Санкт-Петербургский государственный университет

Дорохин Александр Игоревич

Выпускная квалификационная работа

Распределение чисел Кармайкла специального вида

Уровень образования: бакалавриат
Направление 01.03.01 «Математика»
Основная образовательная программа СВ.5000.2019 «Математика»

Научный руководитель:
член-корреспондент РАН,
профессор кафедры высшей
алгебры и теории чисел
математико-механического
факультета СПбГУ,
доктор ф.-м. наук,
Всемирнов Максим
Александрович

Рецензент:
научный сотрудник
федерального государствен-
ного бюджетного учреждения
науки ПОМИ РАН
им. В.А.Стеклова,
Пастор Алексей
Владимирович

Санкт-Петербург
2023 год

Содержание

1 Введение

1.1 История чисел Кармайкла

Понятие числа Кармайкла неразрывно связано с малой теоремой Ферма – классическим утверждением элементарной теории чисел, возраст которого составляет без малого четыре столетия. Так, в 1640 г. великий французский математик Пьер Ферма в письме своему другу Бернару Френиклю де Бесси сформулировал следующую теорему.

Теорема 1 (Малая теорема Ферма)**.** *Для простого p и целого a, не делящегося на p, $p \mid a^{p-1} - 1$.*

На протяжении почти трёх столетий оставался открытым вопрос о справедливости обратного утверждения. Первый шаг к его опровержению сделал Пьер Саррюс, доказавший в 1820 г., что $341 \mid 2^{341} - 1$, тем самым, опровергнув гипотезу для $a = 2$. В конце XIX века Алвин Корсельт в работе [1] сформулировал критерий, позволяющий установить, верна ли теорема Ферма для числа n, не обязательно являющегося простым.

Теорема 2 (критерий Корсельта [1])**.** *Если бесквадратное число n таково, что для любого его простого делителя p выполнено $p - 1 \mid n - 1$, то*

$$n \mid a^{n-1} - 1 \text{ для любого целого } a, \text{ взаимно простого с } n. \tag{1}$$

Кроме того, верно и обратное: если верно (1), то число n свободно от квадратов и для любого простого делителя p числа n выполнено $p - 1 \mid n - 1$.

К сожалению, Корсельту не удалось привести пример такого числа n. Первым, кто смог справиться с этой задачей, стал Роберт Кармайкл, указавший пример в статье [2]. Поэтому составные числа, для которых справедливо утвержение малой теоремы Ферма, называются числами Кармайкла.

Определение. Числом Кармайкла называется составное число n, такое, что для любого целого a, взаимно простого с n, $n \mid a^{n-1} - 1$.

В тот раз Кармайкл ограничился рассмотрением чисел вида $n = p_1 p_2 p_3$, где p_1, p_2, p_3 – простые числа. Он привёл четыре примера: 561, 1105, 2821 и 15841.

Теорема 3. *Если (561, a)=1, то* $561 \mid a^{560} - 1$. *Аналогичное утверждение верно для чисел 1105, 2821 и 15841.*

Двумя годами позднее в своей статье [3] он высказал гипотезу, что «этот список (чисел Кармайкла) может быть расширен бесконечно». И действительно, в 1994 году в статье [4] было показано, что существует бесконечно много чисел Кармайкла.

1.2 Существующие результаты

К новейшим результатам в этой области можно отнести работу [5], в которой получено, что при фиксированном нечётном k существует лишь конечное количество чисел Кармайкла вида $k \cdot 2^n + 1$, $n \in \mathbb{N}$. Более того, приведена явная оценка на $n(k)$, а именно, получен следующий результат.

Теорема 4. *Пусть n достаточно велико, а именно,*

$$n > n(k) = 2^{2 \cdot 10^7 \tau^2(k) \ln^2(k) \omega^2(k)},$$

где $\tau(k)$ - число делителей числа k, а $\omega(k)$ - число различных простых делителей числа k. Тогда $N = k \cdot 2^n + 1$ – не число Кармайкла.

Вместе с тем много задач, свзанных с числами Кармайкла, остаётся открытыми. В [4] установлена оценка

$$C(x) > x^{2/7},\ x \in \mathbb{R}$$

где $C(x)$ - количество чисел Кармайкла от 1 до x. Позднее показатель был усилен до $1/3$. Пал Эрдёш предположил, что

$$C(x) = x^{1-o(1)},$$

используя эвристические аргументы. В дальнейшем эти эвристические аргументы были уточнены Карлом Померансом в [6], а именно, он предположил, что

$$C(x) = x \cdot L(x)^{-1+o(1)},$$

где

$$L(x) = \exp\left(\frac{\log x \cdot \log\log\log x}{\log\log x}\right)$$

но строгого доказательства ни одному из них получить не удалось.
Также существуют и условные результаты о числах Кармайкла. Сформулируем одну важнейшую гипотезу.

Гипотеза 1 (Гипотеза Диксона)**.** *Пусть $\{a_i\}_{i=1}^k, \{b_i\}_{i=1}^k$, – целые числа, причём $a_i \neq 0$ для любого $i, 1 \leqslant i \leqslant k$. Предположим, что не существует простого p, такого, что $p \mid \prod\limits_{i=1}^{k}(a_i n + b_i)$ для любого целого n. Тогда найдётся бесконечно много n, таких, что для любого $i, 1 \leqslant i \leqslant k$, число $a_i n + b_i$ – простое.*

В случае её истинности справедлива (см. также [7]) следующая теорема.

Теорема 5. *Для любого $n \geqslant 3$ существует такой многочлен $P(x)$ степени n, что среди его значений в целых точках найдётся бесконечно много чисел Кармайкла. Более того, такое число Кармайкла будет иметь ровно n простых делителей.*

Доказательство (в предположении гипотезы Диксона). Положим

$$P(x) = (6x+1)(12x+1)(18x+1)(36x+1)...(9 \cdot 2^{n-2}x+1),$$

и применим гипотезу Диксона для $a_1 = 6$, $a_2 = 12$, $a_3 = 18$, ..., $a_n = 9 \cdot 2^{n-2}$ и $b_i = 1$ для $1 \leqslant i \leqslant n$. Получим бесконечно много m_i, таких, что числа $6m_i + 1$, $12m_i + 1$, $18m_i + 1$, ..., $9 \cdot 2^{n-2}m_i + 1$ одновременно являются простыми. Очевидно, требование гипотезы выполнено, и поэтому все одночлены, участвующие в произведении, будут иметь простые значения. Также легко заметить, что $9 \cdot 2^{n-2}x \mid P(x) - 1$ в кольце многочленов с целыми коэффициентами $\mathbb{Z}[x]$, а поэтому критерий Корсельта выполнен. Значит, полученное число $P(m_i)$ действительно является числом Кармайкла с n простыми делителями, как и требовалось. □

1.3 Результаты, полученные в этой работе

Данная работа посвящена исследованию множества $\mathbb{K}$, которое определяется как

$$\mathbb{K} = \{k : \text{существует } n, \text{ такое, что } N = 2^n k + 1 - \text{число Кармайкла}\}.$$

В [8] показано, что $\mathbb{K}$ имеет нулевую асимптотическую плотность, то есть,

$$\lim_{n\to\infty} \frac{\mathbb{K} \cap [1; n]}{n} = 0.$$

В то же время, определить принадлежность заданного составного числа k множеству $\mathbb{K}$ практически невозможно, за исключением тех случаев, когда число Кармайкла $N = 2^n k + 1$ найдено явно. В [5] показано, что 9, 15, 21 и 25 не принадлежат $\mathbb{K}$.
В этой работе построена армфметическая прогрессия, члены которой, являющиеся утроенными простыми числами, не являются элементами $\mathbb{K}$. Прогрессия построена таким образом, что она содержит бесконечно много подходящих чисел, поэтому главный результат работы позволяет явно привести пример сколь угодно большого числа k, не входящее в $\mathbb{K}$.

