(\frac{\alpha}{\nu}\right).$$

В самом деле, используя тождество

$$2\tilde{\gamma}+\tilde{\nu}\left(\frac{\tilde{\alpha}}{\tilde{\nu}}\right)_x-\frac{1}{2}\frac{(\tilde{\alpha})^2}{\tilde{\nu}}=2\gamma+\nu\left(\frac{\alpha}{\nu}\right)_x-\frac{1}{2}\frac{\alpha^2}{\nu}-\frac{2\lambda_t}{\lambda},$$

мы получаем:

$$\frac{\partial}{\partial x}\left(2\tilde{\gamma}+\tilde{\nu}\left(\frac{\tilde{\alpha}}{\tilde{\nu}}\right)_x-\frac{1}{2}\frac{(\tilde{\alpha})^2}{\tilde{\nu}}\right)-\frac{\partial}{\partial t}\left(\frac{\tilde{\alpha}}{\tilde{\nu}}\right)=\frac{\partial}{\partial x}\left(2\gamma+\nu\left(\frac{\alpha}{\nu}\right)_x-\frac{1}{2}\frac{\alpha^2}{\nu}\right)-\frac{\partial}{\partial t}\left(\frac{\alpha}{\nu}\right).$$

Эти инварианты найдены в подразделе 206 книги Форсайта [2]. В подразделе 207 Форсайт показывает, что функции I и J образуют полную систему инвариантов для уравнений вида (7) относительно линейных преобразований вида (8). Другими словами, два уравнения вида (7), для которых функции I и J соответственно совпадают, могут быть переведены одно в другое с помощью замены вида (8).

Сформулируем частный случай этого утверждения, который часто ошибочно принимают (см. напр., [10]) за подстановку, сводящую уравнение Бюргерса к линейному уравнению теплопроводности.

Теорема. *Уравнение* (7) *может быть сведено к форме*

$$v_t=\nu(t,x)v_{xx}$$

с помощью подстановки (8) *тогда и только тогда, когда* $J(t,x)\equiv 0$. *При этом* $\lambda(t,x)=e^{\theta(t,x)}$, *где* $\theta(t,x)$ — *функция, удовлетворяющая условиям:*

$$\frac{\partial\theta}{\partial x}=\frac{\alpha}{2\nu},$$
$$\frac{\partial\theta}{\partial t}=\gamma+\frac{\nu}{2}\left(\frac{\alpha}{\nu}\right)_x-\frac{1}{4}\frac{\alpha^2}{\nu}.$$

В случае $\nu=Const$ условие $J(t,x)\equiv 0$ является ни чем иным, как уравнением Бюргерса относительно α:

$$\alpha_t+\alpha\alpha_x=\nu\alpha_{xx}+2\nu\gamma_x\,. \tag{9}$$

Отметим, что выше изложенное является современной интерпретацией исследований Форсайта, которые в оригинале были выполнены в математическом стиле начала XX века. Кроме этого, Форсайт использовал нормализацию, в которой коэффициент при u_{xx} равняется единице. Тогда как в уравнении (7) мы нормализуем коэффициент при u_t. Соответственно, форма инвариантов I и J в нашем изложении по сравнению с изложением Форсайта претерпела необходимые изменения.

Уравнение Бюргерса в монографии Форсайта [2] действительно встречается в подразделах 206 и 207. Например, в упражнении 3 на странице 102 оно возникает всего лишь как *вспомогательное* условие при специальных линейных преобразованиях. Однако, в монографии [2] уравнение Бюргерса нигде не было преобразовано к уравнению теплопроводности. Эта задача автором и не рассматривалась. Так как, стоит заметить, что вспомогательное уравнение Бюргерса (9) может быть преобразовано к уравнению теплопроводности $\varphi_t-\nu\Delta\varphi+\gamma\varphi=0$ с помощью подстановки $\alpha=-2\nu\left(\ln\varphi\right)_x$, т.е. $\varphi=\lambda^{-1}$ (см. §1). Ничего аналогичного у Форсайта не встречается.

Таким образом, анализ имеющихся источников свидетельствует, что преобразование нелинейного уравнения Бюргерса к линейному уравнению теплопроводности впервые было сделано в работе Флорина [1] в 1948 году.

Дополнение. Теорема единственности для уравнения теплопроводности в классе неотрицательных функций.

