Компьютерные инструменты в образовании, 2021
№ -: 1–53
УДК: 51, 510, 511, 512, 004, 003
http://ipo.spb.ru/journal
doi:

# КОМПЬЮТЕР КАК НОВАЯ РЕАЛЬНОСТЬ МАТЕМАТИКИ: V. ЛЕГКАЯ ПРОБЛЕМА ВАРИНГА

Н. А. Вавилов
СПбГУ

**Аннотация**

В этой части я продолжаю обсуждать роль компьютера в современных исследованиях по аддитивной теории чисел, в первую очередь по *легкой* проблеме Варинга. Эта проблема состоит в нахождении для каждого натурального $k$ минимального $s = v(k)$ такого, что все натуральные числа $n$ могут быть представлены как суммы $k$-х степеней целых чисел $n = \pm x_1^k \pm \ldots \pm x_s^k$ в количестве $s$ штук *со знаками*. Как оказалось, эта задача намного сложнее исходной проблемы Варинга и теснейшим образом связана с несколькими другими задачами арифметической и диофантовой геометрии. В настоящей статье обсуждаются различные аспекты этой классической задачи и нескольких близких проблем — рациональной проблемы Варинга, проблемы Варинга для конечных полей, проблемы Варинга для других числовых колец, проблемы Варинга для многочленов, с особым акцентом на связь с полиномиальными тождествами и роль компьютеров в их решении. К настоящему времени решение этих проблем близко не завершено и предоставляет широчайшие возможности для использования этого материала в образовании и самостоятельного эксперимента, в том числе на уровне бытовых компьютеров.

**Ключевые слова:** *суммы степеней со знаками, легкая проблема Варинга, суммы кубов, рациональная проблема Варинга, тождества типа Фролова, проблема Варинга для числовых полей, проблема Варинга для многочленов, полиномиальная компьютерная алгебра*

**Цитирование:** Н. А. Вавилов Компьютер как новая реальность математики // Компьютерные инструменты в образовании, 2021. № -. С. 1–53 .

**Благодарности:** *Настоящая статья возникла в процессе работы над грантом РФФИ 19-29-14141.*

## 1. ВВЕДЕНИЕ

Настоящий текст является непосредственным продолжением предыдущих работ автора [1–4], посвященных влиянию компьютеров на понимание математики и, в особенности, на развитие теории чисел. Общий пафос этих статей состоял в следующем. В конце XIX и начале XX века произошло радикальное переосмысление математики, в результате которого изменились сами формулировки классических задач. Сегодня, с появлением компьютеров, мы можем снова восстановить недостижимый с XVIII века баланс идей и вычислений. В том числе, решить эти задачи именно в том духе, как их ставили классики XVII–XIX веков — или даже в еще более точном смысле!

В частности, в работе [2] мы обсуждали различные аспекты классической проблемы Варинга и роль компьютеров и, более широко, *вычислений* в ее решении. Напомним, что эта проблема, в той форме, как ее сформулировали математики XVIII века, состояла в следующем.

• **Проблема Варинга**. Найти для каждого натурального $k$ *наименьшее* натуральное $s = g(k)$ такое, что любое натуральное число $m$ можно представить как сумму $k$-х степеней *неотрицательных* целых чисел

$$m = x_1^k + \ldots + x_s^k$$

в количестве $s$ штук.

В действительности в 1770–1772 годах Эдвард Варинг и Иоганн Альбрехт Эйлер высказали *точную гипотезу*.

• **Идеальная проблема Варинга**. Доказать, что $g(3) = 9$, $g(4) = 19$, и вообще для любого натурального $k$ имеет место равенство

$$g(k) = 2^k + q - 2,$$

где $3^k = q \cdot 2^k + r$, $1 \leq r \leq 2^k - 1$.

В такой форме эта проблема была *в основном* решена в 1909–1936 годах, для $k = 3$ Виферихом, а для $k \geq 7$ Диксоном и Пиллаем. Последние три значения $g(6) = 73$, $g(5) = 37$ и $g(4) = 19$ вычислены, соответственно, в 1940, 1964 и 1984 году, см. [2].

Разумеется, до этого в 1909 году Гильберт *переформулировал* проблему Варинга следующим образом, и сам же ее в такой форме и решил, не предъявив, впрочем, *никакого* значения $s$.

• **Дешевая проблема Варинга**. Доказать, что для каждого натурального $k$ существует *какое-то* натуральное $s$ такое, что любое натуральное число $m$ можно представить как сумму $k$-х степеней *неотрицательных* целых чисел $m = x_1^k + \ldots + x_s^k$ в количестве $s$ штук.

Однако в XIX–XX веках эта проблема была переформулирована более интересным образом и в таком виде все еще *весьма* далека от своего решения.

• **Асимптотическая проблема Варинга**. Найти для каждого натурального $k$ наименьшее натуральное $s$ такое, что *почти все* натуральные числа $m$ можно представить как сумму $k$-х степеней *неотрицательных* целых чисел $m = x_1^k + \ldots + x_s^k$ в количестве $s$ штук.

Разумеется, конкретный смысл этой проблемы зависит от понимания здесь выражения почти все. Вот два основных толкования.

• По **Якоби**, как “все, кроме конечного числа” = “все начиная с некоторого места”. Соответствующее минимальное значение $s$ обозначается $G(k)$.

• По **Харди—Литтлвуду**, как “почти все в смысле натуральной плотности”. Исключений может быть бесконечно много, но с ростом $n$ они встречаются все реже, их количество растет как $o(n)$. Соответствующее минимальное значение $s$ обозначается $G^+(k)$.

Однако, кроме известного еще Лагранжу случая сумм квадратов,

$$G^+(2) = G(2) = g(2) = 4,$$

и еще 4–5 примеров, асимптотическая проблема не решена ни в том, ни в другом смысле.

Более того, Харди, Литтлвуд и их последователи далее уточнили и конкретизировали смысл ответа (выполнение *асимптотических формул* специального вида для количества представлений). С другой стороны, проблеме в смысле Якоби тоже придают теперь гораздо более точный смысл.

• **Алгоритмическая проблема Варинга**. Найти *точное место*, начиная с которого каждое натуральное число есть сумма $\leq G(k)$ неотрицательных $k$-степеней и *полный список* исключений.

В *таком* виде эти проблемы решены еще ровно для одного случая, сумм биквадратов,

$$g(4) = 19, \qquad G(4) = 16, \qquad G^{+}(4) = 15,$$

и близко не решены даже для сумм кубов или пятых степеней. Все это детально обсуждается в [2], где можно найти много дальнейших ссылок.

В этой части мы планируем обсудить еще несколько известных задач в том же направлении, также сформулированных в XVIII, XIX и начале XX века, где апостериори роль компьютеров оказалась еще гораздо больше.

В той или иной форме все они связаны со следующей центральной задачей, которую [Эдвард] Майтланд Райт *злополучно*[1] окрестил [более] *легкой* проблемой Варинга = **easier Waring problem**, [275].

• **Легкая проблема Варинга**. Найти для каждого натурального $k$ наименьшее натуральное $s = v(k)$ такое, что любое целое число $m$ можно представить как сумму $k$-х степеней целых чисел *со знаками*[2]

$$n = \pm x_1^k \pm \ldots \pm x_s^k$$

в количестве $s$ штук.

Для нечетного $k$ эта задача отличается от исходной проблемы Варинга тем, что теперь мы ищем *целые* решения, а не только натуральные, для четных $k$ разница еще гораздо больше. Райт называл эту проблему “легкой” потому, что ее *дешевая* версия с экспоненциальной оценкой $v(k)$ совершенно тривиальна, [119].

В то же время, с *вычислительной* точки зрения сама эта задача *значительно* сложнее исходной проблемы Варинга, так как там $|x_1|, \ldots, |x_s|$ были ограничены по модулю $\sqrt[k]{n}$, на чем и основан метод Виноградова. Теперь никакого такого ограничения нет, так что $|x_1|, \ldots, |x_s|$ могут превосходить $n$ на много порядков.

По-французски эта задача называется **означенной проблемой Варинга** = *le problème de Waring signé*[3]. В отличие от исходной *трудной* проблемы Варинга, которая, как мы узнали в [2], решена на 99.9999%, *легкая* проблема Варинга не решена к настоящему моменту *ни для одного* нетривиального случая, даже для $k = 3$, несмотря на сотни опубликованных на эту тему работ. Скажем, даже возможность представления *индивидуальных* чисел в виде сумм трех кубов целых часто требует чрезвычайно серьезных вычислений, которые были ЗАВЕДОМО НЕДОСТУПНЫ МАТЕМАТИКАМ ПРЕДШЕСТВУЮЩИХ ВЕКОВ.

[1] Лоран Абсигер делает по этому поводу такое замечание: “Le problème de Waring signé (que Wright [275]. avait *malencontreusement* baptisé problème de Waring "plus facile"), [116].

[2] Впрочем, многие профессионалы называет такую сумму со знаками просто **суммой $k$-степеней**, а фигурирующую в обычной проблеме Варинга сумму положительных степеней — **чистой суммой $k$-х степеней**.

[3] Или по-русски все же принято говорить **проблема Варинга со знаками**? В алгебре мы рутинно переводим *signed base* как *означенный базис* и т.д. Это удобно, но мне трудно судить, насколько такое словоупотребление общепринято и понятно за пределами профессионального арго.

Так, еще в 1953 году Морделл предложил [185] найти дальнейшие решения уравнения $x^3 + y^3 + z^3 = 3$, кроме очевидных,

$$1^3 + 1^3 + 1^3 = 3, \qquad 4^3 + 4^3 - 5^3 = 3.$$

Некоторые авторы даже высказывали предположение, что никаких других решений у этого уравнения нет, см., например, [228, 229].

На самом деле, как выяснилось в 2019–2021 годах, решений у него несколько больше, но и сами эти решения *гораздо* больше. Вот, для примера, следующее самое маленькое из них

$$569936821221962380720^3 - 569936821113563493509^3 - 472715493453327032^3 = 3$$

см. [42]. Для его поиска была создана сеть распределенных вычислений, состоящая из 400.000–500.000 компьютеров.

Кроме самой этой задачи мы планируем обсудить также несколько дальнейших тесно связанных с ней задач, в частности, **рациональную проблему Варинга**, в которой предлагается найти рациональные $x_1, \dots, x_s$, и **проблему Варинга в нуле**, которая вкючает в себя как очень частные случаи великую теорему Ферма и являющуюся ее обобщением проблему Эйлера.

• **Рациональная проблема Варинга.** Найти для каждого натурального $k$ *наименьшее* натуральное $s = \rho(k)$ такое, что любое рациональное число $x$ можно представить как сумму/разность $k$-х степеней рациональных чисел

$$x = \pm x_1^k \pm \dots \pm x_s^k$$

в количестве $s$ штук.

• **Положительная рациональная проблема Варинга.**. Найти для каждого натурального $k$ *наименьшее* натуральное $s$ такое, что любое положительное рациональное число $x$ можно представить как сумму $k$-х степеней *неотрицательных* рациональных чисел

$$x = x_1^k + \dots + x_s^k.$$

В свою очередь, эти задачи теснейшим образом связаны с еще одной знаменитой классической задачей, которой будет посвящена следующая статья этой серии.

• **Проблема Варинга в нуле.** Найти для каждого натурального $k$ наименьшее $s = \theta(k)$ такое, что 0 допускает *нетривиальное* представление в виде сумм/разностей $k$-х степеней целых чисел

$$\pm x_1^k \pm x_2^k \pm \dots \pm x_s^k = 0.$$

Существование пифагоровых троек означает, что $\theta(2) = 3$. Великая **теорема Ферма** [270] утверждает, что $\theta(k) \geq 4$ для всех $k \geq 3$. Используя геометрию эллиптических кривых, де Ферма и Эйлер [до некоторой степени] доказали, что уравнения Ферма $x^3 + y^3 = z^3$ и $x^4 + y^4 = z^4$ не имеют нетривиальных решений и, таким образом, $\theta(3) = 4$ (кубы Платона!) и $\theta(4) \geq 4$.

Эйлер даже высказал гораздо более сильное предположение, что $\theta(k) \geq k + 1$, которое оказалось *безнадежно* неверным, как в идейном, так и в фактическом плане. В частности, уже $\theta(4) = 4$ и $4 \leq \theta(5) \leq 5$. Однако точное значение $\theta(5)$ до сих пор не известно!

Оказывается, получение оценок во всех этих задачах связано с построением **полиномиальных тождеств** некоторого специального вида. В свою очередь, многие из этих тождеств связаны с решением, казалось бы, совершенно искусственных задач, исторически рассматривавшихся в **развлекательной математике** = recreational mathematics.

• **Taxicab numbers** и, более общо, **equal sums of like powers**, т.е. поиск натуральных решений степенных уравнений

$$x_1^k + \ldots + x_s^k = y_1^k + \ldots + y_t^k,$$

• **Проблема Пруэ[4]—Тарри[5]—Эскотта[6]**, коротко **проблема PTE** о существовании *совместных* решений у систем степенных уравнений

$$\begin{gathered} x_1 + \ldots + x_s = y_1 + \ldots + y_s, \\ x_1^2 + \ldots + x_s^2 = y_1^2 + \ldots + y_s^2, \\ \ldots\ldots\ldots\ldots\ldots \\ x_1^k + \ldots + x_s^k = y_1^k + \ldots + y_s^k. \end{gathered}$$

Как и в работах [2–4] я не делаю *никакой* попытки дать хоть сколь-нибудь *систематический* обзор литературы — в том, что касается вариантов и и обобщений проблемы Варинга это было бы совершенно невозможно сделать, по нескольким причинам.

• С научной точки зрения, все эти задачи относятся к **арифметической геометрии** или, еще точнее, к ее центральному разделу, **диофантовой геометрии**, занимающемуся изучением целых и рациональных точек на алгебраических многообразия. В этой области опубликованы многие десятки тысяч работ, большинство из которых предполагает совершенно другой уровень математической софистикации. При этом, строго говоря, вообще непонятно, где ставить отсечку. Например, относится ли изучение произвольных **диагональных уравнений** — в том числе с произвольными коэффициентами, неоднородных, и т.д. — к задачам варинговского типа?

• В совершенно другом направлении имеется столь же гигантская и необозримая литература в аналитическом духе, связанная с оценками, асимптотиками и всем таким,

[4]Эжен Пруэ, 1817–1867, был учителем математики и репетитором в l'École Polytechnique. Его мемуар с первым решением проблемы PTE, то, что сегодня известно как последовательность Пруэ—Туэ—Морзе, был в 1851 году представлен в Парижскую академию наук, но в 1852 году возвращен автору и так и не был никогда опубликован. Его результаты были частично переоткрыты Тарри и Эскоттом в 1910–1912 годах. После смерти Олри Теркема [4] в 1862 году Пруэ стал коредактором "Nouvelles annales de mathématiques", где и опубликовано большинство его геометрических работ. Очень забавно читать там все его антикватернионизмы: "…inventer des expressions qui par elles-mêmes n'offrent aucun sens à l'esprit, et chercher ensuite à leur en donner un par ce que l'on appelle une interprétation géométrique, n'est-ce pas comme si, après avoir construit une belle phrase, on cherchait quelle pensée on pourrait bien y mettre?"

[5]В большинстве научно-популярных текстов по-русски ошибочно пишут "Тэрри". На самом деле, Гастон Тарри, 1843–1913, с ударением на последнем слоге, был любителем математики, чиновником французской финансовой администрации, *Service des Contributions directes de l'Administration des Finances*, в Алжире. Он был автором вполне серьезных работ по комбинаторике, самой знаменитой из которых является решение в 1901 году проблемы Эйлера о 36 офицерах.

[6]Эдвард Бринд Эскотт Jr., 1868–1946, был преподавателем математики и актуарием в страховых компаниях. Он уже упоминался в [3] в связи с открытием 233 дружественных пар. В свое время чрезвычайно популярной была головоломка Escott sliding-block puzzle, о которой много писал Мартин Гарднер (она изображена, например, на задней обложке журнала "Квант", 1971, no.6). Трудность головоломки состоит в том, что 6 из 10 плашек имеют L-образную форму разных ориентаций и поворачивать их нельзя, даже если для этого есть место.

разобраться к которой часто не проще, чем в геометрических работах. Например, с аналитической точки зрения оценка количества решений проблемы PTE называется **теоремой Виноградова о среднем** [200], и это вполне высоколобый **гармонический анализ**, преобразование Радона и все такое.

• Даже если ограничиваться элементарными результатами, непосредственно посвященными суммам и чистым суммам степеней, изрядная доля этих работ опубликована в журналах учебного, популярного или развлекательного характера, которые невозможно найти по обычным математическим базам данных.

Поэтому я ограничиваюсь в основном классическими результатами, основанными на элементарных и *алгебраических* методах, и теми современными исследованиями, где использовался *компьютерный* поиск и эксперимент. Как и первая часть [2], эта вторая часть имеет не научный и не исторический, а именно *методологический* и *методический* характер. Цель ее троякая:

• Напомнить несколько классических задач варинговского типа, которые были сформулированы сотни лет назад. В отличие от исходной проблемы Варинга, эти более "легкие" задачи не решены. Более того, у нас часто нет даже гипотез о том, как должен выглядеть ответ, а многие оценки не удалось уточнить за последние 80–90 лет.

• Привлечь внимание к *широчайшим* возможностям использования этого материала в образовании. В нашем курсе "Математика и компьютер" [5, 146] мы фактически предлагали большое количество задач на эти темы, ровно потому, что они классические, занимательные, легко формулируются, легко программируются, а в то же время никаких простых общих ответов на них нет.

• Сформулировать варианты проблемы Варинга как вызов для **полиномиальной компьютерной алгебры** — в действительности настоящая статья является расширенной версией моего доклада [261] на PCA-2020. Большинство полученных за последний век явных вычислений и улучшений оценок здесь обусловлено открытием все более изощренных **полиномиальных тождеств**.

Две последние цели тесно связаны между собой. Возможности компьютерного эксперимента, причем как для профессиональных математиков, так и для профессиональных программистов и начинающих, здесь *огромные*. Мне кажется, что как поиск решений конкретных диофантовых уравнений, так и поиск полиномиальных тождеств требуемого типа (для получения точных оценок в рациональной и легкой проблемах Варинга, их аналогов в числовых полях, в положительной характеристике и т.д.) могли бы стать *замечательными* проектами распределенных вычислений как для энтузиастов, так и при тестировании нового поколения систем компьютерной алгебры.

## 2. СУММЫ РАЦИОНАЛЬНЫХ КУБОВ

### 2.1. Суммы трех рациональных кубов

Еще Платон знал, что сумма кубов сторон египетского треугольника сама является кубом, $3^3+4^3+5^3=6^3$, о чем он упоминает в своем диалоге "Politéia", известном по-русски как "Государство" или "Республика". Кстати, это самое маленькое решение уравнения $x^3+y^3+z^3=w^3$ в натуральных числах, следующее $1^3+6^3+8^3=9^3$. В частности, это дает представление 1 как суммы трех кубов *рациональных* чисел:

$$1=\left(\frac{3}{6}\right)^3+\left(\frac{4}{6}\right)^3+\left(\frac{5}{6}\right)^3.$$

• Очевидно, что *каждое* рациональное число является суммой *четырех* кубов рациональных чисел, причем бесконечным числом способов, это школьная алгебра:

$$x=\left(\frac{x+6t^3}{6t^2}\right)^3+\left(\frac{x-6t^3}{6t^2}\right)^3+\left(\frac{-x}{6t^2}\right)^3+\left(\frac{-x}{6t^2}\right)^3.$$

• Диксон [77], 727–728, упоминает, что, используя несколько раз тождество

$$u^3-v^3=u^3\left(\frac{u^3-2v^3}{u^3+v^3}\right)^3+v^3\left(\frac{2u^3-v^3}{u^3+v^3}\right)^3,$$

Гульельмо Либри в 1829 году вывел отсюда, что каждое положительное рациональное число является суммой четырех кубов *положительных* рациональных чисел — по крайней мере так утверждал сам Либри на заседании Парижской Академии Наук в 1840 году (см. следующий пункт).

• Не позже 1859 года Виктор-Амадей Лебег предложил *явную формулу*, выражающую каждое положительное рациональное число как сумму четырех положительных рациональных кубов:

$$x=\left(\frac{x}{6y^2}\right)^3\left((2-a)^3+a^3(b-1)^3+b^3(c-1)^3+c^3\right),$$

где $y$ — произвольное рациональное число такое, что $x/12<y^3<x/6$, а

$$a=1+\frac{6m^3}{n},\qquad b=2-\frac{3}{a^3+1},\qquad c=2-\frac{3}{b^3+1}.$$

см. [163] — напомним, что этот текст уже упоминался в [2] в связи с результатом Лиувилля о суммах биквадратов!

Используя `Mathematica` я проверил, что формула Лебега верна — рекомендую всем сомневающимся проделать то же самое и посмотреть, какие коэффициенты при этом возникают!

• На самом деле, если не накладывать ограничение на знаки, классически известно, что каждое рациональное число является суммой *трех* кубов рациональных чисел. Этот поразительный результат был открыт С. Райли, школьным учителем из Лидса, в 1825 году, доказательства можно найти в [77, 119]. Его обсуждают, в частности Ричмонд, Морделл и Белл. Век спустя Герберт Ричмонд объяснил тождество Райли

$$x=\left(\frac{x^3-3^6}{3^2x^2+3^4x+3^6}\right)^3+\left(\frac{-x^3+3^5x+3^6}{3^2x^2+3^4x+3^6}\right)^3+\left(\frac{3^3x^2+3^5x}{3^2x^2+3^4x+3^6}\right)^3$$

и написал аналогичные тождества с параметрами, см. [71, 220]. Это наблюдение является одной из отправных точек при изучении рациональных решений кубических уравнений, т.е. рациональных точек на кубических поверхностях, см. [11, 12].

В § 4 мы займемся решениями уравнения $x^3+y^3+z^3=m$ в *целых* числах и это окажется уже гораздо более трудной задачей.

### 2.2. Талантливый мистер Либри

Разумеется, упомянутый в предыдущем пункте Либри, это граф Гульельмо Брутус Ичилиус Тимолеоне Либри-Каруччи делла Соммайа. Сама жизнь Гульельмо Либри читается как роман. Друг (и покровитель) Либри Франсуа Гизо говорил: “Vous voulez des romans? Lisez de l’histoire.” Я узнал об *афере Либри* и противостоянии Либри и Лиувилля из статьи Сергея Сергеевича Демидова [75][7].

В связи с тем, что известно как *дело Либри* = *l’affaire Libri*, генеральной репетиции дела Дрейфуса, принято обесценивать Либри как математика. Этой истории посвящена *огромная* литература, при этом современные французские и итальянские авторы излагают ее с диаметрально противоположных позиций. В отношении фактологии я следовал, в основном, [74, 173], где приведены многие сотни дальнейших ссылок.

Граф Либри, 1803–1869, происходил из старинного флорентийского рода[8]. Потомственный революционер, в 1820-е годы он присоединился к карбонариям и в 1830 году был обвинен в подрывной деятельности: “il se rendit coupable d’opinions sinon d’actions taxées, dans ce temps, de subversives”, [48]. Перспектива стать узником совести его не вдохновила и он предпочел бежать во Францию.