1.4 Значение полученных результатов

Как следует из определения, числа Кармайкла – суть контрпример к утверждению, обратному теореме Ферма. Поэтому вероятностный тест простоты Ферма, основанный на проверке гипотезы, что $a^{n-1} \equiv 1 \pmod{n}$ для некоторого числа a, не сможет определить, является ли число n простым. Но если удастся доказать, что некоторый класс чисел не содержит ни одного числа Кармайкла, то для этого класса справедлива обратная теорема Ферма, что позволяет применять тест Ферма без каких-либо дополнительных проверок на соответствие числа критерию Корсельта. Тест Ферма может быть значительно эффективнее, чем любые другие, за счёт возможности возведения в степень $n - 1$ по модулю n за $O(\log n)$ вычислений по модулю n. В данной работе сформулировано достаточное условие, которому должно удовлетворять натуральное число k, чтобы среди чисел $k \cdot 2^n + 1$,

$n \in \mathbb{N}$ не нашлось ни одного числа Кармайкла. Кроме того, показано, что существует бесконечно много таких составных k, что расширяет результат, полученный в [9], согласно которому в предположении истинности гипотезы о том, что максимальное простое число Ферма – это 65537, не существует чисел Кармайкла вида $p \cdot 2^n + 1$, $n \in \mathbb{N}$, где $p > 127$ – простое число.

1.5 Обозначения

Все значения переменных, если не оговорено иное – неотрицательные целые числа. В работе приняты следующие обозначения:

(a, b) – наибольший общий делитель чисел a и b;
p или p_i – простое число, $\mathbb{P}$ – множество простых чисел;
$\left(\frac{a}{p}\right)$ – символ Лежандра, равный 1, если сравнение $a \equiv x^2 \pmod{p}$ разрешимо и $p \nmid a$, равный -1, если это сравнение неразрешимо, и 0, если $p \mid a$;
$\nu_p(m)$ – степень вхождения p в m, то есть, такое число l, что $p^l \mid m$, но $p^{l+1} \nmid m$;
$\mathrm{ord}_p(b)$ - показатель числа b по модулю p, то есть такое число l, что $b^l \equiv 1 \pmod{p}$, но $b^k \not\equiv 1 \pmod{p}$ для $1 \leqslant k \leqslant l - 1$.

2 Главный результат

В этом разделе будет предъявлена требуемая арифметическая прогрессия. Идея доказательства её существования основана на следующем наблюдении.

Лемма 1. *Для любых чисел $a_1, \ldots, a_n$ и $b_1, \ldots, b_n$, таких, что $(a_1, \ldots, a_n) = 1$ и $(a_i, b_i) = 1$ для любого i, $1 \leqslant i \leqslant n$, найдётся бесконечно много простых чисел p, для которых верно сравнение $p \equiv b_i \pmod{a_i}$ для всех i, $1 \leqslant i \leqslant n$.*

Доказательство. Немедленно следует из теоремы Дирихле о простых числах и китайской теоремы об остатках. □

Теперь мы сформулируем главный результат работы.

Теорема 6. *Существует бесконечно много нечётных составных k вида $k = 3q$, где $q = A + mB$ - простое число, для которых в множестве $\{k \cdot 2^n + 1, n > 0\}$ не найдётся ни одного числа Кармайкла. Более того, числа A и B могут быть явно вычислены, что даёт возможность эффективной проверки заданного числа k на соответствие критерию.*

Напомним классический результат элементарной теории чисел, впервые доказанный Карлом Фридрихом Гауссом.

Теорема 7 (Квадратичный закон взаимности, без доказательства)**.** *Если p, r - различные простые числа, то $\left(\frac{p}{r}\right) \cdot \left(\frac{r}{p}\right) = (-1)^{\frac{(p-1)(r-1)}{4}}$. В частности, если $p \equiv 1 \pmod 8$, а $r = 3$, то $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(3-1)(r-1)}{4}} = 1$.*

Лемма 2. *Пусть число $N = 3q \cdot 2^n + 1$ является числом Кармайкла, причём $(6, q) = 1$. Тогда N не имеет простых делителей вида $p = q \cdot 2^b + 1$, $b \geqslant 3$.*

Доказательство. Пусть $p = q \cdot 2^b + 1$, $N = 3q \cdot 2^n + 1$ и $p \mid N$. Так как $p \equiv 1 \pmod 8$, то $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1$. По свойству символа Лежандра

$$1 = \left(\frac{-1}{p}\right) = \left(\frac{2^b \cdot q}{p}\right) = \left(\frac{2^b}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right),$$

а также

$$1 = \left(\frac{-1}{p}\right) = \left(\frac{2^n \cdot 3q}{p}\right) = \left(\frac{2^n}{p}\right)\left(\frac{3}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{3}{p}\right).$$

В силу квадратичного закона взаимности, а также того, что $p \equiv 1 \pmod 8$, $\left(\frac{p}{3}\right) = 1$. Значит, $p \equiv 1 \pmod 3$, то есть, $2^b \cdot q \equiv 0 \pmod 3$, что невозможно, так как $(6, q) = 1$. Лемма доказана. □

Лемма 3. *Пусть натуральное число N представимо в виде $N = d_1 d_2 d_3$, причём*

$$\nu_2(d_1 - 1) = a, \nu_2(d_3 - 1) \geqslant a + 1, \nu_2(N - 1) \geqslant a + 1$$

для некоторого $a \geqslant 1$. Тогда $\nu_2(d_2 - 1) = a$.

Доказательство. Очевидно. □

Лемма 4. *Пусть* $s \geqslant 3$, $q \equiv 3 \pmod 8$, $N \equiv 1 \pmod{2^{s+3}}$, N *свободно от квадратов и представимо в виде* $N = d_1 d_2 d_3$, *где*

$$d_1 = d_{11} d_{12},$$

$$d_2 = d_{21} d_{22} d_{23} d_{24}.$$

Причём

$$d_{11} \equiv 3 \cdot 2^s + 1 \pmod{2^{s+3}}$$
$$d_{12} \equiv 3q \cdot 2^s + 1 \pmod{2^{s+3}}$$
$$d_{21} \equiv M_{s+1,3} \cdot 2^{s+1} + 1 \pmod{2^{s+3}},\ M_{s+1,3} \in \{0, 3\}$$
$$d_{22} \equiv M_{s+2,3} \cdot 2^{s+2} + 1 \pmod{2^{s+3}},\ M_{s+2,3} \in \{0, 3\}$$
$$d_{23} \equiv M_{s+1,3q} \cdot 2^{s+1} + 1 \pmod{2^{s+3}},\ M_{s+1,3q} \in \{0, 3q\}$$
$$d_{24} \equiv M_{s+2,3q} \cdot 2^{s+2} + 1 \pmod{2^{s+3}},\ M_{s+2,3q} \in \{0, 3q\}$$
$$d_3 \equiv 1 \pmod{2^{s+3}}$$

Тогда одно из чисел $M_{s+2,3}$ *и* $M_{s+2,3q}$ *не равно нулю.*

Доказательство. Заметим, что так как $q \equiv 3 \pmod 8$, то

$$d_{12} \equiv 3q \cdot 2^s + 1 \equiv 2^s + 1 \pmod{2^{s+3}}.$$

Так как $s \geqslant 3$, то $2^{2s} \equiv 0 \pmod{2^{s+3}}$. Применим предыдущую лемму с $a = s + 2$: действительно, нетрудно заметить, что $\nu_2(d_1 - 1) = s + 2$, $\nu_2(d_3 - 1) \geqslant s + 3$, $\nu_2(N - 1) \geqslant s + 3$. Значит, $\nu_2(d_2 - 1) = s + 2$. Прямое раскрытие скобок показывает, что

$$d_2 \equiv M_{s+1,3} \cdot 2^{s+1} + M_{s+2,3} \cdot 2^{s+2} + M_{s+1,3q} \cdot 2^{s+1} + M_{s+2,3q} \cdot 2^{s+2} + 1 \pmod{2^{s+3}},$$

но $\nu_2(d_2 - 1) = s + 2$ влечёт

$$d_2 \equiv 2^{s+2} + 1 \pmod{2^{s+3}},$$

или же

$$M_{s+1,3} + M_{s+2,3} \cdot 2 + M_{s+1,3q} + M_{s+2,3q} \cdot 2 \equiv 2 \pmod 4,$$

из чего очевидным образом следует утверждение леммы. □

Пусть n – наперёд заданное число. Если предположить, что число Кармайкла $N = 3q \cdot 2^n + 1$ не имеет простых делителей вида $3q \cdot 2^b + 1$ для $b \leqslant n$, а также $2q + 1$ и $4q + 1$, то в силу критерия Корсельта оно сможет иметь лишь конечное число простых делителей вида $1 \cdot 2^b + 1$ и $3 \cdot 2^b + 1$ для $b \leqslant n$, а поэтому само будет ограничено. Значит, при достаточно больших значениях q число N обязательно должно иметь простой делитель вида $2q+1$, $4q+1$ или $3q \cdot 2^b + 1$, где $b \leqslant n$. Но если все вышеперечисленные числа окажутся составными, q не сможет принимать достаточно большие значения. Формализуем это. Для удобства введём следующее обозначение.

