ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования
"Московский физико-технический институт
(Национальный исследовательский университет)"

Кафедра теоретической астрофизики и квантовой теории поля

# Об одном диофантовом уравнении, неразрешимость которого эквивалентна гипотезе Римана

(Выпускная квалификационная работа на степень бакалавра)

**Выполнил:**
студент 521 группы
Норкин Алексей Алексеевич

**Научный руководитель:**
профессор Б.З. Мороз

Долгопрудный
2019

# Содержание


Введение 3

1 Дзета-функция Римана 4

2 Диофантовы множества 5

3 Теорема Матиясевича 7

4 Диофантова переформулировка гипотезы Римана 17

Заключение 22

Список литературы 23

**Введение**

В данной работе мы ставим целью рассмотрение и исследование гипотезы Римана при помощи техники диофантовых представлений. Теоретическая возможность построения эквивалентной формулировки в терминах диофантовых уравнений известна давно; однако уже построенные к этому времени в предыдущих работах на эту тему полиномы отличаются большим числом переменных и особой громоздкостью. В свете недавно вышедшей работы Ю.В.Матиясевича представляется возможным построить такое диофантовое уравнение, ограничиваясь всего лишь 193-мя переменными. Мы исследуем новую переформулировку гипотезы Римана и выполняем построение сравнительно простого диофантового уравнения, неразрешимость которого эквивалентна гипотезе Римана.

Работа состоит из четырёх параграфов, заключения и списка литературы.

Параграфы §1 и §2 носят вводный характер. В параграфе §1 обсуждаются основные понятия, связанные с дзета-функцией Римана и её свойствами, а также знаменитая гипотеза Римана и её классические переформулировки. Параграф §2 посвящён обсуждению диофантовых множеств. Даются определения диофантовых множеств и представлений, приводятся простые и примеры диофантовых множеств и представлений. Рассматривается техника диофантовых представлений для объединений и пересечений диофантовых множеств. Обсуждается возможность построения полиномиального уравнения, выражающего зависимость экспоненциального роста. Наконец, демонстрируется теоретическая возможность переформулировки гипотезы Римана в терминах неразрешимости диофантового уравнения.

В параграфе §3 обсуждается недавний результат Ю.В.Матиясевича. Подробно рассматривается новая система условий, не являющаяся совместной, если гипотеза Римана верна, и имеющая бесконечно много решений, если гипотеза Римана не верна. Параграф §3 целиком посвящён обсуждению этого результата и его доказательству. Доказательство существенно опирается на материалы, изложенные в параграфе §1.

Наконец, в параграфе §4 выполняется построение такого диофантового уравнения, неразрешимость которого эквивалентна гипотезе Римана. При построении мы будем пользоваться результатами из параграфов §2 и §3.

Нумерация формул выполнена следующим образом. Отсчёт каждой формулы производится от начала параграфа, в котором она содержится. Ссылаясь на формулу из другого параграфа, мы будем добавлять к номеру формулы номер параграфа, ей соответствующего. Так, например, ссылка на 2-ю формулу 3-го параграфа внутри него будет иметь вид (2), в то время как ссылка на неё же вне 3-го параграфа будет иметь вид (3.2).

## §1. Дзета-функция Римана

Дзета-функция Римана $\zeta(s)$ есть мероморфная на всей комплексной плоскости функция $\mathbb{C}$, представимая в полуплоскости $\mathbb{C}_1 := \{s|s \in \mathbb{C}\}, \mathrm{Re}\, s > 1$ абсолютно сходящимся рядом Дирихле:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, s \in \mathbb{C}_1. \tag{1}$$

В указанной области $\mathbb{C}_1$ выполняется знаменитое тождество - разложение дзета-функции в бесконечное произведение:

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}, s \in \mathbb{C}_1, \tag{2}$$

где произведение берётся по всем простым числам $p$ (см., например, [1]).

Функция $s \mapsto \zeta(s)$ имеет единственный полюс в точке $s = 1$ с вычетом, равным единице, так что

$$\zeta(s) = \frac{1}{s-1} + \sum_{i=0}^{\infty} a_i s^i \text{ при } s \in \mathbb{C}, \{a_i | 0 \leqslant i < \infty\} \subseteq \mathbb{C}, \tag{3}$$

причём ряд (3) компактно сходится в $\mathbb{C}$ и удовлетворяет функциональному уравнению:

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\frac{\pi s}{2})\zeta(s), \tag{4}$$

которое иногда записывают в виде $\xi(s) = \xi(1-s)$, где $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ и где $\Gamma(s)$ - гамма-функция Эйлера[1].

Из функционального уравнения (4) явно следует, что дзета-функция обладает так называемыми тривиальными нулями: легко видеть, что $\zeta(-2n) = 0$ при $n \in \mathbb{N}$; из (1), в свою очередь, вытекает, что $\zeta(s) \neq 0$ при $s \in \mathbb{C}_1$. Таким образом, все нули, не являющиеся тривиальнымии, лежат в полосе $\{s|s \in \mathbb{C}, 0 \leqslant \mathrm{Re}\, s \leqslant 1\}$. Знаменитая гипотеза Римана утверждает, что все нетривиальные нули дзета-функции имеют действительную часть, равную $\frac{1}{2}$.

<u>Гипотеза Римана</u>. Если $\zeta(s) = 0$ и $s \notin \{-2n|n \in \mathbb{N}\}$, то $\mathrm{Re}\, s = \frac{1}{2}$.

До сих пор эта гипотеза не доказана и не опровергнута; однако большое количество результатов в области распределения простых чисел зиждется на предположении, что эта гипотеза истинна. При попытках доказать гипотезу Римана было найдено немалое количество эквивалентных формулировок, многие из которых основываются на тождестве Эйлера.

Классическая эквивалентность в терминах пси-функции Чебышёва, восходящая к работам начала 20-го века, имеет вид

$$\psi(n) = n + O(\sqrt{n}(\ln n)^2), \quad (5),$$

где $\psi(n) = \ln \text{НОК}(1, ...., n)$. Позднее этот результат был улучшен Л. Шёнфильдом [2] - он устранил неявную константу и установил, что гипотеза Римана эквивалентна неравенству:

$$|\psi(n) - n| < \frac{1}{8\pi}\sqrt{n}(\ln n)^2 \text{ при } n \geqslant 74. \quad (6)$$

В дальнейшем мы будем существенно опираться на данное неравенство.

## §2. Диофантовы множества

Диофантовыми уравнениями называют уравнения следующего вида:

$$P(x_1, \ldots, x_m) = 0, \quad (1)$$

где $P$ - полином с целыми рациональными коэффициентами, а решения суть целые или натуральные числа. Мы, однако, будет рассматривать только уравнения с натуральными числами, в случае необходимости сводя решение такого уравнения в натуральных числах к решению в целых числах по теореме Лагранжа о четырёх квадратах.