Во Франции он натурализовался, приобрел множество друзей, и сделал совершенно блестящую карьеру. Уже в 1833 году он был избран в Парижскую Академию Наук по классу геометрии как преемник Лежандра[9]. При этом он получил в первом туре 37 голосов, против 17 у Жана-Мари Дюамеля. В 1843 году[10] он выиграл позицию в *Collège de France* у Лиувилля и Коши. Вот результаты голосования по турам:

| | Коши | Либри | Лиувилль |
|---|---|---|---|
| Тур 1 | 3 | 12 | 9 |
| Тур 2 | 1 | 11 | 12 |
| Тур 3 | 1 | 13 | 10 |

Для объективности стоит заметить, что время было летнее, присутствовало только 24 академика, остальные 28 поехали обедать в деревню. Таким образом, больше половины академиков не голосовало ни за одного из кандидатов, и им достаточно было получить больше половины от числа присутствовавших. Особенно радует один голос, поданный за Коши (вероятно, по ошибке, либо самим Коши). Чтобы было совсем смешно, в 1850-м году, после того как Либри был официально осужден во Франции и *изгнан из Академии*, именно на эту позицию избрали Габриэля Ламе!

Этот конкурс стал началом конца Либри. Коши был совершенно взбешен и начал действовать своим обычным образом, через клерикальные круги. Повод к этому давало то, что в 1841 году Либри был назначен “Secrétaire de la Commission du Catalogue général

[7] Сергей Сергеевич подробно обсуждает эту тему в своем недавнем докладе `http://www.mathnet.ru/php/seminars.phtml?presentid=29388&option_lang=rus`.

[8] “А у них война гвельфов и гибеллинов сплошь отражена на таких больших гобеленах, что смотри хоть всю жизнь подряд — нить окажется слишком длинной, слишком соленой, слишком непостоянной.”

[9] Раз уж мы обсуждаем роль компьютеров в математике, упомянем еще одно весьма необычное приложение. Несколько поколений математиков с детства знают портрет Лежандра, в профиль с косичкой. Как выяснилось, это не портрет математика Адриена-Мари Лежандра, 1752–1833, а портрет депутата Конвента мясника Луи Лежандра, 1752–1797. Это заметили в 2005 году студенты университета Страсбурга с использованием поисковых систем, а в 2008 году в архивах Академии был обнаружен акварельный портрет Адриена-Мари Лежандра, см. [80]. Ничего общего! Embarassing!

[10] В [75] утверждается, что Либри получил кафедру в *Collège de France* в 1832 году. Это не так, в 1832 году он читал там свой первый курс, а кафедру получил в 1843 году.

des manuscrits des bibliothèques publiques de France". В 1846 году он был анонимно обвинен в хищении книг и рукописей из муниципальных библиотек, которые он инспектировал. Долгое время его друзьям и покровителям удавалось предотвращать предъявление прямого обвинения.

Но тут внезапно случилась февральская революция 1848 года и, не дожидаясь 29 февраля, Либри, вместе с 18 сундуками книг и рукописей, сбежал в Англию. Дальше началась обычная французская комедия на тему *esprit de corps* — то, что по-английски называется *team spirit*, а по-русски *честь мундира*. В 1850 году он был *заочно* приговорен французским судом к 10 годам заключения. Несмотря на протесты таких людей как Проспер Мериме и Виктор Гюго, приговор так никогда и не был отменен — французские магистраты не могут ошибаться, особенно в отношении иностранцев.

Впрочем, с точки зрения излагаемой здесь истории не имеет никакого значения, крал Либри книги из муниципальных библиотек, или нет[11]. Сами эти библиотеки образовались случайным образом в 1797 году из выморочного имущества французских аристократов. Внезапно ставшие достоянием городов коллекции не были надлежащим образом описаны, не охранялись, содержались в чудовищных условиях. Легко представить себе, что Либри *мог* считать, что он ВОССТАНАВЛИВАЕТ СПРАВЕДЛИВОСТЬ и *спасает* эти книги и документы, конфискуя их у недостойных и случайных ап[п]роприаторов — и, скорее всего, именно так и считал!

В результате развивавшегося начиная с 1837 года конфликта с Лиувиллем[12], интересы Либри сместились из математики в историю математики. Сегодня большинство из нас воспринимают его как автора *одной* книги [168]. Это еще один совершенно феерический опус, представление о котором не может дать ни один перевод — примерно половина текста там состоит из примечаний на латыни и итальянском. Независимо от того, что мы думаем о Гульельмо Либри как математике, человеке и историке математики, это *великая* книга. Что потрясает в первую очередь, это совершенно экстраординарный уровень свободы, с которой он распоряжается *французским* языком.

Я не мог бы резюмировать свои впечатления от ее чтения точнее, чем это сделал в 1900 году Морис Кантор: "Ces précautions prises, il est indiscutable que Libri a rendu des services énormes à l'Historiographie des Mathématiques. Il a étudié nombre de manuscrits dont il donne des extraits pour la plus grande partie trés exacts, et, comme je le disais déjà, il manie la langue avec un art tout à fait hors ligne. Son *Histoire des Mathématiques en Italie* se lit comme un roman, même dans les parties où elle n'en est pas un" , [48].

Либри пытался блокировать избрание Лиувилля в Академию, потом в жесткой борьбе выиграл у него позицию в *Collège de France*. Понятно, что Лиувилль изучал *все* математические работы Либри под микроскопом. Отсюда произошел и интерес Лиувилля к мемуарам Абеля и Галуа, и его результаты по проблеме Варинга. *Сегодня* мы воспринимаем Лиувилля как *несравнимо* более значительного математика. Конечно, он и был гораздо более сильным математиком и легко отжал Либри по всем фронтам.

Но я совершенно не уверен, что без этой работы Либри Лиувилль бы вообще заинтересовался проблемой Варинга.

[11]"An ethical sympathy in an artist is an unpardonable mannerism of style." Любые моральные оценки тем более недопустимы при обсуждении прошлого, "The past is a foreign country; they do things differently there."

[12]Собственно противоборство Лиувилля и Либри детально обсуждается в статье Каролины Эрхардт [84]. Очевидно, они перевели культуру математической дискуссии на совершенно новый уровень, особенно начиная с августа 1843 года: "Le seul mémoire ou M. Libri ait un peu développé ses méthodes ...est rempli d'assertions hasardées et même d'erreurs graves" — "M. Liouville avait même ajouté que toutes les démonstrations de M. Libri étaient fausses, mais ces paroles ont été un peu adoucies à l'impression dans le compte rendu."

## 3. РАЦИОНАЛЬНАЯ ПРОБЛЕМА ВАРИНГА

### 3.1. Решение дешевой рациональной проблемы Варинга

Если верить Диксону, первое решение рациональной проблемы Варинга — даже не в смысле Гильберта, а в гораздо более точном смысле — получил в 1851 году Плачидо Тарди [249], см. [77], p. 728 — потом то же тождество на тему “$2^n n!$ is the answer, what is the question” [113], снова появляется в работе[13] Огюста Бутена 1910 года, [77], p. 723.

Это решение является непосредственным обобщением формулы

$$4xy = (x+y)^2 - (x-y)^2,$$

из которой сразу вытекает, что любое рациональное число является разностью двух квадратов[14]:

$$x = \left(\frac{x+t^2}{2t}\right)^2 - \left(\frac{x-t^2}{2t}\right)^2.$$

Еще Гаусс [109] заметил, что эта формула следующим образом обобщается на кубы

$$24xyz = (x+y+z)^3 - (x+y-z)^3 - (x-y+z)^3 + (x-y-z)^3.$$

Разумеется, подставляя сюда *любые* $y, z$ такие, что $24yz$ является кубом, не обязательно $y = z = 3t^3$, как мы это делали выше, мы получим много представлений рационального числа как суммы четырех рациональных кубов.

Так вот, Тарди написал подобное **тождество Тарди** с $2^{k-1}$ слагаемым для *всех* степеней $k$. Следующий случай, явно приведенный в конце его статьи, это тождество для биквадратов[15]:

$$\begin{aligned}192xyzw = {} & (x+y+z+w)^4 - (x+y+z-w)^4 - (x+y-z+w)^4 - (x-y+z+w)^4 + \\ & (x+y-z-w)^4 + (x-y+z-w)^4 + (x-y-z+w)^4 - (x-y-z-w)^4.\end{aligned}$$

И вообще $k!2^{k-1}x_1 \dots x_k$ является суммой $2^{k-1}$ штук $k$-х степеней всевозможных выражений вида $x_1 \pm x_2 \pm \dots \pm x_k$, где знаки пробегаются независимо.

[13] Эти работы не проиндексированы ни в американской базе данных `MathSciNet`, ни в европейской `zbMath`, так что узнать про них невозможно, unless. Placido Tardy (именно так, на французский манер, более того, некоторые его статьи подписаны Placide Tardy) был довольно известным человеком в истории итальянской математики. Чрезвычайно внушают просто сами годы его жизни, 1816–1914. Журнал Annali di scienze matematiche e fisiche compilati da Barnaba Tortolini, в котором впервые опубликовано тождество Тарди, издавался в 1850–1857 годах, и полностью дигитализован на archive.org. В свою очередь, L’Intermédiaire des Mathématiciens издавался с 1894 до 1920 и потом снова с 1922 до 1925 год, но, к сожалению, пока дигитализован не полностью.

[14] Это было известно даже не Диофанту, а еще Эвклиду и составляет содержание предложения 5 его книги II. Скептики могут усомниться, так как Эвклид отдельно складывал длины, площади и объемы. Ну так у Эвклида это и записано как равенство двух площадей $xy + \big((x+y)/2 - y\big)^2 = \big((x+y)/2\big)^2$.

[15] Фактически вместо $(x-y-z-w)^4$ Тарди, конечно, пишет $(-x+y+z+w)^4$, в приведенной здесь форме это тождество приводит Бутен. Интересно, что дальше он суммирует по всем $2^k$ расстановкам знаков, т.е. по всем вершинам $k$-мерного куба, а не по половине из них, как это делает Тарди. Но нам сегодня проще всего воспринимать это тождество как суммирование по одной грани $k$-мерного куба. В качестве связи с [2] упомяну, что после обучения в Милане Тарди некоторое время учился в Париже у Лиувилля. Поэтому не вызывает никакого сомнения, что Лиувилль знал уже тождество Тарди со знаками, когда писал свое знаменитое тождество без знаков.

Отсюда, конечно, сразу следует, что каждое рациональное число является суммой *восьми* биквадратов рациональных чисел со знаками, причем многими способами. Точно так же, каждое рациональное число является суммой *шестнадцати* пятых степеней рациональных чисел, суммой *тридцати двух* шестых степеней рациональных чисел со знаками, и т.д.

Но в действительности, как мы вскоре увидим, отсюда вытекает гораздо более того!

### 3.2. Суммы четырех рациональных биквадратов, шести пятых степеней,...

Однако, как мы могли понять уже из случая кубов, получающаяся на пути Тарди оценка на количество слагаемых сильно завышена.

• Так, в 1911 году Роберт Норри [194] написал свое знаменитое **тождество Норри**

$$x=\left(\frac{a^2(a^8-b^8+2x)}{2(a^8-b^8)}\right)^4-\left(\frac{a^2(a^8-b^8-2x)}{2(a^8-b^8)}\right)^4+\left(\frac{2a^4x-b^4(a^8-b^8)}{2ab(a^8-b^8)}\right)^4-\left(\frac{2a^4x+b^4(a^8-b^8)}{2ab(a^8-b^8)}\right)^4,$$

которое до сих пор используется во многих работах на эту тему, см., например, [52, 102]. Из этого тождества вытекает, что каждое рациональное число является суммой *четырех* рациональных биквадратов со знаками.

В этом месте глава XXV второго тома диксоновской “Истории” внезапно обрывается. И в общем даже довольно понятно, почему. Написать от руки аналогичные тождества, дающие хорошие оценки для нескольких следующих степеней, хотя бы для $k=5,6,7,8,9$, это занятие не для слабых духом.

• В 1938 году Субба Рао [246] доказал, что $\rho(5)\le 8$. В 1988 году Аджай Чоудхри[16] [57] улучшил эту оценку до $\rho(5)\le 6$. Он пишет некоторое тождество от $t$ и $x$, левая часть которого является алгебраической суммой шести квадратов, а правая часть линейна по $x$ — и имеет степень 70 по $t$. Решая это тождество в `Mathematica`, получаем

$$\begin{aligned}
x&=\left(\frac{2-22t^{10}-80t^{20}-60t^{30}+20t^{40}+80t^{50}+58t^{60}+2t^{70}+x}{40t^8(-1-t^{10}+t^{30}+t^{40})}\right)^5\\
&+\left(\frac{2+40t^5-22t^{10}+40t^{15}-40t^{20}-20t^{30}-40t^{35}+20t^{40}-40t^{45}+40t^{50}+18t^{60}+2t^{70}+x}{40t^8(-1-t^{10}+t^{30}+t^{40})}\right)^5\\
&+\left(\frac{2+18t^{10}+40t^{20}+40t^{25}+20t^{30}+40t^{35}-20t^{40}-40t^{50}-40t^{55}-22t^{60}-40t^{65}+2t^{70}+x}{40t^8(-1-t^{10}+t^{30}+t^{40})}\right)^5\\
&-\left(\frac{2+58t^{10}+80t^{20}+20t^{30}-60t^{40}-80t^{50}-22t^{60}+2t^{70}+x}{40t^8(-1-t^{10}+t^{30}+t^{40})}\right)^5\\
&-\left(\frac{2-40t^5-22t^{10}-40t^{15}-40t^{20}-20t^{30}+40t^{35}+20t^{40}+40t^{45}+40t^{50}+18t^{60}+2t^{70}+x}{40t^8(-1-t^{10}+t^{30}+t^{40})}\right)^5\\
&-\left(\frac{2+18t^{10}+40t^{20}-40t^{25}+20t^{30}-40t^{35}-20t^{40}-40t^{50}+40t^{55}-22t^{60}+40t^{65}+2t^{70}+x}{40t^8(-1-t^{10}+t^{30}+t^{40})}\right)^5.
\end{aligned}$$

[16] Один из самых активных авторов по этой проблематике, опубликовавший за последние 30–35 лет около сотни статей. Вероятно, любитель, во всяком случае, во всех его работах, кроме самых недавних, в качестве адреса указаны Посольства и Высокие Комиссии Республики Индия в самых разных точках мира — Варшава, Сингапур, Бруней, и т.д. А в нескольких из них Чоудхри подписывается как Посол Республики Индия в Ливане.

В дальнейшем было получено много такого типа тождеств, например, тождества Рао, Чоудхри, Пиесаса, Васерштейна, Рейни, показывающие, что каждое рациональное число является суммой/разностью $\leq 8$ шестых степеней, $\leq 8$ седьмых степеней, $\leq 12$ восьмых степеней рациональных чисел и так далее. Их легко обработать таким же образом, доведя до явных ответов. Однако, помещать эти явные выражения для $x$ на стандартную журнальную страницу с ростом $k$ становится все труднее, поэтому в дальнейшем мы не будем даже пытаться решать их относительно $x$.

## 4. ЛЕГКАЯ ПРОБЛЕМА ВАРИНГА

Оказывается, рациональную проблему Варинга естественно рассматривать одновременно с легкой проблемой Варинга, получающиеся при этом оценки $v(k)$ и $\rho(k)$ тесно связаны между собой.

Напомним, что а настоящей проблеме Варинга разрешается складывать положительные $k$-е степени. Напротив, в легкой проблеме Варинга $k$-е степени натуральных чисел можно не только складывать, но и вычитать. Иными словами, речь идет о задаче представления натуральных $m$ в виде

$$m = \pm x_1^k \pm x_2^m \pm \ldots \pm x_s^k.$$

Это то, что в параграфе 21.7 книги Харди и Райта [119] называется “sums affected with signs”. Разумеется, для нечетных степеней это то же самое, что поиск решений обычного уравнения Варинга без знаков, но не в натуральных, а в целых числах.

В 1933 году Вацлав Веселий[17] [262] заметил, что доказать *конечность* $v(k)$ в легкой проблеме Варинга можно независимо от положительного решения настоящей проблемы Варинга. В 1934 году Майтланд Райт [275] обозвал эту задачу “легкой проблемой Варинга” = easier Waring problem.

### 4.1. Решение дешевой легкой проблемы Варинга

*Существование* такого $v(m)$, если не бороться за его точное значение, доказать действительно очень легко. В самом деле, Райт дает *очевидную* оценку

$$v(k) \leq 2^{k-1} + \frac{k!}{2},$$

которая сразу вытекает из **исчисления конечных разностей**, Харди и Райт [119], Теоремы 400 и 401. Напомним, что **разностными тождествами** называются полиномиальные тождества

$$\begin{aligned}
&(x+1)^2 - x^2 = 2x+1,\\
&(x+2)^3 - 2(x+1)^3 + x^3 = 6x+6,\\
&(x+3)^4 - 3(x+2)^4 + 3(x+1)^4 - x^4 = 24x+36,\\
&(x+4)^5 - 4(x+3)^5 + 6(x+2)^5 - 4(x+1)^5 - x^5 = 120x+240,
\end{aligned}$$

и так далее. В следующем пункте мы объясним, как именно они используются.

[17] Тут я в глубокой задумчивости. Традиционно по-русски пишут “Веселы”, как если бы по-чешски было “Vesely”. Но по-чешски, все-таки, там долгая, закрытая, переднего ряда, “Veselý” — “non didici geometrias, critica et alogas naenias, sed lapidarias litteras scio, partes centum dico ad aes, ad pondus, ad nummum”.

**Упражнение.** Напишите, не проводя никаких вычислений, разностное тождество произвольной степени.

Вот еще одна очевидная оценка, уже полиномиальная — но все еще очень слабая! Для любого $m$ найдется натуральное $n$ такое, что $m+n^k$ есть сумма $k$-х степеней *натуральных* чисел в количестве $\le G(k)$. Таким образом,

$$m = x_1^k + \ldots + x_s^k - n^k,$$

с единственным отрицательным слагаемым в правой части. В частности,

$$v(k) \le G(k)+1.$$

Таким образом, оценка Виноградова в асимптотической проблеме Варинга дает

$$v(k) = O(k \log(k)).$$

Гипотетическая же оценка $v(k)$ в легкой проблеме имеет порядок $O(k)$.

А вот явно *вычислить* $v(k)$ безумно сложно.

• Разумеется, со времен Пифагора известно, что $v(2)=3$. В самом деле, как мы только что вспомнили, любое нечетное число $m=2n+1$ является разностью двух последовательных квадратов

$$m = 2n+1 = (n+1)^2 - n^2.$$

Тем самым, любое четное число $m=2n$ можно записать в виде

$$m = 2n = (n+1)^2 - n^2 - 1^2.$$

С другой стороны, разность двух квадратов сравнима с $0, 1, -1$ по модулю 4. Это значит, что число вида $m=4n+2$ представимо в виде суммы или разности двух квадратов в том и только том случае, когда оно представимо в виде суммы $x^2+y^2$. Но очевидно, что 6 не представимо в таком виде.

Но это *единственное* известное сегодня точное значение $v(k)$. Вот что, например, известно для кубов.

• В 1894 году Габриэль Ольтрамаре[18] заметил, что каждое целое $m$ является суммой *пяти* целых кубов, $m = x^3+y^3+z^3+u^3+v^3$, иными словами, $v(3)\le 5$.

Он отправляется от тождества

$$6n = (n+1)^3 + (n-1)^3 - n^3 - n^3,$$

из которого вытекает, что каждое делящееся на 6 число $m=6n$ является суммой четырех кубов. Чтобы осознать связь легкой и рациональных проблем Варинга, на что понадобилось еще почти полвека, заметим, что это тождество получается из тождества Тарди для кубов в результате подстановки $x=n$, $y=z=1/2$. С другой стороны, это и есть разностное тождество для кубов, после сдвига $x=n+1$.

Остается заметить, что каждый нетривиальный класс по модулю 6 содержит куб. Но это очевидно, так как по китайской теореме об остатках и малой теореме Ферма $x^3 \equiv x \pmod 6$, так что $1^3, 2^3, 3^3, 4^3, 5^3$ как раз и являются требуемыми представителями.

[18] Габриэль Ольтрамаре, 1816–1906, был профессором в Женеве, одним из организаторов *первого* Математического Конгресса в 1897 году.

С другой стороны, так как любой куб целого числа дает при делении на 9 остаток 0, $+1$ или $-1$, то числа $m$ сравнимые с 4 и $-4$ по модулю 9 нельзя представить в виде суммы *трех* целых кубов $m = x^3 + y^3 + z^3$, так что $v(3) = 4$ или $v(3) = 5$, причем за 125+ лет нам так и не удалось это выяснить!

Про следующие значения $v(k)$ мы также знаем лишь, что

$$9 \le v(4) \le 10, \qquad 5 \le v(5) \le 10, \qquad 6 \le v(6) \le 14,$$

и так далее. Эти неравенства известны 80–90 лет, но так и не были с тех пор превращены в равенства.

Кстати, все лучшие известные сегодня верхние оценки $v(k)$ для небольших значений $k$ получаются из **явных тождеств**, в частности, из **тождеств Фролова**, связанных с решениями **проблем PTE** и других задач такого типа, самым существенным образом зависящих от $k$. Эти оценки намного лучше тех, которые можно вывести из обычной проблемы Варинга и сейчас мы начнем обсуждать, как это работает.

### 4.2. Связь с полиномиальными тождествами

Почти сразу же, в 1936 году, Белл [30] — кстати, тот самый Эрик Темпл Белл, “Men of Mathematics” и т.д. — заметил, что фактически решение *дешевой* легкой проблемы Варинга, вместе с оценкой того же порядка, что у Райта, могло быть получено в любое время начиная с 1851 года.

С 1851 года потому, что именно в этом году было опубликовано тождество Тарди, которое, если взглянуть на него непредвзято, доказывает, что любое целое кратное $k!2^{k-1}$ является суммой/разностью не более $2^{k-1}$ штук $k$-х степеней натуральных чисел.

Но это значит, что для решения *дешевой* легкой проблемы Варинга нам остается только найти в каждом классе вычетов по модулю $n = k!2^{k-1}$ представитель, который можно выразить как сумму/разность ограниченного количества $k$-х степеней. Но кольцо $\mathbb{Z}/n\mathbb{Z}$ само конечно, так что мы можем, если нас не интересует фактическая оценка, записать любой его элемент просто как сумму/разность $\le n/2$ единиц!

Конечно, само это рассуждение смоделировано на первом доказательстве такого типа, решении Лиувилля проблемы Варинга для биквадратов. И, поскольку на самом деле нас интересует получение линейных, а не экспоненциальных по $k$ оценок, нам нужно осознать, что здесь в действительности происходит.

Итак, прежде всего, нам нужно **полиномиальное тождество** вида

$$\pm f_1(x)^k \pm \ldots \pm f_t(x)^k = nx + r,$$

где $t, n, r \in \mathbb{Z}$ — натуральные числа, а $f_1, \ldots, f_t \in \mathbb{Z}[x]$ — целочисленные многочлены.

Обозначим наименьшее $t$, для которого существует такое тождество, через $v_*(k)$. Тождество Тарди означает, что

$$v_*(k) \le 2^{k-1},$$

ровно та же оценка получается и из доказательства Райта с конечными разностями. Но доказательство Райта чуть лучше, так как в нем $n = k!$, в то время как в доказательстве Тарди—Белла $n = k!2^{k-1}$.

Таким образом, борьба за улучшение оценок состоит в построении все более изощренных полиномиальных тождеств с возможно меньшими значениями $t$ и $n$ — однако, как мы увидим в следующем пункте, роль играет не собственно величина $n$, а его арифметическая струтура.

Вот, для примера, как были получены лучшие известные сегодня оценки для $v(4)$.

• Из результата Райта следует, что $v(4) \le 12$. Так как четвертая степень сравнима с $0, 1$ по модулю 16, то число вида $m = 16n + 8$ представляется как сумма или разность четвертых степеней в том и только том случае, когда все они одного знака. Но число 24 требует для своего представления 9 четвертых степеней! Поэтому $v(4) \ge 9$.

