ЧЕБЫШЕВСКИЙ СБОРНИК

Том 19. Выпуск 3.

УДК 511.313:511.331.1:511.526

DOI 10.22405/2226-8383-2018-19-3-46-60

**Гипотеза Римана как чётность специальных
биномиальных коэффициентов**

Матиясевич Юрий Владимирович — доктор физико-математических наук, профессор, академик Российской академии наук, советник РАН Санкт-Петербургского отделения Математического института им. В. А. Стеклова РАН, президент Санкт-Петербургского математического общества.

e-mail: 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 Π_1^0 арифметической иерархии, имеющие вид “для любых $x_1, \dots, x_m$ имеет место $A(x_1, \dots, x_m)$ ”, 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 Π_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.

Библиография: 36 названий.

Для цитирования:

Ю. В. Матиясевич. Гипотеза Римана как чётность специальных биномиальных коэффициентов // Чебышевский сборник, 2018, т. 19, вып. 3, с. 46–60.

CHEBYSHEVSKII SBORNIK

Vol. 19. No. 3.

UDC 511.313:511.331.1:511.526

DOI 10.22405/2226-8383-2018-19-3-46-60

The Riemann hypothesis as the parity of special binomial coefficients

Matiyasevich Yuri Vladimirovich — doctor of physical and mathematical sciences, professor, full member of Russian Academy of Sciences, RAS Counselor of St. Petersburg department of Steklov Mathematical Institute of Russian Academy of Sciences, president of the St. Petersburg Mathematical society.

e-mail: yumat@pdmi.ras.ru

Abstract

The Riemann Hypothesis has many equivalent reformulations. Some of them are arithmetical, that is, they are statements about properties of integers or natural numbers. Among them the reformulations with the simplest logical structure are those from the class Π_1^0 from the arithmetical hierarchy, that is, having the form “for every $x_1, \dots, x_m$ relation $A(x_1, \dots, x_m)$ holds”, where A is decidable. As an example one can take the reformulation of the Riemann Hypothesis as the assertion that certain Diophantine equation has no solution (such particular equation can be given explicitly).

While the logical structure of this reformulation is indeed very simple, all known methods for constructing such Diophantine equation produce equations occupying several pages. On the other hand, there are known other reformulation also belonging to class Π_1^0 but having rather short wording. As examples one can mention the criteria of the validity of the Riemann Hypothesis proposed by J.-L. Nicolas, by G. Robin, and by J. Lagarias. The shortcoming of these reformulations (as compared to Diophantine equations) consists in the usage of constants and functions which are “more complicated” than integers and addition and multiplication sufficient for constructing Diophantine equations.

The paper presents a system of 9 conditions imposed on 9 variables. In order to state these conditions one needs only addition, multiplication, exponentiation (unary, with fixed base 2), congruences and remainders, inequalities, and binomial coefficient. The whole system can be written explicitly on a single sheet of paper. It is proved that the system is inconsistent if and only if the Riemann Hypothesis is true.

Keywords: the Riemann Hypothesis, binomial coefficients.

Bibliography: 36 titles.

For citation:

Yu. V. Matiyasevich, 2018, "The Riemann hypothesis as the parity of special binomial coefficients", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 46–60.

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 ограничимся 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 Π_2^0 арифметической иерархии. Этот класс может быть описан как класс формул вида

$$\forall x_1 \dots x_m \exists y_1 \dots y_n A(x_1, \dots, x_m, y_1, \dots, y_n), \quad (1)$$

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 Π_2^0 , эквивалентную гипотезе Римана.

Этот результат был усилен Г. Крайзелем [9], который дал переформулировку гипотезы Римана посредством формулы из класса Π_1^0 , состоящего из формул вида

$$\forall x_1 \dots x_m A(x_1, \dots, x_m). \quad (2)$$

Такие формулы можно охарактеризовать, как *эффективно опровергаемые*: если формула (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 каком-либо 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 (2) истина.

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-теоремой¹. Этот результат позволяет по произвольной формуле из класса Π_1^0 построить эквивалентную ей формулу из того же класса, имеющую следующий специальный вид:

$$\forall x_1 \dots x_m P(x_1, \dots, x_m) \neq 0, \quad (3)$$

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

$$R(x_1, \dots, x_m) = 0 \quad (4)$$

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

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 (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 (2) со сложнее проверяемыми, но зато коротко записываемыми отношениями A ; несколько таких примеров приведено ниже.