Запишем произвольное диофантово уравнение с целыми коэффициентами как $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$. Числа $a_1, \ldots, a_n$ в таком уравнении будем называть параметрами. Зададимся вопросом - при каком выборе значений параметров диофантово уравнение будет иметь решение, а при каком - нет? Строго говоря, такое диофантово уравнение, если оно имеет решение, определяет некоторое множество $\mathfrak{R}$, состоящее из всех таких наборов параметров, для которых существует набор неизвестных, удовлетворяющих указанному равенству, так что

$$< a_1, \ldots, a_n > \in \mathfrak{R} \Leftrightarrow \exists x_1, \ldots, x_m [P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]. \quad (2)$$

Такая эквивалентность, или менее аккуратно, такое диофантово уравнение $P$ и называется диофантовым представлением множества $\mathfrak{R}$, а само множество, имеющее диофантово представление, называется диофантовым множеством. Число $n$ в (2) мы назовём размерностью диофантова множества $\mathfrak{R}$.

Приведём несколько простых примеров диофантовых множеств. Очевидно, например, что можно при помощи диофантового уравнения задать множество всех чётных чисел (здесь и далее квантовы $\exists$ и $\forall$ распространяются на натуральные, т.е. целые положительные числа):

$$a - \text{чётное} \Leftrightarrow \exists x \ [2x - a = 0], \quad (3)$$

множество всех нечётных чисел:

$$a - \text{нечётное} \Leftrightarrow \exists x\ [2x - 1 - a = 0], \tag{4}$$

и даже множество всех чисел, не являющихся степенью двойки:

$$a - \text{не степень двойки} \Leftrightarrow \exists x, y\ [(2x+1)y - a = 0]. \tag{5}$$

Также мы выпишем некоторое количество диофантовых множеств, которые впоследствии будем использовать в работе:

$$b \geqslant a \Leftrightarrow \exists x\ [x + a - 1 - b = 0], \tag{6}$$

$$b > a \Leftrightarrow \exists x\ [x + a - b = 0], \tag{7}$$

$$a|b \Leftrightarrow \exists x\ [ax = b], \tag{8}$$

Для более сложных представлений, а именно для записи объединения или пересечения диофантовых множеств одинаковой размерности, будем использовать следующую технику. Нетрудно понять, что если $P_1(a_1, \ldots, a_n, \vec{x}) = 0$ и $P_2(a_1, \ldots, a_n, \vec{y}) = 0$ - диофантовы представления двух диофантовых множеств, то диофантово представление их объединения будет иметь вид:

$$P_1(a_1, \ldots, a_n, \vec{x})P_2(a_1, \ldots, a_n, \vec{y}) = 0, \tag{9}$$

а представление их пересечения - :

$$P_1(a_1, \ldots, a_n, \vec{x})^2 + P_2(a_1, \ldots, a_n, \vec{y})^2 = 0. \tag{10}$$

Таким образом мы можем получить чуть более сложные диофантовые представления, например, функцию $\mathrm{rem}(b, c)$ - остаток от деления $b$ на $c$ :

$$a = \mathrm{rem}(b, c) \Leftrightarrow (c|b-a) \wedge (a < b) \Leftrightarrow \exists x, y\ [(cx-b+a)^2 + (y+a-b)^2 = 0]. \tag{11}$$

Исторически, понятие диофантового представления возникло при попытке решить десятую проблему Гильберта. Важный результат, полученный Ю.Матиясевичем в 1970 г. [3], заключается в том, что существует полиномиальное уравнение, выражающее зависимость экспоненциального роста, то есть:

$$c = a^b \Leftrightarrow \exists \vec{x}[P(a, b, c, \vec{x}) = 0]. \tag{12}$$

Тем самым было показано, что всякое перечислимое множество, то есть множество, задаваемое при помощи некоторого алгоритма, диофантово.

Этот результат, в свою очередь, позволяет переформулировать множество проблем в терминах диофантовых представлений. Так, например, для произвольной формулы из класса $\Pi_1^0$, то есть из класса всех формул вида $\forall x_1 \ldots x_m \; A(x_1, \ldots x_m)$, где $A(x_1, \ldots x_m)$ - алгоритмически проверяемое соотношение между числами $x_1, \ldots, x_m$, можно найти эквивалентную формулу следующего вида:

$$\forall x_1 \ldots x_m \; P(x_1, \ldots, x_m) \neq 0, \tag{13}$$

где $P(x_1, \ldots, x_m)$ - многочлен с целыми коэффициентами.

Г. Крайзелем [4] было доказано, что гипотеза Римана может быть переформулирована как формула из класса $\Pi_1^0$, а, по теореме Матиясевича, такая формула эквивалентна формуле вида (13). Таким образом, можно построить полином $P(x_1, \ldots, x_n)$ такой, что гипотеза Римана эквивалентна неразрешимости диофантового уравнения

$$P(x_1, \ldots, x_n) = 0.$$

же было окончательно установлено, что по произвольной формуле из этого класса $\Pi_1^0$ можно построить такую эквивалентную формулу (13).

Способы построения такого полинома, основанные на неравенстве Шёнфильда (1.6), приводят к довольно сложному полиному от 2286-ти переменных [5],[6] (способ построения такого полинома был описан в [3], [7]). Недавняя работа Матиясевича предлагает новый способ построения диофантового представления. [8]

## §3. Теорема Матиясевича

В [8] была предложена система условий, которая позволяет построить диофантово уравнение, неразрешимость которого будет эквивалентна гипотезе Римана. Предлагается заменить неравенство (1.6) на следующие два условия:

1) *Если гипотеза Римана верна, то для всех* $n > 1$

$$\psi(n) > n - \sqrt{n}\frac{(\ln(n))^2}{(\ln 2)^2}. \tag{1}$$

2) *Если гипотеза Римана не верна, то существует бесконечно много* $n$*, для которых*

$$\psi(n) < n - 20\sqrt{n}\frac{(\ln(n))^2}{(\ln 2)^2}. \tag{2}$$

Неравенство (1) следует непосредственно из неравенства Шёнфильда при $n \geqslant 74$; значения $n = 2, \ldots, 73$ проверяются перебором. Достаточное условие (2) вытекает из $\Omega$-теоремы. Остановимся на утверждении (2) более подробно.

Будем говорить, что

$$f(x) = \Omega(x),$$

если существует такое $c > 0$, не зависящее от $x$, что неравенство

$$|f(x)| > cx$$

выполняется для произвольно больших $x$ (здесь $f : \mathbb{R} \to \mathbb{C}$ - произвольная комплекснозначная функция).