В случае одномерной пространственной переменной теорема единственности положительных решений уравнения теплопроводности была доказана Виддером [5], [6]. Приведем доказательство этого утверждения для многомерного случая.

Теорема. *Пусть неотрицательная непрерывная функция* $u=u(t,\boldsymbol{x})$ *определена в полосе* $[0,T)\times\mathbb{R}^n$. *Предположим, что при* $t>0$ *эта функция обладает двумя непрерывными производными по* $\boldsymbol{x}$, *одной — по* t *и удовлетворяет уравнению* $u_t=\Delta u$.

Тогда, для каждого $t \in (0,T)$ и $\boldsymbol{x} \in \mathbb{R}^n$ справедливо равенство:

$$u(t,\boldsymbol{x}) = \int_{\mathbb{R}^n} G(t,\boldsymbol{x}-\boldsymbol{\xi})u(0,\boldsymbol{\xi})d\boldsymbol{\xi}, \tag{10}$$

где $G(t,\boldsymbol{y}) = \frac{1}{(4\pi t)^{n/2}} e^{-|\boldsymbol{y}|^2/4t}$ — фундаментальное решение уравнения теплопроводности.

Замечание. Сходимость интеграла в правой части (10) является частью утверждения теоремы.

Доказательство. Чтобы доказать равенство (10) мы покажем, что справедливы оба противоположных неравенства "$\geqslant$" и "$\leqslant$" на месте знака равенства в (10).

1° ($\geqslant$). Для каждого фиксированного $A > 0$ рассмотрим функцию:

$$v_A(t,\boldsymbol{x}) = u(t,\boldsymbol{x}) - \int_{|\boldsymbol{\xi}|<A} G(t,\boldsymbol{x}-\boldsymbol{\xi})u(0,\boldsymbol{\xi})d\boldsymbol{\xi}.$$

Достаточно доказать, что для каждого $\varepsilon > 0$ справедливо неравенство $v_A(t,\boldsymbol{x}) \geqslant -\varepsilon$. Для этого мы применим принцип максимума для функции v_A в цилиндре $[0,T) \times \{|\boldsymbol{x}| \leqslant B\}$ для достаточно большого B, замечая, что, $v_A \geqslant -\varepsilon$ на границе цилиндра.

2° ($\leqslant$). В пункте 1° было доказано, что интеграл в правой части (10) сходится и следовательно определяет некоторую функцию v. При этом, опять из результата пункта 1° следует, что функция $\bar{u} = u - v$ является неотрицательным решением уравнения теплопроводности с нулевыми начальными данными.

Остается показать, что неотрицательное решение u уравнения теплопроводности с нулевыми начальными данными равно нулю.

Без ограничения общности мы можем считать, что $u_t \geqslant 0$. В самом деле, иначе мы рассмотрим функцию $\tilde{u}(t,\boldsymbol{x}) = \int_0^t u(\tau,\boldsymbol{x})d\tau$. Чтобы обосновать, что функция $\tilde{u}$ удовлетворяет уравнению теплопроводности, нужно иметь право переставлять операции дифференцирования и интегрирования по времени. Достаточным условием этого является локальная равномерная непрерывность соответствующих производных функции u. Она может быть получена с помощью стандартного усреднения Стеклова по $\boldsymbol{x}$-переменной, т.е. свертки по $\boldsymbol{x}$ с неотрицательной гладкой функцией с компактным носителем. Операция свертки, в силу коммутирования с операциями дифференцирования, сохраняет уравнение теплопроводности.

Теперь мы докажем, что функция u удовлетворяет условиям роста теоремы единственности Тихонова для уравнения теплопроводности (см., например, [7, гл. 3, §4], [8, гл. VI, §1, п.2], [9]). Пусть $\delta > 0$ и $t + \delta < T$, тогда

$$u(t,\boldsymbol{x}) \overset{\Delta u \geqslant 0}{\leqslant} \tfrac{1}{\operatorname{Vol} B(\boldsymbol{x},|\boldsymbol{x}|)} \int_{B(\boldsymbol{x},|\boldsymbol{x}|)} u(t,\boldsymbol{\xi})d\boldsymbol{\xi} \leqslant C|\boldsymbol{x}|^{-n} \int_{B(\boldsymbol{0},2|\boldsymbol{x}|)} u(t,\boldsymbol{\xi})d\boldsymbol{\xi} \leqslant$$

$$\leqslant \tfrac{C|\boldsymbol{x}|^{-n}}{G(\delta,2\boldsymbol{x})} \int_{\mathbb{R}^n} G(\delta,-\boldsymbol{\xi})u(t,\boldsymbol{\xi})d\boldsymbol{\xi} \overset{\text{доказательства}}{\overset{\text{1-ая часть}}{\leqslant}} \tfrac{C(4\pi\delta)^{n/2}}{|\boldsymbol{x}|^n} e^{|\boldsymbol{x}|^2/\delta} u(t+\delta,\boldsymbol{0}).$$