Многие классические результаты близки по форме к (2), но используют, например, символ O -большое, содержащий скрытый квантор существования. Такой квантор можно устранить, найдя явное значение соответствующей константы.

Для построения диофантова уравнения (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 *функции Чебышева* $\psi(n)$, которая определяется следующим образом:

$$\psi(n) = \ln(\text{LCM}(1, \dots, n)) = \ln(2) \log_2(\text{LCM}(1, \dots, n)), \quad (5)$$

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

$$\psi(n) = n + O(\sqrt{n} \ln^2(n)). \quad (6)$$

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

$$\psi_1(n) = \sum_{1 \leq m < n} \psi(m) \quad (7)$$

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

$$\left| \psi_1(m) - \frac{m^2}{2} \right| < 6m\sqrt{m}. \quad (8)$$

Позднее Л. Шёнфельд ([23], см. также [1, теорема 4.9]) нашёл явное значение константы в (6), а именно, доказал, что гипотеза Римана эквивалентна справедливости неравенства

$$|\psi(n) - n| < \frac{1}{8\pi} \sqrt{n} \ln(n)^2, \quad (9)$$

при $n \geq 74$. Как раз использование этого критерия вместо (8) позволило упростить построение многочлена (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

$$e^\gamma \log(\log(N_n)) < \frac{N_n}{\phi(N_n)}, \quad (10)$$

где $e = 2.71828\dots$, $\gamma = 0.577215\dots$ – 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 $n \geq 5040$ неравенства

$$\sigma(n) < e^\gamma n \log(\log(n)), \quad (11)$$

где $\sigma(n)$ – сумма всех делителей n . Это необходимое и достаточное условие известно также как *критерий Рамануджана–Робина*, поскольку С. Рамануджан доказал неравенство (11) для достаточно больших n в предположении гипотезы Римана.

Дж. Лагариас ([26], см. также [1, Теорема 7.18]) заменил правую часть неравенства (11) и получил ещё одно условие, необходимое и достаточное для справедливости гипотезы Римана:

$$\sigma(n) < H_n + e^{H_n} \log(H_n), \quad (12)$$

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

Условия типа (8)–(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 (4). Цель настоящей работы – предложить “компромиссную” переформулировку гипотезы Римана. Её преимущество перед диофантовым уравнением состоит в том, что все условия можно явно выписать на одной странице. Недостатком по сравнению с (4), но преимуществом по сравнению с (8)–(12), является набор используемых функций. Наряду со сложением и умножением в нашем необходимом и достаточном условии участвуют лишь возведение в степень (только унарное, с основанием 2), квадратный корень (легко устранимый), $\text{rem}(a, b)$ (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. Шюе [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. 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 :

$$a = \sum_{k=0}^m a_k p^k, \quad b = \sum_{k=0}^m b_k p^k, \quad 0 \leq a_k < p, \quad 0 \leq b_k < p, \quad k = 0, \dots, m; \quad (13)$$

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 (13). Будем говорить, что a *маскирует* b (и писать $a \succeq b$), если $a_k \geq b_k$ для $k = 0, \dots, m$. Из теоремы Куммера следует такая эквивалентность:

$$\binom{a}{b} \equiv 1 \pmod{2} \iff a \succeq b. \quad (14)$$

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

$$\binom{a}{b} \equiv \binom{a_0}{b_0} \dots \binom{a_m}{b_m} \pmod{p}. \quad (15)$$

2. Новая переформулировка гипотезы Римана

Исходным пунктом для нас будет неравенство (9), модифицированное по-разному в необходимом и достаточном условиях:

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

$$\psi(n) > n - \sqrt{n} \log_2^2(n); \quad (16)$$

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

$$\psi(n) < n - 20\sqrt{n} \log_2^2(n). \quad (17)$$

Мы будем использовать тот факт, что правая часть в необходимом условии (16) больше правой части в достаточном условии (17). Неравенство (16) при $n \geq 74$ следует из неравенства (9), а недостающие случаи $n = 2, \dots, 73$ проверяются непосредственным вычислением. Достаточность условия (17) 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*