• В 1940 году Гарольд Дэвенпорт [70] доказал, что $v(4) \le 11$. Для этого он использовал тождество

$$(x+3)^4 - (11x+1)^4 + (2x+1)^4 + (6x+3)^4 + (6x+37)^4 + \\ (6x-15)^4 + (12x+15)^4 - (10x+30)^4 = 2^4 \cdot 3 \cdot 7 \cdot 647x + 1165573,$$

про которое все еще довольно понятно, как его построить вручную.

Кстати, $n = 217392$ разложено здесь на простые множители не случайно. Как мы увидим в следующем пункте, для получения оценки нужно знать лишь, в каких степенях эти множители $p$ делят показатель степени $k$ и, наоборот, в каких степенях простые делители $k$ делят числа $p-1$.

• В 1941 году Уилльям Хантер [132] доказал, что $v(4) \le 10$. Вот, для примера, одно — далеко не самое сложное! — из тождеств, которые он при этом использовал

$$24x = (4y+11)^4 + (2y-87)^4 + (y-9)^4 + (y-41)^4 + (y-83)^4 + (y+125)^4 + \\ (y^2+603)^4 + (y^2+625)^4 - (y^2+602)^4 - (y^2+626)^4,$$

где $y = x - 10319691$.

Ясно, что с ростом $k$ поиск таких тождеств требует как все более извращенной фантазии, так и все больших вычислительных ресурсов.

### 4.3. Проблемы типа Варинга по модулю $n$

Однако, после того, как такое тождество построено, нас интересуют решения уравнений

$$\pm x_1^k \pm \ldots \pm x_h^k = r,$$

но на этот раз не в самом кольце $\mathbb{Z}$, а в кольце вычетов $\mathbb{Z}/n\mathbb{Z}$ для фигурирующего в этом тождестве модуля $n$. Это мотивирует следующее определение.

• Для натуральных $k$ и $n$ обозначим через $v(k,n)$ наименьшее натуральное $h$ такое, что любое натуральное число $r$ сравнимо по модулю $n$ с суммой $h$ штук $k$-х степеней целых чисел *со знаками*

$$r \equiv \pm x_1^k \pm \ldots \pm x_h^k \pmod{n}.$$

Ясно, что любое решение уравнения в $\mathbb{Z}$ тем более является решением сравнения по любому модулю. Тем самым, для любого $n$ выполняется неравенство $v(k,n) \le v(k)$.

С другой стороны, каждое полиномиальное тождество указанного в предыдущем пункте вида дает оценку $v(k) \le t + v(k,n)$, для фигурирующего в нем $n$.

Объединяя эти неравенства, получаем

$$v(k,n) \le v(k) \le t + v(k,n),$$

причем, как мы сейчас увидим, $v(k,n)$ мало зависит от $n$. Таким образом, вопрос получения хороших оценок для $v(k)$ в значительной степени сводится к поиску тождеств длины близкой к $v_*(k)$, причем есть все основания верить, что $v_*(k) = O(k)$.

• Выше мы уже отмечали, что $v(k,n) \le n/2$. Однако эта оценка является *чрезвычайно* грубой. В действительности, мы могли бы изучать, как это делает Чарльз Смолл [239, 240], аналогичную величину $g(k,n)$ для обычной проблемы Варинга[19], порядок оценок при этом почти не изменится.

А именно для натуральных $k$ и $n$ обозначим через $g(k,n)$ наименьшее натуральное $h$ такое, что любое натуральное число $r$ сравнимо по модулю $n$ с суммой $h$ штук $k$-х степеней *натуральных* чисел

$$r \equiv x_1^k + \ldots + x_h^k \pmod{n}.$$

Снова, так как любое решение уравнения в $\mathbb{Z}$ тем более является решением сравнения по любому модулю, то $g(k,n) \le g(k)$.

С другой стороны, так как чистая сумма тем более является суммой со знаками, то

$$v(k,n) \le g(k,n),$$

причем $v(k,n) = g(k,n)$, если $k$ нечетно.

Перейдем теперь к оценке/вычислению $g(k,n)$ и $v(k,n)$.

• Прежде всего, если

$$n = p_1^{l_1} \ldots p_q^{l_q},$$

— каноническое разложение $n$ на простые, то из **китайской теоремы об остатках** вытекает, что

$$v(k,n) = \max\Big(v\big(k,p_1^{l_1}\big),\ldots,v\big(k,p_q^{l_q}\big)\Big), \qquad g(k,n) = \max\Big(g\big(k,p_1^{l_1}\big),\ldots,g\big(k,p_q^{l_q}\big)\Big),$$

поэтому в дальнейшем достаточно ограничиться случаем *примарного* $n = p^l$.

• С другой стороны, в предположении, что $p$ не делит $k$, из **леммы Гензеля** немедленно вытекает, что

$$v(k,p^l) = v(k,p), \qquad g(k,p) \le g(k,p^l) \le g(k,p)+1.$$

Для случая $g(k,p^l)$ все детали прописаны в работе Смолла [240], §§ 2,3. Случай $v(k,p^l)$ рассматривается точно так же, но проще: в случае чистых сумм $k$-х степеней условие существования решения, для которого $p$ не делит хотя бы одну из компонент $x_i$, в доказательстве Леммы 2.1 нужно было постулировать отдельно, теперь оно выполнено автоматически.

• В свою очередь, для *простого* $p$ константы $v(k,p)$ и $g(k,p)$ легко оценивается сверху любым способом. Прежде всего, **малая теорема Ферма** означает, что

$$v(k,p) = v(d,p), \qquad g(k,p) = g(d,p),$$

где $d = \gcd(k,p-1)$ — наибольший общий делитель $k$ и $p-1$. Таким образом, в дальнейшем мы можем считать, что $k = d$ делит $p-1$.

[19] Обратите внимание, что другие авторы, например, Винтерхольм [271, 272], используют обозначение $g(k.p^l)$ для длины представлений в конечном поле $\mathbb{F}_{p^l}$, а не в кольце вычетов $\mathbb{Z}/p^l\mathbb{Z}$. Разумеется, для интересующего нас случая $l = 1$ это одно и то же.

Фактически еще Харди и Литтлвуд [118] получили универсальную оценку

$$v(d,p) \le g(d,p) \le d.$$

Сегодня эту — и более сильные! — оценки можно получить множеством способов. Например, в [141] приведено элементарное доказательство, которое воспроизводится также в [239].

С другой стороны, неравенство $g(d,p) \le d$ легко вывести также из **теоремы Шевалле—Варнинга**[20,21], такой подход реализован в [142].

• Случай, когда $p$ делит $k$, несколько сложнее. А именно, пусть $p^e \parallel k$ — наибольшая степень $p$, делящая $k$. Снова из леммы Гензеля легко вывести, что

$$g(k,p) \le g(k,p^2) \le \ldots \le g(k,p^{2e+1}) = g(k,p^{2e+2}),$$

см. [239], 2.4; причем для больших $p$ стабилизация наступает раньше. Например, если $e = 1$, то для всех $p \ge 3$ уже $g(k,p^2) = g(k,p^3)$, см. [239], 7.4.

Здесь тоже можно получить такого же рода оценки, но мы не будеми их обсуждать, поскольку единственными реально возникающими в $n$ простыми, которые могут делить $k$ в высокой степени, являются только 2 и 3, а для них легко провести явные вычисления.

## 5. СУММЫ ТРЕХ ЦЕЛЫХ КУБОВ

Рассмотрим теперь чуть подробнее суммы кубов. Оказывается, если допускать отрицательные слагаемые, задача о предствлении натурального числа в виде суммы *целых* кубов внезапно становится гораздо тоньше и приобретает совершенно новое вычислительное измерение. Приведенная в § 2 формула Рейли—Ричмонда дает лишь представление $x$ в виде суммы трех *рациональных* кубов.

Здесь мы обсудим представимость натуральных чисел $m \not\equiv \pm 4 \pmod 9$ в виде суммы трех *целых* кубов, $m = x^3 + y^3 + z^3$, никаких *очевидных* алгебро-геометрических препятствий к такой возможности нет (см., в частности, классическую книгу Юрия Ивановича Манина [11] и статью Жана-Луи Колье-Телена и Оливье Виттенберга [64], где можно найти много дальнейших ссылок).

Поэтому гипотеза состоит в том, что все числа $m \not\equiv \pm 4 \pmod 9$ представляются в таком виде. Отсюда, конечно, сразу вытекало бы, что *все* натуральные числа представляются в виде суммы/разности *четырех* целых кубов — достаточно было бы взять в качестве четвертого куба $0, 1$ или $-1$. Мы вернемся к этому вопросу в следующем параграфе.

[20] В простейшем виде теоремы типа Шевалле—Варнинга утверждают, что количество нулей многочлена степени $d$ от $n > d$ переменных над конечным полем характеристики $p$ делится на $p$. Есть и гораздо более общие и точные варианты [14, 142], в том числе *на границе*, т.е при $n = d$. В современной терминологии это означает, что конечные поля являются полями типа $C_1$, т. е. **квазиалгебраически замкнуты** — и, в действительности, удовлетворяют более сильным условиям Цзена.

[21] Именно так, Эвальд Варнинг. В 1934 году Эмиль Артин предложил ему доказать то, что Шевалле называет “гипотезой Артина”, а именно, утверждение, что конечные поля являются квазиалгебраически замкнутыми. В действительности эту гипотезу сформулировал Леонард Диксон в 1909 году. Саму гипотезу тут же доказал Шевалле, а Варнинг получил более точные результаты со сравнениями и оценками количества корней [267]. Единственная другая работа Варнинга, которую мне удалось найти в базах данных, опубликована четверть века спустя, тоже в Гамбурге, и посвящена аксиоматике Бахмана.

### 5.1. Рукотворные суммы трех кубов

Основная трудность этой задачи состоит в следующем. Пока $x, y, z$ здесь были *натуральными*, они были ограничены сверху $\sqrt[3]{m}$, что позволяло для всех небольших $m$ произвести легкий перебор. Однако, если допустить, что какие-то из этих слагаемых отрицательны, то никаких *очевидных* ограничений на их модуль нет. Поэтому перебор происходит до $|x|, |y|, |z| \le N$, При увеличении области перебора от, скажем, $N = 10^{17}$ до, скажем, $N = 10^{18}$ могут обнаружиться новые решения —что фактически и происходит!!!

• В случае $m = 0$ никаких нетривиальных решений у уравнения $x^3 + y^3 + z^3 = 0$ нет, это частный случай теоремы Ферма—Уайлса [270], фактически установленный еще Эйлером — хотя специалисты до сих пор спорят, мог ли Эйлер заполнить дыры в своем доказательстве доступными в его время средствами, см., например, [164].

• В случае $m \ne 0$ решения уравнения $x^3 + y^3 + z^3 = m$ устроены гораздо загадочнее[22]. Естественно, наибольший интерес представляют **примитивные** решения, для которых $x, y, z$ взаимно просты в совокупности.

На основе вычислений в кубических числовых полях некоторые авторы утверждали, что таких решений мало и в каких-то случаях мы знаем их все. Например, во введении мы уже упоминали “Mordell’s Challenge” относительно решений уравнения $x^3+y^3+z^3 = 3$. Сам Морделл чрезвычайно аккуратен по этому поводу: “. . . it must be very difficult indeed to find out anything about any other solutions. One may wonder if the problem of finding other solutions is comparable in difficulty with that of finding when an assigned sequence, e. g. 123456789, occurs in the decimal expansion of $\pi$.”

Впрочем, Рамачандра [210] упоминает, что сам Морделл тоже верил в то, что любое решение этого уравнения *автоматически* удовлетворяет также уравнению $x + y + z = 3$. В связи с этим вопросом многие авторы искали ограничения на решения этого уравнения. Например, Касселс [54] замечает, что **кубический закон взаимности** (который он оформляет как легкое вычисление в кольце целых Эйзенштейновых чисел) показывает, что $x \equiv y \equiv z \pmod 9$.

• Однако на основе эвристических соображений, связанных с методом Харди—Литтлвуда и поведения решений в локальных полях, в 1992 Хит-Браун [124] высказал гипотезу, что ситуация ПРЯМО ПРОТИВОПОЛОЖНА: для любого ненулевого целого $m \ne \pm 4+9l$, $l \in \mathbb{Z}$. существует БЕСКОНЕЧНО МНОГО троек $(x, y, z) \in \mathbb{Z}^3$ таких, что

$$x^3 + y^3 + z^3 = m.$$

• Исторически, самый ранний результат в этом направлении, который мне удалось найти, это **параметрическое представление** 2 в виде суммы трех кубов

$$(1+6t^3)^3 + (1-6t^3)^3 + (-6t^2)^3 = 2,$$

которое дал в 1908 году Александр Степанович Веребрюсов [6]. Напомню, что *рациональные* параметризации были известны ранее.

Известно, однако, что так параметризуются *не все* представления 2 в виде суммы трех кубов. Например

$$1214928^3 + 3480205^3 - 3528875^3 = 2$$

[22] С элементарной точки зрения разницы между уравнениями $x^3+y^3+z^3 = 0$ и $x^3+y^3+z^3 = 1$ нет. Достаточно, впрочем, взять семестровый курс алгебраической геометрии для малышей, чтобы понимать, что первое из них задает плоскую кубическую кривую, а второе — кубическую поверхность в $\mathbb{P}^3$. Понятно, насколько второе *несопоставимо* сложнее первого.

не имеет такого вида, см. [68, 125]. Но, вроде бы, это единственное известное такое решение. Впрочем, уверенным в такого рода вещах быть нельзя, сегодня с числами такого порядка может считать любой школьник на компьютере, собранном из Lego. Основная масса подобных вычислений вообще не публикуется, а сообщается на любительских сайтах, следить за всеми из которых невозможно.

Заметим, что Александр Степанович Веребрюсов[23] еще один *серьезный* любитель, занимавшийся проблемами варинговского типа. Ему принадлежит несколько десятков простых, но весьма забавных работ по теории чисел. Он работал учителем математики Феодосийской мужской гимназии — той самой, в которой учился Максимилиан Волошин.

• Только в 1936 году Курт Малер [174] нашел аналогичное параметрическое представление для 1:

$$(9t^4)^3 + (3t - 9t^4)^3 + (1 - 9t^3)^3 = 1,$$

что, в частности, опровергало предположение Харди—Литтлвуда относительно асимптотики таких представлений.

Используя **уравнение Пелля** позже Деррик Генри Лемер [165] построил на этой основе дальнейшие такие параметрические представления. Кстати, Лемер был одним из ранних энтузиастов компьютерных вычислений в самой математике, лет на 30 опередив господствующий тренд. Его речь [166] можно *целиком* разбирать на цитаты, я не буду даже пытаться начинать делать это здесь.

• Эти представления уникальны и обнаружить другие такие же до изобретения компьютеров было непросто. Дело в том, что 1942 году Луис Джоэл Морделл [182] доказал, что для любого натурального числа $m \neq 1, 2$ подобное параметрическое представление с рациональными коэффициентами должно иметь степень по крайней мере 5.

Кстати, Морделла я еще застал, совсем незадолго до его смерти. В 1971 году он приезжал в Ленинград и читал в ЛГУ лекции о диофантовых уравнениях. После того, как приставленная к нему от *Интуриста* переводчица перевела в первой же, после приветствия и благодарностей, фразе “Diophantine equations” как “диафонические уравнения”, дальше стал переводить Анатолий Николаевич Андрианов. История ностальгическая, кстати, по типу истории Бруно Понтекорво про нейтринную и нейтронную физику, потому что сегодня, боюсь, еще не выучив слово “диофантов”, многие уже забыли слово “диафонический”. Ну и, кроме того, что лекции на английском еще нуждались в переводе (потому что на слух большинство профессоров старшего поколения понимали только немецкий и, отчасти, французский).

### 5.2. Нерукотворные суммы трех кубов

• В ответ на явно поставленные Морделлом в [183] вопросы в 1954 году Джеффри Миллер и М. Ф. С. Вуллетт провели первый систематический *компьютерный* поиск решений уравнения $x^3 + y^3 + z^3 = m$ при $1 \leq m \leq 100$ и первоначально нашли 345 *примитивных* решений, еще 2 добавлены при корректуре [178]. Для многих допустимых значений $m$, а именно, для $m = 30, 33, 39, 42, 52, 74, 75, 84, 87$, не было найдено вообще ни одного решения.

[23] История находится от нас на расстоянии вытянутой руки. Старший сын Веребрюсова, Иван Александрович, заведовал кафедрой в Военно-Морской Академии и в детстве я, вероятно, должен был встречаться с ним дома у Исаака Рубиновича Фрейдзона и других общих знакомых.

Фактические вычисления производились на компьютере EDSAC в Математической Лаборатории Кембриджского Университета. На эту таблицу интересно взглянуть, чтобы оценить, со сколь маленькими числами имели тогда дело люди, *профессионально* занимавшиеся научными вычислениями. Сегодня задачи такого типа вы даем на практических занятиях в аудитории при первом знакомстве с предметом, а для домашних заданий и контрольных работ выбираются обычно задачи со значительно большим количеством цифр.

• В 1963 году Верна Гардинер, Р. Б. Лазарус и Поль Стайн [108] провели такой же поиск в интервале $1 \leq m \leq 999$ расширив при этом область поиска примерно до $|x|, |y|, |z| < 2^{17}$. Фактические вычисления производились в основном на суперкомпьютерах того времени, IBM STRETCH принадлежавшем Los Alamos Scientific Laboratory Университета Калифорнии, которая находилась тогда в ведении United States Atomic Energy Commission (ядерный проект) и частично на MANIAC II. Среди новых найденных при этом решений

$$87 = 4271^3 - 1972^3 - 4126^3$$

и первое *примитивное* решение для $n = 96$,

$$96 = 15250^3 - 10853^3 - 13139^3$$

— у Миллера и Вуллетта фигурировало только кратное решения $12 = -11^3 + 10^3 + 7^3$.

В рамках журнальной статьи невозможно, конечно, рассказать всю историю с такой степенью подробности. Произведем, поэтому, fast forward на 25–30 лет, сразу в 1990-е годы. Даже при беглом сравнении видно, что за эти 30 лет изменилось **все**, и возможности используемой техники, и глубина понимания алгоритмики и, в первую очередь, уровень чисто *математической* софистикации. Алгоритмы 1960-х годов легко объяснить любому сообразительному школьнику, а вот алгоритмы 1990-х внезапно требуют уже довольно серьезного понимания целочисленных решеток, числовых колец, эллиптических кривых, и всего такого. Мне кажется, это связано с тем, что в 1960-х годах подобными вычислениями занимались все еще программисты — потому что математики не умели! — а в 1990-х уже, несомненно, серьезные математики.

Оценим сложность поиска решения уравнения $x^3 + y^3 + z^3 = m$, с $|x|, |y|, |z| \leq N$. При совсем дуболомном подходе, известном в программировании как brute force[24], происходит перебор *троек* $(x, y, z)$ с компонентами в указанном интервале, что требует $O(N^3)$ арифметических операций.

При чуть менее наивном подходе профессиональных программистов, происходит перебор *пар* $(x, y)$ и выяснение вопроса, является ли $m - x^3 - y^3$ кубом, что все еще требует $O(N^{2+o(1)})$ арифметических операций. Это чуть лучше, но по-прежнему не дает возможности даже приблизиться к значениям $N$ типа $N = 10^{16}$, и нужны какие-то принципиальные улучшения.

• В 1989 году Роджер Хис-Браун [123] предложил новый теоретико-числовой алгоритм, который работал *принципиально* быстрее, чем известные до этого.

Первый шаг напоминает сакраментальную телеграмму ферматистов про перенос $y^m$ в правую часть. А именно, для начала задача переписывается в виде

$$m - z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$

[24]Раньше логики обычно называли это **алгоритмом полного перебора**. Конечно, брутфорс — именно так, по-русски в одно слово — звучит гораздо брутальнее.

и дальше перебор происходит по *одному* параметру $d = x + y$. Именно это обстоятельство позволило в дальнейшем распараллелить вычисления, распределяя интервалы значений $d$ между сотнями тысяч процессоров.

В сочетании с дальнейшими чуть более глубокими теоретико-числовыми идеями это позволяет понизить сложность до примерно $O(N\log(N))$ арифметических операций, что выглядит уже довольно разумным. После этого события резко ускорились.

• В 1991 году этот алгоритм был имплементирован Хис-Брауном, Уолтером Лайоном и Херманом те Риле, см. [125], которые использовали факторизацию в кольце целых поля $\mathbb{Q}(\sqrt[3]{m})$. В частности, они нашли первое представление для $m = 39$,

$$39 = 134476^3 + 117367^3 - 159380^3$$

все еще чрезвычайно маленькое в сравнении с тем, что начнет происходить вскоре после этого. Кроме того, они нашли упомянутое выше решение для $m = 2$, не попадающее в параметризацию Веребрюсова. Фактически вычисления производились на `Cyber 205`.

• В том же 1991 году У. Кон и Леонид Васерштейн [68] нашли то же самое представление для 39, первое представление для $m = 84$

$$84 = 41639611^3 - 41531726^3 - 8241191^3,$$

и, кроме того, 4 примитивных решения для $m = 80$, то же решение для $m = 2$, и 3 новых представления для чисел в интервале $100 \leq m \leq 1000$, а именно, для $m = 556, 870, 960$. Интересно, что во всех этих свершениях они обошлись народными средствами, `Mathematica` на рабочих станциях `Sun 4` и `NeXT`.

• В 1991–1994 годах Кендзи Кояма расширил область поиска до $|x|, |y|, |z| < 2^{21}$, что позволило ему независимо открыть то же самое представление 39 и найти решения еще для 16 новых значений $100 \leq m \leq 1000$, а именно, для

$$143, 180, 231, 312, 321, 367, 439, 462, 516, 542, 556, 660, 663, 754, 777, 870.$$

При этом он использовал суперкомпьютер `Cray`.

• В 1994 Эндрю Бремнер[25] при помощи своего алгоритма нашел на `DEC 5000` решения для $m = 75$,

$$75 = 4381159^3 + 435203083^3 - 435203231^3,$$

и для $m = 600$.

• В диссертации 1995 года Ричард Люкс [172] нашел представления для $m = 110, 435, 478$.

•В 1994–1997 годах Кендзи Кояма, Юкио Цуруока и Хироши Сукигава независимо нашли решения для $m = 75, 600$ и, кроме того, для $m = 435, 444, 501, 618, 912, 969$, опубликовано в 1997 году в [157] .

• Принципиальный прорыв был совершен в 1999–2000 годах. а именно, почти одновременно были предложены два алгоритма, использующие эллиптические кривые, алгоритм Бремнера [45] и алгоритм Элкиса [86].

[25] https://math.la.asu.edu/ andrew/

• В 2007 году в работе Михаэля Бека, Эрика Пайна, Уэйна Тарранта и Кима Йарбро Йенсена [24] имплементирована версия алгоритма Элкиса и, в частности, найдены решения для еще четырех новых значений $m$, в том числе для двух $m < 100$,

$$30 = -283059965^3 - 2218888517^3 + 2220422932^3,$$
$$52 = 60702901317^3 + 23961292454^3 - 61922712865^3,$$

Бьорн Пунен цитирует этот результат в своей статье про неразрешимость в теории чисел [206][26] и реитерирует аналогичный вопрос для $m = 33$: “Does the equation $x^3 + y^3 + z^3 = 29$ have a solution in integers? Yes: $(3, 1, 1)$, for instance. How about $x^3 + y^3 + z^3 = 30$? Again yes, although this was not known until 1999: the smallest solution is $(-283059965, -2218888517, 2220422932)$. And how about $x^3 + y^3 + z^3 = 33$? This is an unsolved problem”.