Будем также говорить, что если $f(x)$ - вещественнозначная функция, и выполняется

$$f(x) > cx,$$

для сколь угодно больших $x$, то

$$f(x) = \Omega_+(x),$$

а если выполняется $f(x) < -cx$ для произвольно больших $x$, то

$$f(x) = \Omega_-(x).$$

Таким образом, для вещественнозначных функций $f(x)$ следует, что $f(x) = \Omega(x)$ эквивалетно утверждению "$f(x) = \Omega_+(x)$ или $f(x) = \Omega_-(x)$"; эквивалентное "$f(x) = \Omega_+(x)$ и $f(x) = \Omega_-(x)$" утверждение мы будем обозначать как $f(x) = \Omega_\pm(x)$.

Имеет место следующая теорема [9]:

Теорема 1. *Для всякого фиксированного положительного* $\delta$

$$\psi(x) - x = \Omega_\pm(x^{\theta-\delta}), \tag{3}$$

*где* $\theta$ *обозначает верхнюю границу вещественных частей нулей* $\zeta(s)$.

Следствие 1. *Если гипотеза Римана не верна, то неравенство* (2) *выполняется для бесконечно многих* $n$.

Доказательство. Предположим, что гипотеза Римана не верна. Тогда $\theta > \frac{1}{2}$. Значит, найдётся $\varepsilon > 0$, что для бесконечного количества натуральных чисел $x$:

$$\psi(x) - x < -c(\delta)x^{\theta-\delta} < -c(\varepsilon)x^{\frac{1}{2}+\varepsilon} < -c(\varepsilon)\sqrt{x}(\ln x)^2.$$

Последнее нeравество очевидно следует из того факта, что степенная функция возрастает быстрее логарифмической. Возьмём $\varepsilon$ таким, что $c(\varepsilon) = \frac{20}{(\ln 2)^2}$. Откуда окончательно:

$$\psi(n) < n - 20\sqrt{n}\frac{(\ln(n))^2}{(\ln 2)^2}.$$

Следствие 1 доказано. ■

Теорема 2 (Ю.В. Матиясевич [8]). *Пусть задана система условий*

$$2^l \leqslant n < 2^{l+1}, \tag{4}$$

$$2^{m-1} \leqslant q < 2^m, \tag{5}$$

$$s = \frac{B^{n+1}(B^{n(n+1)} - (n+1)) + n}{(B^{(n+1)} - 1)^2}, \tag{6}$$

$$t = \frac{(2^m - 1)(B^{n^2} - 1)}{B^n - 1}, \tag{7}$$

$$\operatorname{rem}((2^t + 1)^t, 2^{rt+1}) > 2^{rt} \wedge (r \leqslant t), \tag{8}$$

$$u = \operatorname{rem}(rs, B^{n^2-n}), \tag{9}$$

$$rs - u \equiv \frac{B^{n^2-n}(B^n - 1)}{B - 1} q \ (\operatorname{mod} B^{n^2}), \tag{10}$$

$$p = \operatorname{rem}(r, B^n + 1), \tag{11}$$

$$mp < nq - 15l^2 q\sqrt{n}, \tag{12}$$

*в которой* $B := 2^{l+m+1}$.

I. *Если гипотеза Римана верна, то указанная система не имеет решений в натуральных числах* $l, m, n, p, q, r, s, t, u$.

II. *Если гипотеза Римана не верна, то указанная система имеет бесконечно много решений в натуральных числах.*

Разобьём доказательство этой теоремы на две части. В первой части мы докажем утверждение I, а во второй - утверждение II. В ходе доказательства мы будем использовать следующие леммы.

Лемма 1 (Теорема Куммера [10]) *Пусть числа $a$ и $b$ следующим образом записываются в позиционной системе счисления с простым основанием $p$:*

$$a = \sum_{k=0}^{m} a_k p^k,\ b = \sum_{k=0}^{m} b_k p^k,\ 0 \leqslant a_k < p,\ 0 \leqslant b_k < p,\ k = 0, \ldots, m;$$

*тогда степень, с которой $p$ входит в разложение биномиального коэффициента $\binom{a+b}{b}$, равна количеству переносов из разряда в разряд при сложении чисел $a$ и $b$.*

Следствие 2. *Пусть числа $a, b \subseteq \mathbb{N}$ заданы в условиях леммы 1 для $p = 2$. Кроме того, пусть $a \geqslant b$. Тогда верна следующая эквивалентность:*

$$\binom{a}{b} \equiv 1 \bmod 2 \Leftrightarrow a_k \geqslant b_k.$$

Доказательство следствия 2. Предположим, что $a_k \geqslant b_k$ при $0 \leqslant k \leqslant m$, и пусть $\widetilde{a} := a - b, \widetilde{b} := b$. Тогда легко видеть, что:

$$\widetilde{a} = \sum_{k=0}^{m}(a_k - b_k)2^k,\ \widetilde{b} = \sum_{k=0}^{m} b_k 2^k.$$

Так как $a_k \geqslant b_k$, а $a_k$ и $b_k$ принимают значения либо 0, либо 1, то $a_k - b_k$ и $b_k$ не могут одновременно принимать значение 1; значит, при сложении чисел $\widetilde{a}$ и $\widetilde{b}$ нет переносов из разряда в рязряд. Это, по теореме Куммера, и означает, что

$$\binom{a}{b} \equiv 1 \bmod 2.$$

Обратно. Предположим, что $\binom{a}{b} \equiv 1 \bmod 2$. Из определения биномиальных коэффициента следует, что $a \geqslant b$. Положим

$$c = a - b = \sum_{k=0}^{m} c_k 2^k,$$

где $c_k | 0 \leqslant k \leqslant m \subseteq 0, 1$.Тогда $\binom{a}{b} = \binom{c+b}{b} \equiv 1 \bmod 2$. Из теоремы Куммера следует, что при сложении $c$ и $b$ нет перехода из разряда в разряд. Это означает, что $c_k^2 + b_k^2 \leqslant 1$; с другой стороны, $c + b = a$. Значит, $c_k + b_k = a_k$, откуда следует, что $a_k - b_k = c_k \geqslant 0$. Следствие 2 доказано. ■

Лемма 2. Для целых положительных чисел $t$ и $r$, для которых выполнено условие $t \geqslant r$, верно

$$\mathrm{rem}((2^t + 1)^t, 2^{rt+1}) > 2^{rt} \Leftrightarrow \binom{t}{r} \equiv 1 \bmod 2.$$

