**Препринт ПОМИ 09/2018**
(исправлен 24.06.2019*)

# Гипотеза Римана как чётность биномиальных коэффициентов

Ю. В. Матиясевич

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова
Российской Академии наук

yumat@pdmi.ras.ru

**Аннотация.** Гипотеза Римана имеет много эквивалентных переформулировок. Часть из них является арифметическими, то есть утверждениями о свойствах целых или натуральных чисел. Простейшую логическую структуру имеют переформулировки из класса $\Pi_1^0$ арифметической иерархии, имеющие вид "для любых $x_1, \ldots, x_m$ имеет место $A(x_1, \ldots, x_m)$", где $A$ – алгоритмически проверяемое отношение. Примером может служить переформулировка гипотезы Римана в виде утверждения о том, что некоторое диофантово уравнение не имеет решений (такое конкретное уравнение может быть явно указано).

Хотя логическая структура такой переформулировки очень проста, известные способы построения такого диофантова уравнения приводят к уравнениям, требующим для своей записи нескольких страниц. С другой стороны, известны весьма краткие по записи переформулировки, также принадлежащие классу $\Pi_1^0$. Примерами могут служить три критерия справедливости гипотезы Римана, которые предложили Ж.-Л. Николас, Г. Робин, и Дж. Лагариас. Недостатком этих переформулировок (по сравнению с диофантовым уравнением) является использование более "сложных" констант и функций, чем натуральные числа и сложение и умножение, достаточные для построения диофантова уравнения.

В работе приводится система из 9 условий, налагаемых на 9 переменных. Для формулировки этих условий используются только сложение, умножение, возведение в степень (унарное, с фиксированным основанием 2), функция "остаток от деления", неравенства, сравнения по модулю и биномиальный коэффициент. Вся система может быть явно выписана на одной странице. Доказано, что построенная система условий несовместна в том и только том случае, когда гипотеза Римана верна.

**Ключевые слова:** гипотеза Римана, биномиальные коэффициенты.

*Были исправлены следующие формулы: (2.4), (2.15), (2.16), (2.37), (2.41) и (2.42).

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

PREPRINTS
of the St.Petersburg Department
of Steklov Institute of Mathematics
of Russian Academy of Sciencies

---

# 1 Введение

Гипотеза Римана, подобно большинству великих проблем, имеет огромное количество эквивалентных переформулировок. Их обзору посвящено, например, недавно вышедшее двухтомное издание [1, 2]. Такие переформулировки даются в очень разных терминах, но мощная техника *арифметизации*, развитая К. Гёделем [3] позволяет легко превратить их в утверждения о целых или о натуральных числах. В этой работе мы ограничися такими *арифметическими* переформулировками.

А. Тьюринг, внёсший большой вклад в верификацию гипотезы Римана (см., например, [1, 4, 5, 6, 7]), интересовался также вопросом, сколь простой, *с логической точки зрения*, может быть переформулировка гипотезы Римана. Он ввёл в [8] понятие *теоретико-числовой теоремы*:

> By a number-theoretic theorem we shall mean a theorem of the form "$\theta(x)$ vanishes for infinitely many natural numbers $x$", where $\theta(x)$ is a primitive recursive function. ... An alternative form for number-theoretic theorems is "for each natural number $x$ there exists a natural number $y$ such that $f(x, y)$ vanishes", where $f(x, y)$ is primitive recursive.

Теоретико-числовые теоремы в смысле Тьюринга эквивалентны доказуемым формулам из класса $\Pi_2^0$ *арифметической иерахии*. Этот класс может быть описан как класс формул вида

$$\forall x_1 \dots x_m \exists y_1 \dots y_n A(x_1, \dots, x_m, y_1, \dots, y_n), \tag{1.1}$$

где $A(x_1, \dots, x_m, y_1, \dots, y_n)$ – алгоритмически проверяемое отношение между натуральными числами $x_1, \dots, x_m, y_1, \dots, y_n$. Мотивируя свое определение, Тьюринг построил формулу из класса $\Pi_2^0$, эквивалентную гипотезе Римана.