• В том же 2007 году Андреас-Штефан Эльзенханс и Йорг Янель [87] оптимизировали алгоритм Элкиса, провели поиск для $k < 1000$ и $|x|, |y|, |z| < 10^{14}$ и нашли много новых представлений, в том числе *второе* решение для $m = 30$,

$$30 = 3982933876681^3 - 636600549515^3 - 3977505554546^3.$$

Код и результаты можно найти на сайте

`http://cr.yp.to/threecubes.html`

В 2006–2007 годах несколько авторов, в том числе Даниэль Бернстайн, Леонид Дурман, Майкл Оукс, Хисанори Мишима и другие объявляли о расширении области поиска, как в том, что касается значений $m$, так и значения $N$. Эти результаты упомянуты, например, на сайтах

`http://cr.yp.to/threecubes.html`

`http://www.asahi-net.or.jp/~kc2h-msm/mathland/math04/cube01.htm`

но я не смог найти никаких дефинитивных публикаций.

• Только в 2016 году, увеличив область поиска еще на порядок, $|x|, |y|, |z| < 10^{15}$, Сандер Хюйсман [130] нашел первое решение для $m = 74$,

$$74 = -284650292555885^3 + 66229832190556^3 + 283450105697727^3,$$

и *третье* решение для $m = 30$,

$$30 = -662037799708799^3 + 190809268841284^3 + 656711689254565^3,$$

Таким образом, после его работы оставались неразобранными только 13 значений $m < 1000$, а именно,

$$33, 42, 114, 165, 390, 579, 627, 633, 732, 795, 906, 921, 975.$$

Его результаты собраны на сайте `arXiv`:

`https://arxiv.org/src/1604.07746v1/anc/sumofthreecubes_20160426.txt`

[26] Из заметки Пунена этот пример, в силу своей симптоматичности, попал в ворох научно-популярных и философских текстов, например, [33, 244].

• Наконец в 2019 году Эндрю Букер [41] используя PARI/GP нашел следующее представление для $m = 33$,

$$33 = 8866128975287528^3 - 8778405442862239^3 - 2736111468807040^3.$$

Вычисления проводились на суперкомпьютере (технически, massively parallel cluster) `Bluecrystal Phase 3` в Advanced Computing Research Centre университета Бристоля.

При этом было найдено также следующее новое представление

$$795 = -14219049725358227^3 + 14197965759741571^3 + 2337348783323923^3.$$

После этого из всех чисел $\leq 100$ оставалось нерассмотренным ровно одно, а именно, 42 — “How many roads must a man walk down? Forty-two”, "Six by nine. Forty-two”.

## 5.3. Tlön, Uqbar, Orbis Tertius

Греческие классики учили, что искусство есть имитация реальности, в эстетике эта концепция известна как **мимезис**. Поскольку сама реальность есть имитация мира идей, то искусство есть имитация второго порядка. Однако, как известно, в универсальной библиотеке “un libro que no encierra su contralibro es considerado incompleto”.

Поэтому последние век–полтора стандартным для европейских художников стало противоположное учение, **анти-мимезис**, состоящее в том, что реальность есть имитация искусства. Разумеется, в исходной мягкой форме, человек видит только то, что он знает[27], эта концепция очевидно верна, но абсолютно тривиальна.

Борхес обсуждает гораздо более жесткую форму анти-мимезиса. А именно, он утверждает, что искусство изменяет не только наше *восприятие* реальности, но и саму реальность: “Casi inmediatamente, la realidad cedió en más de un punto. Lo cierto es que anhelaba ceder”. Вся история решения уравнения $x^3 + y^3 + z^3 = 42$ представляется грандиозной натурной верификацией учения Борхеса.

А именно, в 2019 году в результате выполнения проекта под руководством Эндрю Букера и Эндрю Сазерлэнда [42] получен ответ на вопрос Жизни, Вселенной и всего остального. Вот этот ответ:

$$-80538738812075974^3 + 80435758145817515^3 + 12602123297335631^3 = 42.$$

Статья про это событие в новостях MIT

`https://news.mit.edu/2019/answer-life-universe-and-everything-sum-three-cubes-mathematics-0910`

ровно так и называется, “The answer to Life, the Universe, and Everything”.

Выступая в качестве `Капитана Очевидность`, напомню, что сюжет культового цикла Дугласа Адамса — опубликованного в 1979 году романа “The hitchiker’s guide to the galaxy” и 4.5 его сиквелов и приквелов, вместе образующих трилогию в шести книгах — состоит в следующем.

[27] “Things are because we see them, and what we see, and how we see it, depends on the arts that have influenced us” — “We don’t see things as they are, we see them as *we* are”.

После 7.5 миллионов лет вычислений суперкомпьютер `Deep Thought` дает ответ на вопрос Жизни, Вселенной, и всего остального и этот ответ 42[28,29] — "I checked it very thoroughly," said the computer, "and that quite definitely is the answer. I think the problem, to be quite honest with you, is that you've never actually known what the question is".

Чтобы узнать, в чем состоит вопрос, создается еще более мощный суперкомпьютер, `Earth`, который, в связи с наличием биологической компоненты, многие ошибочно принимают за планету. Но за пять 5 минут до того, как этот компьютер должен завершить продолжающееся 10 миллионов лет вычисление, его уничтожают вогоны, порождая, тем самым, загадку числа 42 — what is the question, really?

На самом деле, конечно, каждый [англоязычный] ребенок вспомнит дюжину случаев использования числа 42 и у Льюиса Кэрролла. Эдвард Уэйклинг [266] замечает по этому поводу: "There is little doubt that Lewis Carroll had a certain fascination with the number forty-two; he often used this number in his writings". Вот, навскидку, первое, что приходит в голову: "Rule Forty-two. All persons more than a mile high to leave the court", "Rule 42 of the Code: "No one shall speak to the Man at the Helm"." Или:

He had forty-two boxes, all carefully packed,
With his name painted clearly on each:
But, since he omitted to mention the fact,
They were all left behind on the beach.

Или еще:

"No doubt,"said I, "they settled who
Was fittest to be sent:
Yet still to choose a brat like you
To haunt a man of forty-two[30],
Was no great compliment".

В его книге загадок 42 загадки, первоначально в "Алисе в стране чудес" планировалось 42 иллюстрации. Разумеется, у Кэррола есть и другие, чуть менее очевидные, но совершенно недвусмысленные отсылки к числу 42. Вот еще одна:

'Let's consider your age to begin with — how old are you?'
'I'm seven and a half exactly.'
'You needn't say "exactually,"' the Queen remarked: 'I can believe it without that. Now I'll give you something to believe. I'm just one hundred and one, five months and a day.'

Посмотрев на точную дату и прикинув количество високосных лет, мы видим, что возраст Белой Королевы $37044 = 42^3/2$ дней.

[28]Откуда 42 у Адамса? Ответ очевиден, Infinite Improbability Drive. Общее количество очков на игральном кубике равно 21 = "очко". Жизнь есть игра. Обычно игра происходит двумя кубиками, поэтому 42 — "... а этот черный ящик — и не ящик вовсе, а эвристическая машина, и проходит она под номером сорок вторым, и заявки на нее нет". Опять же, жизнь есть форма существования белковых тел, поэтому шкала медицинского термометра заканчивается на 42 градусах Цельсия.

[29]Специалистам по элементарной теории чисел известно, что $42 = 43-1$, где $3 = 2+1$, $7 = 2\cdot 3+1$, $43 = 2\cdot 3\cdot 7+1$, см., например, [167]. Поэтому 42 является **примарно псевдосовершенным числом**, $1/2+1/3+1/7+1/42 = 1$. Уже одно это делает его совершенно уникальным — "ieder mens is uniek, en ieder getal is dat ook". Следующее примарно псевдосовершенное число 1806. Кстати, для 42 малая теорема Ферма — ну, почти! — принимает форму $a^{42+1} \equiv a \pmod{42}$, для всех $a$. Чему равно следующее число, для которого выполняется сравнение $a^{n+1} \equiv a \pmod{n}$?

[30]В полном собрании сочинений просто "forty". Очевидно, опечатка.

Ну а откуда 42 у Кэрролла? Да откуда угодно, хоть из Апокалипсиса (Глава 13, Стих 5) — “...и дана ему власть действовать сорок два месяца”. Или из “Ромео и Джульетты” (Акт 4, Сцена 1) — “И сорок два часа ты пролежишь”:

And in this borrowed likeness of shrunk death
Thou shalt continue two and forty hours
And then awake as from a pleasant sleep.

Совершенно ясно, что ни под одно другое число, кроме 42, Букеру и Сазерлэнду не удалось бы собрать в 2019 году в этот проект около 400000 энтузиастов, которые предоставили в их распоряжение ресурс, позволивший создать ВИРТУАЛЬНЫЙ СУПЕРКОМПЬЮТЕР, состоящий из примерно 580000 ядер. В предыдущем рекорде 2017 года использовалось около 220000 ядер.

Общий объем проведенных вычислений огромен, в любом случае это *многие сотни* лет процессорного времени — дать более точную оценку практически невозможно в силу неравномерности использования процессоров при крауд-сорсинге. Однако физически все эти вычисления уложились в несколько астрономических недель. Организационно грид был предоставлен в их распоряжение `Charity Engine`, а системно для его формирования использовалась платформа BOINC. Все алгоритмы, оригинальный код и данные по этому проекту доступны на сайте

`https://github.com/AndrewVSutherland/SumsOfThreeCubes`

Для начала Букер и Сазерлэнд понижают сложность алгоритма Хис-Брауна, Лайона и те Риле до $O(N\log\log(N)\log\log\log(N))$ арифметических операций. Еще одна особенность их подхода состоит в том, что перебор происходит по $\min(|x|,|y|,|z|)\le N$, в то время как $\max(|x|,|y|,|z|)$ может быть гораздо больше! Именно это обстоятельство позволило найти то решение для $m=3$, которое приведено во введении.

Оскар Уайльд был бы в восторге! В октябре 1979 года публикуется роман, в котором фигурируют суперкомпьютер `Deep Thought` и планетарный компьютер `Earth`, а в сентябре 2019 года все это САМЫМ БУКВАЛЬНЫМ ОБРАЗОМ воплощается в действительность:

`Deep Thought` $\rightsquigarrow$ `Bluecrystal Phase 3`, `Earth` $\rightsquigarrow$ `Compute Engine`

Однако Борхес претендует на нечто *гораздо* большее.

• Во-первых, люди обычно не имеют опыта ментальных вычислений с числами такого размера. Я [почти] уверен, что никто из читателей не попытается повторить это вычисление вручную. Более того, даже попробовав провести его в школьной тетради, совершенно нельзя быть уверенным, что при этом будет каждый раз получаться один и тот же ответ. Я, скорее, уверен в обратном: “Afirman que la operación de contar modifica las cantidades y las convierte de indefinidas en definidas. El hecho de que varios individuos que cuentan una misma cantidad logran un resultado igual, es para los psicólogos un ejemplo de asociación de ideas o de buen ejercicio de la memoria.”

С точки зрения современных компьютеров числа фигурирующие в этих представлениях все еще довольно маленькие. Но увеличив их еще на какую-нибудь пару тысяч порядков, мы столкнемся с такого же рода проблемами и для них. Уже сегодня в научных вычислениях мы не можем полагаться на внутреннюю архитектуру существующих процессоров, а должны реализовывать все программным образом.

Операции приближенной арифметики не обладают обычными свойствами, например, сложение приближенных чисел неассоциативно, а умножение недистрибутивно относительно сложения. Поэтому, складывая приближенные числа в столбик сверху вниз и снизу вверх, мы всегда получим разные ответы, это подробно обсуждается в трактате Кнута. Откуда мы знаем, что операции над большими целыми числами обладают обычными свойствами?

Но Борхес не останавливается и здесь. Он утверждает, что само приведенное выше решение уравнения $x^3+y^3+z^3=42$ является артефактом, созданным настойчивостью — хрён или надеждой — ур.

• Первая гипотеза состоит в том, что решение уравнения $x^3+y^3+z^3=42$ существовало и имело такой же порядок, как решение соответствующего уравнения для $m=33$. Но в тот момент, когда люди оказались в состоянии искать такие решения до $N=10^{17}$, реальность изменилась и оно стало чуть больше: “Siglos y siglos de idealismo no han dejado de influir en la realidad. No es infrecuente, en las regiones más antiguas de Tlön, la duplicación de objetos perdidos. Dos personas buscan un lápiz; la primera lo encuentra y no dice nada; la segunda encuentra un segundo lápiz no menos real, pero más ajustado a su expectativa. Esos objetos secundarios se llaman *hrönir* y son, aunque de forma desairada, un poco más largos[31].”

• Вторая гипотеза состоит в том, что исходно решения уравнения $x^3+y^3+z^3=42$ не существовало, по крайней мере до $N=10^{18}$. Но воля миллионов болельщиков, которые хотели, чтобы оно существовало, создала это решение: “Más extraño y más puro que todo *hrön* es a veces el *ur*; la cosa producida por sugestión, el objeto educido por la esperanza. La gran máscara de oro que he mencionado es un ilustre ejemplo.”

Обе эти гипотезы могут казаться странными современной прогрессивной общественности. Мне, однако, любая из них представляется СТРОГО ДОКАЗАННЫМ НАУЧНЫМ ФАКТОМ, по сравнению со всем остальным, во что сегодня положено верить этой общественности. Как тогда относиться к утверждению, что XX = XY? Или к утверждению, что рост концентрации углекислого газа в атмосфере является *причиной* климатических изменений — а не их следствием: “…nada sabemos con certidumbre — ni siquiera que es falso. Han sido reformadas la numismática, la farmacología y la arqueología. Entiendo que la biologíia y las matemáticas aguardan también su avalar…”

## 6. СУММЫ ЧЕТЫРЕХ ЦЕЛЫХ КУБОВ

Задача представления натуральных чисел $m$ в виде суммы *четырех* целых кубов, $m=x^3+y^3+z^3+w^3$, также известна с XIX века, и тоже до сих пор решена не полностью, несмотря на довольно значительные усилия. Гипотеза состоит в том, что каждое $m$ допускает *бесконечно много* таких представлений.

### 6.1. Доказательство для $m \not\equiv 4,5 \pmod 9$

• В 1936 году Морделл [182] обсуждает предположение, что каждое целое число представляется в виде суммы четырех целых кубов. Для этого он возвращается к доказательству Ольтрамаре, которое стартует с полиномиального тождества, выражающего $m=6n$

[31] Я знаю первое словарное значение слова `largo` в стандартном испанском. Но это не стандартный испанский, это идиолект! Идиолект человека, который родился в Буэнос-Айресе, где на улице даже сегодня, век спустя, можно обратиться к любому по-итальянски, и тебе ответят. Идиолект человека с португальскими корнями, в семье которого говорили по-английски и который провел годы взросления во французской языковой среде. В данном случае, я однозначно воспринимаю `largo` в том смысле, который это слово имеет в португальском, т.е. как синоним *одновременно* английского и французского `large` = `grande` и итальянского `largo` = `ancho`, `amplio`.

в виде суммы четырех целых кубов и предлагает искать полиномиальные тождества такого же типа, дающие такие выражения для других классов по модулю 6.

Например, представимость чисел вида $m \equiv 3 \pmod 6$ сразу вытекает из тождества

$$6n+3 = n^3 - (n-4)^3 + (2n-5)^3 - (2n+4)^3$$

или из тождества

$$6n+3 = (n+1)^3 - (n+5)^3 + (2n+7)^3 - (2n+6)^3$$

(в действительности оба эти тождества являются специализациями полиномиального тождества от двух переменных).

Однако угадать такого типа тождества для других классов по модулю 6 сразу не удается, поэтому Морделл начинает искать тождества по модулю 18. Вот несколько типичных примеров того, что у него получается:

$$\begin{aligned}
18n+1 &= (3n+30)^3 - (2n+26)^3 - (2n+23)^3 + (2n+14)^3,\\
18n+7 &= (n+2)^3 + (6n-1)^3 + (8n-2)^3 - (9n-2)^3,\\
18n+8 &= (n-5)^3 - (n-14)^3 + (3n-30)^3 - (3n-29)^3.
\end{aligned}$$

Поупражнявшись таким образом по модулю 36, 54, 72, 108, 216, и дойдя до модуля 432, ему удается доказать, что любое целое $m$ является суммой четырех целых кубов, кроме, возможно $m \equiv \pm 4 \mod 9$ и $m \equiv \pm 2 \mod 18$, итого 54 исключительных класса по модулю 216.

Однако, как выяснилось, большинство из этих результатов, включая приведенные выше тождества для $6n+3$ и $18n+8$, *другое* тождество для $18n+1$, и многое другое, содержались уже в статье Ричмонда 1922 года [221]. Воспроизведу целиком опубликованные в 1937 году “Corrections” к статье Морделла, где прекрасно чуть более, чем все: “Prof. Landau has called my attention to H. W. Richmond’s paper, “An elementary note upon Waring’s problem for cubes, positive and negative”, Messenger of Math., 51 (1922), 177–186. Richmond has anticipated me and my correspondents in the formulae of decomposition (3), (8), (9), (11), (13), (14), (15), (16), (17) in § 1, including in particular the formulae giving the decompositions into four integer cubes of $6k+3$, $18k+1$, $18k+8$. The result in § 3, that corresponding formulae for $9k+4$ are impossible, has also been given by him”. Как нам не хватает таких Ландау и таких “Corrections” сегодня!

Ну и, для совсем полного реализма, отрывок из опубликованного еще через 20 лет “Corrigendum”: “Prof. Sierpiński has kindly pointed out that the proof does not hold when $a = b$, $c = d$, etc. Hence it is not known if $x^3 + y^3 + z^3 + w^3 = 2a^2 + 2b^2$ has an infinity of integer solutions.” Сам этот факт, конечно, тут же доказали Серпиньский и Шинцель [231], но мне почему-то кажется, что если бы современные авторы были столь же добросовестны и щепетильны в этом отношении, как классики, то математические журналы должны были бы состоять из подобных корригендумов процентов на 95–98 (а все остальные — процентов на 200–300).

• В том же номере, что и статья Морделла, опубликована заметка Чао Ко [148], который нашел представление всех таких $m \le 100$, кроме $m = 76$, в виде $m = x^3 + y^3 + 2z^3$. В дальнейшем А.С.Банг[32] [21] и Агне Вальгрен [265] нашли бесконечно много представлений в виде $m = x^3 + y^3 + z^3 + w^3$ для $m \le 100$, $m \equiv \pm 4 \pmod 9$.

[32] Тот самый Банг, очевидно, из теоремы Банга—Жигмонди. Поскольку статья про теорему Банга—Жигмонди опубликована в 1886 году, а статья про суммы трех и четырех кубов — в 1940 году, интересно, сколько лет дедушке было на тот момент? Я не смог найти биографию Банга, чтобы удовлетворить свое лю-

Много позже, уже в 1959 году в связи с гипотезой Серпиньского, Монковский [175] продолжил эти вычисления для $101 < m < 220$ и нашел такие представления для всех $m$, кроме $m = 113, 148, 183, 190, 195$.

• В 1960 году Вацлав Серпиньский [237] явно высказал предположение, что каждое натуральное число $m$ допускает *бесконечное* число различных представлений в виде

$$m = x^3 + y^3 - z^3 - w^3,$$

разумеется, знаки здесь нужно понимать в том смысле, что сами $x, y, z, w$ неотрицательны. Он сделал и более точные предположения такого типа, в частности, о представимости $m$ в виде $m = x^3 + y^3 + 2z^3$,

Представимость в таком виде 0,

$$x^3 + y^3 - z^3 - w^3 = 0, \qquad x^3 + y^3 + z^3 - w^3,$$

это `equal sums of like powers`, т. е. разрешимость уравнений

$$x^3 + y^3 = z^3 + w^3, \quad x^3 + y^3 + z^3 = w^3,$$

которой посвящена огромная литература, начиная с XVI века. Здесь мы не будем даже начинать обсуждать эту огромную отдельную тему, в надежде вернуться к ней в следующей статье этой серии.

• В 1966 году Вадим Андреевич Демьяненко[33] [10] делает следующий важный шаг. А именно, довольно хитроумным рассуждением он доказывает гипотезу Серпиньского для чисел $m \equiv \pm 2 \pmod{18}$. В некоторых случаях ему удается написать тождества того же типа, что у Ричмонда и Морделла, в частности,

$$\begin{aligned} 54x + 2 &= (29484x^2 + 2211x + 43)^3 - (29484x^2 + 2157x + 41)^3 + \\ &\qquad\qquad (9828x^2 + 485x + 4)^3 - (9828x^2 + 971x + 22)^3, \\ 54x + 20 &= (3x - 11)^3 - (3x - 10)^3 + (x + 2)^3 - (x - 7)^3, \end{aligned}$$

и так далее. В действительности, конечно, поскольку его интересует не просто представимость, а существование бесконечного количества представлений, он пишет соответствующие тождества с параметрами, частные случаи которых мы здесь воспроизводим.

Однако для оставшихся случаев рассуждение Демьяненко слишком технично, чтобы воспроизвести его здесь. Только в 1983 году Филиппу Ревуа [213] удается полностью

бопытство. Статья Банга написана по-датски, а дополняющая ее статья Вальгрена — по-шведски. Конечно, в Zentralblatt указано, что тоже по-датски, но это потому, что из Германии в плохую погоду не всегда видно, на том берегу пролива город Лунд, или еще на этом. В названии статьи Вальгрена в библиографии [231] две ностальгических опечатки, “on” вместо “om” и “ar” вместо “av”, показывающие, что текст переписывался от руки. Меня уже довольно давно волнует вопрос: и кому это все мешало?

[33] На сайте МИАН упоминается, что в 1967–1969 годах Демьяненко работал в отделе алгебры, а после 1969 года — в ИМ Уральского отделения АН. Он был первым, кто заметил связь между рациональными точками на кривых Ферма и точками конечного порядка на эллиптических кривых, то, что обычно связывается с именами Эллегуарша и Фрая [93], именно на этом пути Уайлс и получил полное решение проблемы Ферма. Если верить `mathnet.ru`, Демьяненко, 1937–2007, был *кандидатом* наук. Посмотрев его работы, я в шоке. Либо я забыл, какие требования предъявлялись в советское время к докторским диссертациям, что, конечно, очень может быть. Либо за этим скрывается еще один эпизод истории математики, о котором лучше не знать.

прояснить, в чем состоит сложность построения явных тождеств в этих случаях, и предложить чуть более простую трактовку. В действительности можно написать еще много такого типа тождеств

$$72x+56=-(9x-4)^3+(x+4)^3+(6x-2)^3+(8x-4)^3,$$
$$108x+2=-(x+22)^3+(x+4)^3-(3x+41)^3+(3x+43)^3,$$

дополняющих или упрощающих написанные выше. Но все равно нужно либо продолжать писать такого типа тождества по все большим модулям, либо в какой-то момент использовать для остающихся классов метод Демьяненко, который, вообще говоря, дает решения со многими сотнями цифр. Дарио Альперн имплементировал этот алгоритм как HTML-апплет:

`https://www.alpertron.com.ar/FCUBES.HTM`

• Случай $m \equiv \pm 4 \pmod 9$ продолжает оставаться открытым с того времени. Более того, шансы решить его на том же пути довольно сомнительны. Дело в том, что в 1968 году Анджей Шинцель [230] доказал, что любое нетривиальное тождество вида

$$f_1(x)^3+f_2(x)^2+f_3(x)^3+f_4(x)^3=nx+r,$$

с $r \equiv \pm 4 \pmod 9$, должно иметь степень по крайней мере 5. Морделл тут же [188, 189] предложил более простое доказательство этого факта, а в дальнейшем совместно с Джоном Коном [67] проверил, что и тождеств степеней 5 и 6 тоже нет. Таким образом, скорее всего, здесь нужна какая-то принципиально новая идея.