Определение.

$$f(c) = \frac{1}{6} \prod_{\substack{1 \leqslant i \leqslant c-1 \\ 1 \cdot 2^i + 1 \in \mathbb{P}}} (1 \cdot 2^i + 1) \prod_{\substack{1 \leqslant i \leqslant c-1 \\ 3 \cdot 2^i + 1 \in \mathbb{P}}} (3 \cdot 2^i + 1)$$

Лемма 5. *Пусть простое число $q > 3$ и натуральные числа n, c таковы, что*

1. *$q > f(c)$;*
2. *Числа $\{3q \cdot 2^b + 1, 1 \leqslant b \leqslant c-1\}$, а также $2q+1$ и $4q+1$ являются составными;*
3. *Число $N = 3q \cdot 2^n + 1$ является числом Кармайкла.*

Тогда $n \geqslant c$.

Доказательство. Пусть $n \leqslant c-1$. Согласно лемме 2 и предположению 2, число N не может иметь простых делителей вида $q \cdot 2^b + 1$. Запишем N в виде

$$N = \prod_{1 \leqslant i \leqslant s} (1 \cdot 2^{a_i} + 1) \prod_{1 \leqslant i \leqslant t} (3 \cdot 2^{b_i} + 1) \prod_{1 \leqslant i \leqslant u} (3q \cdot 2^{c_i} + 1),$$

где $a_1 < \ldots < a_s$, $b_1 < \ldots < b_t$ и $c_1 < \ldots < c_u$. Если $s = 0$, $t = 0$ или $u = 0$, положим $a_1 = \infty$, $b_1 = \infty$ или $c_1 = \infty$ соответственно.
Если какое-то из a_i, b_i или c_i конечно и не меньше c, то по критерию Корсельта $1 \cdot 2^{a_i} \mid 3q \cdot 2^n$, $3 \cdot 2^{b_i} \mid 3q \cdot 2^n$ или $3q \cdot 2^{c_i} \mid 3q \cdot 2^n$, что невозможно. Если бы оказалось, что $c_1 < c$, то число $3q \cdot 2^{c_1} + 1$ было бы простым, что противоречит предположению 2.
Итак, среди делителей числа N найдутся только простые числа вида $1 \cdot 2^{a_i} + 1$ и $3 \cdot 2^{b_j} + 1$ с $1 \leqslant a_i, b_i \leqslant c-1$, причём N - бесквадратное, поэтому каждое из этих простых чисел встретится в факторизации N не более одного раза. Значит,

$$N \leqslant \prod_{\substack{1 \leqslant i \leqslant c-1 \\ 1 \cdot 2^i + 1 \in \mathbb{P}}} (1 \cdot 2^i + 1) \prod_{\substack{1 \leqslant i \leqslant c-1 \\ 3 \cdot 2^i + 1 \in \mathbb{P}}} (3 \cdot 2^i + 1) = 6f(c),$$

что конечно. Осталось заметить, что $N = 3q \cdot 2^n + 1 \geqslant 3q \cdot 2 + 1 > 6f(c)$, что противоречит вышесказанному. □

Лемма 6. *Пусть $n \geqslant c$, $N = k \cdot 2^n + 1$ - число Кармайкла, $d_1, d_2 \mid k$, $a = \min\limits_{p \mid N} \nu_2(p-1)$ и для всех $b, 1 \leqslant b \leqslant c-1$, выполнено одно из условий:*

1. *Среди чисел $d \cdot 2^b + 1$ (для фиксированного b и всевозможных $d \mid k$) не найдётся двух простых;*
2. *Ни для какой пары простых чисел $p_1 = d_1 \cdot 2^b + 1$ и $p_2 = d_2 \cdot 2^b + 1$ не найдётся m, такого, что $p_1 p_2 \mid k \cdot 2^m + 1$.*

Тогда $a \geqslant c$.

Доказательство. Предположим, что $a \leqslant c-1$ и применим одно из предположений для $b=a$. Получим, что если у числа N и найдётся простой делитель вида $p_1 = d_1 \cdot 2^a + 1$, то лишь один. В силу того, что $n \geqslant c \geqslant a+1$, $N \equiv 1 \pmod{2^{a+1}}$, в то время как

$$(d_1 \cdot 2^a + 1) \prod_{\substack{a+1 \leqslant i \leqslant n \\ d \mid k \\ d \cdot 2^i + 1 \mid N \\ d \cdot 2^i + 1 \in \mathbb{P}}} (d \cdot 2^i + 1) \equiv 2^a + 1 \pmod{2^{a+1}}$$

Значит, $a \geqslant c$. □

Для того, чтобы избавиться от необходимости разбирать лишние случаи, выберем q с определённым остатком при делении на определённое число.

Лемма 7. *Если* $q \equiv 13227 \pmod{1042245396920}$, *то* $3, 17, 21, 65, 257, 65537 \nmid 3q \cdot 2^n + 1$ *для любого* n.

Доказательство. Так как $17, 257, 65537 \mid 2^{32} - 1 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$, а также $3, 21, 65 \mid 2^{12} - 1 = 3^2 \cdot 5 \cdot 7 \cdot 13$, то достаточно проверить требуемое утверждение для $0 \leqslant n \leqslant 31$. Понятно, что $3 \nmid 3q \cdot 2^n + 1$ для любого n. Так как $17, 21, 65, 257, 65537 \mid 1042245396920 = 2^3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 257 \cdot 65537$, то достаточно убедиться, что $17, 21, 65, 257, 65537 \nmid 3 \cdot 13227 \cdot 2^n + 1$ для любого n, $0 \leqslant n \leqslant 31$. Это несложно сделать с помощью компьютерной программы. □

Итак, при указанном в предыдущей лемме условии ни одно из известных простых чисел Ферма не делит $3q \cdot 2^n + 1$.
Сначала рассмотрим случай, когда ни одно из простых чисел Ферма, больших 65537, не делит N. Заметим, что здесь, а также в следующей лемме, не используется гипотеза о том, что таких чисел не существует.

Лемма 8. *Пусть* $N = 3q \cdot 2^n + 1$, $q \equiv 13227 \pmod{1042245396920}$ - *простое число,* $2q+1$, $4q+1$, $6q+1$, $12q+1$ - *составные числа,* $a = \min\limits_{p \mid N} \nu_2(p-1)$, *ни одно из чисел* $2^a+1, 2^{a+1}+1, 2^{a+2}+1$ *не является простым делителем* N, *отличным от 5 (в частности, последнее условие выполнено, если* N *не имеет простых делителей вида* $2^{2^l}+1, l \geqslant 5$*). Тогда* N *не является числом Кармайкла.*

Доказательство. Предположим противное, что N - число Кармайкла, имеющее вид

$$N = \prod_{1 \leqslant i \leqslant s} (\delta_i \cdot 2^{a_i} + 1),\ \delta_i \in \{1, 3, q, 3q\}$$

Сначала проверим, что N не имеет делителей из множества {3, 17, 257, 65537} – это доказано в лемме 7. Также заметим, что найдутся хотя бы два индекса i таких, что $a_i = a$. Действительно, если бы нашёлся только один, N было бы представимо в виде

$$N = 3q \cdot 2^n + 1 = (\delta_1 \cdot 2^a + 1) \prod_{\substack{2 \leqslant i \leqslant s \\ a_i \geqslant a+1}} (\delta_i \cdot 2^{a_i} + 1), \delta_i \in \{1, 3, q, 3q\},$$