Этот результат был усилен Г. Крайзелем [9], который дал переформулировку гипотезы Римана посредством формулы из класса $\Pi_1^0$, состоящего из формул вида

$$\forall x_1 \dots x_m A(x_1, \dots, x_m). \tag{1.2}$$

Такие формулы можно охарактеризовать, как *эффективно опровергаемые*: если формула (1.2) является ложной, то для установления этого достаточно предъявить один конкретный набор чисел $x_1 \dots x_n$, не находящихся в отношении $A$. Пользуясь алгоритической разрешимостью этого отношения, можно построить, например, машину Тьюринга (или написать программу на какомлибо языке программирования), которая будет перебирать по очереди всевозможные значения $x_1 \dots x_n$ в поисках требуемого контрпримера. Такая машина/программа будет работать неограниченно долго в том и только случае, когда формула (1.2) истинна.

Благодаря результату Крайзеля появилась возможность указать такую машину/программу для гипотезы Римана, и в ряде работ это было сделано. С. Ааронсон и А. Едидиа [10] построили машину Тьюринга с двухбуквенным ленточным алфавитом, которая, начав работу с пустой лентой, никогда не остановится, если и только если гипотеза Римана верна. В [10] машина имеет 5372 состояния; это было в дальнейшем улучшено до 744 состояний (см. [11]). Х. Калуд, Е. Калуд и М. Динин [12, 13] и автор [14] построили разные версии *регистровых машин* с аналогичным свойством.

В 1970 году автор сделал последний шаг в доказательстве того, что сейчас часто называется ДПРМ-теоремой[1]. Этот результат позволяет по произвольной формуле из класса $\Pi_1^0$ построить эквивалентную ей формулу из того же класса, имеющую следующий специальный вид:

$$\forall x_1 \dots x_m P(x_1, \dots, x_m) \neq 0, \tag{1.3}$$

где $P(x_1, \dots, x_m)$ – многочлен с целыми коэффициентами. В частности, можно явно указать многочлен $R(x_1, \dots, x_m)$ такой, что гипотеза Римана эквивалентна утверждению о том, что диофантово уравнение

$$R(x_1, \dots, x_m) = 0 \tag{1.4}$$

не имеет решений. Способы построения такого многочлена описаны в [17, раздел 2] и [16, параграф 6.4]; больше деталей дано в [18, 19]; см. также [20].

Переформулировка гипотезы Римана в виде (1.3) имеет, несомненно, чрезвычайно простую *структуру*: используются только кванторы общности, а проверяемое условие сводится к вычислению значения многочлена. С другой стороны, хотя в таком многочлене может быть всего 9 переменных ([21], детали см. в [22]), все ранее известные способы дают многочлены, требующие нескольких страниц для своего явного выписывания.

Известно немало других переформулировок гипотезы Римана в виде (1.2) со сложнее проверяемыми, но зато коротко записываемыми отношениями $A$; несколько таких примеров приведено ниже.

Многие классические результаты близки по форме к (1.2), но используют, например, символ $O$-большое, содержащий скрытый квантор существования. Такой квантор можно устранить, найдя явное значение соответствующей константы.

Для построения диофантова уравнения (1.4) в [17] и машины Тьюринга в [10] была использована переформулировка гипотезы Римана, которую предложил Х. Шапиро (см. [17, раздел 2] и [1, раздел 10.2]). Она даётся в терминах

[1] По первым буквам фамилий авторов теоремы – М. Дейвиса, Х. Патнема, Дж. Робинсон и автора этой статьи; детальные доказательства теоремы приведены, например, в [15, 16].

*функции Чебышева* $\psi(n)$, которая определяется следующим образом:

$$\psi(n) = \ln(\mathrm{LCM}(1, \ldots, n)) = \ln(2) \log_2(\mathrm{LCM}(1, \ldots, n)), \tag{1.5}$$

где LCM обозначает наименьшее общее кратное. Гипотеза Римана эквивалентна утверждению, что

$$\psi(n) = n + O\sqrt{n} \ln^2(n). \tag{1.6}$$

Для устранения неявной константы, подразумеваемой здесь в символе $O$-большое, Шапиро рассмотрел сумматорную функцию

$$\psi_1(n) = \sum_{1 \le m < n} \psi(m) \tag{1.7}$$

и доказал, что гипотеза Римана эквивалентна следующему неравенству с явной константой:

$$\left| \psi_1(m) - \frac{m^2}{2} \right| < 6m\sqrt{m}. \tag{1.8}$$

Позднее Л. Шёнфельд ([23], см. также [1, теорема 4.9]) нашёл явное значение константы в (1.6), а именно, доказал, что гипотеза Римана эквивалентна справедливости неравенства

$$|\psi(n) - n| < \frac{1}{8\pi} \sqrt{n} \ln(n)^2, \tag{1.9}$$

при $n \ge 74$. Как раз использование этого критерия вместо (1.8) позволило упростить построение многочлена (1.3) в [16] и уменьшить количество состояний у машины Тьюринга в [11].