$$2^l \leq n < 2^{l+1}, \quad (18)$$

$$2^m \leq 2q < 2^{m+1}, \quad (19)$$

$$s = \frac{B^{(n+1)} (B^{(n+1)n} - n - 1) + n}{(B^{(n+1)} - 1)^2}, \quad (20)$$

$$t = \frac{(2^m - 1) (B^{n^2} - 1)}{B^n - 1}, \quad (21)$$

$$\binom{t}{r} \equiv 1 \pmod{2}, \quad (22)$$

$$u = \text{rem}(rs, B^{n^2-n}), \quad (23)$$

$$rs - u \equiv \frac{B^{n^2-n}(B^n - 1)}{B - 1} q \pmod{B^{n^2}}, \quad (24)$$

$$p = \text{rem}(r, B^n + 1), \quad (25)$$

$$mp < nq - 15l^2 q \sqrt{n}, \quad (26)$$

в которой B обозначает 2^{l+m+1} .

(А) Если гипотеза Римана верна, то система (18)–(26) не имеет решений в положительных целых числах $l, m, n, p, q, r, s, t, u$.

(Б) Если гипотеза Римана не верна, то система (18)–(26) имеет бесконечно много таких решений.

ДОКАЗАТЕЛЬСТВО части (А) мы проведём “от противного”. Предположим, что нашлись числа l, m, n, p, q, r, s, t и u , удовлетворяющие условиям (18)–(26).

Согласно (18),

$$n > 1 \quad (27)$$

и

$$l = \lfloor \log_2(n) \rfloor. \quad (28)$$

Очевидно, что

$$1 \leq l, \quad 0 \leq \log_2(n) - l < 1. \quad (29)$$

Аналогично согласно (19)

$$m = \lfloor \log_2(q) \rfloor + 1 \quad (30)$$

и

$$0 < m - \log_2(q) \leq 1. \quad (31)$$

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

Легко проверить, что из (20) следует, что

$$s = \sum_{j=1}^n j B^{(n-j)(n+1)}. \quad (32)$$

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

Аналогично из (21) следует, что

$$t = \sum_{k=1}^n (2^m - 1) B^{(k-1)n}, \quad (33)$$

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 (14) из (22) следует, что $t \succeq r$ и, и потому число r имеет вид

$$r = \sum_{k=1}^n r_k B^{(k-1)n}, \quad (34)$$

где

$$r_k \leq 2^m - 1, \quad k = 1, \dots, n. \quad (35)$$

Пусть

$$rs = \sum_{i=0}^{2n^2} d_i B^i, \quad 0 \leq d_i < B, \quad i = 0, \dots, 2n^2. \quad (36)$$

Согласно (32) и (34)

$$rs = \sum_{j=1}^n \sum_{k=1}^n jr_k B^{(n-j)(n+1)+(k-1)n}. \quad (37)$$

Легко проверить, что при $1 \leq j \leq n$, $1 \leq k \leq n$ среди чисел вида $(n-j)(n+1) + (k-1)n$ нет двух одинаковых. Кроме того, из (18) и (34) следует, что

$$jr_k \leq n(2^m - 1) < 2^{l+1}(2^m - 1) < 2^{l+m+1} = B. \quad (38)$$

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

$$d_i = \begin{cases} jr_k, & \text{если } i = (n-j)(n+1) + (k-1)n \\ 0, & \text{в противном случае.} \end{cases} \quad (39)$$

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

$$d_{n^2-k} = kr_k, \quad k = 1, \dots, n. \quad (40)$$

Согласно (23) и (36)

$$u = \sum_{i=0}^{n^2-n-1} d_i B^i. \quad (41)$$

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

$$rs - u = \sum_{i=n^2-n}^{2n^2} d_i B^i \equiv \sum_{i=n^2-n}^{n^2-1} d_i B^i \pmod{B^{n^2}}. \quad (42)$$

Имеет место тождество

$$\sum_{i=n^2-n}^{n^2-1} q B^i = \frac{(B^n - 1) B^{n^2-n}}{B - 1} q, \quad (43)$$