причём N имеет хотя бы три простых делителя и согласно критерию Корсельта $n \geqslant a+1$. Применим лемму 3 с

$$d_1 = \delta_1 \cdot 2^a + 1,$$

$$d_2 = 1,$$

$$d_3 = \prod_{\substack{2 \leqslant i \leqslant s \\ a_i \geqslant a+1}} (\delta_i \cdot 2^{a_i} + 1), \delta_i \in \{1, 3, q, 3q\}.$$

Тогда $\nu_2(d_1 - 1) = a, \nu_2(d_3 - 1) \geqslant a + 1, \nu_2(N - 1) \geqslant a + 1$, а значит, $\nu_2(1 - 1) = a$, что невозможно. Значит, действительно найдутся хотя бы два индекса i таких, что $a_i = a$.
Так как $q \geqslant 13227 > 1365 = 6f(3)$, а $6q + 1$ и $12q + 1$ являются составными, мы можем применить лемму 5 с $c = 3$, поэтому $n \geqslant 3$.
Теперь применим лемму 6 для $k = 3q$ и $c = 3$. Для этого убедимся, что необходимые условия выполнены.
Согласно лемме 2 и предположению текущей леммы, число вида $q \cdot 2^b + 1$ не может быть простым делителем N ни при каком b. Убедимся, что для каждой тройки чисел $(3, 7, 6q + 1), (5, 13, 12q + 1)$ выполнено второе предположение леммы 6. Заметим, что $6q+1$ и $12q+1$ не являются простыми числами по предположению текущей леммы. По лемме 7, для любого n верно, что $21, 65 \nmid 3q \cdot 2^n + 1$. Поэтому лемма 6 выполнена и $n, a \geqslant 3$, в частности, $5 \nmid N$.
Кроме того, так как $2^a + 1$ не является простым делителем N, то $p_1 = 3 \cdot 2^a + 1$ и $p_2 = 3q \cdot 2^a + 1$ делят N. Для удобства рассуждений среди простых делителей N вида $\delta_i \cdot 2^{a_i} + 1$ выделим такие, что $a \leqslant a_i \leqslant a + 2$. В силу того, что $p_1 p_2 \equiv 2^{a+2} + 1 \pmod{2^{a+3}}$, а числа $2^{a+1} + 1, 2^{a+2} + 1$ тоже не являются простыми делителями N, имеем $N = d_1 d_2 d_3$, где $d_1 = d_{11} d_{12}$, $d_2 = d_{21} d_{22} d_{23} d_{24}$, причём

$$d_{11} = p_1 = 3 \cdot 2^a + 1,$$

$$d_{12} = p_2 = 3q \cdot 2^a + 1,$$

$$d_{21} = M_{a+1,3} \cdot 2^{a+1} + 1, \ M_{a+1,3} \in \{0, 3\},$$

$$d_{22} = M_{a+2,3} \cdot 2^{a+2} + 1, \ M_{a+2,3} \in \{0, 3\},$$

$$d_{23} = M_{a+1,3q} \cdot 2^{a+1} + 1, \ M_{a+1,3q} \in \{0, 3q\},$$

$$d_{24} = M_{a+2,3q} \cdot 2^{a+2} + 1, \ M_{a+2,3q} \in \{0, 3q\},$$

$$d_3 = \prod_{\substack{1 \leqslant i \leqslant s \\ a_i \geqslant a+3 \\ \delta_i \in \{1,3,q,3q\}}} (\delta_i \cdot 2^{a_i} + 1),$$

причём

$$d_{11} \equiv 3 \cdot 2^a + 1 \pmod{2^{a+3}}$$

$$d_{12} \equiv 3q \cdot 2^a + 1 \equiv 2^a + 1 \pmod{2^{a+3}}$$

$$d_{21} \equiv M_{a+1,3} \cdot 2^{a+1} + 1 \pmod{2^{a+3}}, \ M_{a+1,3} \in \{0, 3\}$$

$$d_{22} \equiv M_{a+2,3} \cdot 2^{a+2} + 1 \pmod{2^{a+3}},\ M_{a+2,3} \in \{0, 3\}$$
$$d_{23} \equiv M_{a+1,3q} \cdot 2^{a+1} + 1 \pmod{2^{a+3}},\ M_{a+1,3q} \in \{0, 3q\}$$
$$d_{24} \equiv M_{a+2,3q} \cdot 2^{a+2} + 1 \pmod{2^{a+3}},\ M_{a+2,3q} \in \{0, 3q\}$$
$$d_3 \equiv 1 \pmod{2^{a+3}},$$

как в лемме 4. Значит, одно из чисел $p_3 = 3 \cdot 2^{a+2} + 1$ и $p_4 = 3q \cdot 2^{a+2} + 1$ – простой делитель N. Покажем, что такого не может произойти – разберём два случая.

1. $p_1, p_2, p_3 \mid N$. Покажем, что хотя бы одно из этих чисел делится на 5, 7 или 13. Отсюда будет следовать, что они не могут быть простыми, потому что $p_1, p_2, p_3 \geqslant 3 \cdot 2^3 + 1 = 25$. В таблице 1 указано, какой делитель имеет одно из этих чисел в зависимости от остатка a при делении на 12.

2. $p_1, p_2, p_4 \mid N$. Аналогично случаю (1) – см. таблицу 2.

□

Таблица 1: случай 1

$a \pmod{12}$	p_i	$r \in \{5,7,13\}, r \mid p_i$
0	$p_3 = 3 \cdot 2^{a+2} + 1$	13
1	$p_1 = 3 \cdot 2^a + 1$	7
2	$p_1 = 3 \cdot 2^a + 1$	13
3	$p_1 = 3 \cdot 2^a + 1$	5
4	$p_1 = 3 \cdot 2^a + 1$	7
5	$p_2 = 3q \cdot 2^a + 1$	7
6	$p_2 = 3q \cdot 2^a + 1$	5
7	$p_1 = 3 \cdot 2^a + 1$	7
8	$p_2 = 3q \cdot 2^a + 1$	7
9	$p_2 = 3q \cdot 2^a + 1$	13
10	$p_1 = 3 \cdot 2^a + 1$	7
11	$p_1 = 3 \cdot 2^a + 1$	5

Таблица 2: случай 2

$a \pmod{12}$	p_i	$r \in \{5,7,13\}, r \mid p_i$
0	$p_4 = 3q \cdot 2^{a+2} + 1$	5
1	$p_1 = 3 \cdot 2^a + 1$	7
2	$p_1 = 3 \cdot 2^a + 1$	13
3	$p_1 = 3 \cdot 2^a + 1$	5
4	$p_1 = 3 \cdot 2^a + 1$	7
5	$p_2 = 3q \cdot 2^a + 1$	7
6	$p_2 = 3q \cdot 2^a + 1$	5
7	$p_1 = 3 \cdot 2^a + 1$	7
8	$p_2 = 3q \cdot 2^a + 1$	7
9	$p_2 = 3q \cdot 2^a + 1$	13
10	$p_1 = 3 \cdot 2^a + 1$	7
11	$p_1 = 3 \cdot 2^a + 1$	5

Теперь мы можем перейти к рассмотрению случая, когда N имеет простой делитель вида $2^{2^l}+1$ для $l \geqslant 5$. Известно [10], что числа вида $2^{2^l}+1$ являются составными при $5 \leqslant l \leqslant 32$.

Лемма 9. *Пусть $q > f(7)$, $q \equiv 13227 \pmod{1042245396920}$ – простое число, n – натуральное число, $2q+1$ и $4q+1$ – составные числа, $N = 3q \cdot 2^n + 1$ делится на простое $P_l = 2^{2^l}+1, l > 32$ и ни одно из чисел $2^{2^t}+1, 2 \leqslant t < l$, не является простым делителем N. Кроме того, пусть для некоторого s, $6 \leqslant s < l$ верно следующее: для каждого $b \in [0;6] \cup [2^s-2; 2^s-1]$ выполнено $1 < (3q \cdot 2^b + 1, \frac{2^{2^s}-1}{2^{2^5}-1}) < 3q \cdot 2^b + 1$.*
Тогда N не является числом Кармайкла.