Ж.-Л. Николас ([24], см. также [1, теорема 5.31]) установил, что гипотеза Римана эквивалентна неравенству

$$\mathrm{e}^\gamma \log(\log(N_n)) < \frac{N_n}{\phi(N_n)}, \tag{1.10}$$

где $\mathrm{e} = 2.71828\ldots$, $\gamma = 0.577215\ldots$ – постоянная Эйлера, $N_n$ – произведение $n$ первых простых чисел, $\phi(m)$ – функция Эйлера (количество чисел, которые меньше $m$ и взаимно просты с этим числом).

Г. Робин ([25], см. также [1, теорема 7.16]) установил, что гипотеза Римана эквивалентна справедливости при $n \ge 5040$ неравенства

$$\sigma(n) < \mathrm{e}^\gamma n \log(\log(n)), \tag{1.11}$$

где $\sigma(n)$ – сумма всех делителей $n$. Это необходимое и достаточное условие известно также как *критерий Рамануджана–Робина*, поскольку С. Рамануджан доказал неравенство (1.11) для достаточно больших $n$ в предположении гипотезы Римана.

Дж. Лагариас ([26], см. также [1, Теорема 7.18]) заменил правую часть неравенства (1.11) и получил ещё одно условие, необходимое и достаточное для справедливости гипотезы Римана:

$$\sigma(n) < H_n + \mathrm{e}^{H_n} \log(H_n), \tag{1.12}$$

где $H_n = 1 + 1/2 + \cdots + 1/n$ и $n$ может быть произвольным.

Условия типа (1.8)–(1.12) коротко записываются и алгоритмически проверяются, однако они содержат константы и функции, такие как $\psi(n)$, $N_n$, $\phi(n)$, $\sigma(n)$, которые являются "сложными" по сравнению с целыми коэффициентами и операциями сложения и умножения, используемыми в (1.4). Цель настоящей работы – предложить "компромисную" переформулировку гипотезы Римана. Её преимущество перед диофантовым уравнением состоит в том, что все условия можно явно выписать на одной странице. Недостатком по сравнению с (1.4), но преимуществом по сравнению с (1.8)–(1.12), является набор используемых функции. Наряду со сложением и умножением в нашем необходимом и достаточном условии участвуют лишь возведение в степень (только унарное, с основанием 2), квадратный корень (легко устраняемый), $\mathrm{rem}(a, b)$ (остаток от деления $a$ на $b$), неравенства и сравнения по модулю, а также биномиальный коэффициент, играющий ключевую роль.

Биномиальные коэффициенты обладают удивительно большой выразительной силой. Х. Манн и Д. Шенкс [27] дали критерий простоты в виде делимости определённых элементов треугольника Паскаля. Л. Шю и Р. Шуе [28] перереформулировали Великую теорему Ферма в виде равенства нулю некоторой комбинаторной суммы произведений биномиальных коэффициентов. Автор [29] дал в виде делимости одного биномиального коэффициента критерии того, что

1. число $p$ является простым;
2. числа $p$ и $p + 2$ являются простыми числами-близнецами;
3. число $p$ является простым числом Ферма;
4. число $p$ является простым числом Мерсенна.

В [30] автор переформулировал гипотезу (ныне теорему) о четырёх красках в виде неделимости некоторого произведения биномиальных коэффициентов. В аналогичном виде М. Маргенштерн и автор [31] переформулировали известную $3x + 1$ проблему.

Конструкции в [29, 30, 31] основаны на следующем свойстве биномиальных коэффициентов.

Теорема (Э. Куммер [32]). *Пусть числа $a$ и $b$ следующим образом записываются в позиционной системе счисления с простым основанием $p$:*

$$a = \sum_{k=0}^{m} a_k p^k,\ b = \sum_{k=0}^{m} b_k p^k,\ 0 \le a_k < p,\ 0 \le b_k < p,\ k = 0, \ldots, m; \qquad (1.13)$$

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

Этот результат Куммера долго оставался малоизвестным и был переоткрыт разными авторами; доказательство теоремы можно найти также, например, в [16, 33].