Доказательство леммы 2. Действительно. Пусть

$$(2^t + 1)^t = 2^{rt+1}a + b, b < 2^{rt+1}.$$

Заметим, что:

$$(2^t + 1)^t = 1 + \binom{t}{1}2^t + \ldots + \binom{t}{r}2^{rt} + \ldots + 2^{t^2}.$$

Понятно, что приведённая запись есть запись $(2^t+1)^t$ в системе счисления с основанием $2^t$, так как $\forall j \leqslant t(\binom{t}{j} < 2^t)$. Запишем теперь это число в системе счисления с основанием 2. Для этого каждую цифру, то есть биномиальный коэффициент, запишем в двоичном виде, дополняя её спереди количеством нулей до длины $t$. Тогда условие, что $\binom{t}{r}$ нечётно, будет означать равенство цифры на $rt-$м месте (отсчёт производится с нуля) единице. Вместе с тем, для того, чтобы число $(2^t+1)^t - b$ делилось на $2^{rt+1}$, необходимо и достаточно, чтобы разложение числа $b$ в двоичной системе счисления совпадало с таковым числа $(2^t+1)^t$ на отрезке длины $rt+1$. Это означает, наконец, что цифра на $rt-$м месте в разложении числа $b$ равна 1, а, значит, $b \geqslant 2^{rt}$. Однако легко видеть, что цифра на 0-м месте также равняется 1, т.к. $(2^t+1)^t$ нечётно. Это и означает, что $b > 2^{rt} \Leftrightarrow \binom{t}{r} \equiv 1 \bmod 2$. Лемма 2 доказана. ■

Доказательство теоремы 2. Докажем первую часть теоремы. Предположим, что существуют такие числа $l, m, n, p, q, r, s, t, u$, удовлетворяющие условиям (4)-(12).

Из (4) немедленно следует, что

$$n > 1 \wedge l = \lfloor \log_2(n) \rfloor \tag{13}$$

и

$$1 \leqslant l \wedge 0 \leqslant \log_2(n) - l < 1. \tag{14}$$

Аналогично из (5)

$$q > 1 \wedge m - 1 = \lfloor \log_2(q) \rfloor \tag{15}$$

и

$$1 \leqslant m \wedge 0 \leqslant \log_2(q) - m + 1 < 1. \tag{16}$$

Далее. Несложно проверить, что $s$ можно представить в виде

$$s = \sum_{j=1}^{n} jB^{(n-j)(n+1)}. \tag{17}$$

Действительно - следует заметить, что

$$(\sum_{j=1}^{n} jB^{(n-j)(n+1)})(B^{2(n+1)}-2B^{n+1}+1)=\sum_{j=1}^{n} jB^{(n+1)(n+2-j)}-2\sum_{j=1}^{n} jB^{(n+1)(n+1-j)}$$

$$+\sum_{j=1}^{n} jB^{(n-j)(n+1)}=B^{(n+1)(n+1)}-\sum_{j=1}^{n-2} jB^{(n+1)(n-j)}-2nB^{n+1}+$$

$$+\sum_{j=1}^{n-2} jB^{(n+1)(n-j)}+(n-1)B^{n+1}+n=$$

$$=B^{(n+1)(n+1)}-(n+1)B^{n+1}+n=B^{(n+1)}(B^{(n+1)n}-(n+1))+n.$$

Отсюда

$$\sum_{j=1}^{n} jB^{(n-j)(n+1)})=\frac{B^{(n+1)}(B^{(n+1)n}-(n+1))+n}{(B^{2(n+1)}-2B^{n+1}+1)}=s.$$

Ясно, что

$$t=\sum_{k=1}^{n}(2^m-1)B^{(k-1)n}. \tag{18}$$

Так как

$$\sum_{k=1}^{n} B^{(k-1)n}=\frac{B^{n^2}-1}{B^n-1},$$

то равенство становится очевидным.

Рассмотрим теперь условие (8). Заметим, что оно, по лемме 2, эквивалентно

$$\operatorname{rem}((2^t+1)^t,2^{rt+1})>2^{rt}\Leftrightarrow\binom{t}{r}\equiv 1 \bmod 2. \tag{19}$$

Воспользуемся леммой 1. Записав число $r$ в двоичном виде, мы немедленно получим из леммы 1, (8), и (19)

$$r=\sum_{k=1}^{n} r_kB^{(k-1)n},\ r_k\leqslant 2^m-1,\ k=1,\dots,n. \tag{20}$$

Найдём вид чисел $r_k$. Рассмотрим произведение $rs$. Согласно указанным представлениям, оно имеет вид:

$$rs=\sum_{j=1}^{n}\sum_{k=1}^{n} jr_kB^{(n-j)(n+1)+(k-1)n}. \tag{21}$$

Легко видеть из условий на неравенства, что $jr_k \leqslant n(2^m-1) < 2^{l+1}(2^m-1) < 2^{l+m+1} = B$; кроме того, в ряду вида $(n-j)(n+1)+(k-1)n$ нет двух одинаковых чисел, в диапазоне индексов $1 \leqslant j \leqslant n, 1 \leqslant k \leqslant n$. Это означает, что мы можем записать $rs$ в следующем виде:

$$rs = \sum_{i=0}^{2n^2} d_i B^i, 0 \leqslant d_i < B, \tag{22}$$

где

$$d_i = \begin{Bmatrix} jr_k, & \text{если} i = (n-j)(n+1)+(k-1)n \\ 0, & \text{в противном случае.} \end{Bmatrix}. \tag{23}$$

Легко видеть, что при такой записи $r$ и $s$, число $u$ из (9), являющееся остатком от деления $rs$ на $B^{n^2-n}$, имеет вид:

$$u = \sum_{i=0}^{n^2-n-1} d_i B^i. \tag{24}$$

Тогда имеет место очевидное сравнение:

$$rs - u = \sum_{i=n^2-n}^{2n^2} d_i B^i \equiv \sum_{i=n^2-n}^{n^2-1} d_i B^i \bmod B^{n^2}. \tag{25}$$