Последнее неравенство, а также сходимость интеграла следуют из уже доказанного факта, что в (10) справедливо неравенство "$\geqslant$" (пункт 1°).

Поскольку для каждого $\varepsilon > 0$ функция u является ограниченной на компакте $[0,T-\varepsilon] \times \{|\boldsymbol{x}| \leqslant 1\}$, мы получаем, что для подходящей константы C_2 справедливо неравенство

$$u(t,\boldsymbol{x}) \leqslant C_2 e^{2|\boldsymbol{x}|^2/\varepsilon},$$

в полосе $[0,T-\varepsilon] \times \mathbb{R}^n$. Таким образом, мы показали, что выполняются условия Тихонова. Теорема доказана. □

Автор благодарен профессорам С. Б. Куксину и А. В. Фурсикову, а также Александру Боричеву за полезные обсуждения и ценные замечания.

Список литературы

[1] В. А. Флорин, *Некоторые простейшие нелинейные задачи консолидации водонасыщенной земляной среды.* Известия Акад. Наук СССР. Отд. техн. наук **1948**, №9 (1948), 1389–1402.

[2] A. R. Forsyth, *Theory of differential equations,* Vol 6, Cambridge University Press, 1906.

[3] E. Hopf, *The partial differential equation* $u_t + uu_x = \mu u_{xx}$. Comm. Pure Appl. Math. **3**, (1950), 201–230.

[4] J. D. Cole, On a quasi-linear parabolic equation occurring in aerodynamics. Quart. Appl. Math. **9**, (1951), 225–236.

[5] D. V. Widder, *The heat equation.* Academic Press, 1975.

[6] D. V. Widder, *Positive temperatures on an infinite rod.* Trans. Amer. Math. Soc. **55**, (1944) 85–95.

[7] Е. М. Ландис, *Уравнения второго порядка эллиптического и параболического типов,* Наука, М., 1971.

[8] В. П. Михайлов, *Дифференциальные уравнения в частных производных.* М.: Наука, 1976.

[9] А. Н. Тихонов, *Théorems̀ d'unicité pour l'équation de la chaleur.* Матем. сб. **42**, (1935), 199–216.

[10] F. Gesztesy, H. Holden, "The Cole-Hopf and Miura transformations revisited", In *Mathematical Physics and Stochastic Analysis. Essays in Honor of Ludwig Streit*, S. Albeverio, Ph. Blanchard, L. Ferreira, T. Hida, Y. Kondratiev, and R. Vilela Mendes (eds.), World Scientific, Singapore, 2000, pp. 198-214.

А. Э. Бирюк (A. Biryuk)
Кубанский государственный университет
E-mail: abiryuk@kubsu.ru

Работа поддержана фондом «Династия».

Приложение 2.

Алгебраические утверждения и компьютерные вычисления.

Работа выполнена в мае 2012 года.

Сведения об авторах:

Зелёный Андрей Сергеевич — студент 1 года обучения (весна 2012г.) факультета математики и компьютерных наук, КубГУ, Краснодар.

Бирюк Андрей Эдуардович — доцент кафедры теории функций факультета математики и компьютерных наук, КубГУ. Работа выполнена при частичной поддержке фонда «Династия».

Абстракт. На примере задачи вычисления последних не нулевых цифр десятичного представления числа $n!$ демонстрируется как алгебраические утверждения из теории групп и колец (теории вычетов) помогают значительно сократить компьютерные вычисления и тем самым вычислять за секунды компьютерные задачи, прямое вычисление которых заняло бы столетия. Алгебраические утверждения полученные на этом пути представляют самостоятельный интерес. Например, классическая задача о том, что числитель дроби $\sum_{i=1}^{p-1}\frac{1}{i}$, где $p>3$ – простое, делится на p^2 обобщена до задачи о делимости на n^2 числителя дроби $\sum_{i\in\mathbb{Z}_n^*}\frac{1}{i}$. Найдены необходимые и достаточные условия на n, когда это утверждение справедливо.