Мы будем использовать такое следствие теоремы Куммера для случая $p = 2$ в (1.13). Будем говорить, что $a$ *маскирует* $b$ (и писать $a \succeq b$), если $a_k \ge b_k$ для $k = 0, \ldots, m$. Из теоремы Куммера следует такая эквивалентность:

$$\binom{a}{b} \equiv 1 \pmod 2 \iff a \succeq b. \qquad (1.14)$$

Это можно также вывести из частного случая теоремы Люка [34, раздел XXI]:

$$\binom{a}{b} \equiv \binom{a_0}{b_0} \ldots \binom{a_m}{b_m} \pmod p. \qquad (1.15)$$

# 2 Новая переформулировка гипотезы Римана

Исходным пунктом для нас будет неравенство (1.9), модифицированное по-разному в необходимом и достаточном условиях:

- *из гипотезы Римана следует, что для всех $n > 1$*

$$\psi(n) > n - \sqrt{n}\log_2^2(n); \qquad (2.1)$$

- *если гипотеза Римана не верна, то существует бесконечно много значений $n$, для которых*

$$\psi(n) < n - 20\sqrt{n}\log_2^2(n). \qquad (2.2)$$

Мы будем использовать тот факт, что правая часть в необходимом условии (2.1) больше правой части в достаточном условии (2.2). Неравенство (2.1) при $n \geq 74$ следует из неравества (1.9), а недостающие случаи $n = 2, \ldots, 73$ проверяются непосредственным вычислением. Достаточность условия (2.2) следует из $\Omega_{\pm}$-результата для функции $\psi(n)$, который получил Е. Шмидт ([35], см. также [36, теорема 32], [1, теорема 4.8]).

**Теорема 1.** *Рассмотрим систему условий*

$$2^l \leq n < 2^{l+1}, \tag{2.3}$$

$$2^m \leq 2q < 2^{m+1}, \tag{2.4}$$

$$s = \frac{B^{n+1}\left(B^{(n+1)n} - n - 1\right) + n}{\left(B^{n+1} - 1\right)^2}, \tag{2.5}$$

$$t = \frac{(2^m - 1)\left(B^{n^2} - 1\right)}{B^n - 1}, \tag{2.6}$$

$$\binom{t}{r} \equiv 1 \pmod 2, \tag{2.7}$$

$$u = \operatorname{rem}\left(rs, B^{n^2-n}\right), \tag{2.8}$$

$$rs - u \equiv \frac{B^{n^2-n}\left(B^n - 1\right)}{B - 1} q \pmod{B^{n^2}}, \tag{2.9}$$

$$p = \operatorname{rem}(r, B^n + 1), \tag{2.10}$$

$$mp < nq - 15l^2 q\sqrt{n}, \tag{2.11}$$

*в которой $B$ обозначает $2^{l+m+1}$.*

*(А) Если гипотеза Римана верна, то система* (2.3)–(2.11) *не имеет решений в положительных целых числах $l, m, n, p, q, r, s, t, u$.*

*(Б) Если гипотеза Римана не верна, то система* (2.3)–(2.11) *имеет бесконечно много таких решений.*

**Доказательство части (A)** мы проведём "от противного". Предположим, что нашлись числа $l, m, n, p, q, r, s, t$ и $u$, удовлетворяющие условиям (2.3)–(2.11).

Согласно (2.3),

$$n > 1 \tag{2.12}$$

и

$$l = \lfloor \log_2(n) \rfloor. \tag{2.13}$$

Очевидно, что

$$1 \le l, \quad 0 \le \log_2(n) - l < 1. \tag{2.14}$$

Аналогично согласно (2.4)

$$m = \lfloor \log_2(q) \rfloor + 1 \tag{2.15}$$

и

$$0 < m - \log_2(q) \le 1. \tag{2.16}$$

Рассмотрим записи чисел $s$, $t$, $r$ и $rs$ в позиционной системе счисления с основанием $B$.

Легко проверить, что из (2.5) следует, что

$$s = \sum_{j=1}^{n} j B^{(n-j)(n+1)}. \tag{2.17}$$

Это означает, что единственными ненулевыми цифрами числа $s$ являются числа $1, \ldots, n$, и они разделены блоками из $n$ нулей.