Также можно заметить, что

$$\frac{(B^n-1)B^{n^2-n}}{B-1} q = \sum_{i=n^2-n}^{n^2-1} qB^i, \tag{26}$$

а поэтому $q = d_{n^2-k}$; но $kr_k = d_{n^2-k}$, поэтому $kr_k = d_{n^2-k} = q$. Значит, мы получаем представление для чисел $r_k$:

$$r_k = \frac{q}{k},\ k = 1, \ldots, n. \tag{27}$$

Так как $q$ делится на каждое из чисел $k = 1, \ldots, n$, то имеет место очевидное неравенство

$$q \geqslant \text{НОК}(1, \ldots, n). \tag{28}$$

Обратимся к условию (11). По определению,

$$p = \sum_{k=1}^{n} r_k B^{n(k-1)} - (B^n+1)f, \tag{29}$$

где $f$ - некоторое натуральное число. Несложно видеть, что

$$\sum_{k=1}^{n} r_k(B^{n(k-1)} + (-1)^k \equiv 0 \mod (B^n + 1).$$

Поэтому

$$p \equiv \sum_{k=1}^{n} (-1)^{k-1} r_k \mod (B^n + 1). \tag{30}$$

Легко видеть, что указанная сумма положительна, но не превосходит $q$ (т.к. $r_k \leqslant q$ и $r_k$ монотонно убывает, что очевидно следует из представления чисел $r_k$). Так как $q < B^n + 1$, а $p < B^n + 1$ по определению, то получаем, что

$$p = \sum_{k=1}^{n} (-1)^{k-1} r_k. \tag{31}$$

Значит,

$$\frac{p}{q} = \sum_{k=1}^{n} \frac{(-1)^{k-1} r_k}{q} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}. \tag{32}$$

Правая часть данного выражения при устремлении $n$ к бесконечности представляет собой известный ряд $\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} = \ln 2$. Поэтому справедливы неравенства:

$$\frac{1}{2} \leqslant \frac{p}{q}, \quad |\frac{p}{q} - \ln 2| < \frac{1}{2n}. \tag{33}$$

С одной стороны,

$$\frac{p}{q}m > (\ln 2 - \frac{1}{2n})m > (\ln 2 - \frac{1}{2n}) \log_2 q > \ln 2 \ln \text{НОК}(1, \ldots, n) - \frac{\log_2 q}{2n} >$$
$$> \psi(n) - \frac{m}{2n} > \psi(n) - 2 > \psi(n) - \sqrt{n} \log_2^2(n). \tag{34}$$

С другой стороны, с учётом последнего неравенства и условия (12), мы немеделенно выводим, что

$$\frac{p}{q}m < n - 15l^2\sqrt{n} < n - 3\sqrt{n} \log_2^2(n). \tag{35}$$

Отсюда немедленно следует, что

$$\psi(n) - 2\sqrt{n} \log_2^2(n) < \frac{p}{q}m < n - 3\sqrt{n} \log_2^2(n), \tag{36}$$

т.е. $\psi(n) < n - \sqrt{n} \log_2^2(n)$, что противоречит предположению об истинности гипотезы Римана. Мы, тем самым, доказали первую часть теоремы.

Докажем теперь вторую часть теоремы.

Предположим, что гипотеза Римана верна. Тогда найдётся $n$, большее 1, для которого $\psi(n) < n - 20\sqrt{n}\log_2^2 n$. Положим

$$l = \lfloor \log_2 n \rfloor, \tag{37}$$

$$q = \text{НОК}(1, \ldots, n), \tag{38}$$

$$m = \lfloor \log_2 q \rfloor + 1, \tag{39}$$

$$s = \sum_{j=1}^{n} jB^{(n-j)(n+1)}, \tag{40}$$

$$r_k = \frac{q}{k}, \tag{41}$$

и

$$r = \sum_{k=1}^{n} r_k B^{(k-1)n}, \tag{42}$$

где $B = 2^{l+m+1}$. При таком выборе чисел $r_k$ и $r$ будут верны следующие неравенства:

$$r_k \leqslant 2^m - 1, \tag{43}$$

$$jr_k \leqslant n(2^m - 1) < 2^{l+1}(2^m - 1) < 2^{l+m+1} = B. \tag{44}$$

Выберем

$$t = \sum_{k=1}^{n} (2^m - 1)B^{(k-1)n}. \tag{45}$$

Это значит, что все ненулевые цифры в записи этого числа имеют вид $2^m - 1$. Мы можем применить следствие 2:

$$2^m - 1 \geqslant r_k \Leftrightarrow \binom{t}{r} \equiv 1 \mod 2. \tag{46}$$

Запишем произведение $rs$ как сумму:

$$rs = \sum_{1 \leqslant j,k \leqslant n} jr_k B^{(n-j)(n+1)+(k-1)n} := \sum_{i=0}^{2n^2} d_i B^i, \tag{47}$$

где $d_i = jr_k$, если $i = (n-j)(n+1) + (k-1)n$, и $d_i = 0$, в противном случае; при этом $d_{n^2-k} = kr_k, d_i = q$ при $n^2 - n \leqslant i < n^2$.

Выберем

$$u = \sum_{i=0}^{n^2-n-1} d_i B^i. \tag{48}$$

Тогда

$$rs - u = \sum_{i=n^2-n}^{2n^2} d_i B^i; \tag{49}$$

Отсюда следует, во-первых, что

$$\exists v (rs - u = vB^{n^2-n}),$$

и, во-вторых, что

$$rs - u \equiv \sum_{n^2-n \leqslant i \leqslant n^2-1} qB^i = qB^{n^2-n} \sum_{0 \leqslant i \leqslant n-1} B^i = B^{n^2-n} \frac{B^n - 1}{B - 1} q \mod B^{n^2}$$

Введём $p$ как остаток от деления $r$ на $B^n + 1$. Тогда из определения $r$ следует, что

$$p \equiv \sum_{k=1}^{n} (-1)^{k-1} r_k \mod B^n + 1. \tag{50}$$

Так как $p < B^n + 1$ как остаток, а

$$\sum_{k=1}^{n} (-1)^{k-1} r_k < q < B^n + 1, \tag{51}$$

то

$$p = \sum_{k=1}^{n} (-1)^{k-1} r_k = \sum_{k=1}^{n} \frac{(-1)^{k-1} q}{k}. \tag{52}$$

Тогда справедливы неравенства

$$\frac{1}{2} \leqslant \frac{p}{q}, \quad |\frac{p}{q} - \ln 2| < \frac{1}{2n}. \tag{53}$$

Используя выбор числа $n$ и неравенство (2), запишем следующее неравенство

$$\log_2(q) = \frac{\ln q}{\ln 2} = \frac{\ln \text{НОК}(1, \ldots, n)}{\ln 2} = \frac{\psi(n)}{\ln 2} < 2\psi(n) < 4n. \tag{54}$$

Из (39), (53), (54) немедленно следует, что

$$\begin{gathered} \frac{p}{q} m < (\ln 2 + \frac{1}{2n})(\log_2 q + 1) = \ln 2 \log_2 q + \ln 2 + \frac{\log_2 q}{2n} + \frac{1}{2n} = \\ = \psi(n) + \frac{1}{2n} \frac{\psi(n)}{\ln 2} + \ln 2 + \frac{1}{2n} < \psi(n) + 2 + \ln 2 + \frac{1}{2n} < \\ < \psi(n) + 4 < \psi(n) + 4\sqrt{n}(\log_2 n)^2 < n - 20\sqrt{n}(\log_2 n)^2 + 4\sqrt{n}(\log_2 n)^2 = \\ = n - 16\sqrt{n}(\log_2 n)^2 = n - 16\sqrt{n} l^2 < n - 15\sqrt{n} l^2. \end{gathered}$$

Таким образом, условие (12) выполнено.