Факториал натурального числа n обозначается $n!$ и определяется как произведение всех натуральных чисел не превосходящих n, т.е. $n! = 1\cdot 2\cdot \ldots \cdot n$. Кроме того, по определению полагается $0! = 1$. Количество нулей $zeros(n!)$ в конце десятичного представления числа $n!$ определяется сравнительно просто. Поскольку $10 = 2\cdot 5$, то выделив степени простых множителей 2 и 5 в числе $n! = 2^{k_2}5^{k_5}A$, где A не делится ни на 2 ни на 5, получим $zeros(n!) = \min(k_2, k_5)$. Поскольку всегда $k_2 \geqslant k_5$ (равенство достигается лишь при $n = 0, 1$), получаем, что $zeros(n!) = k_5$ или

$$zeros(n!) = \sum_{i=1}^{\infty}\Big[\frac{n}{5^i}\Big].$$

Здесь $[\cdot]$ обозначает целую часть числа, а сумма всегда конечна, т.к. содержит лишь конечное число (равное $[\log_5(n)]$ при $n > 0$) не нулевых слагаемых. Поскольку $n! = A2^{k_2-k_5}10^{k_5}$, то задача нахождения d последних не нулевых цифр десятичного разложения числа $n!$ сводится к задаче нахождения последних d цифр числа $A2^{k_2-k_5}$ или попросту к отысканию остатка $A2^{k_2-k_5}\, mod\, 10^d$. Для каждого $i = 1..n$ определим a_i из разложения $i = 2^{\alpha_i}5^{\beta_i}a_i$, где a_i не делится ни на 2 ни на 5. Тогда нас интересует следующее число $(2^{k_2-k_5}\prod_{i=1}^{n}a_i) mod 10^d$. Приведенный ниже фрагмент программы на языке Паскаль вычисляет это значение для $d = 4$ (все переменные – целочисленного типа).

```
cifry:=1  {здесь будут храниться d=4 последние не нулевые цифры }
FOR i := 1 TO n DO BEGIN a:=i;
  WHILE (a mod 5) = 0 DO a:=a div 5; {освобождаем число от степени 5-рок}
  WHILE (a mod 2) = 0 DO a:=a div 2; {освобождаем число от степени двоек}
  cifry:=(cifry*(a mod 10000)) mod 10000;
END;
k2:=0;k5:=0;
m:=n; WHILE m <> 0 DO BEGIN m := m div 5; k5:=k5+m; end;
m:=n; WHILE m <> 0 DO BEGIN m := m div 2; k2:=k2+m; end;
FOR i := 1 TO k2-k5 DO cifry:=(cifry*2) mod 10000;
WriteLn(n,'! = ...',cifry:4,'*10^',k5);
```

На современных компьютерах с частотой 1-3 Ггц приведенный код выдает ответ для входных значений n порядка 10^7 — 10^8 за время порядка секунды или несколько секунд. Наша следующая цель — научиться обрабатывать значения n порядка 10^{100} — 10^{200}. Мы сделаем это за счет нахождения регулярных структур в, на первый взгляд, достаточно нерегулярной последовательности чисел a_i. Для этого, мы введем двумерную систему "этажей" на множестве натуральных чисел $\mathbb{N}$. Мы скажем, что натуральное число i находится на этаже (α, β), соответствующему числу $2^{\alpha}5^{\beta}$, где α и

β — целые не отрицательные числа, если простые числа 2 и 5 входят в n с соответственно степенями α и β. Отметим, что на каждом этаже последовательность a_i имеет простую структуру: это возрастающая последовательность всех натуральных чисел, взаимно простых с числом 10.