Аналогично из (2.6) следует, что

$$t = \sum_{k=1}^{n} (2^m - 1) B^{(k-1)n}, \tag{2.18}$$

иными словами, все ненулевые цифры числа $t$ равны $2^m - 1$, и они разделены блоками из $n - 1$ нуля.

Двоичная запись некоторого числа $a$ получается из его записи в системе счисления с основанием $B$ посредством замены каждой $B$-ичной цифры на её двоичную запись, при необходимости дополненную спереди нулями до длины $l + m + 1$. По этой причине $a$ маскирует $b$ тогда и только тогда, когда каждая $B$-ичная цифра $a$ маскирует соответствующую цифру числа $b$.

Согласно (1.14) из (2.7) следует, что $t \succeq r$, и потому число $r$ имеет вид

$$r = \sum_{k=1}^{n} r_k B^{(k-1)n}, \tag{2.19}$$

где

$$r_k \le 2^m - 1, \quad k = 1, \ldots, n. \tag{2.20}$$

Пусть

$$rs = \sum_{i=0}^{2n^2} d_i B^i, \quad 0 \le d_i < B, \quad i = 0, \ldots 2n^2. \tag{2.21}$$

Согласно (2.17) и (2.19)

$$rs = \sum_{j=1}^{n} \sum_{k=1}^{n} j r_k B^{(n-j)(n+1)+(k-1)n}. \tag{2.22}$$

Легко проверить, что при $1 \le j \le n$, $1 \le k \le n$ среди чисел вида $(n-j)(n+1)+(k-1)n$ нет двух одинаковых. Кроме того, из (2.3) и (2.19) следует, что

$$j r_k \le n(2^m - 1) < 2^{l+1}(2^m - 1) < 2^{l+m+1} = B. \tag{2.23}$$

Таким образом, всевозможные произведения вида $jr_k$ являются единственными ненулевыми цифрами числа $rs$, точнее,

$$d_i = \begin{cases} j r_k, & \text{если } i = (n-j)(n+1)+(k-1)n \\ 0, & \text{в противном случае.} \end{cases} \tag{2.24}$$

В частности, при $j = k$ получаем, что

$$d_{n^2-k} = k r_k, \quad k = 1, \ldots, n. \tag{2.25}$$

Согласно (2.8) и (2.21)

$$u = \sum_{i=0}^{n^2-n-1} d_i B^i. \tag{2.26}$$

Иными словами, число $u$ – это "хвост" записи произведения $rs$, состоящий из её последних $n^2 - n$ цифр. Соответственно,

$$rs - u = \sum_{i=n^2-n}^{2n^2} d_i B^i \equiv \sum_{i=n^2-n}^{n^2-1} d_i B^m \pmod{B^{n^2}}. \tag{2.27}$$

Имеет место тождество

$$\sum_{i=n^2-n}^{n^2-1} q B^i = \frac{(B^n - 1)\, B^{n^2-n}}{B-1} q, \tag{2.28}$$

благодаря которому из (2.9), (2.25) и (2.27) следует, что

$$kr_k = d_{n^2-k} = q, \quad k = 1, \ldots, n. \tag{2.29}$$

Отсюда мы получаем следующие значения цифр числа $r$:

$$r_k = \frac{q}{k}, \quad k = 1, \ldots, n. \tag{2.30}$$

Согласно (2.29) $q$ делится на $1, \ldots, n$, следовательно,

$$\mathrm{LCM}(1, \ldots, n) \le q. \tag{2.31}$$

Из очевидного сравнения

$$B^n \equiv -1 \pmod{B^n + 1} \tag{2.32}$$

и равенства (2.19) следует, что

$$p \equiv \sum_{k=1}^{n} (-1)^{k-1} r_k \pmod{B^n + 1}. \tag{2.33}$$

Слагаемые в знакопеременной сумме в (2.33) по абсолютной величине монотонно убывают, первое слагаемое равно $q$, следовательно, сумма положительна и не превосходит $q$. Таким образом, в сравнении (2.33) левая и правая части положительны и не превосходят его модуля, следовательно, они равны. Соответственно,

$$\frac{p}{q} = \sum_{k=1}^{n} \frac{(-1)^{k-1} r_k}{q} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \approx \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} = \ln(2) \tag{2.34}$$

и справедливы элементарные неравенства

$$\frac{1}{2} \le \frac{p}{q}, \quad \left| \frac{p}{q} - \ln(2) \right| < \frac{1}{2n}. \tag{2.35}$$