Мы показали, что при выборе произвольного $n$, удовлетворяющего достаточному условию, мы можем выбрать также все числа $l, m, p, q, r, s, t, u$ так, что система (4)-(12) будет совместна; более того, так как таких чисел $n$ бесконечно много, что следует из условия Шмидта, то и таких решений системы $l, m, n, p, q, r, s, t, u$ будет бесконечно много.

Тем самым, мы доказали вторую часть теоремы.

Теорема 2 доказана ■.

## §4. Диофантова переформулировка гипотезы Римана

Теорема Ю.В.Матиясевича о диофантовости возведения в степень позволяет нам переформулировать условия (3.4)-(3.12) в терминах диофантовых представлений, то есть построить такие полиномы $G_1(n, l; \vec{x}^{(1)})$, $G_2(q, m; \vec{x}^{(2)})$, $\ldots$, $G_9(l, m, n, p, q; \vec{x}^{(9)})$ с целыми коэффициентами, что

$$\exists \vec{x}^{(1)} \in \mathbb{N}\ (G_1(n, l; \vec{x}^{(1)})) = 0 \Longleftrightarrow (3.4),$$

$$\exists \vec{x}^{(2)} \in \mathbb{N}\ (G_2(q, m; \vec{x}^{(2)})) = 0 \Longleftrightarrow (3.5),$$

$$\ldots\ldots$$

$$\exists \vec{x}^{(9)} \in \mathbb{N}\ (G_9(l, m, n, p, q; \vec{x}^{(9)})) = 0 \Longleftrightarrow (3.12).$$

Воспользуемся известным диофантовым представлением функции $m = n^k$ (см., например, [11]):

$$m = n^k \Longleftrightarrow (\exists \vec{x}) f(m, n, k; \vec{x}) = 0,$$

где

$$\begin{gathered} f(m, n, k; \vec{x}) := (x_1^2 - (x_2^2 - 1)x_3^2 - 1)^2 + (x_4^2 - (x_2^2 - 1)x_5^2 - 1)^2 + \\ +(x_6^2 - (x_7^2 - 1)x_8^2 - 1)^2 + (x_5 - x_9 x_3^2)^2 + \\ (x_7 - 1 - 4x_{10}x_3)^2 + (x_7 - x_2 - x_{11}x_4)^2 + (x_6 - x_1 - x_{12}x_4)^2 + \\ +(x_8 - k - 4(x_{13} - 1)x_3)^2 + (x_3 - k - x_{14} + 1)^2 + (x_{17} - n - x_{18})^2 + \\ +(x_{17} - k - x_{19})^2 + ((x_1 - x_3(x_2 - n) - m)^2 - (x_{15} - 1)^2(2x_2 n - n^2 - 1)^2)^2 + \\ +(m + x_{16} - 2x_2 n + n^2 + 1)^2 + (x_2^2 - (x_{17}^2 - 1)(x_{17} - 1)^2 x_{20}^2 - 1)^2 \end{gathered}$$

и $\vec{x} := (x_1, \ldots, x_{20})$.

Построим многочлен $G_1$, являющийся диофантовым представлением (3.4).

Пусть $\psi_1 := 2^l$. Тогда диофантовым представлением такого $\psi$ будет уравнение $f(\psi_1, 2, l, \vec{x_1}^{(1)}) = 0$, где $\vec{x_1}^{(1)} = (x_1, \ldots, x_{20}) \in \mathbb{N}^{20}$. Условие же (3.4) переформулируется в виде

$$\psi_1 \leqslant n < 2\psi_1,$$

для которого диофантово представление можно построить элементарно, используя (2.6):

$$\psi_1 \leqslant n \Leftrightarrow \exists x_{21}\ (x_{21} + \psi_1 - 1 - n = 0),$$

$$n < 2\psi_1 \Leftrightarrow \exists x_{22}\ (x_{22} + n - 2\psi_1 = 0).$$

Таким образом, диофантовым представлением условия (3.4) будет уравнение:

$$G_1(\psi_1, n, l, \vec{x}^{(1)}) = 0, \tag{1}$$

где

$$G_1(\psi_1, n, l, \vec{x}^{(1)}) = f(\psi_1, 2, l; \vec{x_1}^{(1)})^2 + (x_{21} + \psi_1 - 1 - n)^2 + (x_{22} + n - 2\psi_1)^2$$

и $\vec{x}^{(1)} := (x_1, \ldots, x_{22})$.

Понятно, что таким же образом строится диофантово представление условия (3.5):

$$G_2(\psi_2, q, m, \vec{x}^{(2)}) = 0, \tag{2}$$

$$G_2(\psi_2, q, m, \vec{x}^{(2)}) := f(\psi_2, 2, m-1; \vec{x_1}^{(2)})^2 + (x_{43} + \psi_2 - 1 - q)^2 + (x_{44} + q - 2\psi_2)^2$$

и $\psi_2 := 2^{m-1}, \vec{x_1}^{(2)} := (x_{23}, \ldots, x_{42})$, а $\vec{x}^{(2)} := (\vec{x_1}^{(2)}, x_{43}, x_{44})$.

Имеем далее

$$\exists \vec{x_1}^{(3)}\ (f(\psi_3, 2, l + m + 1, \vec{x_1}^{(3)}) = 0) \Leftrightarrow \psi_3 = B,$$

где $\vec{x_1}^{(3)} := (x_{45}, \ldots, x_{64})$, и

$$\exists \vec{x_2}^{(3)}\ (f(\psi_4, 2, nl + nm + n, \vec{x_2}^{(3)}) = 0) \Leftrightarrow \psi_4 = B^n,$$

где $\vec{x_2}^{(3)} := (x_{65}, \ldots, x_{84})$, и

$$\exists \vec{x_3}^{(3)}\ (f(\psi_5, 2, n^2 l + n^2 m + n^2, \vec{x_3}^{(3)}) = 0) \Leftrightarrow \psi_5 = B^{n^2},$$

где $\vec{x_3}^{(3)} = (x_{85}, \ldots, x_{104})$.

