О числах Новака

А.Б. Калмынин

1 Введение

Числами Новака называются такие натуральные N, что $N \mid 2^N+1$. Их можно рассматривать как некоторый аналог псевдопростых чисел по основанию 2, то есть таких N, что $N \mid 2^{N-1}-1$. В свете аналогии с псевдопростыми числами, естественно было бы задаться вопросом, почему нужно брать именно $N \mid 2^N+1$, а не $N \mid 2^N-1$. Оказывается, второй вариант тривиален — такое число только одно.

Множество чисел Новака обладает многочисленными дополнительными структурами. Например, в отличие от чисел Роткевича (см. [Rot]), т.е. таких N, что $N \mid 2^{N-2}-1$, достаточно очевидно, что чисел Новака бесконечно много: множество чисел Новака содержит число 3 и при этом НОД, НОК и произведение любых двух чисел Новака снова являются числами Новака (см. раздел 3), стало быть, для любого $k \in \mathbb{N}$ выполнено $3^k \mid 2^{3^k}+1$. Кроме того, если N — число Новака, то тем же свойством обладает и число $M = 2^N+1$. В самом деле, если $M = 2^N+1 = Nk$, где k — целое, то, в силу нечётности M, k также нечётно, поэтому

$$2^M + 1 = 2^{Nk} + 1 = (2^N+1)(2^{N(k-1)} - 2^{N(k-2)} + \ldots + 1) = ML,$$

где L — целое число. Таким образом, $M \mid 2^M + 1$, что и требовалось доказать. В этой работе мы изучаем распределение чисел Новака, а именно получаем некоторые новые нижние границы для количества чисел Новака, не превосходящих числа x. Здесь и далее эта величина будет обозначаться $\mathcal{N}_B(x)$, в честь Бржетислава Новака, который и доказал первые нетривиальные оценки для $\mathcal{N}_B(x)$([KaPoRV1],[KaPoRV2]).

В своей статье [GLPS] Люка, Померанс, Шпарлинский и Альба Гонзалез доказали, среди прочего, следующий факт:

Теорема. *Для некоторой положительной константы c и достаточно больших x выполнена двойная оценка*

$$xe^{-(1+o(1))\sqrt{\ln x \ln\ln x}} \gg \mathcal{N}_B(x) \gg e^{c(\ln\ln x)^2}$$

Цель нашей работы — доказательство существенно лучшей оценки снизу.

Теорема 1. *Существуют положительные c_2 и x_2, такие, что для любого $x > x_2$ справедливо неравенство*

$$\mathcal{N}_B(x) \gg e^{e^{c_2(\ln\ln\ln x)^2}}$$

На самом деле, процесс наращивания башни из экспонент можно продолжать и дальше.

Теорема 2. *Для всякого натурального n существуют положительные c_n и X_n, такие, что для любого $x > X_n$ выполняется следующая нижняя оценка:*

$$\mathcal{N}_B(x) \gg_n e_n(c_n(\ln_{n+1} x)^2)$$

где $e_0(x) = x = \ln_0(x)$, и для всех $i \geq 0$ выполнено $e_{i+1}(x) = e^{e_i(x)}$ и $\ln_{i+1}(x) = \ln(\ln_i(x))$.

Теоремы 1 и 2 допускают обобщение на более широкий класс последовательностей. Например, они остаются в силе для таких N, что $N \mid a^N - b^N$, где $a - b \neq 0, \pm 1$.
В четвертом разделе статьи мы также обсудим распределение простых чисел Новака, то есть таких простых p, что $p \mid N$ для некоторого числа Новака N. Методы получения оценок для числа таких простых чисел будут существенно опираться на Обобщенную Гипотезу Римана (см. следующий раздел).

2 Обозначения и некоторые леммы

В этот раздел мы поместим некоторые полезные для дальнейших рассуждений леммы и обозначения.
Здесь и далее для рационального числа q $\nu_p(q)$ обозначает p-адическое нормирование q, то есть такое целое k, что $q = p^k \frac{a}{b}$, где a и b — целые числа взаимно простые числа, не делящиеся на k. Для натурального N число делителей N обозначим $\tau(N)$, а число простых делителей без учёта кратности $\omega(N)$. Для пары натуральных чисел N и M их НОД и НОК обозначаются (N, M) и $[N, M]$ соответственно. Если p — простое число, а a и b — целые взаимно простые числа, не делящиеся на p, то $\ell_p(\frac{a}{b})$ означает мультипликативный порядок числа $\frac{a}{b}$ в кольце остатков по модулю p, то есть наименьшее такое натуральное k, что

$$a^k \equiv b^k \pmod{p}.$$

Нам потребуются два относительно элементарных утверждения о делимости чисел вида $a^n \pm b^n$.