Обозначение. Для целых чисел n и k, через (n, k) будем обозначать их наибольший общий делитель. Для каждого $n \in \mathbb{N}$, будем рассматривать подмножество натуральных чисел не превосходящих n и взаимно простых с n:

$$\mathbb{Z}_n^* = \{k \in \mathbb{N} : k \leqslant n,\ (k, n) = 1\}.$$

По модулю n, множество $\mathbb{Z}_n^*$ образует мультипликативную группу. Пусть $\varphi(n)$ обозначает количество элементов в $\mathbb{Z}_n^*$ (функция Эйлера). Отметим известные свойства функции Эйлера: $\varphi(mn) = \varphi(m)\varphi(n)$, если m и n взаимно просты, а если p – простое, то для $k \in \mathbb{N}$ выполнено $\varphi(p^k) = (p-1)(p^{k-1})$. Таким образом, при $n > 2$ число $\varphi(n)$ является четным.

Лемма. Произведение всех элементов группы $\mathbb{Z}_n^*$:

$$\prod_{a \in \mathbb{Z}_n^*} a = \begin{cases} -1 \,(\mathrm{mod}\, n), \text{ если группа } \mathbb{Z}_n^* \text{ – циклическая;} \\ \ \ 1 \,(\mathrm{mod}\, n), \text{ если группа } \mathbb{Z}_n^* \text{ – не циклическая.} \end{cases}$$

Доказательство. Если группа $\mathbb{Z}_n^*$ – циклическая, то найдется примитивный элемент $e \in \mathbb{Z}_n^*$, такой, что все остальные являются различными степенями элемента e. Тогда

$$\prod_{a \in \mathbb{Z}_n^*} a = e^{0+1+\ldots+(\varphi(n)-1)} = e^{(\varphi(n)/2)(\varphi(n)-1)} = -1.$$

Здесь мы использовали свойство примитивного элемента $e^{(\varphi(n)/2)} = -1$, а также то, что число $\varphi(n)-1$ является нечетным. Если группа $\mathbb{Z}_n^*$ – не циклическая, то она разлагается в прямое произведение циклических групп, каждая из которых будет четного порядка, поэтому минус единица в каждой компоненте будет возведена в четную степень. □

Известно, что группа $\mathbb{Z}_n^*$ – циклическая, тогда и только тогда, когда $n = 2, 4,\ p^k,\ 2p^k$, где p — нечетное простое число.

Следствие. Пусть целое число $d \geqslant 2$ и $N = 10^d$, тогда для любого $k \in \mathbb{Z}$

$$\prod_{a \in \mathbb{Z}_N^*} (kN + a) \equiv 1 \bmod N.$$

Это следствие позволяет значительно ускорить алгоритм вычисления. А именно для каждого этажа (α, β) достаточно перемножать лишь те взаимно простые с 10-ю числа, которые попадают в промежуток kN, до $\left[\frac{n}{2^\alpha 5^\beta}\right]$ включительно, где $k = \left[\frac{n}{2^\alpha 5^\beta N}\right]$. Эквивалентно, нам достаточно перемножить все числа, оканчивающиеся на цифры 1, 3, 7 или 9 из промежутка от 1 до $\left(\left[\frac{n}{2^\alpha 5^\beta}\right] \bmod N\right)$ включительно.

Вычисление величины $2^{k2-k5} \bmod N$ тоже необходимо оптимизировать, применив стандартный алгоритм быстрого возведения в степень, основанный на двоичном представлении числа $k2 - k5$.

На этом этапе мы способны вычислять последние d ненулевых цифр числа $n!$ за разумное время (не более нескольких секунд на современных компьютерах) для $n < 10^{200}$, к сожалению, количество цифр $d = 4$ ($N = 10000$) не слишком велико. Связано это с тем, что нам требуется проходить циклы длины 10^d. Поэтому увеличение d на единицу приводит к увеличению времени в 10 раз.

Мы не останавливаемся на проблеме переполнения стандартных числовых типов, т.к. реализовать представление «огромных» чисел можно с помощью строковых типов, а арифметические действия с ними с помощью стандартных действий «в столбик».

Остаток статьи посвящен описанию алгебраического приема, с помощью которого можно легко утроить количество d вычисляемых цифр за не большую вычислительную «плату», не превосходящую вычислительным затратам по увелечению d на единицу предыдущем методом.

Лемма 2. Пусть натуральное число $N > 2$. Тогда

$$\sum_{a \in \mathbb{Z}_N^*} a \equiv 0 \,(\mathrm{mod}\, N).$$

В частности, эта сумма является четным числом для четного $N > 2$.