## 6.2. Экспериментальные свидетельства для $m \equiv 4,5 \pmod 9$

Первоначально систематические попытки проверки гипотезы четырех целых кубов для небольших значений $m$ особенно рьяно проводились для отмеченного Серпиньским частного случая, когда два из этих кубов равны. А именно, речь идет о решении уравнения

$$x^3+y^3+2z^3=m,$$

которое с вычислительной точки зрения *чрезвычайно* похоже на задачу трех кубов. Конечно, в данном случае никаких очевидных ограничений, вытекающих из сравнений, нет. Поэтому гипотеза состоит в том, что *все* натуральные числа представляются в таком виде.

• В 1969 году Манге Лал, Расселл и Бландон [160] провели на `IMB 1620, Model 1` систематический поиск решений уравнения $x^3+y^3+2z^3=m$, $0<m<10^3$, в предположении $|x|,|y|,|z|<10^5$ При этом обнаружилось ровно 19 значений $k$, которые не представляются в таком виде, а именно:

$$k=76,148,183,230,253,356,418,428,445,482,491,519,580,671,734,788,923,931,967$$

В своей статье они сообщают душераздирающие подробности своего вычисления. Вначале они написали свою программу на Фортране и она считала около 15 часов. Тогда они решили переписать программу в языке ассемблера, и она работала примерно в 15 раз быстрее, что позволило им расширить область поиска и найти 20 новых представлений. Это вычисление потребовало около 1000 часов машинного времен и заняло в фоновом режиме год работы! Это в 1968–1969 годах!

• Однако, как мы уже обсуждали в [2], в 1981–1982 годах были проведены обширные компьютерные вычисления и эксперименты, которые дают самые серьезные основания считать, что все достаточно большие натуральные числа — вероятно уже все числа большие, чем 7373170279850, — являются суммами четырех *неотрицательных* кубов. Иными словами, предполагается, что 7373170279850 это самое большое натуральное число, которое нельзя записать в виде

$$7373170279850 = x^3 + y^3 + z^3 + w^3,$$

с неотрицательными $x, y, z, w$.

При этом — гипотетически! — ровно 113936676 натуральных чисел требуют для своего представления 5 неотрицательных кубов, ровно 3922 — 6 неотрицательных кубов, ровно 121 — 7 неотрицательных кубов. И, как уже известно, ровно 15 чисел требуют 8 неотрицательных кубов и ровно 2 — 9 неотрицательных кубов. Все это излагается в [2], § 8, и мы не будем повторять оттуда ни сами эти экспериментальные результаты, ни точные формулировки гипотез.

• В книге Ричарда Гая [114] задача о четырех целых кубах обсуждается в параграфе **D5**. При этом чрезвычайно поучительно сравнить, как меняется текст этого параграфа между изданиями 1981, 1994 и 2004 годов.

Впрочем, даже в третьем издании Гай пишет, что Люкс в диссертации [172] доказал, что все $m < 10^7$ представляются как суммы четырех целых кубов — судя по другим текстам, скажем [115], он ссылается на препринт 1994 года[34], который я не смог найти. В действительности в диссертации 1995 года Люкс делает гораздо больше, а именно, проверяет, что все $m < 2 \cdot 10^8$ допускают представление в таком виде. В сочетании с другими результатами, в частности, с теми, которые упомянуты в предыдущем пункте, это дает весьма веские основания верить, что $v(3) = 4$.

Диссертация Люкса содержит довольно подробное описание алгоритма и много технических деталей. К сожалению, эти результаты никогда не были опубликованы.

• В том же параграфе Гай обсуждает и гораздо более трудную задачу представления $m$ в виде $m = x^3 + y^3 + 2z^3$. Еще в издании 1994 года он упоминает 15 чисел $m < 1000$, для которых такое представление неизвестно, а именно

$$m = 76, 148, 183, 230, 356, 418, 428, 445, 482, 491, 580, 671, 788, 931, 967.$$

Однако в статье [156] Кояма ссылается на письмо Джона Коя Ричарду Гаю 1995 года, в котором получено решение

$$76 = -21167^3 - 122171^3 + 2 \cdot 97135^3$$

и представления чисел 230, 356, 418, 428, 445, 482, 580, 967, впрочем, все еще довольно маленькие.

• В 2000 году Кендзи Кояма [156] предложил существенное улучшение алгоритма поиска решений и довел анализ до $|z| \le 5 \cdot 10^7$. В этом интервале он нашел три новых решения $< 1000$, а именно

$$183 = 4170061^3 - 4494438^3 + 2 \cdot 2090533^3,$$
$$491 = 13476659^3 + 13584908^3 - 2 \cdot 13531000^3,$$
$$931 = -6942368^3 - 23115371^3 + 2 \cdot 18510883^3.$$

[34] Richard F. Lukes, All numbers less than 10 million can be represented as the sum of four cubes, 1994 preprint.

Начиная примерно с 2000 года Жан-Шарль Мейриньяк, Соичиру Ичида, Майкл Оукс, Хисанори Мисима и, возможно, многие другие, объявляли о попытках расширения области поиска решений уравнения $x^3 + y^3 + 2z^3 = m$. Информацию об этом можно найти, например, на сайтах

`http://www.asahi-net.or.jp/˜kc2h-msm/mathland/math04/cube02.htm`

`http://www.asahi-net.or.jp/˜kc2h-msm/`

но мне также не удалось найти дефинитивных публикаций.

## 7. ПОЛИНОМИАЛЬНЫЕ ТОЖДЕСТВА ТИПА ФРОЛОВА

Как мы убедились в двух предыдущих параграфах, легкая проблема Варинга не решена сегодня даже для кубов. Рациональная проблема Варинга решена для кубов и четвертых степеней. Для более высоких степеней речь идет пока только о нахождении хороших верхних оценок. Например, предполагается, что $\rho(k) \leq k$, но это, насколько мне известно, не доказано пока даже для пятых степеней.

С другой стороны, получение хороших верхних оценок в этих задачах связано с построением все более изощренных полиномиальных тождеств некоторого специального вида. Известно, что Рамануджану формулы диктовала во сне богиня Намаккал[35]. Большинство обычных[36] людей, даже среди соотечественников Рамануджана, не имеют доступа к такого рода ресурсам.

Поэтому здесь мы расскажем об идее систематического построения таких тождеств, предложенной в конце XIX века генералом *Мишелем* Фроловым. Это *кажется* шуткой, но это не шутка! Конечно, из докладов Ефима Исааковича Зельманова все мы знаем про генерала Бернсайда: “general Burnside problem”. Но в данном случае геометрические работы *генерала* Фролова неоднократно упоминаются в примечаниях к “Пангеометрии” Лобачевского [170].

### 7.1. Le Général Franco-Russe Michel Frolow

Из 23 русских генералов с фамилией Фролов, поименованных в словаре [7], ровно два Михаила. Но в качестве кандидата на роль Мишеля Фролова из них годится ровно один[37]. Это военный инженер Михаил Михеевич Фролов, 1833–1908, хорошо известный любителям военной истории как участник обороны Севастополя в 1854–1855 годах, а потом ближайший сотрудник Эдуарда Ивановича Тотлебена, принимавший участие в написании книги “Описание обороны г. Севастополя”, автор знаменитого дополнения к ней [13]. Он был произведен в генерал-майоры в 1870 году и в генерал-лейтенанты в 1882 году, в связи с уходом в отставку. В 1871–1879 годах служил начальником инженеров Финляндского военного округа (позже снова объединенного с Санкт-Петербургским военным округом). Через некоторое время после отставки он переехал во Францию, где

[35] “While asleep, I had an unusual experience. There was a red screen formed by flowing blood, as it were. I was observing it. Suddenly a hand began to write on the screen. I became all attention. That hand wrote a number of elliptic integrals. They stuck to my mind. As soon as I woke up, I committed them to writing.”

[36] “Мать Математика К. Гаусса Видела Невооружённым глазом Фазы Венеры И некоторые Спутники Юпитера.”

[37] В 1880-х годах он уже упоминается во французской литературе как генерал, в то время как Михаил Михайлович Фролов был произведен в генерал-майоры только в 1907 году.

весьма бодро принимал участие в научной жизни — все его математические статьи написаны по-французски и опубликованы во французских журналах — “Vous voulez des romans? Lisez de l’histoire.”

Первоначально мои поиски были направлены в ложную сторону тем, что многие, включая столь компетентных математиков и *историков* математики, как Атанас Пападопулос[38], утверждают, что Мишель Фролов был генералом *французской* армии. Так, в [170], с.274, Атанас совершенно недвусмысленно пишет: “Michel Frolov, a mathematician who was also a general in the French army.” На самом деле, мне кажется, что, если Фролов и был генералом французской армии, то только в том смысле, что работая над книгой [13] он полностью изучил как русские, так и французские журналы подземных работ (найдя в них несоответствия).

Потом, конечно, я обратил внимание на то, что Фролов подписывал свои книги 1884 и 1886 годов [96, 97] скромно, “инженер Фролов”. В 1886 году Михаил Фролов был Почетным Председателем сессии “Association française pour l’avancement des sciences” в Нанси. Там он поименован как “M. le Géneral Frolow[39], major général du génie russe“, т.е. “*российский* генерал-майор *инженерных* войск”, см. [179]. Что, кстати, тоже не соответствовало действительности, так как на тот момент он был уже генерал-лейтенантом в отставке.

Первоначально Фролов интересовался магическими квадратами и другими комбинаторными задачами. Этому посвящены его книги [96, 97], первая из которых издана еще в Петербурге, а вторая уже в Париже. Читать эти книги и сегодня огромное удовольствие. Первая из них открывается обширной отсылкой к Лейбницу[40]: “Leibnitz attachait une grande importance aux jeux mathématiques et aux problèmes destiné à servir de récréation. D’après lui, les hommes ne se montrent jamais plus ingénieux que dans le jeux qui sont basés, non sur le hasard, mais sur l’habilité.”

Там масса другого интересного. Следующая мысль перекликается с фрагментом из Эйлера, воспроизведенным в [2]: “Toutes les branches des mathématiques ont entre elles des liens tellement intimes que si l’une d’elles, en apparence incapable de rendre jamais aucun service à l’humanité, vient à réaliser quelque progrès, ce progrès peut influer sur le développement des autres branches. L’histoire nous fournit plus d’une preuve de cette vérité.” Это пишет военный инженер, т.е., казалось бы, человек сугубо практический. Много ли *сегодня* в мире людей из тех, кто принимает решения, обладающих подобной перспективой и подобным пониманием? Другой умиливший меня там фрагмент, это как раз ссылка на Либри, в ряду Лейбница, Ферма, Декарта, Эйлера: “Un mathématicien bien connu, Libri, présenta en 1842 à l’Académie des Sciences de Paris. . . ”

Увлечение магическими квадратами привело Фролова к изучению равенств в нескольких степенях, тому, что сегодня известно как проблема Пруэ—Тарри—Эскотта и ее варианты. Работы [98, 99], на которые мы здесь ссылаемся, написаны лет за 20 до работ Тарри и Эскотта.

Что касается его работ с опровержениями неэвклидовой геометрии [100], к ним, ко-

[38]В 2019–2020 годах Атанас занимал кафедру Ламе в Санкт-Петербурге `https://math-cs.spbu.ru/news/atanas-papadopulos-laureat-konkursa-kafedra-lame-2019/`, но мы с ним тогда это не обсуждали.

[39]До 1886 года сам генерал Фролов писал свою фамилию по-немецки, Frolow, а после этого обычно по-французски, Frolov.

[40]“1) Les hommes ne paraissent jamais plus ingènieux que dans les jeux, et les philosophes devraient en profiter pour perfectionner l’art des arts, qui est l’art de penser. 2) Maxime scientiae substant ludi qui unice arti eventum, nihil casui debent, in quibus haud dubie eminet ludus scacchicus seu regius, etc. 3) Optarem ut aliquis omnis generis ludos mathematice tractaret et tam regularum seu legum rationem redderet, quum artificia primaria traderet. 4) Je voudrais qu’un habile homme traitât en mathématicien et en physicien de toute sorte de jeux.”

нечно, можно отнестись как к любительскому бреду, в духе опровержений Зенкина канторовского диагонального процесса. Небольшой нюанс состоит, однако, в том, что в отличие от того же Зенкина, Фролов указывает на *фактические* математические ошибки в письмах Гаусса Шумахеру. Вот, что, например, говорит по этому поводу Атанас Пападопулос (ibid., p.277): “We must admit that strictly speaking, Frolov is right in pointing out what can be considered as a mistake by Gauss, since the limit of the triangle, in the most natural sense that can be given to the word limit, is not the tripod, but a figure that is called today an “ideal triangle”…”

## 7.2. Тождества Фролова

Зафиксируем натуральные числе $s$ и $h$ такие, что $s > h$. Сформулированная в переписке Гольдбаха и Эйлера 1750–1751 годов **проблема Пруэ—Тарри—Эскотта** состоит в нахождении двух непересекающихся *наборов* (= multisets, множеств с повторяющимися элементами) целых чисел $A = [a_1,\dots,a_s]$ и $B = [b_1,\dots,b_s]$, таких, что для всех $i = 1,\dots,h$ выполняются равенства

$$a_1^i + \ldots + a_s^i = b_1^i + \ldots + b_s^i.$$

Спустя ровно век в 1851 году Эжен Пруэ предложил первое систематическое решение несколько более общей задачи. Исторически наибольший интерес вызывали **идеальные решения**, для которых $s = h+1$. Идеальные решения известны для $2 \le h \le 9$ и для $h = 11$ и неизвестны в остальных случаях. Случай, когда количество слагаемых слева и справа различно, не расширяет общность, а просто означает, что какие-то из $x_i$ или $y_i$ равны 0. Мы вернемся к подробному обсуждению этой задачи в следующей статье серии.

Вот для примера одно из старинных идеальных решений для $h = 3$:

$$A = [0,4,7,11], \qquad B = [1,2,9,10].$$

В самом деле,

$$\begin{aligned}
&0+4+7+11 = 22 = 1+2+9+10 = 22,\\
&0^2+4^2+7^2+11^2 = 186 = 1^2+2^2+9^2+10^2,\\
&0^3+4^3+7^3+11^3 = 1738 = 1^3+2^3+9^3+10^3.
\end{aligned}$$

Важность проблемы PTE состоит в том, что — как заметил Фролов [98, 99] за 20++ лет до работ Тарри и Эскотта! — ее решения в точности соответствуют **тождествам Фролова**, т.е. полиномиальным тождествам вида

$$(x+a_1)^h + \ldots + (x+a_s)^h = (x+b_1)^h + \ldots + (x+b_s)^h.$$

Например, указанное выше решение для $h = 3$ эквивалентно тождеству

$$x^3 + (x+4)^3 + (x+7)^3 + (x+11)^3 = (x+1)^3 + (x+2)^3 + (x+9)^3 + (x+10)^3.$$

Перенося здесь все слагаемые в левую часть, мы получим равенство алгебраической суммы $2s$ штук $h$-х степеней нулю.

Но в действительности, самое интересное здесь только начинается. Фролов заметил, что если мы продолжим возводить те же самые линейные многочлены в степени $k > h$, то каждый раз старшие $h+1$ степеней будут сокращаться, давая нам выражение *какого-то* многочлена степени $k-h-1$ как алгебраической суммы $k$-х степеней.

Так, например, наше идеальное решение для $h = 3$ дает при возведении в степень $k = 4$ тождество

$$x^4 + (x+4)^4 + (x+7)^4 + (x+11)^4 - (x+1)^4 - (x+2)^4 - (x+9)^4 - (x+10)^4 = 720,$$

а при возведении в степень $k = 5$ — тождество

$$x^5 + (x+4)^5 + (x+7)^5 + (x+11)^5 - (x+1)^5 - (x+2)^5 - (x+9)^5 - (x+10)^5 = 2^4 \cdot 3^2 \cdot 5^2 t + 19800,$$

— но это, внезапно, и есть тождество именно того вида, который требовался нам для решения легкой проблемы Варинга для $k = 5$. Но, естественно, подобные тождества будут получаться и для более высоких степеней,

$$x^6 + (x+4)^6 + (x+7)^6 + (x+11)^6 - (x+1)^6 - (x+2)^6 - (x+9)^6 - (x+10)^6 = \\ 10800x^2 + 118800x + 361800,$$

и так далее.

### 7.3. Переборы с вариациями

В действительности, Михаил Фролов сделал несколько больше. А именно, он заметил, что для получения подобных тождеств нам достаточно найти решения **частичной проблемы PTE** — то, что сегодня известно как **mehrgradige Gleichungen**.

Не пытаясь объяснять его идеи в самом общем случае, ограничимся следующей простой вариацией. Ясно, что в $(x+a)^k + (x-a)^k$ автоматически сокращаются нечетные степени $a$, а в $(x+a)^k - (x-a)^k$ сокращаются четные степени $a$. Поэтому вместо решения полной проблемы PTE достаточно рассматривать следующие два ее варианта.

- **Четная проблема PTE.** Найти непересекающиеся наборы целых чисел $A = [a_1, \ldots, a_s]$ и $B = [b_1, \ldots, b_s]$, такие, что для всех $i = 1, \ldots, h$ выполняются равенства

$$a_1^{2i} + \ldots + a_s^{2i} = b_1^{2i} + \ldots + b_s^{2i}.$$

- **Нечетная проблема PTE.** Найти непересекающиеся наборы целых чисел $A = [a_1, \ldots, a_s]$ и $B = [b_1, \ldots, b_s]$, такие, что для всех $i = 1, \ldots, h$ выполняются равенства

$$a_1^{2i-1} + \ldots + a_s^{2i-1} = b_1^{2i-1} + \ldots + b_s^{2i-1}.$$

Как мы только что заметили, каждое решение четной проблемы PTE приводит к тождеству вида

$$(x+a_1)^h + (x-a_1)^h + \ldots + (x+a_s)^h + (x-a_s)^h = (x+b_1)^h + (x-b_1)^h + \ldots + (x+b_s)^h + (x-b_s)^h,$$

а каждое решение нечетной проблемы PTE — к тождеству вида

$$(x+a_1)^h + \ldots + (x+a_s)^h + (x+b_1)^h + \ldots + (x+b_s)^h = (x-a_1)^h + \ldots + (x-a_s)^h + (x-b_1)^h + \ldots + (x-b_s)^h.$$

Эти тождества и дальнейшие тождества такого типа, получающиеся при варьировании показателя степени $k$, линейных заменах переменных и т.д., называются **тождествами типа Фролова**. Вот пара замечательных тождеств, получающихся на этом пути.

• В 2000 году Аджай Чоудхри [59] доказал, что $\nu(7) \leq 12$. Для этого он использовал тождество

$$(x+a)^7+(x-a)^7+(2x+b)^7+(2x-b)^7-(x+c)^7-(x-c)^7-(2x+d)^7-(2x-d)^7=ex$$

где

$$a = 534407060429869176086407612538177, \qquad b = 859793943610761912321826231621886,$$
$$c = 292565171139318137956759657471297, \qquad d = 863420822620431936290192229011966.$$

Непосредственное вычисление[41] показывает, что

$$e = 2^{30}\cdot 3^4\cdot 5^3\cdot 7^4\cdot 11^3\cdot 13^3\cdot 17^3.43\cdot 59^3\cdot 71^3\cdot 79^3\cdot 83^3\cdot 127\cdot 151^3\cdot 397^3\cdot 1163^3\cdot$$
$$1223^3\cdot 3347^3\cdot 4513^3\cdot 12497^3\cdot 87383^3\cdot 3729161^3\cdot 7135459^3\cdot 23260673^3.$$

Методами пункта 4.3 легко убедиться в том, что каждый класс кольца $\mathbb{Z}/e\mathbb{Z}$ представляется как сумма не более, чем четырех 7-х степеней.

Я сильно сомневаюсь, что кто-то мог бы найти это тождество вручную. Мне почему-то кажется даже, что никто не стал бы и пытаться искать подобное тождество вручную, без поддержки компьютера и современных систем символьных вычислений.

• В 2008 году Аджай Чоудхри и Ярослав Врублевский [60] доказали, что $\nu(13) \leq 27$. Они использовали наименьшее известное решение [идеальной] **четной проблемы PTE**:

$$a_1^{2i}+\ldots+a_6^{2i}=b_1^{2i}+\ldots+b_6^{2i}, \qquad i=1,2,3,4,5,$$

равное

$$A=[22,61,86,127,140,151] \qquad B=[35,47,94,121,146,148],$$

чтобы построить тождество

$$\sum_{i=1}^{6}\Big((x+a_i)^{13}+(x-a_i)^{13}\Big)-\sum_{i=1}^{6}\Big((x+b_i)^{13}+(x-b_i)^{13}\Big)=cx,$$

где

$$c=2^{14}\cdot 3^{10}\cdot 5^3\cdot 7^2\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31.$$

Методами пункта 4.3 легко убедиться в том, что каждый класс кольца $\mathbb{Z}/c\mathbb{Z}$ представляется как сумма не более, чем трех 13-х степеней.

Мне кажется, что систематическое построение тождеств типа Фролова могло бы стать субстратом замечательного проекта распределенных вычислений для школьников и любителей математики. Требования к математической подготовке здесь минимальные, шансы получения новых результатов более, чем реальны, а исторический интерес огромен.

[41] “This identity can be readily verified by direct computation using any computer package such as `Maple`”, [59], p. 268.

### 7.4. Симметрические тождества

Известно очень мало других тождеств, которые дают бы такую же или лучшую оценку слабой константы Варинга $v(k)$, как тождества типа Фролова. Вот два самые знаменитые из них.

• Одно из ранних таких тождеств, это **тождество Рао** для *шестых* степеней, которое было использовано в [246] для доказательства оценки $v(6) \le 14$. Вот это тождество

$$12abcd(c^4-d^4)(a^{24}-b^{24})x = (a^5c+bdx)^6+(a^5d-bcx)^6+(b^5c-adx)^6+(b^5d+acx)^6 \\ -(a^5c-bdx)^6-(a^5d+bcx)^6-(b^5c+adx)^6-(b^5d-acx)^6.$$

• Построить аналогичное тождество *восьмой* степени довольно долго не удавалось, пока его не открыл Леонид Васерштейн [259], который получил с его помощью оценку $v(8) \le 28$. Вот **тождество Васерштейна**, после творческой переработки Лораном Абсигером:

$$16(uvw)^6(u^{48}v^{64}+v^{48}w^{64}+w^{48}u^{64}-u^{48}w^{64}-v^{48}u^{64}-w^{48}v^{64})y = \\ (u^7v^{10}+u^5w^6y)^8+(u^7w^{10}-u^5v^6y)^8+(v^7w^{10}+v^5u^6y)^8+(v^7u^{10}-v^5w^6y)^8 \\ +(w^7u^{10}+w^5v^6y)^8+(w^7v^{10}-w^5u^6y)^8-(u^7v^{10}-u^5w^6y)^8-(u^7w^{10}+u^5v^6y)^8 \\ -(v^7w^{10}-v^5u^6y)^8-(v^7u^{10}+v^5w^6y)^8-(w^7u^{10}-w^5v^6y)^8-(w^7v^{10}+w^5u^6y)^8$$

В действительности в работе Васерштейна это тождество выражено в совершенно другой, гораздо менее симметричной форме. Приведенная здесь форма получается в результате весьма замысловатой замены переменных с дробными показателями степени. Кроме того, как отмечается в [116], работа Васерштейна, как обычно, не свободна от опечаток. Так, например, вместо члена $a^{15}b^{63}c^{63}$ следует читать $a^{15}b^{28}c^{98}$, вместо члена $a^{80}b^{229}c^{395}$ следует читать $a^{80}b^{-16}c^{640}$, и так далее.