Лемма 1 (Лемма об уточнении показателя)**.** *Пусть p — простое число, а a, b — такие целые, не делящиеся на p, что $\nu_p(a-b) > 0$. Тогда для любого $k > 0$ имеет место равенство*

$$\nu_p(a^k - b^k) = \nu_p(a-b) + \nu_p(k)$$

Лемма 2 (Теорема Зигмонди для сумм)**.** *Пусть $a > b$ — взаимно простые натуральные числа. Если $(a,b,n) \neq (2,1,3)$, то существует такое простое p (оно называется примитивным простым), что p делит $a^n + b^n$, но не делит $a^k + b^k$ при $k < n$.*

Доказательства этих утверждений см. в работе [M].
Помимо этих лемм, нами будет использоваться следующий факт:

Лемма 3. *Пусть $g \neq 0, \pm 1$ — фиксированное рациональное число. Если верна Обобщенная Гипотеза Римана, то для всех x и всех $1 \leq L \leq \frac{\ln x}{\ln \ln x}$ выполнена верхняя оценка:*

$$\left| \left\{ p \leq x : \ell_g(p) \leq \frac{p-1}{L} \right\} \right| \ll_g \frac{\pi(x)}{L}$$

Доказательство утверждения см. в [KP].
Эта лемма — единственное утверждение в настоящей статье, опирающееся на Обобщенную Гипотезу Римана.
Дадим здесь также удобную для применений формулировку неравенства большого решета:

Лемма 4 (Большое Решето)**.** *Пусть N и Q — натуральные числа, $f(p) \in \mathbb{N}$ для всех простых $p \leq Q$ и $0 < f(p) < p$. Зафиксируем $f(p)$ классов вычетов по модулю каждого из таких простых. Пусть $\mathcal{A}$ — множество натуральных чисел, не превосходящих N, и не попадающих ни в один из зафиксированных классов вычетов. Тогда для количества элементов в множестве $\mathcal{A}$ справедлива оценка*

$$|\mathcal{A}| \ll \frac{N + Q^2}{S},$$

где

$$S = \sum_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{f(p)}{p - f(p)}$$

.

3 Доказательство основных теорем

В этой части работы мы докажем Теоремы 1 и 2.
Как уже было отмечено ранее, множество чисел Новака обладает разнообразными структурами. Например, если N и M — числа Новака, то (N,M) и $[N,M]$ также являются числами Новака. Действительно, если N делит $2^N + 1$ и M делит $2^M + 1$, то N и M нечётны и $(2^N + 1, 2^M + 1)$ делится на (N,M). Таким образом, $2^{(N,M)} + 1$ делится на (N,M). С другой стороны, $[2^N + 1, 2^M + 1]$ делится на $[N,M]$, но $2^{[N,M]} + 1$ делится и на $2^N + 1$, и на

$2^M + 1$, поэтому $2^{[N,M]} + 1$ делится на $[2^N + 1, 2^M + 1]$ и, тем самым, на $[N, M]$. Чуть труднее доказать, что произведение двух чисел Новака также является числом Новака. Этот факт является следствием следующего общего утверждения:

Лемма 5. *Пусть N — число Новака и $p_1, \ldots, p_k$ — простые делители числа 2^N+1. Тогда для произвольных неотрицательных целых чисел $\alpha_1, \ldots, \alpha_k$ число $Np_1^{\alpha_1} \ldots p_k^{\alpha_k}$ также является числом Новака.*