Доказательство. Предположим противное. Заметим, что мы можем применить лемму 5 с $c = 7$, поэтому $n \geqslant 7$. Пусть, как и прежде, $a = \min\limits_{p|N} \nu_2(p-1)$ и пусть для некоторого $\delta_a \mid 3q$ число $p_a = \delta_a \cdot 2^a + 1$ – простой делитель N, на котором достигается минимум. Рассмотрим три случая.

1. $p_a = q \cdot 2^a + 1$. Тогда в силу леммы 2, $a \in \{1, 2\}$, что невозможно в силу предположения.

2. $p_a = 3q \cdot 2^a + 1$. Пусть $a \equiv b \pmod{2^s}$, причём $b \in [0; 2^s - 1]$. Рассмотрим два случая.

   (a) $b \in [0;6] \cup [2^s-2; 2^s-1]$. Тогда

   $$p_a = 3q \cdot 2^a + 1 \equiv 3q \cdot 2^b + 1 \pmod{2^{2^s}-1},$$

   значит,

   $$p_a = 3q \cdot 2^a + 1 \equiv 3q \cdot 2^b + 1 \pmod{\frac{2^{2^s}-1}{2^{2^5}-1}},$$

   причём в силу того, что $1 < (3q \cdot 2^b + 1, \frac{2^{2^s}-1}{2^{2^5}-1}) < 3q \cdot 2^b + 1 \leqslant p_a$, число p_a является составным.

   (b) $b \in [7; 2^s - 3]$. В частности, $a \geqslant 7$ и ни одно из чисел $a, a+1, a+2$ не является степенью двойки с показателем больше l. По лемме 7 сравнение $q \equiv 13227 \pmod{1042245396920}$ влечёт, что $257, 65537 \nmid 3q \cdot 2^n + 1$ для любого n. Из всего этого следует, что ни одно из чисел $1 \cdot 2^a + 1, 1 \cdot 2^{a+1} + 1, 1 \cdot 2^{a+2} + 1$ не является простым делителем N.
   Пусть, как и раньше, $p_1 = 3 \cdot 2^a + 1$, $p_2 = 3q \cdot 2^a + 1$, $p_3 = 3 \cdot 2^{a+2} + 1$ и $p_4 = 3q \cdot 2^{a+2} + 1$. Тогда аналогично лемме 8 или $p_1, p_2, p_3 \mid N$, или $p_1, p_2, p_4 \mid N$. Теми же рассуждениями, что в лемме 8, получаем, что ни одна тройка (p_1, p_2, p_3), (p_1, p_2, p_4) не может состоять из трёх простых чисел, что завершает разбор этого случая.

3. $p_a = 1 \cdot 2^a + 1$. Сначала, как и в лемме 8, убедимся, что $5 \nmid N$. Так как $2^l > 2^{32} > 3$, $n \geqslant 3$ по критерию Корсельта. Согласно лемме 2 и предположению текущей леммы, число вида $q \cdot 2^b + 1$ не может быть простым делителем N ни при каком

b. Убедимся, что для каждой тройки чисел $(3, 7, 6q+1), (5, 13, 12q+1)$ выполнено второе предположение леммы 6. Заметим, что $6q+1$ и $12q+1$ не являются простыми числами по предположению текущей леммы. По лемме 7, для любого n верно, что $21, 65 \nmid 3q \cdot 2^n + 1$. Поэтому лемма 6 выполнена и $n, a \geqslant 3$, в частности, $5 \nmid N$. Кроме того, по лемме 7 верно, что $3, 17, 257, 65537 \nmid N$. Это значит, что $a = 2^l, l > 32$ – то же самое, что и в условии леммы. В частности, $a \equiv 0 \pmod{2^s}$. В силу критерия Корсельта $n \geqslant a$.
Пусть $n \leqslant a + 6$. Как и в пункте 2.(a), заметим, что при $0 \leqslant b \leqslant 6$

$$3q \cdot 2^{a+b} + 1 \equiv 3q \cdot 2^b + 1 \pmod{\frac{2^{2^s}-1}{2^{2^5}-1}},$$

то есть, N делится на $d = (3q \cdot 2^b + 1, \frac{2^{2^s}-1}{2^{2^5}-1})$. Но согласно предположениям $1 < d < 2^{2^s} < 2^a$, что противоречит выбору a. Значит, $n \geqslant a + 7$. Более того, мы доказали, что среди чисел $3q \cdot 2^{a+b} + 1$ для $0 \leqslant b \leqslant 6$ нет простых. Значит, $p_2 = 3 \cdot 2^a + 1$ - делитель N и $p_1 p_2 = 3 \cdot 2^{2a} + 2^{a+2} + 1$ - тоже. Заметим также, что $a \not\equiv 1 \pmod 3$, так как иначе $7 \mid p_2$. Так как среди чисел вида $1 \cdot 2^{a+b} + 1$ для $1 \leqslant b < a$, очевидно, простых не найдётся, по лемме 3 $p_3 = 3 \cdot 2^{a+2} + 1$ - тоже делитель N. Из этого следует, что $p_1 p_2 p_3 = (2M_1 + 1) \cdot 2^{a+4} + 1$ – тоже делитель N, а значит, и $p_4 = 3 \cdot 2^{a+4} + 1$. Наконец, $p_1 p_2 p_3 p_4 = (2M_2 + 1) \cdot 2^{a+6} + 1$ - делитель N и $p_5 = 3 \cdot 2^{a+6} + 1$. Но так как $a \equiv 0 \pmod 4$, $a \not\equiv 1 \pmod 3$ и $a \not\equiv 0 \pmod{12}$, $a \equiv 8 \pmod{12}$, а это значит, что $13 \mid 3 \cdot 2^{a+6} + 1$ и p_5 не простое. Значит, этот случай также невозможен, что завершает доказательство леммы.

□

Для доказательства теоремы осталось лишь указать бесконечно много пар $(q; s)$, удовлетворяющих нижеперечисленным условиям.

Лемма 10. *Пусть числа q и $s \geqslant 6$ таковы, что:*

1. *q - простое;*
2. *$q > f(7)$;*
3. *$q \equiv 13227 \pmod{1042245396920}$;*
4. *Для каждого $b \in [0; 6] \cup [2^s - 2; 2^s - 1]$ выполнено $1 < (3q \cdot 2^b + 1, \frac{2^{2^s}-1}{2^{2^5}-1}) < 3q \cdot 2^b + 1$; (в частности, числа $6q + 1$ и $12q + 1$ - составные)*
5. *Числа $2q + 1$ и $4q + 1$ – составные;*
6. *Число $N = 3q \cdot 2^n + 1$ не имеет простых делителей вида $2^{2^t} + 1$ для $2 \leqslant t \leqslant s$.*

Тогда не существует чисел Кармайкла вида $N = 3q \cdot 2^n + 1$.

Доказательство. Возможны два случая: или N имеет простой делитель $p_l = 2^{2^l} + 1$ для $l > 32$, или не имеет. Разберём оба случая, применив в них леммы 8 и 9 соответственно.

1. N не имеет простого делителя $p_l = 2^{2^l} + 1$ для $l > 32$. Тогда предположения 1, 3, 4 и 5 влекут истинность леммы 8.

2. N имеет простой делитель $p_l = 2^{2^l} + 1$ для $l > 32$. Тогда предположения 1, 2, 3, 4, 5 и 6 влекут истинность леммы 9.