Тогда диофантово представление условия (3.6) имеет вид

$$G_3(\psi_3, \psi_4, \psi_5, l, m, n, \vec{x}^{(3)}, s) = 0, \tag{3}$$

где

$$G_3(\psi_3, \psi_4, \psi_5, l, m, n, \vec{x}^{(3)}, s) := f(\psi_3, 2, l + m + 1, \vec{x_1}^{(3)})^2 +$$
$$f(\psi_4, 2, nl + nm + n, \vec{x_2}^{(3)})^2 + f(\psi_5, 2, n^2 l + n^2 m + n^2, \vec{x_3}^{(3)})^2 +$$
$$+ (s(\psi_4\psi_3 - 1)^2 - (\psi_4\psi_3(\psi_5\psi_4 - n - 1) + n))^2$$

и $\vec{x}^{(3)} = (x_{45}, \dots, x_{104})$.

Условие (3.7) можно переписать в уже известных переменных $\psi_2, \psi_4$ и $\psi_5$:

$$t = \frac{(\psi_2 - 1)(\psi_5 - 1)}{\psi_4 - 1}.$$

Введём полином $G_4$ следующим образом:

$$G_4(\psi_2, \psi_3, \psi_4, \psi_5, l, m, n, s, t) := (t(\psi_4 - 1) - (\psi_2 - 1)(\psi_5 - 1))^2,$$

и диофантово представление (3.7) запишем как

$$G_4(\psi_2, \psi_3, \psi_4, \psi_5, l, m, n, s, t) = 0. \tag{4}$$

Построим диофантово представление условия (3.8). Пусть $\psi_6 := 2^t$, $\psi_7 := (\psi_6 + 1)^t$, а $\psi_8 := 2^{rt}$. Тогда условие (3.8) запишется в виде:

$$(\mathrm{rem}(\psi_7, 2\psi_8) > \psi_8)) \wedge (r \leqslant t).$$

Введём теперь

$$\psi_9 := \mathrm{rem}(\psi_7, 2\psi_8) \Leftrightarrow \psi_9 < 2\psi_8 \wedge \exists y(\psi_7 - \psi_9 = 2y\psi_8).$$

Тогда $G_5$, диофантово представляющее условие (3.8), имеет вид:

$$G_5(\psi_6, \psi_7, \psi_8, \psi_9, t, r, \vec{x}^{(5)}) = 0, \tag{5}$$

где

$$\begin{gathered} G_5(\psi_6, \psi_7, \psi_8, \psi_9, t, r, \vec{x}^{(5)}) := f(\psi_6, 2, t, \vec{x_1}^{(5)})^2 + f(\psi_7, \psi_6 + 1, t, \vec{x_2}^{(5)})^2 + \\ + f(\psi_8, 2, rt, \vec{x_3}^{(5)})^2 + (x_{165} + \psi_8 - \psi_9)^2 + (x_{166} + \psi_9 - 2\psi_8)^2 + \\ (2x_{167}\psi_8 + \psi_9 - \psi_7)^2 + (x_{168} + r - t - 1)^2 \end{gathered}$$

и

$$\begin{gathered} \vec{x_1}^{(5)} := (x_{105}, \dots, x_{124}), \\ \vec{x_2}^{(5)} := (x_{125}, \dots, x_{144}), \\ \vec{x_3}^{(5)} := (x_{145}, \dots, x_{164}), \\ \vec{x}^{(5)} := (x_{105}, \dots, x_{168}). \end{gathered}$$

Заметим, что так как условия (3.4)-(3.12) выполняются одновременно, то можно воспользоваться уже предложенными представлениями для чисел $\psi_i$. Так, условие (3.9) в терминах $\psi_i$ запишется в виде:

$$u = \operatorname{rem}(rs, \frac{\psi_5}{\psi_4}) \Leftrightarrow (u\psi_4 < \psi_5) \ \wedge \exists y \ (\psi_4 rs = 2y\psi_5 + u\psi_4).$$

Поэтому естественно записать диофантово представление (3.9) как

$$G_6(\psi_4, \psi_5, u, r, s, \vec{x}^{(6)}) = 0, \tag{6}$$

где

$$G_6(\psi_4, \psi_5, u, r, s, \vec{x}^{(6)}) := (x_{169} + u\psi_4 - \psi_5)^2 + (\psi_4 rs - 2x_{170}\psi_5 - u\psi_4)^2$$

и $\vec{x}^{(6)} := (x_{169}, x_{170})$.

Рассмотрим условие (3.10). В терминах $\psi_i$ оно запишется как

$$rs - u \equiv \frac{\psi_5(\psi_4 - 1)}{\psi_4(\psi_3 - 1)} q \mod \psi_5,$$

поэтому его представление имеет очевидный вид:

$$\exists y \ ((rs - u)\psi_4(\psi_3 - 1) - \psi_5(\psi_4 - 1)q - \psi_4\psi_5(\psi_3 - 1)y = 0).$$

Понятно, что мы получили тем самым диофантово представление условия (3.10):

$$G_7(\psi_3, \psi_4, \psi_5, u, r, s, q, \vec{x}^{(7)}) = 0, \tag{7}$$

где

$$G_7(\psi_3, \psi_4, \psi_5, u, r, s, q, \vec{x}^{(7)}) := \psi_4\psi_5(\psi_3 - 1)x_{171} + \psi_5(\psi_4 - 1)q - (rs - u)\psi_4(\psi_3 - 1)$$

и $\vec{x}^{(7)} = x_{171}$.

Условие (3.11) так же можно записать в терминах $\psi_i$:

$$p = \operatorname{rem}(r, \psi_4 + 1) \Leftrightarrow \exists y \ (r - y(\psi_4 + 1) - p = 0 \wedge p < \psi_4 + 1),$$

диофантово представление которого теперь очевидно:

$$G_8(\psi_4, r, p, \vec{x}^{(8)}) = 0, \tag{8}$$

где

$$G_8(\psi_4, r, p, \vec{x}^{(8)}) := (x_{172}(\psi_4 + 1) + p - r)^2 + (x_{173} + p - \psi_4 - 1)^2$$

и $\vec{x}^{(8)} = (x_{172}, x_{173})$.