Доказательство. Поскольку $a \neq N/2$, все слагаемые можно разбить на пары $a + (N - a)$. $\square$

Лемма 3. Пусть натуральное число $N > 2$ обладает следующими двумя свойствами:
1) Если N делится на 2, то оно имеет простой делитель вида $4k + 1$ или более чем один различных простых делителя, т.е., не является числом вида $2^a p^b$, где $a \geqslant 1$, $b \geqslant 0$, и простое $p = 4k - 1$.
2) Если оно делится на 3, то оно имеет простой делитель вида $6k + 1$.
Тогда

$$\sum_{a \in \mathbb{Z}_N^*, a < N/2} a^2 \equiv 0 \,(\mathrm{mod}\, N).$$

Доказательство. Если число N является степенью простого числа: $N = p^\alpha$, то удвоенная $(\mathrm{mod}\, N)$ сумма может быть вычислена явно:

$$\sum_{a \in \mathbb{Z}_N^*} a^2 = \frac{(p-1)(2p^{2\alpha-1} - 1)p^\alpha}{6}\,.$$

В общем случае разложим число N на простые множители: $N = p^\alpha q_1^{\alpha_1} \cdot \ldots \cdot q_m^{\alpha_m}$. Нам достаточно проверить сравнение по модулю степени каждого простого множителя. Проверим сравнение по модулю p^α. Согласно китайской теореме об остатках

$$\sum_{a \in \mathbb{Z}_N^*} a^2 \mod p^\alpha = \varphi(q_1^{\alpha_1}) \cdot \ldots \cdot \varphi(q_m^{\alpha_m}) \sum_{a \in \mathbb{Z}_{p^\alpha}^*} a^2 \mod p^\alpha\,.$$

Явно выписав функцию Эйлера φ и сумму квадратов, получаем:

$$\sum_{a \in \mathbb{Z}_N^*} a^2 \mod p^\alpha = \frac{(p-1)(2p^{2\alpha-1} - 1)p^\alpha}{6} \prod_j^m \big(q_j^{\alpha_j - 1}(q_j - 1)\big) \mod p^\alpha\,.$$

При $p > 3$ это выражение имеет остаток нуль из за множителя p^α. При $p = 3$ это выражение имеет остаток нуль при условии, что найдется простой множитель q_j вида $6k + 1$ и тем самым "добирается" еще одна степень тройки. При $p = 2$ нам нужно "добрать" две степени двойки. Это достигается двумя простыми множителями либо одним вида $4k + 1$. $\square$

Лемма 3а. Пусть $N = 2^a p^b$, где p — простое вида $4k - 1$ и оба показателя a и b больше нуля. Тогда

$$\sum_{a \in \mathbb{Z}_N^*, a < N/2} a^2 \equiv \frac{N}{2} \,(\mathrm{mod}\, N).$$

Доказательство вполне аналогично доказательству предыдущей леммы, поэтому не приводится.

Лемма 4. Пусть натуральное число $N > 2$. Тогда

$$\sum_{i < j \in Z_N^*} i \cdot j \equiv - \sum_{a \in \mathbb{Z}_N^*, a < N/2} a^2 \,(\mathrm{mod}\, N).$$

Доказательство. Используем тождество

$$2 \sum_{i < j \in \mathbb{Z}_N^*} ij = (\sum_{i \in \mathbb{Z}_N^*} i)^2 - (\sum_{i \in \mathbb{Z}_N^*} i^2)\,.$$

Для нечетных N, рассмотрим его $\mod N$ и учитывая, что $a^2 \equiv (N - a)^2 \mod N$, умножим на элемент обратный к 2 в $\mathbb{Z}_N^*$. Для четных N, рассмотрим его $\mod 2N$ и учитывая, что $a^2 \equiv (N-a)^2 \mod 2N$, поделим на 2, получив сравнение $\mod N$. Применив лемму 2, завершаем доказательство. $\square$

Лемма 5. Для каждого натурального числа $N > 2$ обозначим

$$P_0(N) = \prod_{a \in \mathbb{Z}_N^*} a\,, \quad P_1(N) = P_0(N) \sum_{i \in \mathbb{Z}_N^*} \frac{1}{i}\,, \quad P_2(N) = P_0(N) \sum_{i < j \in \mathbb{Z}_N^*} \frac{1}{ij}\,.$$

Тогда при $N > 2$ имеем:

$$P_1(N) \equiv NP_2(N) \equiv -NP_0(N) \sum_{a \in \mathbb{Z}_N^*, a < N/2} a^2 \mod N^2\,.$$