В обоих случаях число вида $N = 3q \cdot 2^n + 1$ не является числом Кармайкла, что и требовалось. □

Лемма 11. *Чисел q, удовлетворяющих лемме 10 при $s = 10$, бесконечно много. В частности, верна теорема 6.*

Доказательство. Воспользуемся известными результатами о разложении чисел Ферма на простые множители. Так, кроме 3, 5, 17, 257 и 65537 число $2^{2^{10}} - 1 = \prod\limits_{1 \leqslant i \leqslant 9} (2^{2^i} + 1)$ имеет следующие делители (в скобках указаны имена учёных, впервые получивших разложение на множители):

$$2^{2^5} + 1 = 641 \cdot 6700417 \quad \text{(Л. Эйлер)}$$

$$2^{2^6} + 1 = 274177 \cdot 67280421310721 \quad \text{(Т. Клаузен)}$$

$$2^{2^7} + 1 = 59649589127497217 \cdot 5704689200685129054721 \quad \text{(М. А. Моррисон и Дж. Бриллхэрт, [11])}$$

$$2^{2^8} + 1 = 1238926361552897 \cdot p_{62}, \quad \text{(Р. Брент и Дж. Поллард, [12])}$$

$$2^{2^9} + 1 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot p_{99}.$$

$$\text{(А. Ленстра, Х. Ленстра, М. Манасс и Дж. Поллард, [13])}$$

Здесь p_{62} и p_{99} - простые числа, содержащие 62 и 99 цифр соответственно. Заметим, что любое простое число p из этого списка делит $\frac{2^{2^{10}}-1}{2^{2^5}-1} = \prod\limits_{5 \leqslant i \leqslant 9} (2^{2^i} + 1)$. Также заметим, что $(3q \cdot 2^{2^{10}-c} + 1, 2^{2^{10}} - 1) = (3q \cdot 2^{2^{10}-c} + 1, 3q \cdot 2^{2^{10}} - 3q) = (3q \cdot 2^{2^{10}-c} + 1, -2^c - 3q) = (3q \cdot 2^{2^{10}-c} + 1, 2^c + 3q)$ для любого $c \in [0; 2^{10}]$. Значит, в лемме 9 можно положить $s = 10$. Потребуем, чтобы:

1. $q > 10^{300}$;

2. $q \equiv 13227 \pmod{1042245396920}$;

3. $3q + 1$ делилось на 647;

4. $3q + 2$ делилось на 6700417;

5. $3q + 4$ делилось на 274177;

6. $6q + 1$ делилось на 67280421310721;

7. $12q+1$ делилось на 59649589127497217;
8. $24q+1$ делилось на 5704689200685129054721;
9. $48q+1$ делилось на 1238926361552897;
10. $96q+1$ делилось на p_{62};
11. $192q+1$ делилось на 2424833;
12. $2q+1$ делилось на 74556028256478842083373957362004549187833663426 57;
13. $4q+1$ делилось на p_{99}.

Эти требования обеспечивают выполнение пунктов 2, 3, 6 и 7 леммы 10, так как остаток в требовании 2 выбран так, чтобы q удовлетворяло лемме 7, поэтому $3, 17, 257, 65537 \nmid 3q \cdot 2^n + 1$ при любом n. Осталось убедиться, что выполнены предположения 1, 4 и 5 леммы 10. При для $b \in [0; 6] \cup [2^{10} - 2; 2^{10} - 1]$ действительно выполнено $1 < (3q \cdot 2^b + 1, \frac{2^{2^{10}}-1}{2^{2^5}-1}) < 3q \cdot 2^b + 1$. Действительно, $1 < (3q \cdot 2^b + 1, \frac{2^{2^{10}}-1}{2^{2^5}-1})$ по выбору q. Кроме того, так как $3q \cdot 2^b + 1 > 3 \cdot 10^{300} > \frac{2^{2^{10}}-1}{2^{2^5}-1}$, то $(3q \cdot 2^b + 1, \frac{2^{2^{10}}-1}{2^{2^5}-1}) < 3q \cdot 2^b + 1$.
Те числа, для которых выполняются все эти делимости, по китайской теореме об остатках удовлетворяют сравнению $q \equiv A \pmod{B}$ для некоторых A, B таких, что $(A, B) = 1$, то есть, являются членами арифметической прогрессии, в которой первый член взаимно прост с разностью. А по теореме Дирихле в любой такой арифметической прогрессии найдётся бесконечно много простых чисел, что обеспечивает выполнение пункта 1 леммы 10 и завершает доказательство.

Примечание. Можно заметить, что $B = \frac{8 \cdot 7 \cdot 13}{3}(F_{10} - 2) = \frac{8 \cdot 7 \cdot 13}{3} \cdot (2^{2^{10}} - 1)$.

Примечание. Также нетрудно понять, что всего существует 11! способов перестановки простых делителей в пунктах 3-13. Следовательно, найдётся $11! = 39916800$ чисел A таких, что $0 < A < B$ и простые числа q такие, что $q \equiv A \pmod{B}$, удовлетворяют всем условиям.

□

3 Случаи некоторых малых k

В этом разделе рассматриваются частные случаи, где k - фиксированное число. А именно, будет показано, что для трёх значений k не найдётся ни одного числа Кармайкла вида $k \cdot 2^n + 1$.

Теорема 8. *Не существует чисел Кармайкла вида $k \cdot 2^n + 1$ для $k = 49$, $k = 121$ и $k = 169$.*

При доказательстве нам потребуется некоторый технический результат. Сформулируем данный результат в наиболее общем виде, в котором его удалось получить, используя вычислительную мощность одного персонального компьютера.

Лемма 12. *Пусть $k < 256$. Тогда не существует чисел Кармайкла вида $k \cdot 2^n + 1$ для $n < 5 \cdot 10^4$, кроме 561, 1105, 1729, 2465 и 8355841.*

Доказательство. Из критерия Корсельта следует, что если $p \mid N$, то $p = 2^a d+1$, где $l \leqslant m$ и $d \mid k$. Соотвестственно, если N не может быть полностью разложено на простые вида $p = 2^l d+1$, то N не является числом Кармайкла. Список таких простых чисел для $d < 740$ и $l < 4 \cdot 10^6$ известен и опубликован по адресу [14], поэтому доказательство утверждения сводится к компьютерной проверке по следующему алгоритму:

Алгоритм 1 Проверка числа $N = k \cdot 2^n + 1$ на соответствие критерию Корсельта

```
X = N
Цикл от d = 1 до k, d | k выполнять
    Цикл от l = 1 до n выполнять
        Если p = 2^l d + 1 есть в списке, p | N и p^2 ∤ N тогда
            X ← X/p
        Конец условия
    Конец цикла
Конец цикла
Если X = 1 тогда
    Вернуть N - число Кармайкла
Конец условия
Если X ≠ 1 тогда
    Вернуть N - не число Кармайкла
Конец условия
```

Проверка была произведена на процессоре Intel Core i7-6700HQ CPU @ 2.60GHz, что заняло 8 часов 48 минут. □

Так как доказательство теоремы 8 во многом повторяет результаты, полученные в [5], нам потребуются некоторые леммы, доказанные в этой статье. Здесь мы ограничимся приведением формулировок.

Лемма 13. *(лемма 2 из [5]) Если $k \geqslant 3$ и $p = 2^{2^a} + 1$ является простым делителем $N = k \cdot 2^n + 1$, то $p < k^2$.*

Лемма 14. *(лемма 3 из [5]) Если $d \mid k$ и $p = d \cdot 2^m + 1$ является простым делителем $N = k \cdot 2^n + 1$, причём $p - 1 = d \cdot 2^m$ и $N - 1 = k \cdot 2^n$ мультипликативно зависимы, то есть $\frac{\ln 2^n k}{\ln 2^m d} \in \mathbb{Q}$, то $p < 2^{n/3} k^{1/3} + 1$. Иначе говоря, если для некоторого рационального r верно, что $p - 1 = (N-1)^r$, то $r \leqslant \frac{1}{3}$. В частности, $m \leqslant \frac{n}{3}$.*

Лемма 15. *(лемма 4 из [5]) Если $d \mid k$, $d > 1$ и $p = d \cdot 2^m + 1$ является простым делителем числа Кармайкла $N = k \cdot 2^n + 1$, причём $p - 1 = d \cdot 2^m$ и $N - 1 = k \cdot 2^n$ мультипликативно независимы, то $m < 7\sqrt{n \ln k}$, если $n > 3 \ln k$.*

Лемма 16. *(модифицированная версия леммы 7.2 из [5]) Пусть число $N = k \cdot 2^n + 1$ кармайклово, $k < 256$ и $a = \min\limits_{\substack{p \in \mathbb{P} \\ p \mid N}} \nu_2(p-1)$. Тогда $n > a + 20$, если $n > 328$.*

Примечание. Условие $n > a + 20$ здесь избыточно, достаточно, чтобы выполнялось $n > a + 1$. Однако, чтобы сохранить соответствие статье [5] и оставить пространство для дальнейших рассуждений, лемма приведена именно в такой формулировке.