Из (2.11) и (2.35) следует, что

$$m < \frac{n - 15l^2 p\sqrt{n}}{p/q} \le 2n. \tag{2.36}$$

Далее, согласно (2.35), (2.36), (2.16), (2.31), (1.5) и (2.12), имеем:

$$\begin{aligned} \frac{p}{q} m > \left( \ln(2) - \frac{1}{2n} \right) m = \ln(2) m - \frac{m}{2n} > \ln(2) \log_2(q) - 1 = \\ \ln(q) - 1 \ge \ln(\mathrm{LCM}(1, 2, \ldots, n)) - 1 = \\ \psi(n) - 1 > \psi(n) - 2\sqrt{n} \log_2^2(n). \end{aligned} \tag{2.37}$$

С другой стороны, согласно (2.11) и (2.14)

$$\frac{p}{q}m < n - 15l^2\sqrt{n} < n - 3\sqrt{n}\log_2^2(n). \tag{2.38}$$

Три неравенства, (2.1), (2.37) и (2.38), дают требуемое противоречие.

Часть (А) доказана.

**Доказательство части (Б).** В качестве $n$ мы возьмём произвольное из чисел, превосходящих 1 и удовлетворяющих неравенству (2.2). Из доказательства части (А) видно, что значения остальных переменных почти однозначно определяются значением $n$.

Выберем $l$ согласно (2.13), так что условие (2.3) будет выполнено и будут справедливы неравенства (2.14).

Положим

$$q = \mathrm{LCM}(1, \ldots, n), \tag{2.39}$$

и выберем $m$ согласно (2.15), так что условие (2.4) будет выполнено и будут справедливы неравенства (2.16).

Выберем $s$ согласно (2.17), так что условие (2.5) будет выполнено.

Определим числа $r_k$ и $r$ согласно (2.30) и (2.19), при этом согласно (2.16) будут справедливы неравенства (2.20) и (2.23). Поскольку двоичная запись числа $2^m - 1$ состоит из $m$ единиц, из (2.23) следует, что

$$2^m - 1 \succeq r_k, \quad k = 1, \ldots, n. \tag{2.40}$$

Выберем $t$ согласно (2.18), так что условие (2.6) будет выполнено. Все ненулевые цифры числа $t$ равны $2^m - 1$, и согласно (2.40) они маскируют соответствующие цифры числа $r$. Отсюда следует, что $t \succeq r$ и, согласно (1.14), условие (2.7) выполнено.

Точно так же, как в доказательстве части (А) мы заключаем, что в представлении (2.21) цифры $d_i$ определяются равенством (2.24) и его частным случаем (2.25).

Выберем $u$ согласно (2.26), тогда будут выполнены условие (2.8) и сравнение (2.27), в котором согласно (2.25) во второй сумме все $d_i$ равны $q$. Поскольку меет место тождество (2.28), то выполнено и условие (2.9).

Точно так же, как в доказательстве части (А) мы заключаем, что справедливы неравенства (2.35).

Согласно (2.39), (1.5) и (2.2)

$$\log_2(q) = \log_2\big(\mathrm{LCM}(1, \ldots, n)\big) = \psi(n)/\ln(2) < 2\psi(n) < 3n. \tag{2.41}$$

Используя, кроме того, (2.35), (2.16), (2.12), (2.2) и (2.14), отсюда получаем, что

$$\frac{p}{q}m < \left(\ln(2) + \frac{1}{2n}\right)(\log_2(q)+1) = \psi(n) + \frac{\log_2(q)}{2n} + \ln(2) + \frac{1}{2n} < \\ < \psi(n) + 3\sqrt{n}\log_2^2(n) < n - 17\sqrt{n}\log_2^2(n) < n - 17\sqrt{n}l^2 \quad (2.42)$$

и, следовательно, условие (2.11) выполнено.

Часть (Б) доказана. Теорема доказана.

Замечание. Если разрешить возведение в степень произвольных чисел (а не только числа 2 как в (2.3)–(2.11)), то можно избежать использования биномиального коэффициента. А именно,

$$\binom{t}{r} \equiv 1 \pmod 2 \iff \mathrm{rem}((2^t+1)^t, 2^{rt+1}) > 2^{rt}. \quad (2.43)$$

Заменив условие (2.7) на правую часть в (2.43), мы получим систему условий, каждое из которых легко может быть преобразовано в экспоненциально диофантово уравнение за счёт введения дополнительных неизвестных. Все эти уравнения могут быть объединены в одно экспоненциально диофантово уравнение, неразрешимость которого эквивалентна гипотезе Римана. Стандартная техника (см., например, [15, 16]) позволяет преобразовать это экспоненциально диофантово уравнение в эквивалентное ему диофантово уравнение с дополнительными переменными, допускающее сравнительно короткую запись.