Доказательство. Отметим, что $\mathbb{Z}_N^*$ — множество обратимых элементов кольца $\mathbb{Z}_N$, а деление на обратимый элемент кольца это все равно, что умножение на его обратный. Пусть k_i обозначает вычет обратный к $i \pmod N$ Тогда $P_0(N)/(ij) \equiv P_0(N)k_ik_j \mod N$. Следовательно

$$P_2(N) \equiv P_0(N) \sum_{i<j\in\mathbb{Z}_N^*} k_ik_j \equiv P_0(N) \sum_{i<j\in\mathbb{Z}_N^*} ij \equiv -P_0(N) \sum_{a\in\mathbb{Z}_N^*, a<N/2} a^2 \mod N.$$

Здесь было использовано, что $\sum_{i<j\in\mathbb{Z}_N^*} k_ik_j = \sum_{i<j\in\mathbb{Z}_N^*} ij$, (суммируется одно и тоже множество слагаемых, — это сумма произведений неупорядоченных пар обратимых элементов кольца $\mathbb{Z}_N^*$) и лемма 4.

Вычислим значение $P_1(N) \mod N^2$. Разбив сумму $\sum_{i\in\mathbb{Z}_N^*} \frac{1}{i}$ на слагаемые $\frac{1}{i} + \frac{1}{N-i}$ мы получим:

$$P_1(N) = NP_0(N) \sum_{i\in\mathbb{Z}_N^*, i<N/2} \frac{1}{i(N-i)}.$$

Пусть $x_i = \frac{P_0(N)}{i(N-i)} \bmod N$. Нужно вычислить $\sum\limits_{i\in\mathbb{Z}_N^*, i<N/2} x_i \bmod N$. Имеем: $i(N-i)x_i = P_0(N) \mod N$ или $i^2x_i = -P_0(N) \mod N$. Пусть k_i обозначает вычет обратный к $i \pmod N$. Тогда $x_i = -k_i^2P_0(N) \mod N$. Если i пробегает все обратимые вычеты $\mathbb{Z}_N^*$, то k_i тоже пробегает все обратимые вычеты. Кроме этого,

$$\sum_{i\in\mathbb{Z}_N^*, i<N/2} i^2 \equiv \sum_{i\in\mathbb{Z}_N^*, i<N/2} k_i^2 \mod N.$$

В самом деле, в каждой сумме из каждой пары a^2, $(N-a)^2$ взято ровно по одному слагаемому. Поэтому $\sum\limits_{i\in\mathbb{Z}_N^*, i<N/2} x_i = -P_0(N)\Big(\sum\limits_{j\in\mathbb{Z}_N^*, j<N/2} j^2\Big) \mod N$. □

Лемма 6. Пусть натуральное число N не является степенью числа 2 и либо не делится на 3, либо делится на 3 но тогда и на некоторое простое число вида $6k+1$. Тогда остаток

$$\prod_{a\in\mathbb{Z}_N^*} (kN+a) \pmod{N^3}$$

не зависит от $k \in \mathbb{Z}$.

Доказательство. Разложим это выражение по степеням N:

$$\prod_{a\in\mathbb{Z}_N^*} (kN+a) = k^2N^2P_2(N) + kNP_1(N) + P_0(N) \pmod{N^3},$$

где $P_0(N) = \prod_{a\in\mathbb{Z}_N^*}(a)$, $P_1(N) = P_0(N)\sum_{i\in\mathbb{Z}_N^*} \frac{1}{i}$, $P_2(N) = P_0(N)\sum_{i<j\in\mathbb{Z}_N^*} \frac{1}{ij}$.

По лемме 5

$$k^2N^2P_2(N) + kNP_1(N) = -k(k+1)N^2P_0(N) \sum_{a\in\mathbb{Z}_N^*, a<N/2} a^2 \mod N^3.$$

По леммам 3 и 3а имеем, что

$$\text{либо} \sum_{a\in\mathbb{Z}_N^*, a<N/2} a^2 \equiv 0 \mod N, \quad \text{либо} \sum_{a\in\mathbb{Z}_N^*, a<N/2} a^2 \equiv \frac{N}{2} \mod N.$$

Поскольку $k(k+1)$ — четно, то $k^2N^2P_2(N) + kNP_1(N) \equiv 0 \mod N^3$. □