Доказательство. Будем действовать так же, как и при доказательстве леммы 7.2 из [5]. Пусть $p = 2^a d + 1$ – простой делитель N. Если p – простое число Ферма, которое является делителем N, то по лемме 13 $p \in \{3, 5, 17, 257\}$ и $a \leqslant \nu_2(p-1) \leqslant \nu_2(257 - 1) = 8 < n - 20$ при $n \geqslant 30$. Если $2^n k$ и $2^a d$ мультипликативно зависимы, то есть, $\frac{\ln 2^n k}{\ln 2^a d} \in \mathbb{Q}$, лемма 14 утверждает, что $a \leqslant n/3$, и поэтому $a \leqslant n + 20$ для $n \geqslant 30$. Если $2^n k$ и $2^a d$ мультипликативно независимы, то по лемме 15 $a < 7\sqrt{n \ln k} < 17\sqrt{n}$ при $n > 17 > 3 \ln k$. Поэтому если $n \leqslant a + 20$, то $n < 17\sqrt{n} + 20$, что не выполняется при $n > 328$. Следовательно, $n > a + 20$. □

Мы проверим три случая: $k = 49, 121, 169$. Эти числа удобны для рассмотрения, потому что представляют собой квадрат простого числа. Итак, пусть $k = p^2$, $p = 7, 11, 13$. Как и в [5], представим $N = p^2 \cdot 2^n + 1$ в виде произведения простых сомножителей

$$\prod_{i=1}^{s}(1 \cdot 2^{a_i} + 1) \prod_{j=1}^{t}(p \cdot 2^{b_j} + 1) \prod_{k=1}^{u}(p^2 \cdot 2^{c_k} + 1),$$

где $a_1 < \ldots < a_s$, $b_1 < \ldots < b_t$ и $c_1 < \ldots < c_u$. Если $s = 0$, $t = 0$ или $u = 0$, положим $a_1 = \infty$, $b_1 = \infty$ или $c_1 = \infty$ соответственно. Как и прежде, положим $a = \min(a_1, b_1, c_1)$. Очевидно, что $a \geqslant 1$, значит, $2^{2a} \equiv 0 \pmod{2^{a+1}}$.

Лемма 17. *Среди чисел a_1, b_1, c_1 не может быть трёх различных.*

Доказательство. Пусть все они различны. Тогда $N \equiv 1 \pmod{2^{a+1}}$. С другой стороны N бесквадратно, в частности, $a_1 < a_2$, $b_1 < b_2$, $c_1 < c_2$, поэтому

$$\prod_{i=1}^{s}(1 \cdot 2^{a_i} + 1) \prod_{j=1}^{t}(p \cdot 2^{b_j} + 1) \prod_{k=1}^{u}(p^2 \cdot 2^{c_k} + 1) \equiv 1 \cdot 2^{a_1} + p \cdot 2^{b_1} + p^2 \cdot 2^{c_1} + 1 \pmod{2^{a+1}},$$

то есть,

$$0 \equiv 1 \cdot 2^{a_1} + p \cdot 2^{b_1} + p^2 \cdot 2^{c_1} \pmod{2^{a+1}},$$

или, что то же самое,

$$0 \equiv 2^{a_1-a} + 2^{b_1-a} + 2^{c_1-a} \pmod{2}.$$

Но если a_1, b_1, c_1 различны, то среди чисел $2^{a_1-a}, 2^{b_1-a}, 2^{c_1-a}$ есть два чётных и одно нечётное, чего, очевидно, не может быть. Значит, среди чисел a_1, b_1, c_1 есть два одинаковых, причём они совпадают с a. □

Здесь удобно сначала рассмотреть случай $a \geqslant 5, a \neq 8$. Итак, если p_0 - простое число Ферма, являющееся делителем N, то $p_0 < 169^2 = 28561$. Так как $a \geqslant 5$, то p_0 не может принимать значения 3, 5 или 17. Если $p_0 = 257$, то $a_1 = 8 \neq a$, то есть, $a_1 < a$ (что, очевидно, невозможно) или $a_1 > a$. Если же не найдётся простого числа Ферма, являющегося делителем N, то $a_1 = \infty$ и также выполнено неравенство $a_1 > a$. Значит, по лемме 17 $a = b_1 = c_1$. В частности, оба числа $p_1 = p \cdot 2^a + 1$ и $p_2 = p^2 \cdot 2^a + 1$ являются простыми. Очевидно, что имеют место сравнения

$$2^n \cdot p^2 \equiv -1 \pmod{p_1},$$

и

$$2^{2a} \cdot p^2 \equiv 1 \pmod{p_1}$$

Значит, выполняется

$$2^{n-2a} \equiv -1 \pmod{p_1},$$

то есть

$$2^{2n-4a} \equiv 1 \pmod{p_1}$$

В частности, $\mathrm{ord}_{p_1}(2) \mid 2n - 4a$. Аналогично

$$2^n \cdot p^2 \equiv -1 \pmod{p_2},$$

а также

$$2^a \cdot p^2 \equiv -1 \pmod{p_2}$$

Значит, верно

$$2^{n-a} \equiv 1 \pmod{p_2}$$

и $\mathrm{ord}_{p_2}(2) \mid n - a \mid 4n - 4a$. Так как $\mathrm{ord}_p(b) \mid p - 1$ для любых взаимно простых b и p, то $\mathrm{ord}_{p_1}(2) \mid p^2 \cdot 2^a$ и $\mathrm{ord}_{p_2}(2) \mid p^2 \cdot 2^a$.
Пусть $\alpha = \min\left(\nu_2(\mathrm{ord}_{p_1}(2)), \nu_2(\mathrm{ord}_{p_2}(2))\right)$ – минимальная из степеней двойки, содержащихся в разложении $\mathrm{ord}_{p_1}(2)$ и $\mathrm{ord}_{p_2}(2)$ на простые множители. Пусть $i \in \{1, 2\}$ - тот индекс, на котором достигается данный минимум. Тогда

$$2n \equiv 4a \equiv 4n \pmod{2^\alpha} \Rightarrow 2n \equiv 0 \pmod{2^\alpha}$$

В частности, $\mathrm{ord}_{p_i}(2) \mid 2np^2$ и $p_i \mid 2^{np^2} - 1$. Но по нашему предположению p_i - делитель числа Кармайкла, то есть,

$$p_i \mid p^2 \cdot 2^n + 1 \mid (p^2 \cdot 2^n)^{2p^2} - 1$$

или же

$$p_i \mid p^{4p^2}(2^{np^2}-1)-(p^2\cdot 2^n)^{2p^2}+1=-(p^{4p^2}-1).$$

Итак, мы доказали следующую лемму.

Лемма 18. *Если* $p\in\{7,11,13\}$, $N=p^2\cdot 2^n+1$ - *число Кармайкла,* $a=\min\limits_{\substack{p\in\mathbb{P}\\ p\mid N}}\nu_2(p-1)$ *и число* $p^{4p^2}-1$ *не имеет простых делителей вида* $p\cdot 2^b+1$ *и* $p^2\cdot 2^b+1$ *для* $b\geq 5, b\neq 8$, *то* $a=1,2,3,4$ *или* 8.

При рассмотрении случаев $a=1,2,3,4,8$ некоторые из них можно сразу отбросить, так как среди чисел $1\cdot 2^a+1, p\cdot 2^a+1, p^2\cdot 2^a+1$ может не найтись двух простых. Для удобства проверки также заметим, что условие $p_0\mid k\cdot 2^n+1$ эквивалентно сравнению

$$n\equiv \operatorname{dlog}_{2,p_0}\frac{-1}{k}\pmod{\operatorname{ord}_{p_0}(2)},$$

где $\operatorname{dlog}_{2,p_0}\frac{-1}{k}$ означает дискретный логарифм $\frac{-1}{k}$ по модулю p_0 и основанию 2.

Случай 1. $k=49$. Как обычно, $a=\min\limits_{\substack{p\in\mathbb{P}\\ p\mid N}}\nu_2(p-1)$.

Случай $a=1$. Предполагаемые делители равны 3, 15 и 99, но среди этих чисел нет двух простых.