благодаря которому из (24), (40) и (42) следует, что

$$kr_k = d_{n^2-k} = q, \quad k = 1, \dots, n. \quad (44)$$

Отсюда мы получаем следующие значения цифр числа r :

$$r_k = \frac{q}{k}, \quad k = 1, \dots, n. \quad (45)$$

Согласно (44) q делится на $1, \dots, n$, следовательно,

$$\text{LCM}(1, \dots, n) \leq q. \quad (46)$$

Из очевидного сравнения

$$B^n \equiv -1 \pmod{B^n + 1} \quad (47)$$

и равенства (34) следует, что

$$p \equiv \sum_{k=1}^n (-1)^{k-1} r_k \pmod{B^n + 1}. \quad (48)$$

Слагаемые в знакопеременной сумме в (48) по абсолютной величине монотонно убывают, первое слагаемое равно q , следовательно, сумма положительна и не превосходит q . Таким образом, в сравнении (48) левая и правая части не превосходят его модуля, следовательно, они равны. Соответственно,

$$\frac{p}{q} = \sum_{k=1}^n \frac{(-1)^{k-1} r_k}{q} = \sum_{k=1}^n \frac{(-1)^{k-1}}{k} \approx \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} = \ln(2) \quad (49)$$

и справедливы элементарные неравенства

$$\frac{1}{2} \leq \frac{p}{q}, \quad \left| \frac{p}{q} - \ln(2) \right| < \frac{1}{2n}. \quad (50)$$

Из (26) и (50) следует, что

$$m < \frac{n - 15l^2 p \sqrt{n}}{p/q} \leq 2n. \quad (51)$$

Далее, согласно (50), (51), (31), (5) и (27), имеем:

$$\begin{aligned} \frac{p}{q} m &> \left(\ln(2) - \frac{1}{2n} \right) m = \ln(2)m - \frac{m}{2n} > \ln(2) \log_2(q) - 1 = \\ &= \ln(q) - 1 \geq \ln(\text{LCM}(1, \dots, n)) - 1 = \\ &= \psi(n) - 1 > \psi(n) - 2\sqrt{n} \log_2^2(n). \end{aligned} \quad (52)$$

С другой стороны, согласно (26) и (29)

$$\frac{p}{q} m < n - 15l^2 \sqrt{n} < n - 3\sqrt{n} \log_2^2(n). \quad (53)$$

Три неравенства, (16), (52) и (53), дают требуемое противоречие. Часть (А) доказана.
ДОКАЗАТЕЛЬСТВО части (Б). В качестве n мы возьмём произвольное из чисел, превосходящих 1 и удовлетворяющих неравенству (17). Из доказательства части (А) видно, что значения остальных переменных почти однозначно определяются значением n .

Выберем l согласно (28), так что условие (18) будет выполнено и будут справедливы неравенства (29).

Положим

$$q = \text{LCM}(1, \dots, n), \quad (54)$$

и выберем m согласно (30), так что условие (19) будет выполнено и будут справедливы неравенства (31).

Выберем s согласно (32), так что условие (20) будет выполнено.

Определим числа r_k и r согласно (45) и (34), при этом согласно (31) будут справедливы неравенства (35) и (38). Поскольку двоичная запись числа $2^m - 1$ состоит из m единиц, из (38) следует, что

$$2^m - 1 \succeq r_k, \quad k = 1, \dots, n. \quad (55)$$

Выберем t согласно (33), так что условие (21) будет выполнено. Все ненулевые цифры числа t равны $2^m - 1$, и согласно (55) они маскируют соответствующие цифры числа r . Отсюда следует, что $t \succeq r$ и, согласно (14), условие (22) выполнено.

Точно так же, как в доказательстве части (А) мы заключаем, что в представлении (36) цифры d_i определяются равенством (39) и его частным случаем (40).

Выберем u согласно (41), тогда будут выполнены условие (23) и сравнение (42), в котором согласно (40) во второй сумме все d_i равны q . Поскольку имеет место тождество (43), то выполнено и условие (24).

Точно так же, как в доказательстве части (А) мы заключаем, что справедливы неравенства (50).

Согласно (54), (5) и (17)

$$\log_2(q) = \log_2(\text{LCM}(1, \dots, n)) = \psi(n)/\ln(2) < 2\psi(n) < 3n. \quad (56)$$

Используя, кроме того, (50), (31), (27), (17) и (29), отсюда получаем, что

$$\begin{aligned} \frac{p}{q}m &< \left(\ln(2) + \frac{1}{2n}\right)(\log_2(q) + 1) = \psi(n) + \frac{\log_2(q)}{2n} + \ln(2) + \frac{1}{2n} < \\ &< \psi(n) + 3\sqrt{n}\log_2^2(n) < n - 17\sqrt{n}\log_2^2(n) < n - 17\sqrt{nl}^2 \end{aligned} \quad (57)$$

и, следовательно, условие (26) выполнено.