В этот момент каждому тренированному математику становится очевидной связь с **теорией представлений конечных групп**. И действительно, Абсигер в работах [116, 117] предложил конструкцию таких тождеств по следующим данным: i) конечная группа $G$, ii) представление $\pi$ группы $G$, iii) ее одномерный характер $\varepsilon$, iv) некоторый зависящий от $(\pi, \varepsilon)$ набор целых параметров.

Сама комбинаторная конструкция Абсигера слишком технична, чтобы излагать ее здесь. Отметим лишь, что в качестве самых первых примеров для совсем крошечных групп получаются следующие тождества.

• Для группы $C_2$ второго порядка — тождество Норри.

• Для четверной группы $V = C_2 \times C_2$ — тождество Рао.

• Для симметрической группы $S_3$ при одном выборе параметров — тождество Васерштейна.

• Для симметрической группы $S_3$ при другом выборе параметров — новое **тождество Абсигера** степени 7:

$$14(abc)^4(c^7-a^7)(b^7-a^7)(c^7-b^7)(a^{14}+b^{14}+c^{14}+a^7b^7+b^7c^7+a^7c^7)x = \\ (a^4x+b^3x^{10})^7+(b^4x+a^{10}c^3)^7+(c^4x+a^3b^{10})^7+(a^4x-b^3c^{10})^7+ \\ (b^4x-a^{10}c^3)^7+(c^4x-a^3b^{10})^7+(-a^4x+b^{10}c^3)^7+(-b^4x+a^3c^{10})^7+ \\ (-c^4x+a^{10}b^3)^7+(-a^4x-b^{10}c^3)^7+(-b^4x-a^3c^10)^7+(-c^4x-a^{10}b^3)^7.$$

Однако, это тождество дает худшую оценку для $v(7)$, чем приведенное в предыдущем пункте тождество Чоудхри.

Мы не будем пытаться воспроизводить дальнейшие тождества такого типа. Из них только тождества Рао и Васерштейна дают лучшие оценки в легкой проблеме Варинга, чем тождества типа Фролова. Я не предлагаю также принимать участие в поиске тождеств такого типа неспециалистам, так как здесь гораздо выше требования к пониманию математической стороны дела, в частности, собственно теории групп и теории представлений.

## 8. ПРОБЛЕМА ВАРИНГА В ЧИСЛОВЫХ КОЛЬЦАХ

Для сегодняшнего профессионального алгебраиста ограничение исключительно *рациональными* целыми представляет собой дань традиции и желание обойтись минимальными пререквизитами — вполне допустимые, впрочем, в преподавании и пропаганде математики.

С точки зрения же самой математики, все те же вопросы, которые здесь обсуждались для $\mathbb{Q}$ и $\mathbb{Z}$, *естественно* ставить *как минимум* для любого поля $K$ алгебраических чисел и его кольца целых $R = \mathcal{O}_K$. А на самом деле, после надлежащей модификации формулировок, и в гораздо более общих ситуациях.

Более того, в этом случае многие из них становятся проще или *гораздо* проще и допускают единообразные естественные ответы. Кольцо $\mathbb{Z}$ исключительно даже среди числовых колец. Например, в нем слишком мало обратимых элементов.

### 8.1. Суммы четырех кубов в кольце $\mathbb{Z}[i]$

В качестве первой иллюстрации приведем результат Джона Кона [65], утверждающий, что каждое целое гауссово число $u \in \mathbb{Z}[i]$ является суммой четырех кубов целых гауссовых чисел:

$$u = x^3 + y^3 + z^3 + w^3.$$

Для этого заметим, что, так как $-1, i, -i$ являются кубами в группе единиц $\mathbb{Z}[i]^*$, то элемент $u \in \mathbb{Z}[i]$ в том и только том случае выражается таким образом, когда так выражаются $-u, iu$ и $-iu$. Число 3 продолжает оставаться простым в кольце $\mathbb{Z}[i]$. Вид разложения зависит от того, делится $u$ на 3 или нет.

• Если $u \equiv 0 \pmod 3$, то нам достаточно рассмотреть три класса $u \equiv 0, 3, 3+3i \pmod 6$, Поскольку для чисел вида $6v$ и $6v+3$ мы уже знаем тождества, выражающие их как суммы трех или четырех кубов с целыми коэффициентами, рассмотрение этого случая завершается предъявлением такого же тождества для класса $6v+3+3i$:

$$6v + 3 + 3i = (iv)^3 + (iv - 1 + i)^3 - (iv + i)^3 - (iv - 1)^3.$$

• Если же $u \not\equiv 0 \pmod 3$, то нам достаточно рассмотреть четыре класса $u \equiv 1, 2, 1+i, 1+2i \pmod{(3+3i)}$. Однако, представимость $u$ из этих классов сразу вытекает из тождеств:

$$3(1+i)v + 1 = -(v+1-i)^3 + \big((2i-1)v + i - 3\big)^3 + \big((1-3i)v + 3 - 2i\big)^3 - \big((2+2i)v + 1 + 3i\big)^3,$$

$$3(1+i)v + 2 = (v+1)^3 + (iv+1)^3 - (iv)^3 - v^3,$$

$$3(1+i)v + 1 + i = \big((1+2i)v + 24 + 12i\big)^3 + (2v + 18 - 15i)^3 + (v + 12 - 10i)^3 + \big((i-1)v + 18i - 5\big)^3,$$

$$3(1+i)v + 1 + 2i = (v-i)^3 + \big((1+i)v + 1\big)^3 - \big((1+i)v\big)^3 + (v+i)^3.$$

Впечатляет? Здесь важно не то, что для кубов в кольце целых гауссовых чисел — в отличие от обычных целых рациональных чисел — легкая проблема Варинга полностью решается. Важно то, *насколько* она проще классической проблемы, и что она полностью решается МЕТОДАМИ ШКОЛЬНОЙ АЛГЕБРЫ — это решение, при желании, мог написать в XIX веке всякий любитель — если бы ему, конечно, пришел в голову такой вопрос. Впрочем, профессионал как раз и отличается от любителя не способностью давать ответы, а способностью осознавать вопросы.

### 8.2. Суммы 12 биквадратов в кольце $\mathbb{Z}[\omega]$

Воспроизведем теперь для разнообразия результат Филиппа Ревуа [211], утверждающий, что каждое целое эйзенштейново число $x \in \mathbb{Z}[\omega]$ является суммой 12 биквадратов целых эйзенштейновых чисел. Здесь $\omega$ — первообразный кубический корень из 1, так что $1+\omega+\omega^2=0$.

• Заметим, прежде всего, что каждое целое эйзенштейново число является суммой трех квадратов. Поскольку этот факт очевиден, и, несомненно, известен со времени Эйзенштейна, я не стал искать точную историческую ссылку, так как само рассуждение написано в большом количестве источников (например, [140, 199]).

Для начала вспомним, что в любом коммутативном кольце любой элемент, который представляется как сумма *любого* количества квадратов, есть алгебраическая сумма трех квадратов. В самом деле,

$$x_1^2+\ldots+x_s^2=(x_1+\ldots+x_2+1)^2-(2y+1)=(x_1+\ldots+x_2+1)^2-y^2+(y+1)^2,$$

где

$$y=(x_1x_2+x_1x_3+\ldots+x_{s-1}x_2)+(x_1+\ldots+x_s),$$

Поскольку $1=1^2$, $\omega=(\omega^2)^2$ и $\omega^2$ — квадраты, любое Эйзенштейново число есть сумма квадратов и, значит, представляется в виде $u=x^2-y^2-z^2$. Осталось вспомнить, что $-1=\omega+\omega^2$ есть сумма двух квадратов. Тем самым,

$$u=x^2+(\omega+\omega^2)(y^2+z^2),$$

но, как мы знаем, произведение сумм двух квадратов снова является суммой двух квадратов (норма комплексного числа).

• Вместо тождества Лиувилля можно теперь воспользоваться гораздо более простым тождеством

$$2(x^2+xy+y^2)^2=x^4+(x+y)^4+y^4,$$

которое, впрочем, является частным случаем тождества Лиувилля.

• Так как

$$-3u=(u-1)^2+(u-1)(\omega(u+1)+1)+(\omega(u+1)+1)^2,$$

из тождества Лиувилля следует, что $18u^2$ является суммой трех биквадратов. В сочетании с тем, что каждый элемент $\mathbb{Z}[\omega]$ есть сумма трех квадратов, это означает, что любой элемент $18\mathbb{Z}[\omega]$ есть сумма 9 биквадратов.

• С другой стороны, так как

$$v=u(1+2\omega)+1=u^2+u(\omega u+1)+(\omega u+1)^2,$$

то снова по тождеству Лиувилля $2v^2$ есть сумма трех биквадратов

Применяя теперь тождество

$$6z = (z+1)^2 + (\omega z + \omega^2)^2 + (\omega^2 z + \omega)^2,$$

к $z = (1+2\omega)u$, мы видим, что каждый элемент вида $12(1+2\omega)u$ тоже есть сумма 9 биквадратов.

• Таким образом, нам остается только показать, что по модулю 18 любой элемент $\mathbb{Z}[\omega]$ является суммой 3 биквадратов. Но по китайской теореме об остатках

$$\mathbb{Z}[\omega]/18\mathbb{Z}[\omega] \cong \mathbb{F}_4 \oplus \mathbb{Z}[x]/\big(9\mathbb{Z}[x] + (x^2+3)\mathbb{Z}[x]\big),$$

а это ровно та ситуация, которую мы обсуждали в § 4. Каждый элемент поля $\mathbb{F}_4$ есть биквадрат, а каждый элемент второго слагаемого представляется как сумма трех биквадратов по лемме Гензеля.

Впечатляет? Снова важно здесь именно то, что все делается методами школьной алгебры — ну, по крайней мере для того, кто знает комплексные числа.

В этот момент все задумались над тем, насколько можно сократить перебор и сколько же еще новых тождеств такого типа можно построить при наличии в кольце других корней из 1 — да и вообще других обратимых элементов! Систематическое построение тождеств такого типа могло бы стать крупным и чрезвычайно поучительным распределенным проектом для школьников, в процессе которого они могли бы выучить огромный фрагмент *реально* содержательной математики, полезный, в отличие от того, чему их сейчас обычно учат, для *сегодняшних* приложений.

## 9. ПОЛИНОМИАЛЬНАЯ ПРОБЛЕМА ВАРИНГА

Те же вопросы, которые сформулированы во введении, естественно задавать не только для поля $\mathbb{Q}$ и кольца $\mathbb{Z}$, но для произвольных полей и колец. Пусть, например, $K$ — произвольное поле. Формула Райли—Ричмонда по прежнему дает выражение произвольного $x \in K$ как суммы трех кубов.

• Конечно, у нас будут небольшие проблемы в характеристике 3. Но это как раз понятно, в характеристике 3 сумм кубов очень мало,

$$u^3 + v^3 + w^3 = (u+v+w)^3.$$

Но ведь в общем случае совсем не любой элемент обязан быть кубом.

• Но, в любом случае, эта формула является *рациональной*, в ней есть *знаменатели*. Иными словами, это формула в поле рациональных дробей $K(x)$. Естественно возникает вопрос, существуют ли аналогичные полиномиальные формулы. Иными словами, формулы, выражающие $x$ как суммы трех кубов *многочленов* от $x$?

Оказывается, этот вопрос допускает различные уточнения, и то, насколько сложен ответ на него, зависит от многих обстоятельств.

### 9.1. Как сформулировать полиномиальную проблему Варинга?

Ясно, что тот же вопрос можно задавать для любого количества любых степеней — не обязательно трех, не обязательно кубов. Как мы только что заметили, в случае, когда char$(K)$ делит $k$, надеяться на положительный ответ не приходится. Поэтому всюду в дальнейшем мы предполагаем, что $k$ не делится на характеристику основного поля.

• **Наивная полиномиальная проблема Варинга**. Найти для каждого натурального $k$ *наименьшее* натуральное $s$ такое, что любой многочлен $f \in K[x]$ можно представить как сумму $k$-х степеней многочленов $f_1, \dots, f_s \in K[x]$,

$$f = f_1^k + \ldots + f_s^k,$$

в количестве $s$ штук.

Однако, если вдуматься, здесь сформулирован аналог не исходной проблемы Варинга, а *какой-то*[42] слабой версии! Ведь в исходной проблеме предлагалось найти сумму $k$-х степеней не всех целых чисел, а только натуральных. Иными словами, мы выбираем в каждом классе ассоциированных ненулевых целых чисел положительное. Аналогом *знака* в кольце многочленов естественно считать *старший коэффициент*: в каждом классе ассоциированных ненулевых многочленов есть единственный нормированный[43]. Таким образом, настоящий аналог классической проблемы Варинга должен выглядеть следующим образом.

• **Полиномиальная проблема Варинга**. Найти для каждого натурального $k$ *наименьшее* натуральное $s = g_{K[x]}(k)$ такое, что любой многочлен $f \in K[x]$ можно представить как сумму $k$-х степеней *нормированных* многочленов $f_1, \dots, f_s \in K[x]$,

$$f = f_1^k + \ldots + f_s^k,$$

в количестве $\leq s$ штук.

Чтобы избежать обсуждения трудных арифметических условий, оставим в стороне характеристику 0 — в этом случае нахождение явной константы совершенно нетривиально уже для квадратов[44] в самом поле $K$, этому посвящена огромная литература.

Для колец многочленов $\mathbb{F}_q[x]$ над конечным полем $\mathbb{F}_q$ из $q = p^h$ элементов проблему Варинга примерно в такой форме с дополнительным равномерным ограничением на степени

$$\deg(f_1), \dots, \deg(f_s) \leq n \cdot \deg(f),$$

где $n$ и $s$ зависят от $k$, решил Пэли[45] в 1933 году [197]. Мы не будем аккуратно формулировать его теорему и дальнейшие результаты в таком духе, где приходится делать массу оговорок, чтобы исключить очевидные запреты и т.д. Доказательство Пэли основано на использовании метода Харди—Литтлвуда. Разумеется, сегодня известны чисто алгебраические доказательства более сильных фактов. Например, теорема Пэли является очень частным случаем результатов Васерштейна [256, 257].

[42] Какой именно, зависит от количества $k$-х степеней в поле $K$. Для маленьких $K$ это может быть аналог классической или легкой проблемы Варинга, но в общем случае что-то еще менее ограничительное.

[43] В книге [91] Эффинджер и Хайес даже называют нормированные многочлены *положительными*.

[44] Разумеется — как мы вспомнили в предыдущем параграфе! — с точностью до тонких настроек речь идет о нахождении **ступени** поля $K$, т.е. длины $s(K)$ самого короткого представления $-1 = x_1^2 + \ldots + x_s^2$. **Теорема Пфистера** утверждает, что если $s(K)$ конечна, то она является степенью двойки, $s(K) = 2^h$, $h \in \mathbb{N}$. При этом, если $s(K) = 1$, то $g(K, 2) = 1, 2, 3$. Если $s(K) = 2^h$, $h \geq 2$, то $g(K, 2) = 2^h, 2^h + 1$. Но, если ступень поля $K$ бесконечна, т.е. $-1$ не является там суммой квадратов, как это происходит для формально вещественных полей, то $g(K, 2)$ может быть вообще произвольным.

[45] Тот самый Пэли, Раймонд Эдвард Алан Кристофер, который Пэли—Винер, преобразование Фурье в комплексной области. На вид довольно неожиданно, но на самом деле, нет, так как метод Харди—Литтлвуда это именно комплексный анализ.

Однако еще в 1930-е годы Леонард Карлиц[46] заметил, что, если не накладывать *априорных* ограничений на степени $f_1,\dots,f_s$, таких представлений слишком много, за счет сокращений в старших степенях. Сам Карлиц предложил рассматривать следующую гораздо более трудную задачу, в которой степени многочленов $f_1,\dots,f_s$ минимальные возможные, с тем, вообще чтобы никаких сокращений, кроме строго необходимых, при сложении их $k$-х степеней не происходило.

• **Строгая полиномиальная проблема Варинга**. Найти для каждого натурального $k$ *наименьшее* натуральное $s = s_{K[x]}(k)$ такое, что любой многочлен $f \in K[x]$ можно представитьможно представить как сумму

$$f = f_1^k + \ldots + f_s^k,$$

$k$-х степеней многочленов $f_1,\dots,f_s \in K[x]$ в количестве $s$ штук, причем их степени удовлетворяют неравенствам

$$\deg(f_1),\dots,\deg(f_s) \le \left\lceil \frac{\deg(f)}{k} \right\rceil.$$

Наложенные здесь ограничения на степень оказались слишком сильными. Проблема в таком виде все еще решается, по крайней мере для больших $p$, но в ее решении вовсю используется теория полей классов, гипотезы Вейля и многое другое в таком духе. Поэтому сегодня часто рассматривают промежуточные варианты включающие *какие-то* априорные ограничения на степени $f_1,\dots,f_s$, но такие, которые не запрещали бы использование полиномиальных тождеств. Вот одна из самых популярных версий.

• **Домашняя полиномиальная проблема Варинга**. Найти для каждого натурального $k$ *наименьшее* натуральное $s = t_{K[x]}(k)$ такое, что любой многочлен $f \in K[x]$ можно представитьможно представить как сумму

$$f = f_1^k + \ldots + f_s^k,$$

$k$-х степеней многочленов $f_1,\dots,f_s \in K[x]$ в количестве $s$ штук, причем их степени удовлетворяют неравенствам

$$\deg(f_1),\dots,\deg(f_s) \le \deg(f).$$

Здесь нет, разумеется, никакой возможности обсуждать полиномиальную проблему Варинга во всех вариантах и рамификациях. Ограничимся, поэтому, одним небольшим примером.

[46] Книга [91] начинается с рассказа о приезде Леонарда Карли[т]ца, 1907—1999, в Кэмбридж в 1930–1932 годах, где он, собственно, и предложил Пэли заняться полиномиальной проблемой Варинга. В 1933–1937 годах сам Карлиц исследовал строгую полиномиальную проблему Варинга для квадратов, в дальнейшем в 1950-е годы и для старших степеней. Однако я испытываю некоторые затруднения с тем, чтобы выбрать из его примерно 800 публикаций, общим объемом 7000–8000 страниц — большинство из которых посвящены именно многочленам над конечными полями! — те, которые следует включить в библиографию к настоящей статье, и подожду, пожалуй, окончания публикации его избранных трудов, чтобы сослаться сразу на все. Я хорошо помню свой шок начала 1970-х годов, когда приходя на выставку свежих поступлений в библиотеку ПОМИ, видел его статью в каждом номере каждого журнала. Вот как примерно это излагает Дэвид Хайес: “In 1953 he published a record 44 papers. His most active decade was 1960–69, when he averaged 27 papers per year. . . . On more than one day I observed him reading a journal paper raising a question that he found of interest, that evening writing up a paper of his own answering the question, and having it typed and sent off to a journal the following day.”, [121].

### 9.2. Суммы трех кубов в кольце $K[x]$

Обсудим, следуя [51, 91, 260] представимость элементов $\mathbb{F}_q[x]$ суммами трех кубов. Как обычно, мы предполагаем, что $\mathrm{char}(K) \neq 0, 3$.

• Легко убедиться в том, что при $q \neq 2, 2^2, 2^4, 7, 13$ в поле $\mathbb{F}_q$ найдутся такие $a, b \neq 0$, что $a^3 + b^3 = 1$. В этом случае имеет место **тождество Серра**[47]:

$$f = \left(\frac{f + a^3 + 1}{3a}\right)^3 + \left(\frac{f + a^3 - 2}{3b}\right)^3 - \left(\frac{f - 2a^3 + 1}{3ab}\right)^3,$$

выражающее любой многочлен как *домашнюю* сумму кубов — степени всех многочленов решения не превосходят степень самого $f$. Однако, это тождество не дает, вообще говоря, решения строгой проблемы Варинга.

• В характеристике 7 имеет место равенство

$$x = -(x^5 + 3x^3 - x)^3 - (x^6 - 3x^4 + x^3 + x + 1)^3 + (x^6 + 3x^4 + x^3 + x - 1)^3.$$

так что, если не интересоваться степенями слагаемых, каждый многочлен представляется как сумма трех кубов.

А вот с ограничением степени ответ чуть сложнее. Конечно, случай многочленов над полями $\mathbb{F}_{7^h}$, $h \geq 2$, охватываются предыдущим пунктом. Но в поле $\mathbb{F}_7$ сумма трех ненулевых кубов не может равняться нулю, поэтому линейный многочлен в $\mathbb{F}_7[x]$ невозможно представить как сумму трех кубов линейных многочленов.

В то же время, домашние представления как суммы *четырех* кубов легко написать и в этом случае, например:

$$x = (x+1)^3 + (x-1)^3 - (x+3)^3 - (x-3)^3.$$

• В характеристике 13 имеет место равенство

$$x = (x^4 + 6x^3 + 5x^2 - 4x)^3 + (5x^3 - 3x^4 - 5x^3 + x^2 + 4x + 1)^3 - (5x^5 - 3x^4 - 5x^3 + 5x^2 - 5x + 1)^3.$$

Но над полем $\mathbb{F}_{13}$ лучшее, что удается сделать, если ограничивать степень, это получить разложение в сумму *четырех* кубов, например

$$f = (x+1)^3 + (x-1)^3 - (x+4)^3 - (x-4)^3.$$

Случай $\mathrm{char}(K) = 2$ тоже разобран, но мы не будем воспроизводить детали.

Опять все делается методами школьной алгебры — ну, по крайней мере для того, кто знает конечные поля. Систематическое построение тождеств такого типа в разных характеристиках, с разными ограничениями на степени и т.д. могло бы стать еще одним чрезвычайно интересным распределенным проектом для школьников.

[47] Тот самый Жан-Пьер Серр. На вид довольно неожиданно, но на самом деле, нет. Именно Серр дал ответ на аналогичный вопрос для квадратов. Относительно этой формулы для кубов Хайес и Васерштейн ссылаются на письма Серра, датированные 1982 годом. Сам он по всей видимости эти результаты для кубов не публиковал. Скорее всего, ровно потому, что не хотел публиковать незаконченный результат, а формулы в исключительных характеристиках без компьютера вдруг не напишешь.

## 10. ПРОДОЛЖЕНИЕ ТЫСЯЧЕЛЕТНЕЙ ТРАДИЦИИ ДРУГИМИ СРЕДСТВАМИ

Мой главный тезис состоит в том, что появление компьютеров и систем компьютерной алгебры резко расширило наши возможности и сам предмет теории чисел. Я не верю, что сформулированные в [2–4] и в настоящей работе недавние результаты могли бы быть получены без компьютера, что кто-либо вообще мог задаваться такого рода вопросами *в такой форме*. Еще значительнее роль компьютеров в опровержении гипотез. Вот что, например, говорит по этому поводу Анджей Шинцель: "Za to niewątpliwie w rozwoju teorii liczb pomógł rozwój komputerów – maszyn liczących. Dzięki nim obalono hipotezy, które utrzymywały się przez ponad 100 lat, a w jednym przypadku nawet 250 lat."

Я *полностью* солидарен с тем, что по этому поводу говорит Джонатан Борвайн: "the power of modern computers matched with that of modern mathematical software and the sophistication of current mathematics is changing the way we do mathematics", [43]. С тем, что вторая часть этого высказывания столь же важна, как первая. Современный *фантастический* прогресс в решении классических вопросов, которые до этого были открыты много веков, в такой же степени обязан и росту собственно математической софистикации, тому, что новые поколения математиков с рождения владеют не только математикой 1890–1950 годов, математикой Гильберта и Бурбаки, но и теми невероятными идеями математики 1950–1970 годов, символической фигурой для которых был Александр Гротендик.