Случай $a=2$. Предполагаемые делители равны 5, 29 и 197. Вычислим, какие ограничения на n влечёт за собой делимость на то или иное простое число. Итак, условие $5\mid N$ равносильно условию $n\equiv 0\pmod 4$, условие $29\mid N$ равносильно условию $n\equiv 18\pmod{28}$, условие $197\mid N$ равносильно условию $n\equiv 2\pmod{196}$. Очевидно, никакие два из этих сравнений не могут выполняться одновременно.

Случай $a=3$. Предполагаемые делители равны 9, 57, 393. Среди этих чисел нет ни одного простого.

Случай $a=4$. Предполагаемые делители равны 17, 113 и 785, из которых только первые два являются простыми. Как и в случае $a=2$, рассмотрим условия, которые накладывает такая делимость на число n. Условие $17\mid N$ равносильно условию $n\equiv 7\pmod 8$, условие $113\mid N$ равносильно условию $n\equiv 22\pmod{28}$. Опять же, оба этих условия не могут выполняться одновременно.

Случай $a=8$. Как и прежде, убедимся в том, что оба числа $7\cdot 2^8+1=1793=11\cdot 163$ и $49\cdot 2^8+1=12545=5\cdot 13\cdot 193$ являются составными.

Для завершения доказательства необходимо проверить выполнение леммы 18. Иначе говоря. надо разложить на простые множители число $49^{98}-1=4.357283753...\cdot 10^{165}$ и убедиться, что оно не имеет простых делителей вида $7\cdot 2^b+1$ и $49\cdot 2^b+1$ для $b\geq 5, b\neq 8$. Это число было разложено на множители с помощью библиотеки primefac 2.0.12 на процессоре Intel Core i7-6700HQ CPU @ 2.60GHz. Итак,

$$49^{98}-1=2^5\cdot 3\cdot 5^2\cdot 29\cdot 113\cdot 197\cdot 883\cdot 911\cdot 3529\cdot 3823\cdot 4733\cdot 16073\cdot 161309\cdot 1074473\cdot 1445599\times$$

$$\times 13473433\cdot 19847549\cdot 101361401\cdot 13564461457\cdot 1933665951863017\cdot 6106505825833677713\times$$

$$\times 10148051647066664017 \cdot 308584634651706890352352946242481.$$

Прямым подсчётом можно убедиться, что простых делителей вида $7 \cdot 2^b + 1$ и $49 \cdot 2^b + 1$ у этого числа нет. Значит, чисел Кармайкла вида $49 \cdot 2^n + 1$ не существует.

Случай 2. $k = 121$.
Случай $a = 1$. Предполагаемые делители равны 3, 23 и 243, число 243 является составным. Если $3 \mid 121 \cdot 2^n + 1$, то $n \equiv 1 \pmod 2$. А сравнение $121 \cdot 2^n + 1 \equiv 0 \pmod{23}$ неразрешимо.
Случай $a = 2$. Предполагаемые делители равны 5, 45 и 485. Среди этих чисел нет двух простых.
Случай $a = 3$. Предполагаемые делители равны 9, 89 и 969. Среди этих чисел нет двух простых.
Случай $a = 4$. Предполагаемые делители равны 17, 177 и 1937, из которых только 17 является простым.
Случай $a = 8$. Число $11 \cdot 2^8 + 1 = 2817 = 3^2 \cdot 313$ является составным, а $1 \cdot 2^8 + 1 = 257$ и $121 \cdot 2^8 + 1 = 30977$ являются простыми. Но $257 \nmid 121 \cdot 2^n + 1$ ни при каком n.
Для завершения доказательства необходимо, как и в случае $k = 49$, убедиться в том, что число $11^{484} - 1$ не имеет простых делителей вида $11 \cdot 2^b + 1$ и $121 \cdot 2^b + 1$. Такие простые делители не могут превосходить самого числа $11^{484} - 1$, а значит, $2^a < 11^{483}$ или же $a < 483 \log_2 11 = 1670,905\ldots$. Прямым подсчётом (см. также лемму 10) можно убедиться, что простых делителей вида $11 \cdot 2^b + 1$ и $121 \cdot 2^b + 1$ у этого числа нет. Значит, чисел Кармайкла вида $121 \cdot 2^n + 1$ не существует.

Случай 3. $k = 169$.
Случай $a = 1$. Предполагаемые делители равны 3, 27, 339. Среди этих чисел нет двух простых.
Случай $a = 2$. Предполагаемые делители равны 5, 53 и 667. Все эти числа - простые, поэтому вычислим

$$\operatorname{dlog}_{2,p_0} \frac{-1}{k},\ p_0 = 5,\ 53,\ 677.$$

Получим, что число n должно удовлетворять по меньшей мере двум из трёх сравнений

$$n \equiv 0 \pmod 4,$$

$$n \equiv 30 \pmod{52},$$

$$n \equiv 2 \pmod{676},$$

что невозможно.
Случай $a = 3$. Предполагаемые делители равны 9, 105 и 1353. Среди этих чисел нет двух простых.
Случай $a = 4$. Предполагаемые делители равны 17, 209 и 2705, из которых только 17 является простым.
Случай $a = 8$. Число $13 \cdot 2^8 + 1 = 3329$ является простым, а $169 \cdot 2^8 + 1 = 43265 = 5 \cdot 17 \cdot 509$ является составным. Но $257 \nmid 169 \cdot 2^n + 1$.

Для завершения доказательства необходимо, как и в двух предыдущих случаях, убедиться в том, что число $13^{676} - 1$ не имеет простых делителей вида $13 \cdot 2^b + 1$ и $169 \cdot 2^b + 1$. Такие простые делители не могут превосходить самого числа $13^{676} - 1$, а значит, $2^a < 13^{675}$ или же $a < 675 \log_2 13 = 2497,796\ldots$. Как и в предыдущем случае, прямым подсчётом можно убедиться, что простых делителей искомого вида у этого числа нет. Значит, чисел Кармайкла вида $169 \cdot 2^n + 1$ не существует.

Примечание. Составное число M такое, что $M = 13 \cdot 2^b + 1 \mid 13^{676} - 1$ и $b \geqslant 5, b \not\equiv 8$, всё же существует – это $13 \cdot 2^{15} + 1 = 425985$.

Итак, для $k = 49, 121$ и 169, показано, что не существует чисел Кармайкла вида $k \cdot 2^n + 1$, что завершает доказательство теоремы 8.

4 Список литературы

[1] A. Korselt, Problème chinois. // L'intermédiaire math. — 1899. – Vol. 6. – p. 143.

[2] R. D. Carmichael, Note on a new number theory function // Bull. Amer. Math. Soc. – 1910. - Vol. 16. No. 5. p. 232-238.

[3] R. D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$ // The American Mathematical Monthly. - 1912. - Vol. 19. No. 2. p. 22-27.

[4] W. R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers // Annals of Mathematics - 1994. - Vol. 139. No. 3. p. 703-722.

[5] J. Cilleruelo, F. Luca, A. Pizzaro-Madariaga, Carmichael numbers in the sequence $(2^n k + 1)_{n \geqslant 1}$ // Mathematics of Computation - 2015. - Vol. 85. No. 297. p. 357-377.

[6] C. Pomerance, On the distribution of pseudoprimes // Mathematics of Computation - 1981. - Vol. 37. No. 156. p. 587-593.

[7] J. Chernick, On Fermat's simple theorem // Bull. Amer. Math. Soc - 1939. - Vol. 45. No. 4. p. 269-274

[8] W. Banks, C. Finch, F. Luca [et al.], Sierpinski and Carmichael numbers // Trans. of the Amer. Math. Soc. – 2015. - Vol. 367. No. 1. p. 355-376..

[9] T. Wright, The impossibility of certain types of Carmichael numbers // Integers - 2012. - Vol. 12. No. 5. p. 951-964.

[10] http://www.prothsearch.com/fermat.html

[11] Michael A. Morrison, J. Brillhart, A method of factoring and the factorization of F_7 // Mathematics of Computation - 1975. - Vol. 29. No. 129. p. 183-205.

[12] R. P. Brent, J.P. Pollard, Factorization of the eighth Fermât number // Mathematics of Computation - 1981. - Vol. 36. No. 154. p. 627-630.

[13] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, The factorization of the ninth Fermat number // Mathematics of Computation - 1993. - Vol. 61. No. 203. p. 319-349.

[14] http://www.prothsearch.com/riesel1.html