Часть (Б) доказана. Теорема доказана.

ЗАМЕЧАНИЕ. Если разрешить возведение в степень произвольных чисел (а не только числа 2 как в (18)–(26)), то можно избежать использования биномиального коэффициента. А именно,

$$\binom{t}{r} \equiv 1 \pmod{2} \iff \text{rem}((2^t + 1)^t, 2^{rt+1}) > 2^{rt}. \quad (58)$$

Заменив условие (22) на правую часть в (58), 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 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 (18)–(26). Представляется интересным исследовать системы условий, получающиеся из (18)–(26) удалением одного из них или заменой его на более слабое. Например, допускают ли хорошее описание решения системы, получающейся заменой биномиального условия (22) на вытекающее из него неравенство $r \leq t$?

СПИСОК ЦИТИРОВАННОЙ 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. — P. 5–341. — (Итоги науки и техн. Сер. Современ. 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. Nayebe A. On the Riemann Hypothesis and Hilbert's Tenth Problem. — Unpublished Manuscript, 2012.
— URL: http://web.stanford.edu/~anayebe/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/zns12015>.
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.

REFERENCES

1. Broughan, K. 2017, *Equivalents of the Riemann hypothesis. Volume 1: Arithmetic equivalents.*, Cambridge University Press, Cambridge.
2. Broughan, K. 2017, *Equivalents of the Riemann hypothesis. Volume 2: Analytic equivalents.*, Cambridge University Press, Cambridge. DOI: 10.1017/9781108178266.
3. Gödel, K. 1931, “Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme. I.”, *Monatsh. Math. Phys.* vol. 38, pp 173–198. DOI: 10.1007/BF01700692.
4. Booker, A. R. 2006, “Turing and the Riemann hypothesis”, *Notices Am. Math. Soc.* vol. 53, no. 10, pp 1208–1211.
5. Booker, A. R. 2006, “Artin’s conjecture, Turing’s method, and the Riemann hypothesis”, *Exp. Math.* vol. 15, no. 4, pp 385–407. DOI: 10.1080/10586458.2006.10128976.
6. Cooper, S. B. & van Leeuwen, J. (eds) 2013, *Alan Turing – His Work and Impact*, Elsevier Science. ISBN 978-0-12-386980-7. DOI: 10.1016/C2010-0-66380-2.
7. Matiyasevich Yu. V. 2012, “Alan Turing and number theory” (in Russian), *Matematika v vysshem obrazovanii*, vol. 10, pp 111–134. Available at: http://www.unn.ru/math/no/10/_nom10_012_matiyasevich.pdf.
8. Turing, A. M. 1936, “On computable numbers, with an application to the Entscheidungsproblem”, *Proc. London Math. Soc* vol. 42, no. 2, pp 230–265.
9. Kreisel, G. 1958, “Mathematical significance of consistency proofs”, *Journal of Symbolic Logic* vol. 23, no. 2, pp 155–182.
10. Yedidia, A. & Aaronson, S. 2016, “A relatively small Turing machine whose behavior is independent of set theory”, *Complex Systems* vol. 25, pp 297–327. DOI 10.25088/ComplexSystems.25.4.297.
11. Aaronson, S. 2016, *The blog*. Available at: <https://www.scottaaronson.com/blog/?p=2741>.
12. Calude, C. S., Calude, E. & Dinneen, M. J. 2006, “A new measure of the difficulty of problems”, *J. Mult.-Val. Log. Soft Comput.* vol. 12, no. 3–4, pp 285–307.
13. Calude, E. 2012, “The complexity of Riemann’s hypothesis”, *J. Mult.-Val. Log. Soft Comput.* vol. 18, no. 3–4, pp 257–265.
14. Matiyasevich, Yu. V. 2018, “The Riemann hypothesis in computer science”, *Preprints of St.Petersburg Department of Steklov Mathematical Institute*, no. 07. DOI: 10.13140/RG.2.2.14041.83041 Available at: <http://www.pdmi.ras.ru/preprint/2018/18-07.html>.
15. Manin Yu. I. & Panchishkin A. A. 2005. *Introduction to modern number theory. Fundamental problems, ideas and theories*. Transl. from the Russian. 2nd revised ed. Springer, Berlin.