Вместе с тем, при всех произошедших изменениях, как с точки зрения наших вычислительных возможностей, так и математических идей, я, как и Андре Вейль полвека назад, воспринимаю то, чем мы делаем сегодня, как продолжение тысячелетней традиции другими средствами: "The main thesis will be the continuity of number theory for the last three hundred years and the fact that what we are doing now is in direct continuation of what has been done by the greatest number-theorists since Fermat started it all in the seventeenth century", [268].

Я благодарен Сергею Позднякову, который убедил меня написать этот цикл статей, за чрезвычайно полезные обсуждения.

### Список литературы

1. *Вавилов Н. А.* Компьютеры как новая реальность математики: I. Personal account. Компьютерные инструменты в Образовании, 2020. No 2, 5–26. doi:10.32603/2071-2340-2020-2-5-26
2. *Вавилов Н. А.* Компьютеры как новая реальность математики: II. Проблема Варинга. Компьютерные инструменты в Образовании, 2020, No. 3, 5–55. doi: 10.32603/2071-2340-2020-3-5-55
3. *Вавилов Н. А.* Компьютер как новая реальность математики: III. Числа Мерсенна и суммы делителей Компьютерные инструменты в Образовании, 2020, No. 4, 5–58. https://doi.org/10.32603/2071-2340-2020-4-5-58
4. *Вавилов Н. А.* Компьютер как новая реальность математики: IV. Гипотеза Гольдбаха. Компьютерные инструменты в Образовании, 2020, No.
5. *Вавилов Н. А., Халин В. Г., Юрков А. В.* Mathematica для нематематика, М., МЦНМО, 2021, 484с.
6. *Веребрюсовъ А. С.* Объ уравненіи $x^3 + y^3 + z^3 = 2u^3$, Матем. сб., **26** (1908), no 4, 622–624.
7. *Волков С. В.* Генералитет Российской Империи: энциклопедический словарь генералов и адмиралов от Петра I до Николая II. В 2 т. М., Центрополиграф, 2009.
8. *Демидов С. С.* К истории теории линейных дифференциальных уравнений, Историко-математические Исследования, 1985, вып. 28, 78–98.
9. *Демьяненко В. А.* Об уравнении $x^3 + y^3 + z^3 - t^3 = 1$, Изв. вузов. Матем., 1965, no. 5, 57

10. *Демьяненко В. А.* О суммах четырех кубов, Изв. вузов. Матем., 1966, no. 5, 64–69, английский перевод на сайте Анри Коэна `http://www.math.u-bordeaux.fr/~cohen`
11. *Манин Ю. И.* Кубические формы, Наука, М., 1972, 304с.
12. *Манин Ю. И., Панчишкин А. А.* Введение в теорию чисел, Современные Проблемы Математики, т.49, ВИНИТИ, М., 1990, 348с.
13. *Фролов М. М.* Минная война въ Севастополѣ въ 1854–1855г. подъ руководствомъ генералъ-адъютанта Тотлебена. СПб., Типографія Н. Тиблена и Комп. (Н. Неклюдова), В. О., 1868, 172с. `https://www.prlib.ru/item/343533`. Переиздано как приложение к: Тотлебен Э. И. Описание Обороны г. Севастополя, М., Принципиум, 2017, 392с.
14. *Хис-Браун Д. Р.* К теоремам Шевалле–Варнинга, Успехи Мат. Наук, **66** (2011), no. 2 (398), 223–232.
15. *Alnaser A. J.* Bounds for Waring's number mod $\mathscr{P}^m$ in number fields. J. Number Theory **133** (2013), no. 1, 72–82.
16. *Alnaser A., Cochrane T.* Waring's number mod $m$. J. Number Theory **128** (2008), no. 9, 2582–2590.
17. *Avagyan A., Dallakyan G.* A new method in the problem of three cubes. Universal Journal of Computational Mathematics, **5** (2017), no. 3, 45–56, DOI: 10.13189/ujcmj.2017.050301
18. *Bagis N. D.* On the numbers that are sums of three cubes. arXiv:2009.11972v1.[math.GM], 24 Sep 2020, 14p.
19. *Ballico E., De Paris A.* Generic power sum decompositions and bounds for the Waring rank. Discrete Comput. Geom. **57** (2017), no. 4, 896–914.
20. *Banerjee D.P.* On the solution of the "easier" Waring problem. Bull. Calcutta Math. Soc. **34** (1942), 197–199.
21. *Bang, A. S.* Om Tal, som kan skrives som en Sum af tre eller fire Kubiktal. Mat. Tidsskr. B, København, 1940, 25–40.
22. *Barbin É* Gaston Tarry et la doctrine des combinaisons. Dans: Les travaux combinatoires en France (1870–1914) et leur actualité, 119–144, Savoirs Sci. Prat. Enseign., Presses Univ. Limoges, Limoges, 2017.
23. *Bateman P. T., Stemmler R. M.* Waring's problem for algebraic number fields and primes of the form $(p^r-1)/(p^d-1)$. Illinois J. Math. **6** (1962), 142–156.
24. *Beck M., Pine E., Tarrant W., Yarbrough Jensen K.* New integer representations as the sum of three cubes. Math. Comput. **76** (2007), 1683–1690.
25. *Becker E.* Hereditarily Pythagorean fields, infinite Harrison-primes and sums of $2^n$th powers. Bull. Amer. Math. Soc. **84** (1978), no. 2, 278–280.
26. *Becker E.* The real holomorphy ring and sums of $2n$th powers. Real algebraic geometry and quadratic forms (Rennes, 1981), 139–181, Lecture Notes in Math., **959**, Springer, Berlin-New York, 1982.
27. *Becker E.* Summen $n$-ter Potenzen in Körpern. J. Reine Angew. Math. **307** (1979), 8–30.
28. *Becker E., Berr R., Delon F., Gondard D.* Hilbert's 17th problem for sums of $2n$th powers. J. Reine Angew. Math. **450** (1994), 139–157.
29. *Becker E., Powers V.* Sums of powers in rings and the real holomorphy ring. J. Reine Angew. Math. **480** (1996), 71–103.
30. *Bell E. T.* Note on an easier Waring problem. J. Lond. Math. Soc. **11** (1936), 277–278.
31. *Bell E. T.* Algebraic Identities in the Theory of Numbers, Amer. Math. Monthly, **50** (1943), no. 9, 535–541.
32. *Bell E. T.* A method in rational Diophantine analysis. Proc. Nat. Acad. Sci. U.S.A. **30** (1944), 355–359.
33. *van Bendegem J.-P.* The heterogeneity of mathematical research. Perspectives on interrogative models of inquiry. Developments in inquiry and questions. Başkent, Can (ed.), Cham: Springer. Log. Argum. Reason. 8, 73-94 (2016).
34. *Bergelson V., Best A., Iosevich.* Sums of powers in large finite fields: a mix of methods. Amer. Math. Monthly **128** (2021), no. 8, 701–718.
35. *Berr R., Delon F.* Sums of powers in function fields. J. Pure Appl. Algebra **161** (2001), no. 3, 269–294.
36. *Bhaskaran M.* Sums of $m$th powers in algebraic and Abelian number fields. Arch. Math. (Basel) **17** (1966), 497–504; Corrections , ibid. **22** (1971), 370–371.
37. *Birch B.* Waring's problem in algebraic number fields, Proc. Cambridge Philos. Soc. **57** (1961), 449–459.

38. *Birch B.* Waring's problem for p-adic number fields. Acta Arith. **9** (1964), 169–176.
39. *Bodin A., Car M.* Waring's problem for polynomials in two variables. Proc. Am. Math. Soc. **141** (2013), no. 5, 1577–1589.
40. *Bohman J., Fröberg C.-E.* Numerical investigation of Waring's problem for cubes. BIT **21** (1981), no. 1, 118–122.
41. *Booker, A. R.* Cracking the problem with 33. Res. Number Theory **5** (2019), no. 3, paper no. 26, 1–6.
42. *Booker, A. R., Sutherland A.* On a question of Mordell. Proceedings of the National Academy of Sciences of the United States of America, 118 (2021), no. 11, 12p., [e2022377118]. `https://doi.org/10.1073/pnas.2022377118`
43. *Borwein P.* Computational Excursions in Analysis and Number Theory, CMS books in mathematics 10, Springer-Verlag, New York, 2002. Ch. 12 The Easier Waring Problem
44. *Bovey J. D.* A new upper bound for Waring's problem $\pmod p$. Acta Arith. **32** (1977), no. 2, 157–162. 987), no. 2, 165–180.
45. *Bremner A.* On sums of three cubes, Number theory (Halifax, NS, 1994). In: Conf. Proc., vol. 15, Amer. Math. Soc., Providence, pp.87–91 (1995).
46. *Bremner A., Guy R. K.* A dozen difficult diophantine dilemmas. Am. Math. Mon. **95** (1988), no. 1, 31–36.
47. *Bremner A., Morton P.* A new characterization of the integer 5906. Manuscripta Math. **44** (1983), no. 1–3, 187–229.
48. *Cantor M.* Sur l'historiographie des mathématiques. Paris: Gauthier-Villars. Congr. Intern. des Math. (Paris, 1900), 27–42 (1902).
49. *Car M.* The circle method and the strict Waring problem in function fields. The arithmetic of function fields (Columbus, OH, 1991), 421–433, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.
50. *Car M.* New bounds on some parameters in the Waring problem for polynomials over a finite field. Contemp. Math. **461**, 59–77 (2008)
51. *Car M., Gallardo L.* Sums of cubes of polynomials. Acta Arith. **112** (2004), 41–50.
52. *Car M., Gallardo L. H.* Waring's problem for polynomial biquadrates over a finite field of odd characteristic. Funct. Approx. Comment. Math. **37** (2007), part 1, 39–50.
53. *Carlini E., Catalisano M. V., Geramita A. V.* The solution to the Waring problem for monomials and the sum of coprime monomials. J. Algebra **370** (2012), 5–14.
54. *Cassels J. W. S.* A note on the Diophantine equation $x^3+y^3+z^3=3$. Math. Comput. **44** (1985), 265–266.
55. *Catalisano M. V., Chiantini L., Geramita A. V., Oneto A.* Waring-like decompositions of polynomials, I. Linear Algebra Appl. **533** (2017), 311–325.
56. *Chinburg T.* "Easier" Waring problems for commutative rings. Acta Arith. **35** (1979), no. 4, 303–331.
57. *Choudhry A.* Representation of every rational number as an algebraic sum of fifth powers of rational numbers. Enseign. Math. (2) **35** (1989), no. 1–2, 19–20.
58. *Choudhry A.* On sums of eighth powers. J. Number Theory **39** (1991), no. 1, 104–107.
59. *Choudhry A.* On sums of seventh powers. J. Number Theory **81** (2000), no. 2, 266–269.
60. *Choudhry A., Wróblewski J.* Ideal solutions of the Tarry—Escott problem of degree eleven with applications to sums of thirteenth powers. Hardy-Ramanujan J. **31** (2008), 1–13.
61. *Cipra J. A.* Waring's number in a finite field. Integers **9** (2009), A34, 435–440.
62. *Cipra J. A., Cochraine T., Pinner Ch.* Heilbronn's conjecture on Waring's number $(\bmod p)$. J. Number Theory **125** (2007), no. 2, 289–297.
63. *Clark P. L.* Number theory: a contemporary introduction http://math.uga.edu/~pete/4400FULL.pdf, 272p.
64. *Colliot-Thélène J.-L., Wittenberg O.* Groupe de Brauer et points entiers de deux familles de surfaces cubiques affines. Amer. J. Math. **134** (2012), no. 5, 1303–1327.
65. *Cohn J. H. E.* Sums of cubes of Gaussian integers. Proc. Amer. Math. Soc. **29** (1971), 426.
66. *Cohn J. H. E.* Waring's problem in quadratic number fields, Acta Arithm. **20** (1972), 1–16. Addendum: ibid. **23** (1973), 417–418.
67. *Cohn J. H. E., Mordell L. J.* On sums of four cubes of polynomials. J. London Math. Soc. (2) **5** (1972), 74–78.
68. *Conn W., Vaserstein L. N.*, On Sums of Three Integral Cubes, Contemporary Mathematics **166** (1994),

285–294.
69. *Cooke A., Hamblen S., Whitfield S.* Sums of squares in quaternion rings. Involve **10** (2017), no. 4, 651–664.
70. *Davenport H.* Note on sums of fourth powers. J. London Math. Soc. **16** (1941), 3–4.
71. *Davenport H., Landau E.* On the representation of positive integers as sums of three cubes of positive rational numbers. Abh. Zahlentheorie Analysis, zur Erinnerung an E. Landau, 49–53 (1968).
72. *Davidson M.* Sums of $k$-th powers in number fields. Mathematika **45** (1998), no. 2, 359–370.
73. *Davidson M.* On Waring's problem in number fields. J. London Math. Soc. (2) **59** (1999), no. 2, 435–447.
74. *Del Centina A., Fiocca A.* Guglielmo Libri, matematico e storico della matematica. L'irresistibile ascesa dall'Ateneo pisano all'Institut de France. Cultura e Memoria **47**. Fondi Scientifici della Biblioteca Moreniana II. Leo S. Olschki Editore, Florence, 2010. XXII+320+xxii pp.; CD-ROM: pp. 323–482.
75. *Demiroğlu K. Y.* Waring's problem in finite rings. J. Pure Appl. Algebra **223** (2019), no. 8, 3318–3329.
76. *Dickson L. E.* History of the theory of numbers, vol. I. Divisibility and primality, Chelsea, 1952, 486p.
77. *Dickson L. E.* History of the theory of numbers, vol. II. Diophantine analysis, Chelsea, 1952, 803p.
78. *Dickson L. E.* History of the theory of numbers, vol. III. Quadratic and higher forms, Chelsea, 1952, 313p.
79. *Dolan S. W.* On expressing numbers as the sum of two cubes, Math. Gaz., **66** (1982), 31–38.
80. *Duren P.* Changing faces: the mistaken portrait of Legendre. Notices Amer. Math. Soc. **56** (2009), no. 11, 1440–1443.
81. *Eda Y.* On the Waring problem in an algebraic number field. Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 10, 11p. Inst. Statist. Math., Tokyo, 1971.
82. *Eda Y.* On Waring's problem in algebraic number fields. Rev. Colombiana Mat. **9** (1975), no. 2, 29–73.
83. *Effinger G. W., Hayes D/ B.* Additive number theory of polynomials over a finite field. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1991. xvi+157 pp.
84. *Ehrhardt C.* A quarrel between Joseph Liouville and Guillaume Libri at the French Academy of Sciences in the middle of the nineteenth century. Historia Math. **38** (2011), no. 3, 389–414.
85. *Ecklund, E. F., Jr.* Polynomials which assume infinitely many prime values. Pi Mu Epsilon J. **5** (1971), 182–183.
86. *Elkies N. D.* Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction, Algorithmic number theory (Leiden,2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 33–63 (2000).
87. *Elsenhans A. S., Jahnel J.* New sums of three cubes. Math. Comput. **78** (2009), 1227–1230.
88. *Elsholtz Ch.* The number $\Gamma(k)$ in Waring's problem. Acta Arith. **131** (2008), no. 1, 43–49.
89. *Erdős, P.* On the easier Waring problem for powers of primes, I, II. Proc. Camb. Philos. Soc.; **33** , 6–12 (1937); **35**, 149–165 (1939).
90. *Erdős, P.* On the sum and difference of squares of primes. I, II. J. Lond. Math. Soc. 12, 133–136 (1937); 12, 168–171 (1937).
91. *Estes D. R., Hsia J. S.* Sums of three integer squares in complex quadratic fields. Proc. Amer. Math. Soc. **89** (1983), no. 2, 211–214.
92. *Ford K.* Waring's problem with polynomial summands. J. Lond. Math. Soc. **61**, 671–680 (2000).
93. *Frey G.* Rationale Punkte auf Fermatkurven und getwisteten Modulkurven, J. Reine Angew. Math. **331** (1982), 185–191.
94. *Fröberg R., Ottaviani G., Shapiro B.* On the Waring problem for polynomial rings. PNAS **109** (2012), no. 15, 5600–5602.
95. *Fröberg R., Lundkvist S., Oneto A., Shapiro B.* Algebraic stories from one and from the other pockets. Arnold Math. J. **4** (2018), no. 2, 137–160.
96. *Frolow M.* Le problème d'Euler et les carrés magiques. Avec un atlas. St.-Pétersbourg, Imprimerie Trenké et Fusnot, 1884, 44p.
97. *Frolow M.* Les carrés magiques. Nouvelle étude, avec des notes par MM. Delannoy et Ed. Lucas. Paris. Gauthier-Villars. 1886, 46p. `https://catalog.hathitrust.org/Record/006199561`
98. *Frolov M.* Égalités à deux degrés. Bull. Soc. Math. Fr. **17** (1889), 69–83.
99. *Frolov M.* Égalités à deux et à trois degrés. Bull. Soc. Math. Fr. **20** (1892), 69–84.
100. *Frolov M.* La théorie des parallèles démontrée rigoureusement. 2me édition. Paris, Bâle et Genève:

Carré & Naud., 1899, 43p.
101. *Fuchs, W. H. J.; Wright, E. M.* The 'easier' Waring problem. Quart. J. Math. Oxford Ser. **10** (1939), 190–209.
102. *Gallardo L.* Sums of biquadrates and cubes in $\mathbb{F}_q[t]$. Rocky Mountain J. Math. **33** (2003), no. 3, 865–873.
103. *Gallardo L.* On the restricted Waring problem over $\mathbb{F}_{2^n}[t]$. Acta Arith. **42** (2000), 109–113.
104. *Gallardo L., Vaserstein, L.* The strict Waring problem for polynomial rings. J. Number Theory **128** (2008), 2963–2972.
105. *Gallardo L., Vaserstein, L.* Sums and strict sums of biquadrates in $\mathbb{F}_q[t]$, $q \in \{3,9\}$. Rocky Mountain J. Math. **40** (2010), no. 6, 1863–1874.
106. *Gallardo L., Vaserstein, L.* Constants as sums of polynomial cubes in characteristic 2. J. Comb. Number Theory **5** (2013), no. 1, 1–9.
107. *Gamble, M., Hamblen, S., Schildhauer, B., Truong, C.* Sums of cubes in quaternion rings Journal of Integer Sequences **23**, Issue 4, 2020, Article number 20.4.4, 9 pp.
108. *Gardiner V. L., Lazarus R. B., Stein P. R.*, Solutions of the Diophantine Equation $x^3 + y^3 = z^3 - d$, Mathematics of Computation **18** (1964), 408–413.
109. *Gauß C. F.* Neue Theorie der Zerlegung der Cuben. Werke 1863, Bd.II, S.387–391. `https://archive.org/details/bub_gb_6YHnVQeMjTOC/page/n389/mode/2up`
110. *Gar-el R., Vaserstein L.* On the Diophantine equation $a^3+b^3+c^3+d^3 = 0$. J. Number Theory **94** (2002), 219–223.
111. *Garge A. S.* Matrices over commutative rings as sums of fifth and seventh powers of matrices. Linear Multilinear Algebra **69** (2021), no. 12, 2220–2227.
112. *Geramita A.V.* Waring's Problem for Forms: inverse systems of fat points, secant varieties and Gorenstein algebras. Queen's Papers Pure Appl. Math. **105** (1996), no. 2, 1–129.
113. *Gordon G.* The answer is $2n \cdot n!$ What's the question? Amer. Math. Monthly **106** (1999), no. 7, 636–645.
114. *Guy R. K.* Unsolved problems in number theory, Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics, 1st edition, 1981. xviii+161p.; 2nd edition, 1994. xvi+285p.; 3rd edition, 2004. xviii+437p.
115. *Guy R. K.* Guy, Richard K. Nothing's new in number theory? Amer. Math. Monthly **105** (1998), no. 10, 951–954.
116. *Habsieger L.* Représentations des groupes et identités polynomiales. Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 1, 1–11.
117. *Habsieger L.* Applications of group representation theory to the easier Waring problem. J. Number Theory **45** (1993), no. 1, 92–111.
118. *Hardy G. H., Littlewood J. E.* Some problems of "partitio numerorum". VIII: The number $\Gamma(k)$ in Waring's problem, Proc. London Math. Soc. **28** (1927), 518–542.
119. *Hardy G. H., Wright E. M.* An Introduction to the Theory of Numbers, 5th ed., Oxford University Press, Oxford, 1979.
120. *Harper J. D.* Ramanujan, quadratic forms, and the sum of three cubes. Math. Mag. **86** (2013), no. 4, 275–279.
121. *Hayes D. R.* Leonard Carlitz (1907–1999), Notices Amer. Math. Soc., **48** (2001), no 11, 1322–1324.
122. *Hayman W. K.* Waring's theorem and the super Fermat problem for numbers and functions. Complex Var. Elliptic Equ. **59** (2014), no. 1, 85–90.
123. *Heath-Brown D. R.* Searching for Solutions of $x^3 + y^3 + z^3 = k$, Seminaire de Theorie des Nombres, (1989–1990), 71–76.
124. *Heath-Brown D. R.* The density of zeros of forms for which weak approximation fails. Math.Comput. **59** (1992), 613–623.
125. *Heath-Brown D. R., Lioen W. M., te Riele H. J. J.* On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer. Math. Comput.**61** (1993), 235–244.
126. *Hoffmann, Detlev W.; Leep, David B.* Sums of squares in nonreal commutative rings. Israel J. Math. **221** (2017), no. 2, 803–835.
127. *Hua L. K.* On Waring's problem with polynomial summands. Am. J. Math. **58**, 553–562 (1936)
128. *Hua L. K.* An easier Waring—Kamke problem. J. Lond. Math. Soc. **11** (1936), 4–5.