Наконец, последнее условие (3.12) можно задать диофантовым представлением совсем просто. Заметим, что

$$15l^2 q\sqrt{n} < nq - mp \Leftrightarrow (225 l^4 q^2 n < (nq - mp)^2) \wedge (nq > mp) \wedge (n > 0).$$

Последнее неравенство выполнено по определению. Значит, мы определим $G_9$ как:

$$G_9(l, m, n, p, q, \vec{x}^{(9)}) = (x_{174} + 225l^4q^2n - (nq - mp)^2)^2 + (x_{175} + mp - nq)^2,$$

где $\vec{x}^{(9)} = (x_{174}, x_{175})$, в результате чего диофантовым представлением условия (3.12) является уравнение:

$$G_9(l, m, n, p, q, \vec{x}^{(9)}) = 0. \tag{9}$$

Наконец, определим многочлен $G$ как:

$$\begin{gathered}
G(l, m, n, p, q, r, s, t, u, \vec{x}, \vec{\psi}) = G_1(\psi_1, n, l, \vec{x}^{(1)})^2 + G_2(\psi_2, q, m, \vec{x}^{(2)})^2 + \\
+ G_3(\psi_3, \psi_4, \psi_5, l, m, n, \vec{x}^{(3)}, s)^2 + G_4(\psi_2, \psi_3, \psi_4, \psi_5, l, m, n, s, t)^2 + \\
G_5(\psi_6, \psi_7, \psi_8, \psi_9, t, r, \vec{x}^{(5)})^2 + \\
+ G_6(\psi_4, \psi_5, u, r, s, \vec{x}^{(6)})^2 + G_7(\psi_3, \psi_4, \psi_5, u, r, s, q, \vec{x}^{(7)})^2 + \\
+ G_8(\psi_4, r, p, \vec{x}^{(8)})^2 + G_9(l, m, n, p, q, \vec{x}^{(9)})^2,
\end{gathered}$$

где $\vec{x} = (x_1, \ldots, x_{175})$, а $\vec{\psi} = (\psi_1, \ldots, \psi_9)$. Уравнение

$$G(l, m, n, p, q, r, s, t, u, \vec{x}, \vec{\psi}) = 0 \tag{10}$$

является диофантовым представлением системы (3.4-3.12) по построению, описанному в (2.10).

Далее удобно переобозначить переменные таким образом, чтобы исключить $\psi_i$. Пусть теперь $\psi_1 = x_{176}, \psi_2 = x_{177}, \ldots, \psi_9 = x_{184}$, и

$$\vec{x}^{(1)} = (x_1, \ldots, x_{22}, x_{176}),$$

$$\vec{x}^{(2)} = (x_{23}, \ldots, x_{44}, x_{177}),$$

$$\vec{x}^{(3)} = (x_{45}, \ldots, x_{104}, x_{177}, x_{178}, x_{179}, x_{180}),$$

$$\vec{x}^{(5)} = (x_{105}, \ldots, x_{168}, x_{181}, x_{182}, x_{183}, x_{184}),$$

$$\vec{x}^{(6)} = (x_{169}, x_{170}, x_{179}, x_{180}),$$

$$\vec{x}^{(7)} = (x_{171}, x_{178}, x_{179}, x_{180}),$$

$$\vec{x}^{(8)} = (x_{172}, x_{173}, x_{179}),$$

$$\vec{x}^{(9)} = (x_{174}, x_{175}),$$

а $\vec{x} = (x_1, \dots, x_{184})$. В терминах новых обозначений многочлен запишется просто:

$$G(l, m, n, p, q, r, s, t, u, \vec{x}) = G_1(n, l, \vec{x}^{(1)})^2 + G_2(q, m, \vec{x}^{(2)})^2 +$$
$$+ G_3(l, m, n, \vec{x}^{(3)}, s)^2 + G_4(l, m, n, s, t)^2 + G_5(t, r, \vec{x}^{(5)})^2 +$$
$$+ G_6(u, r, s, \vec{x}^{(6)})^2 + G_7(u, r, s, q, \vec{x}^{(7)})^2 +$$
$$+ G_8(r, p, \vec{x}^{(8)})^2 + G_9(l, m, n, p, q, \vec{x}^{(9)})^2.$$

Подытожив, получим следующее:

$$\text{Гипотеза Римана} \iff (\forall \vec{y} \in \mathbb{N}^{193})\ G(\vec{y}) \neq 0,$$

где $\vec{y} := (l, m, \dots, u, \vec{x})$.

**Заключение**

В данной работе было успешно выполнено исследование новой переформулировки гипотезы Римана и построено диофантово уравнение от 193-х переменных, неразрешимость которого эквивалентна гипотезе Римана. Такая переформулировка, несомненно, представляется на первый взгляд не менее простой, чем уже существующие переформулировки гипотезы Римана; тем не менее, такая переформулировка очень важна в теоретическом плане, так как построение указанного полинома от сравнительно малого количества переменных наглядно демонстрирует развитость диофантовой техники и потенциальную возможность упрощения вида диофантовых представлений. Представляется интересным, тем самым, исследование путей, которые могут ещё более упростить вид эквивалентной гипотезе Римана формулировки в терминах диофантовых уравнений.

**Список литературы**

[1] Карацуба, А.А. "Основы аналитической теории чисел", 2-е изд. — М.: Наука. Главная редакция физико-математической литературы, 1983, стр. 61-67.

[2] Schoenfeld, L. (1976) "Sharper bounds for the Chebyshev functions $\theta$(x) and $\psi$(x). II", Mathematics of Computation, 30 (134): 337–360.

[3] Матиясевич, Ю.В. (1993) "Десятая проблема Гильберта."— М.: Физматлит. 1993.

[4] Kreisel, G. 1958, "Mathematical significance of consistency proofs", Journal of Symbolic Logic vol. 23, no. 2, pp 155–182.

[5] Hernandez Caceres, J.M. "The Riemann Hypothesis and Diophantine equations", Master's Thesis Mathematics, *Mathematical Institute, University of Bonn,* May 2, 2018.

[6] Мороз, Б.З., "Гипотеза Римана и диофантовы уравнения", Препринт Санкт-Петербургского математического общества №3, 2018.

[7] Davis M., Matijasevich Yu., Robinson J. (1976) "Hilbert's tenth problem: Diophantine equations: Positive aspects of a negative solution", Proceedings of Symposia in Pure Mathematics. XXVIII.2. American Mathematical Society. pp. 323–378. ISBN 0-8218-1428-1.

[8] Матиясевич, Ю.В. (2019) "Гипотеза Римана как чётность специальных биномиальных коэффициентов", Чебышевский сборник Том 19. Выпуск 3, УДК 511.313:511.331.1:511.526, DOI 10.22405/2226-8383-2018-19-3-46-60.

[9] Ингам, А.Е. (1936) "Распределение простых чисел", Главная редакция общетехнической литературы и номографии, Москва-Ленинград, стр. 117.

[10] Kummer E. E. "Uber die Erganzungssatze zu den allgemeinen Reciprocitatsgesetzen", // Journal fur die Reine und Angewandte Mathematik. — 1852. — V. 44. — P. 93–146.

[11] M. Carl, B. Z. Moroz, "On a Diophantine representation of the predicate of provability", Zap. Nauchn. Sem. POMI, 2012, Volume 407, 77–104, p.83