16. Matiyasevich Yu. 1993, *Hilbert's Tenth Problem*. Transl. from the Russian. MIT Press, Cambridge (Massachusetts), London.
17. Davis, M., Matijasevič Yu. & Robinson, J. 1976, "Hilbert's tenth problem: Diophantine equations: Positive aspects of a negative solution". *Proc. Symp. Pure Math.* vol. 28, 323–378.
18. Hernandez Caceres, J. M. 2018, *The Riemann Hypothesis and Diophantine equations*. Master's Thesis in Mathematics, Mathematical Institute, University of Bonn, Bonn.
19. Moroz B. Z. 2018, "The Riemann Hypothesis and Diophantine equations" (in Russian), *St. Petersburg Mathematical Society Preprints*, no. 03. Available at: <http://www.mathsoc.spb.ru/preprint/2018/index.html#03>.
20. Nayebi, A. 2012, "On the Riemann Hypothesis and Hilbert's tenth problem", unpublished manuscript. Available at: http://web.stanford.edu/~anayebi/projects/RH_Diophantine.pdf.
21. Matijasevič, Y. V. 1973, "On recursive unsolvability of Hilbert's tenth problem", *Studies in Logic and the Foundations of Mathematics* vol. 74, pp. 89–110.
22. Jones, J. P. 1982, "Universal Diophantine equation", *J. Symb. Log.* vol. 47, pp 549–571. DOI: 10.2307/2273588.
23. Schoenfeld, L. 1976, "Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II", *Math. Comput.* vol. 30, pp 337–360. DOI: 10.2307/2005976.
24. Nicolas, J.-L. 1983, "Petites valeurs de la fonction d'Euler", *J. Number Theory* vol. 17, pp 375–388. DOI: 10.1016/0022-314X(83)90055-0.
25. Robin, G. 1984, "Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann", *J. Math. Pures Appl. (9)* vol. 63, pp 187–213.
26. Lagarias, J. C. 2002, "An elementary problem equivalent to the Riemann hypothesis", *Am. Math. Mon.* vol. 109, no. 6, pp 534–543. DOI: 10.2307/2695443.
27. Mann, H. B. & Shanks, D. 1972, "A necessary and sufficient condition for primality, and its source", *J. Comb. Theory, Ser. A* vol. 13, pp 131–134. DOI: 10.1016/0097-3165(72)90016-7.
28. Hsu, L. & Shiue, P. J.-S. 1997, "On a combinatorial expression concerning Fermat's Last Theorem", *Adv. Appl. Math.* vol. 18, no. 2, pp 216–219. DOI: 10.1006/aama.1996.0510.
29. Matiyasevich Yu. V. 1981, "A class of primality criteria formulated in terms of the divisibility of binomial coefficients". Translation from Russian, *Journal of Soviet Mathematics*, vol. 16, no. 1, pp 874–885. DOI: 10.1007/BF01213897.
30. Matiyasevich, Yu. 2001, "Some arithmetical restatements of the four color conjecture", *Theor. Comput. Sci.* vol. 257, no. 1–2, pp 167–183. DOI 10.1016/S0304-3975(00)00115-8.
31. Margenstern, M. & Matiyasevich, Yu. 1999, "A binomial representation of the $3x+1$ problem", *Acta Arith.* vol. 91, no. 4, pp 367–378. DOI: 10.4064/aa-91-4-367-378.
32. Kummer, E. E. 1852, "Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen", *Journal für die Reine und Angewandte Mathematik* vol. 44, pp 93–146.
33. Singmaster, D. 1974, "Notes on binomial coefficients. I: A generalization of Lucas' congruence", *J. Lond. Math. Soc., II. Ser.* vol. 8, pp 545–548. DOI: 10.1112/jlms/s2-8.3.545.

- 34. Lucas E. 1878. “Théorie des Fonctions Numériques Simplement Périodiques”, *American Journal of Mathematics*, vol. 1, pp 184–240. Available at: <http://www.jstor.org/stable/2369311>.
- 35. Schmidt, E. 1903, “Über die Anzahl der Primzahlen unter gegebener Grenze”, *Math Annalen*, vol. 57, pp 195–203.
- 36. Ingham, A. E. 1932, *The distribution of prime numbers*, Cambridge University Press, London (Cambridge Tracts in Mathematics and Mathematical Physics, vol. 30,); reprinted in 1990.

Получено 17.07.2018

Принято к печати 10.10.2018