129. *Hua L. K.* Improvement of a result of Wright. J. London Math. Soc. **24** (1949), 157–159.
130. *Huisman S. G.* Newer sums of three cubes, (2016), arXiv:1604.07746
131. *Hunter W.* The representation of numbers as the sum of cubes. Math. Gaz., London, **21** (1937), 56–57.
132. *Hunter, W.* The representation of numbers by sums of fourth powers. J. London Math. Soc. **16** (1941), 177–179.
133. *Hürlimann W.* Permutation invariant properties of primitive cubic quadruples. Ramanujan J. **43** (2017), no. 3, 649–662
134. *Hurwitz A.* Zu Graßmanns Note: Lösung der Gleichung $x^3 + y^3 + z^3 + u^3 = 0$ in ganzen Zahlen. Deutsche Math.-Ver. **27** (1918), 55–56.
135. *Im Bo-Hae, Larsen M.* Waring's problem for rational functions in one variable. Q. J. Math. **71** (2020), no. 2, 439–449.
136. *Jagy, William C.; Kaplansky, Irving* Sums of squares, cubes, and higher powers. Experiment. Math. **4** (1995), no. 3, 169–173.
137. *Ji Chun-Gang* Sums of three integral squares in cyclotomic fields. Bull. Austral. Math. Soc. **68** (2003), no. 1, 101–106.
138. *Ji, Chungang; Wang, Yuanhua; Xu, Fei* Sums of three squares over imaginary quadratic fields. Forum Math. **18** (2006), no. 4, 585–601.
139. *Ji, Chun-Gang; Wei, Da-Sheng* Sums of integral squares in cyclotomic fields. C. R. Math. Acad. Sci. Paris **344** (2007), no. 7, 413–416.
140. *Joly J.-R.* Sommes de puissances $m$ièmes dans les anneaux $p$-adiques et les anneaux d'entiers algébriques. Enseign. Math. **14** (1968), 197–204.
141. *Joly J.-R.* Sommes de puissances $d$-ièmes dans un anneau commutatif. Acta Arith. **17** (1970), 37–114.
142. *Joly J.-R.* Équations et variètés algébriques sur un corps fini. Enseign. Math. **19** (1973), 1–117.
143. *Katre S. A., Garge A. S.* Matrices over commutative rings as sums of $k$-th powers. Proc. Amer. Math. Soc. **141** (2013), no. 1, 103–113.
144. *Katre S. A., Khule S A.* Matrices over orders in algebraic number fields as sums of $k$-th powers, Proc. Amer. Math. Soc. **128** (2000), no. 3, 671–675.
145. *Katre S. A., Wadikar K.* Matrices over noncommutative rings as sums of kth powers. Linear Multilinear Algebra **69** (2021), no. 11, 2050–2058.
146. *Khalin V., Vavilov N., Yurkov A.* The skies are falling: Mathematics for non-mathematicians. MDPI Mathematics, 2021, 19p.
147. *Klarner D. A.* Representation of an integer as a sum of four integer cubes and related problems. Am. Math. Mon. **74** (1967), 531–537.
148. *Ko Chao* Decompositions into four cubes, J. London Math. Soc., **11** (1936), 218–219.
149. *Körner O.* Über das Waringsche Problem in algebraischen Zahlkörpern. Math. Ann. **144** (1961), 224–238
150. *Körner O.* Über Mittelwerte trigonometrischer Summen und ihre Anwendung in algebraischen Zahlkörpern. Math. Ann. **147** (1962), 205–239; Berichtigung, ibid. **149** (1963), 462.
151. *Körner O.* Ganze algebraische Zahlen als Summen von Polynomwerten. Math. Ann. **149** (1962/63), 97–104.
152. *Körner O.* Über durch Potenzen erzeugte Ringe und Gruppen in algebraischen Zahlkörpern. Manuscripta Math. **3** (1970), 157–174.
153. *Kononen K.* More exact solutions to Waring's problem for finite fields. Acta Arith. **145** (2010), no. 2, 209–212.
154. *Koyama K.* Tables of solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$, Math. Comp. **62** (1994), 941–942.
155. *Koyama K.* On the solutions of the Diophantine equation $x^3+y^3+z^3 = n$, Trans. of Inst. of Electronics, Information and Communication Engineers (IEICE in Japan), **E78-A** (1995), no. 3, 444–449.
156. *Koyama K.* On searching for solutions of the Diophantine equation $x^3 + y^3 + 2z^3 = n$. (English summary) Math. Comp. **69** (2000), no. 232, 1735–1742.
157. *Koyama K., Tsuruoka Y., Sekigawa H.* On searching for solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$. Math. Comput. **66** (1997), 841–851.
158. *Krug K.* The hitchhickers guide to the integers: die Sache mit der 42. Mitt. Dtsch. Math.-Ver. **27** (2019),

no. 3–4, 124–125.
159. *Kubota R. M.* Waring's problem for $F_q[x]$. Dissertationes Math. **117** (1974), 60p.
160. Lal M., Russell W., Blundon W. J. A note on sums of four cubes. Math. Comp. **23** (1969), 423–424.
161. *Larsen M., Nguyen Dong Quan Ngoc* Waring's problem for unipotent algebraic groups. Ann. Inst. Fourier (Grenoble) **69** (2019), no. 4, 1857–1877.
162. *Lazov B., Vetsov T.* Sum of three cubes via optimisation. arXiv:2005.09710v1 [math.NT] 19 May 2020, 27p.
163. *Lebesgue V.-A.* Exercises d'analyse numérique, Paris, 1859.
164. *Legendre R.* Sur la résolution par Euler de l'équation de Fermat pour l'exposant 3. C. R. Acad. Sci. Paris Sér. A–B **275** (1972), A413–A414.
165. *Lehmer D. H.* On the Diophantine Equation $x^3 + y^3 + z^3 = 1$, Journal of the London Mathematical Society **31** (1956), 275–280.
166. *Lehmer D. H.* Mechanized mathematics. Bull. Amer. Math. Soc. **72** (1966), no. 5, 739–750.
167. Lenstra H. Ode aan het getal 43. Nieuw Arch. Wiskd. **5/10** (2009), no. 4, 240–244.
168. *Libri G.* Histoire des sciences mathématiques en Italie depuis la renaissance des lettres jusqu'à la fin du 17e siècle. Vols. I, II, III, IV. Georg Olms Verlagsbuchhandlung, Hildesheim 1967 Vol. I: xxxii+464 pp.; Vol. II: iv+534 pp.; Vol. III: v+461 pp.; Vol. IV: v+432 pp. (Reprografischer Nachdruck der Ausgabe Paris, 1838–1841, Vols. I, II, J. Renouard, Paris, 1838; Vol. III, 1840; Vol. IV, 1841.)
169. *Liu Yu-Ru, Wooley T. D.* Waring's problem in function fields. J. Reine Angew. Math. **638** (2010), 1–67.
170. *Lobachevsky N. I.* Pangeometry. Edited and translated from the French by Athanase Papadopoulos. Heritage of European Mathematics. European Mathematical Society (EMS), Źurich, 2010. xii+310p. ISBN: 978-3-03719-087-6
171. *Lü Xiaodong; Mu Quanwu* On Waring—Goldbach problem of mixed powers. J. Théor. Nombres Bordeaux **28** (2016), no. 2, 523–538.
172. *Lukes R. F.* A very fast electronic number sieve. Ph. D Thesis, Univ. Manitoba, January 1995, 259p., ISBN:978-0-612-13321-1
173. *Maccioni Ruju P. A., Mostert M.* The life and times of Guglielmo Libri (1802–1869). Scientist, patriot, scholar, journalist, and thief: a nineteenth-century story. Hilversum Verloren Publishers, 1995, 1–447.
174. *Mahler K.* Note on hypothesis $K$ of Hardy and Littlewood. J. London Math. Soc. **11** (1936), no. 2, 136–138.
175. *Makowski A.* Sur quelques problèmes concernant les sommes de quatre cubes, Acta Arith., **5** (1959), 121–123.
176. *Malter A., Schleicher D., Zagier D.* New Looks at Old Number Theory, Amer. Math. Monthly, **120** (2013), no 3, 243–264.
177. *Mebius C. A.* Zahlentheoretische Untersuchungen. III. Die Diophantische Gleichungen $A^3 + B^3 - C^3 - D^3 = E$. Göteborgs Kungl. Vetenskaps- och Vitterhets-Samhälles Handlingar, Ser. B **3** (1945), no. 6, 21p.
178. *Miller J. C. P., Woollett M. F. C.* Solutions of the Diophantine equation $x^3 + y^3 + z^3 = k$, J. Lond. Math. Soc. **30** (1955), 101–110.
179. *Mizuno M. W.* The works of König Dénes (1884–1944) in the domain of mathematical recreations and his treatment of recreational problems in his works of graph theory, Thèse du Dottorat, Histoire des mathématiques, Université Paris–Diderot — Paris VII, 2010, 362p. `https://tel.archives-ouvertes.fr/tel-00591307/document`
180. *Monnier J.-Ph., Quarez R.* Sums of even powers in Archimedean rings. Math. Z. **239** (2002), no. 3, 563–577.
181. *Mordell L. J.* On the representation of a binary cubic form as a sum of cubes. J. Lond. Math. Soc. **11** (1936), 204–208.
182. *Mordell L. J.* On the four integer cubes problem, J. London Math. Soc. **11** (1936), 208–218; Correction: ibid. **12** (1937), 80; Corrigendum: ibid. **32** (1957), 383.
183. *Mordell L. J.* On Sums of Three Cubes, J. Lond. Math. Soc., **17** (1942), 139–144.
184. *Mordell L. J.* On Ryley's solution of $x^3 + y^3 + z^3 = n$. J. London Math. Soc. **17** (1942), 194–196.
185. *Mordell L. J.* On the integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$. J. Lond. Math. Soc., **28**, 500–510 (1953).

186. *Mordell L. J.* On an Infinity of Integer Solutions of $ax^3 + ay^3 + bz^3 = bc^3$, J. Lond. Math. Soc., **30** (1955), 111–113.
187. *Mordell L. J.* Diophantine equations. Pure and Applied Mathematics, 30. London—New York: Academic Press. 312 p. (1969).
188. *Mordell L. J.* On sums of four cubes of polynomials. Acta Arith. **16** (1969/70), 365–369.
189. *Mordell L. J.* On the representation of an integer as the sum of four integer cubes. Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), pp. 115–117. Academic Press, London, 1971.
190. *Mostafa M. I.* A new approach to polynomial identities. Ramanujan J. **8** (2004), no. 4, 423–457.
191. *Mudge M.* Numbers Count: 1729 and all that, Personal Computer World, February 1995, 610.
192. *Narkiewicz W.* Teoria liczb, PWN, Warszawa, 1977, 355s.
193. *Narkiewicz W.* Classical problems in number theory, PWN, Warszawa, 1986, 363p.
194. *Norrie R.* On the algebraic solutions of indeterminate cubic and quartic equations. University of St. Andrews 500th Anniversary Memorial Volume Edinburgh, Scotland (1911), 47–92.
195. *Oltramare G.* L'intermédiaire des Math., **1** (1894), no. 25, 165–166.
196. *Ono K., Trebat-Leder S.* The 1729 K3 surface. Res. Number Theory **2** (2016), Paper no. 26, 6 pp.
197. *Paley R. E. A. C.* Theorems on polynomials in a Galois field. Quarterly Journ. (Oxford Series) **4** (1933), 52–63.
198. *Payne G., Vaserstein L.* Sums of three cubes. The arithmetic of function fields (Columbus, OH, 1991), 443–454, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.
199. *Peters M.* Summen von Quadraten in Zahlringen. J. Reine Angew. Math. **268–269** (1974), 318–323.
200. *Pierce L. B.* The Vinogradov mean value theorem [after Wooley, and Bourgain, Demeter and Guth]. Séminaire Bourbaki. Vol. 2016/2017. Exposés 1120–1135. Astérisque No. **407** (2019), Exp. No. 1134, 479–564.
201. *Piezas T.* A Collection of Algebraic Identities https://sites.google.com/site/tpiezas/Home
202. *Pillai S. S.* On $v(k)$. Proc. Indian Acad. Sci. A **9**, 175–176 (1939).
203. *Pintz J.* Landau's problems on primes, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 357–404.
204. *Pollack P.*. Waring's problem for integral quaternions. Indag. Math. (N.S.) **29** (2018), no. 5, 1259–1269.
205. *Pollack P.*. A remark on the number field analogue of Waring's constant $g(k)$. Math. Nachr. **291** (2018), no. 11–12, 1893–1898.
206. *Poonen B.* Undecidability in number theory. Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350.
207. *Pumplün S.* Sums of $d$-th powers in non-commutative rings. Beiträge Algebra Geom. **48** (2007), no. 1, 291–301.
208. *Rai T.* Easier Waring problem. J. Sci. Res. Benares Hindu Univ. **1** (1950/1951), 5–12.
209. *Ramanujam C. P.* Sums of $m$-th powers in $p$-adic rings. Mathematika **10** (1963), 137–146.
210. *Ramachandra K.* I am fifty-five years old. Hardy—Ramanujan J. **36** (2013), 34–42.
211. *Revoy Ph.* Sommes de bicarrés dans $\mathbb{Z}[\sqrt{-1}]$ et $\mathbb{Z}[\sqrt[3]{1}]$. Enseign. Math. (2) **25** (1979), no. 3–4, 257–260.
212. *Revoy Ph.* Sur les sommes de carrés dans un anneau. Ann. Sci. Univ. Besançon Math. (3) (1979), no. 11, 3–8.
213. *Revoy Ph.* Sur les sommes de quatre cubes. Enseign. Math. (2) **29** (1983), no. 3–4, 209–220.
214. *Revoy Ph.* Le problème facile de Waring. Enseign. Math. **37** (1991), 223–234.
215. *Reynya M. A.* Symmetric homogeneous Diophantine equations of odd degree. Int. J. Number Theory **9** (2013), no. 4, 867–876.
216. *Reynya M. A.* Representations of a rational number as a sum of odd powers. Int. J. Number Theory **12** (2016), no. 4, 903–911.
217. *Reynya M. A.* Representation of a rational number as a sum of ninth or higher odd powers. Funct. Approx. Comment. Math. **58** (2018), no. 1, 79–87
218. *Richman D. R.* The Waring problem for matrices, Linear and Multilinear Algebra **22** (1987), no. 2, 171–192
219. *Richmond H. W.* On integers which satisfy the equation $t^3 \pm x^3 \pm y^3 \pm z^3 = 0$, Trans. Cambridge Phil. Soc. **22** (1920), 389–403.
220. *Richmond H. W.* Every positive rational number is a sum of cubes of three such numbers. Messenger (2) **51** (1921), 171–175.

221. *Richmond H. W.* An elementary note upon Waring's problem for cubes, positive and negative. Messenger Math. **51** (1921/1922), 177–186.
222. *Richmond H. W.* On analogues of Waring's problem for rational numbers. Proc. Lond. Math. Soc. **21** (1922), 401–409.
223. *Richmond H. W.* On rational solutions of $x^3 + y^3 + z^3 = R$. Proceedings Edinburgh Math. Soc. (2) **2** (1930), 92–100.
224. *Richmond H. W.* A note on the four integer cube theorem. J. London math. Soc. **12** (1937), 206.
225. *Richmond H. W.* A note upon Prof. Mordell's paper. J. London Math. Soc. **17** (1942), 196–199.
226. *Rowland E.* Known families of integer solutions of $x^3 + y^3 + z^3 = n$, http://thales.math.uqam.ca/ rowland/papers/ , 1–6.
227. *Ruiz J. M.* A characterization of sums of $2n$th powers of global meromorphic functions. Proc. Amer. Math. Soc. **109** (1990), no. 4, 915–923.
228. *Scarowsky M.* On units of certain cubic fields and the Diophantine equation $x^3 + y^3 + z^3 = 3$, Proc. Amer. Math. Soc. **91** (1984), no. 3, 351–356.
229. *Scarowsky M., Boyarsky A.* A Note on the Diophantine equation $x^n + y^n + z^n = 3$, Math. Comp. **42** (1984), 235–237.
230. *Schinzel A.* On sums of four cubes of polynomials. J. Lond. Math. Soc. **43** (1968), 143–145.
231. *Schinzel A., Sierpiński W.* Sur les sommes de quatre cubes, Acta Arith. **4** (1958), no. 1, 20–30; `http://matwbn.icm.edu.pl/ksiazki/aa/aa4/aa414.pdf`
232. *Schwer S. R., Autebert J.-M.* Henti-Auguste Delannoy, une biographie (première partie), Math. & Sci. human., 43e ann´ee (2006) n 174, 25–67.
233. *Sekigawa H., Koyama K.* Nonexistence conditions of a solution for the congruence $x_1^k + \ldots + x_s^k \equiv N \pmod{p^n}$. Math. Comp. **68** (1999), no. 227, 1283–1297.
234. *Siegel C.* Generalization of Waring's problem to algebraic number fields, Amer. J. Math. **66** (1944), 122–136.
235. *Siegel C.* Sums of $m$th powers of algebraic integers, Ann. of Math. **46** (1945), no. 2, 313–339.
236. *Sierpiński W.* On some unsolved problems of arithmetic, Scripta Math., **25** (1960) 125–136.
237. *Sierpiński W.* Elementary theory of numbers, PWN, Warszawa, 1964, 480p.
238. *Sierpiński W.* A selection of problems in the theory of numbers, Macmillan, New York, 1964, 115p.
239. *Small C.* Waring's problem $\mod n$, Amer. Math. Monthly **84** (1977), 12–25.
240. *Small C.* Solution of Waring's problem $\mod n$, Amer. Math. Monthly **84** (1977), 356–359.
241. *Small C.* Sums of powers in large finite fields. Proc. Amer. Math. Soc., **65** (1977), no. 1, 35–36.
242. *Stemmler R.M.* The easier Waring problem in algebraic number fields. Acta Arith. **6** (1961), 447–468.
243. *Stewart I., Tall D.* Algebraic Number Theory and Fermat's Last Theorem, AK Peters, Massachusetts, 2002.
244. *Stoll M.* How to solve a Diophantine equation. In: An invitation to mathematics. From competitions to research. Schleicher, Dierk (ed.) et al. With a preface by G'unter M. Ziegler. Berlin: Springer (ISBN 978-3-642-19532-7/pbk; 978-3-642-19533-4/ebook). 9–19 (2011).
245. *Subba Rao K.* Some Easier Waring's Problems. Math. Z. **40** (1935), no. 1, 477–483.
246. *Subba Rao K.* Representation of every number as a sum of rational $k$-th powers. J. Lond. Math. Soc. **13** (1938), 14–16.
247. *Sun Qi* On Diophantine equation $x^3 + y^3 + z^3 = n$, Kexue Tongbao, **33** (1988) 2007–2010;
248. *Sutherland A. V.* Sums of three cubes. `https://math.mit.edu/˜ drew/Waterloo2019.pdf`
249. *Tardy P.* Trasformazione di un prodotto di $n$ fattori. Ann. Sci. Mat. Fis., **2** (1851), 287–291. `https://archive.org/details/annalidiscienze06tortgoog/page/n297/mode/2up`
250. *Tatuzawa T.* On the Waring problem in an algebraic number field. J. Math. Soc. Jpn. **10** (1958), 322–341.
251. *Tatuzawa, T.* On Waring's problem in an algebraic number field. Acta Arith. **24** (1973), 37–60.
252. *Tatuzawa, T.* Fourier analysis used in analytic number theory. Acta Arith. **28** (1975), 263–272.
253. *Tatuzawa, T.* On a proof of Siegel's theorem. In: Number Theory and Combinatorics, Japan, 1984, pp. 383–416. World Scientific, Singapore (1985)
254. *Tietäväinen A.* Note on Waring's problem $\mod p$. Ann. Acad. Sci. Fenn., Ser. A 1 Math. **554** (1973), 1–7.

255. *Tongsomporn J., Oswald N., Steuding J.* Waring's problem for Hurwitz quaternion integers Journal of Integer Sequences **22** (2019), no. 8, Article number 19.8.1
256. *Vaserstein L. N.* On the sum of powers of matrices, Linear and Multilinear Algebra **21** (1987), no. 3, 261–270.
257. *Vaserstein L. N.* Waring's problem for algebras over fields, J. Number Theory **26** (1987), no. 3, 286–298.
258. *Vaserstein L. N.* Waring's problem for commutative rings. J. Number Theory **26** (1987), no. 3, 299–307.
259. *Vaserstein L. N.* Every integer is a sum or difference of 28 integral eighth powers. J. Number Theory, **28** (1988), 66–68.
260. *Vaserstein L. N.* Sums of cubes in polynomial rings. Math. Comp. **56** (1991), no. 193, 349–357.
261. *Vavilov N.* Waring problem as an issue of polynomial computer algebra, Intern. Conf. Polynomial Computer Algebra (2020, St Petersburg), October 2020, EIMI, 17p. `https://pca-pdmi.ru/2020/files/53/Vavilov-PCA2020_new.pdf`
262. *Veselý V.* O jedné obdobě Waringova problému. Časopis Mat. Fys. **62** (1933), 123–127.
263. *Villegas F. R., Zagier D.* Which primes are sums of two cubes? Number Theory (Halifax NS 1994) 295–306, CMS Conf Proc, **15**, Amer. Math. Soc, Providence RI, 1995.
264. *Wadikar K. G., Katre S. A.* Matrices over a commutative ring with unity as sums of cubes, Proc. of Internat. Conf. on Emerging Trends in Math. and Comp. Appl., Dec. 16–18, 2010, Sivakasi, India, Allied Publ. (2010), 8–12.
265. *Wahlgren A.* Om tal, som kunna skrivas som en summa av fyra kubiktal, Matematisk Tidssrift B, 1941, 33–41.
266. *Wakeling E.* Lewis Carroll's games and puzzles, New York : Dover Publications in association with the Lewis Carroll Birthplace Trust, Daresbury, Cheshire, England, 1992, 80p.
267. *Warning E.* Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. Abh. Math. Sem. Univ. Hamburg **11** (1935), no. 1, 76–83.
268. *Weil A.* Two lectures on number theory, past and present. Enseign. Math. (2) **20** (1974), 87–110.
269. *Weil A.* Number theory. An approach through history. From Hammurapi to Legendre. Birkhäuser Boston, Inc., Boston, MA, 1984. xxi+375p.
270. *Wiles A.* Modular elliptic curves and Fermat's last theorem. Ann. Math., **141** (1995), 443–551.
271. *Winterhom A.* On Waring's problem in finite fields. Acta Arith. **87** (1998), no. 2, 171–177.
272. *Winterhom A.* A note on Waring's problem in finite fields. Acta Arith. **96** (2001), no. 4, 365–368.
273. *Winterhom A., van de Woestijne Ch.* Exact solutions to Waring's problem for finite fields. Acta Arith. **141** (2010), no. 2, 171–190.
274. *Wright E. M.* An Extension of Waring's Problem Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character **232** (1934), pp. 1–26.
275. *Wright E. M.* An Easier Waring's Problem. J. London Math. Soc. **9** (1934), no. 4, 267–272.
276. *Wright E. M.* The Representation of a Number as a Sum of Three or Four Squares. Proc. London Math. Soc. (2) **42** (1937), no. 7, 481–500.
277. *Zhang Bin, Ji Chun-Gang* Sums of three integral squares in biquadratic fields. J. Number Theory **138** (2014), 37–47.

ГРНТИ 00000

Поступила в редакцию 2 января 2020, окончательный вариант 24 января 2020 г.

Computer tools in education, 2021
№ -: 1–53
http://ipo.spb.ru/journal
doi:

# Computers as novel mathematical reality: V. Easier Waring problem

N. A. Vavilov
SPbU

**Abstract**

In this part I continue the discussion of the role of computers in the current research on the additive number theory, in particular in the solution of the *easier* Waring problem. This problem consists in finding for each natural $k$ the smallest such $s = v(k)$ that all natural numbers $n$ can be written as sums of $s$ integer $k$-th powers $n = \pm x_1^k \pm \ldots \pm x_s^k$ *with signs*. This problem turned out to be much harder than the original Waring problem. It is intimately related with many other problems of arithmetic and diophantine geometry. In this part I discuss various aspects of this problem, and several further related problems, such as the rational Waring problem, and Waring problems for finite fields, other number rings, and polynomials, with special emphasys on connection with polynomial identities and the role of computers in their solution. As of today, these problems are quite far from being fully solved, and provide extremely broad terrain both for the use in education, and amateur computer assisted exploration.

**Keywords:** *sums of powers with signs, easier Waring problem, sums of cubes, rational Waring problem, Frolov type identities, Waring problem for number fields, Waring problem for polynomials, polynomial computer algebra*

**Citation:** N. A. Vavilov. Computers as novel mathematical reality: V. Easier Waring problem. Computer tools in education, 2021. № -. P. 1–53 : DOI: http://dx.doi.org/.

**Acknowledgements:** *The present paper emerged as part of my work on the RFBR grant 19-29-14141.*

Received whatever, 2021, The final version: whatever, 2021

**Nikolai Alexandrovich Vavilov, Dr. Sci., Professor SPbU nikolai-vavilov@yandex.ru**

**Николай Александрович Вавилов,**
**д.ф.-м.н, профессор математики**
**Факультета МКН СПбГУ**
**nikolai-vavilov@yandex.ru**

© Наши авторы, 2021.
Our authors, 2021.