# Заключение

Мы установили, что гипотеза Римана эквивалентна несовместности условий (2.3)–(2.11). Представляется интересным исследовать системы условий, получающиеся из (2.3)–(2.11) удалением одного из них или заменой его на более слабое. Например, допускают ли хорошее описание решения системы, получающейся заменой биномиального условия (2.7) на вытекающее из него неравенство $r \le t$?

# Список литературы

[1] Broughan K. Equivalents of the Riemann hypothesis. Volume 1: Arithmetic equivalents. — Cambridge: Cambridge University Press, 2017. — ISBN 978-1-107-19704-6/hbk.

[2] Broughan K. Equivalents of the Riemann hypothesis. Volume 2: Analytic equivalents. — Cambridge: Cambridge University Press, 2017. — P. xx + 491. — ISBN 978-1-107-19712- 1/hbk; 978-1-108-17826-6/ebook. — DOI: 10.1017/9781108178266.

[3] Gödel K. Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme. I. // Monatsh. Math. Phys. — 1931. — B. 38. — S. 173–198. — ISSN 0026-9255; 1436-5081/e. — DOI: 10.1007/BF01700692.

[4] Booker A. R. Turing and the Riemann hypothesis. // Notices Am. Math. Soc. — 2006. — T. 53, №10. — P. 1208–1211. — ISSN 0002-9920; 1088-9477/e.

[5] Booker A. R. Artin's conjecture, Turing's method, and the Riemann hypothesis. // Exp. Math. — 2006. — V. 15, № 4. — P. 385–407. — ISSN 1058-6458; 1944-950X/e. — DOI: 10.1080/10586458.2006.10128976.

[6] Alan Turing – His Work and Impact / под ред. S. B. Cooper, J. van Leeuwen. — Elsevier Science, 2013. — ISBN 978-0-12-386980-7. — DOI: 10.1016/C2010-0-66380-2.

[7] Матиясевич Ю. В. Алан Тьюринг и теория чисел // Математика в высшем образовании. — 2012. — Т. 10. — С. 111–134. — URL: http://www.unn.ru/math/no/10/_nom10_012_matiyasevich.pdf.

[8] Turing A. M. On computable numbers, with an application to the Entscheidungsproblem // Proc. London Math. Soc. — 1936. — V. 42, №2. — P. 230–265.

[9] Kreisel G. Mathematical significance of consistency proofs // Journal of Symbolic Logic. — 1958. — V. 23, №2. — P. 155–182.

[10] Yedidia A., Aaronson S. A Relatively Small Turing Machine Whose Behavior Is Independent of Set Theory // Complex Systems. — 2016. — V. 25. — DOI: 10.25088/ComplexSystems.25.4.297.

[11] Aaronson S. The blog. — URL: https://www.scottaaronson.com/blog/?p=2741.

[12] Calude C. S., Calude E., Dinneen M. J. A new measure of the difficulty of problems // J. Mult.-Val. Log. Soft Comput. — 2006. — V. 12, №3/4. — P. 285–307. — ISSN 1542-3980; 1542-3999/e.

[13] Calude E. The complexity of Riemann's hypothesis. // J. Mult.-Val. Log. Soft Comput. – 2012. — V. 18, №3/4. — P. 257–265. — ISSN 1542-3980; 1542-3999/e.

[14] Yu. V. Matiyasevich. The Riemann Hypothesis in Computer Science // Препринты Санкт-Петербургского отделения Математического ин-та РАН. — 2018. — № 07. — DOI: 10.13140/RG.2.2.14041.83041. — URL: http://www.pdmi.ras.ru/preprint/2018/18-07.html.

[15] Манин Ю. И., Панчишкин А. А. Введение в теорию чисел. — М.:ВИНИТИ, 1990. — Р. 5–341. — (Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления. Т. 49.).

[16] Матиясевич Ю. В. Десятая проблема Гильберта. — М.:Физматлит, 1993.