Доказательство: Покажем, что для любого числа Новака N и любого простого $p \mid 2^N + 1$ число $2^{Np} + 1$ делится на $p^{\nu_p(N)+1}$. Если $\nu_p(N) = 0$, то, в силу нечётности p и того, что p делит $2^N + 1$, получаем, что $2^N + 1$ делит $2^{Np}+1$, и, стало быть, p делит $2^{Np}+1$. Если же $\nu_p(N) > 0$, то, в силу леммы об уточнении показателя, $\nu_p(2^{Np} + 1) = \nu_p(2^N + 1) + 1 \geq \nu_p(N) + 1$.
Итак, $2^{Np}+1$ делится на N и на $p^{\nu_p(N)+1}$, а значит и на Np. Таким образом, Np является числом Новака. Применяя доказанное утверждение нужное число раз, получаем требуемое. □

Теперь, опираясь на Лемму 5, мы покажем, что для получения хороших нижних оценок на $\mathcal{N}_B(x)$ достаточно уметь строить числа Новака N такие, что число $2^N + 1$ имеет много различных простых делителей.

Лемма 6. *Пусть x — положительное число и $1 < N \leq x$ — число Новака с $\omega(2^N + 1) = k$. Тогда выполнено неравенство*

$$\mathcal{N}_B(x) \geq \left(\frac{\ln \frac{x}{N}}{N} \right)^k$$

Доказательство: Пусть $p_1, \ldots, p_k$ — простые делители $2^N + 1$. Согласно Лемме 5, любое число вида $Np_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где $\alpha_i \geq 0$, является числом Новака. Оценим снизу число таких наборов $(\alpha_1, \ldots, \alpha_k)$, что получившееся число не превосходит x.
Ясно, что $Np_1^{\alpha_1} \ldots p_k^{\alpha_k} \leq x$ тогда и только тогда, когда

$$\alpha_1 \ln p_1 + \ldots + \alpha_k \ln p_k \leq \ln \frac{x}{N}$$

Любой набор, в котором для любого i выполнено неравенство $\alpha_i \ln p_i \leq \frac{\ln \frac{x}{N}}{k}$, очевидно, подходит. Поэтому подходящих наборов по меньшей мере

$$\prod_{i=1}^{k} \left(\left[\frac{\ln \frac{x}{N}}{k \ln p_i} \right] + 1 \right) \geq \prod_{i=1}^{k} \frac{\ln \frac{x}{N}}{k \ln p_i} = \left(\frac{\ln \frac{x}{N}}{k} \right)^k S,$$

где $S = \prod_{i=1}^{k} \frac{1}{\ln p_i}$. Осталось оценить снизу величину S. Для этого заметим, что, в силу делимости $2^N + 1$ на $p_1, \ldots, p_k$ справедливо неравенство

$$\ln p_1 + \ldots + \ln p_k \leq \ln(2^N + 1) \leq N$$

Отсюда, в силу неравенства о средних, получаем

$$\prod_{i=1}^{k} \ln p_i \leq \left(\frac{\ln p_1 + \ldots + \ln p_k}{k} \right)^k \leq \frac{N^k}{k^k}$$

То есть

$$S \geq \frac{k^k}{N^k}$$

.

В силу предыдущих рассуждений, получаем

$$\mathcal{N}_B(x) \geq \left(\frac{\ln \frac{x}{N}}{k} \right)^k S \geq \left(\frac{\ln \frac{x}{N}}{N} \right)^k$$

Что и требовалось. □

Было бы естественно ожидать, что для всякого y среди чисел Новака есть такие $N \leq y$, что $2^N + 1$ имеет *нормальное* по порядку число делителей, то есть $\ln \ln (2^y + 1) \sim \ln y$. Такое эвристическое рассуждение даёт вместе с выбором $y = \sqrt{\ln x}$ нижнюю оценку

$$\mathcal{N}_B(x) \geq e^{c(\ln \ln x)^2},$$

что совпадает по силе с Теоремой 1. Итак, нам нужно, чтобы $2^N + 1$ имело *аномально большое* количество простых делителей.

Следующее простое следствие из теоремы Зигмонди для сумм дает нижнюю оценку для $\omega(2^N + 1)$ в терминах арифметических свойств числа N.