[17] Davis M., Matijasevič Yu., Robinson J. Hilbert's tenth problem: Diophantine equations: Positive aspects of a negative solution // Proc. Symp. Pure Math. — 1976. — V. 28, P. 323–378.

[18] Hernandez Caceres J. M. The Riemann Hypothesis and Diophantine equations. — Master's Thesis in Mathematics, Mathematical Institute, University of Bonn.

[19] Мороз Б. З. Гипотеза Римана и диофантовы уравнения // Препринты Санкт-Петербургского математического общества. — 2018. — №03. — URL: http://www.mathsoc.spb.ru/preprint/2018/index.html#03.

[20] Nayebi A. On the Riemann Hypothesis and Hilbert's Tenth Problem. — Unpublished Manuscript, 2012. — URL: http://web.stanford.edu/~anayebi/projects/RH_Diophantine.pdf.

[21] Matijasevič Yu. V. On recursive unsolvability of Hilbert's tenth problem // Studies in Logic and the Foundations of Mathematics. — V. 74. — P. 89–110.

[22] Jones J. P. Universal Diophantine equation. // J. Symb. Log. — 1982. — V. 47. — P. 549– 571. — ISSN 0022-4812; 1943-5886/e. — DOI: 10.2307/2273588.

[23] Schoenfeld L. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. // Math. Comput. — 1976. — V. 30. — P. 337–360. — ISSN 0025-5718; 1088-6842/e. — DOI: 10.2307/2005976.

[24] Nicolas J.-L. Petites valeurs de la fonction d'Euler // J. Number Theory. — 1983. — V. 17. — P. 375–388. — ISSN 0022-314X; 1096-1658/e. — DOI: 10.1016/0022-314X(83)90055-0.

[25] Robin G. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann // J. Math. Pures Appl. (9). — 1984. — V. 63. — P. 187–213. — ISSN 0021-7824.

[26] Lagarias J. C. An elementary problem equivalent to the Riemann hypothesis // Am. Math. Mon. — 2002. — V. 109, №6. — P. 534–543. — ISSN 0002-9890. — DOI: 10.2307/2695443.

[27] Mann H. B., Shanks D. A necessary and sufficient condition for primality, and its source. // J. Comb. Theory, Ser. A. — 1972. — V. 13. — P. 131–134. — ISSN 0097-3165. — DOI: 10.1016/0097-3165(72)90016-7.

[28] Hsu L., Shiue P. J.-S. On a combinatorial expression concerning Fermat's Last Theorem // Adv. Appl. Math. — 1997. — V. 18, №2. — P. 216–219. — ISSN 0196-8858. — DOI: 10.1006/aama.1996.0510.

[29] Матиясевич Ю. В. Один класс критериев простоты, формулируемых в терминах делимости биномиальных коэффициентов // Зап. научн. сем. ЛОМИ. — 1977. — Т. 67. — P. 167–183. — URL: http://mi.mathnet.ru/znsl2015.

[30] Matiyasevich Yu. Some arithmetical restatements of the four color conjecture. // Theor. Comput. Sci. — 2001. — V. 257, №1/2. — P. 167–183. — ISSN 0304-3975. — DOI: 10.1016/S0304-3975(00)00115-8.

[31] Margenstern M., Matiyasevich Yu. A binomial representation of the $3x + 1$ problem. // Acta Arith. — 1999. — V. 91, №4. — P. 367–378. — ISSN 0065-1036; 1730-6264/e. — DOI: 10.4064/aa-91-4-367-378.

[32] Kummer E. E. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen // Journal für die Reine und Angewandte Mathematik. — 1852. — V. 44. — P. 93–146.

[33] Singmaster D. Notes on binomial coefficients. I: A generalization of Lucas' congruence. // J. Lond. Math. Soc., II. Ser. — 1974. — V. 8. — P. 545–548. — ISSN 0024-6107; 1469-7750/e. — DOI: 10.1112/jlms/s2-8.3.545.

[34] Lucas E. Théorie des Fonctions Numériques Simplement Périodiques // American Journal of Mathematics. — 1878. — V. 1. — P. 184–240. — URL: http://www.jstor.org/stable/2369311.

[35] Schmidt E. 1903, Über die Anzahl der Primzahlen unter gegebener Grenze // Math Annalen. — 1932. — V. 57. — P. 195–203.

[36] Ингам А. Э. *Распределение простых чисел* (перевод с англ.) — М.:Едиториал УРСС, 2005.