Лемма 7. *Для любого нечётного натурального N выполнено неравенство*

$$\omega(2^N + 1) \geq \tau(N) - 1$$

Доказательство: Для каждого делителя d числа N, отличного от 3, выберем какой-нибудь примитивный простой делитель p_d числа $2^d + 1$. В силу теоремы Зигмонди для сумм, это всегда можно сделать. Заметим, что при $d' \neq d$ всегда $p_{d'} \neq p_d$, в силу примитивности и того, что либо $d > d'$, либо, наоборот, $d' > d$. Далее, для любого d имеем $p_d \mid 2^d + 1$, а значит, в силу нечётности числа N, $2^d + 1$ делит $2^N + 1$ и, следовательно, p_d делит $2^N + 1$. Таким образом, простых делителей у $2^N + 1$ не меньше, чем делителей N, отличных от 3. Что и требовалось доказать.

□

Доказанная выше оценка даёт ряд любопытных следствий, полезных для доказательства основной теоремы.

Следствие 1. *Для любого $n \in \mathbb{N}$ выполнено неравенство*

$$\omega(2^{3^n} + 1) \geq n$$

Следствие 2. *Для любых натуральных n и k верна оценка*

$$\omega(2^{(2^{3^n}+1)^k}+1) \geq (k+1)^n - 1 \geq k^n$$

Доказательство: Первое следствие получается напрямую из леммы с $N = 3^n$, так как $\tau(3^n) = n+1$. Для доказательства второго заметим, что

$$\tau((2^{3^n}+1)^k) \geq (k+1)^{\omega(2^{3^n}+1)} \geq (k+1)^n,$$

и применим получившееся неравенство и лемму 7 с $N = (2^{3^n}+1)^k$.

□

Теперь мы готовы доказать теорему 1.

Доказательство: Пусть для каких-нибудь n и k выполнено неравенство $(2^{3^n}+1)^k = N \leq x$.
Согласно Лемме 6, имеем

$$\mathcal{N}_B(x) \geq \left(\frac{\ln \frac{x}{N}}{N}\right)^{\omega(2^N+1)}$$

С другой стороны, в силу следствия 2, $\omega(2^N+1) \geq k^n$.
Поэтому

$$\mathcal{N}_B(x) \geq \left(\frac{\ln \frac{x}{N}}{N}\right)^{k^n}$$

Выберем теперь $k = \left[\frac{\sqrt{\ln\ln x}}{2}\right]$ и $n = \left[\frac{\ln\ln\ln x}{2\ln 3}\right]$.
Тогда $3^n \leq \sqrt{\ln\ln x}$, поэтому $2^{3^n}+1 \leq e^{3^n} \leq e^{\sqrt{\ln\ln x}}$. Стало быть, $N \leq e^{k\sqrt{\ln\ln x}} \leq \sqrt{\ln x}$.
Поэтому, в силу сказанного выше, для достаточно больших x имеем

$$\mathcal{N}_B(x) \geq \exp(k^n/3) \geq \exp(\exp((1/4\ln 3 + o(1))(\ln\ln\ln x)^2)),$$

что и доказывает Теорему 1.

□

Теперь из Теоремы 1 мы выведем Теорему 2.
Для удобства положим

$$d(x) := \max\{\omega(2^N+1) | N \leq x, N - \text{число Новака}\}$$

Из Леммы 6 можно вывести следующее следствие:

Следствие 3. *Для всех $x > 15000$ верна оценка*

$$\mathcal{N}_B(x) \geq e^{d(\sqrt{\ln x})}$$

Доказательство: Если $n \leq \sqrt{\ln x}$ — такое число Новака, что $\omega(2^n+1) = d(\sqrt{\ln x})$, то, в силу Леммы 6, имеем

$$\mathcal{N}_B(X) \geq \exp(d(\sqrt{\ln x}) \ln\left(\frac{\ln \frac{x}{n}}{n}\right))$$

Замечая, что при $x \geq 15000$ выполнено неравенство

$$\ln \frac{\ln \frac{x}{n}}{n} \geq \ln(\sqrt{\ln x}\left(1 - \frac{\ln\ln x}{2\ln x}\right)) = \frac{1}{2}\ln\ln x + \ln\left(1 - \frac{\ln\ln x}{2\ln x}\right) > 1$$

,
приходим к искомому неравенству. □

Таким образом, Теорема 2 следует из аналогичного утверждения для $d(x)$:

Теорема 3. *Для любого натурального n существуют положительные C_n и X_n такие, что для всякого $x > X_n$ выполнена оценка*

$$d(x) \gg_n e_n(C_n(\ln_{n+1} x)^2)$$

Доказательство: Заметим, что из доказательства Теоремы 1 следует истинность Теоремы 3 для $n = 1$ (с любым $C_1 < \frac{1}{4\ln 3}$). Докажем Теорему 3 по индукции.
Пусть верна оценка

$$d(x) \gg e_k(C_n(\ln_{k+1} x)^2)$$

Из Леммы 7 и того, что $2^N + 1$ — число Новака, если N — число Новака, следует, что

$$d(2^x + 1) \geq 2^{d(x)} - 1$$

Действительно, если $n \leq x$ — число Новака с $\omega(n) = d(x)$, то $2^n + 1 \leq 2^x + 1$ — также число Новака и при этом, в силу Леммы 7,

$$\omega(2^n + 1) \geq \tau(n) - 1 \geq 2^{\omega}(n) - 1 = 2^d(x) - 1.$$

Поэтому выполнено неравенство

$$d(x) \gg 2^{d(\log_2(x-1))} - 1 \gg_k 2^{e_k(C_k(\ln_{k+2}(x)))} - 1$$

Таким образом, достаточно взять любое $C_{k+1} < C_k$. □

Итак, мы доказали Теорему 3 и, тем самым, Теорему 2.
Наши теоремы допускают обобщение на специальных класс так называемых последовательностей делимости.

Определение. *Пусть $\mathcal{U} = \{u_n\}$ — последовательность целых чисел. Будем называть её допустимой последовательностью делимости умеренного роста, если выполнены следующие 5 свойств:*

1. **Делимость:** *Если* $n \mid m$, *то* $u_n \mid u_m$
2. **Лемма об уточнении показателя:** *Если* $p \mid u_n$, *то* $pu_n \mid u_{pn}$.
3. **Свойство Зигмонди-Бэнкса:** *Для всех натуральных* n, *за исключением конечного числа, существует такое простое* p, *что* $p \mid u_n$, *но* $p \nmid u_k$ *для всех* $k < n$.
4. **Умеренный рост:** *Существует такое* $a > 0$, *что* $u_n \ll a^n$.
5. **Невырожденность:** $u_1 \neq \pm 1$.

Пользуясь такими же рассуждениями, что и в доказательствах Теорем 1 и 2 можно доказать следующий факт:

Теорема 4. *Пусть* $\mathcal{U}$ *— допустимая последовательность делимости умеренного роста. Определим* $\mathfrak{U} := \{n : n \mid u_n\}$. *Пусть* $U(x) = |\mathfrak{U} \cap [1, x]|$ *— соответствующая считающая функция. Тогда для всякого натурального* n *существуют такие константы* $x(n,\mathcal{U})$ *и* $c(n,\mathcal{U}) > 0$, *что для всех* $x > x(n,\mathcal{U})$ *имеет место оценка*

$$U(x) \gg_n e_n(c(n,\mathcal{U})(\ln_{n+1} x)^2).$$

Условие умеренного роста можно заменить более слабым, скажем, оценкой вида $u_n \ll a^{n^2}$, однако это повлияет на вид левой части неравенства. Условие невырожденности же ослабить нельзя нельзя: например, последовательность $\{2^n - 1\}$ удовлетворяет всем свойствам, кроме невырожденности, но для неё $U(x) \equiv 1$.

4 Простые числа Новака

Будем называть простое p простым числом Новака, если существует число Новака N такое, что $p \mid N$. Будем обозначать множество простых чисел Новака символом $\mathcal{P}_\mathcal{N}$. Нам также будет необходимо рассматривать множество натуральных чисел, не имеющих ни одного простого делителя, являющегося простым Новака. Обозначим его $\overline{P_\mathcal{N}}$. В этом разделе нас будет интересовать распределение простых чисел Новака, то есть порядок роста функции

$$\pi_\mathcal{N}(x) = |\mathcal{P}_\mathcal{N} \cap [1, x]|$$

Мы ожидаем, что простые числа Новака встречаются достаточно редко. Например, число 9137 — это всего лишь седьмой элемент в $\mathcal{P}_\mathcal{N}$. Конечная цель этой части работы — доказательство следующего утверждения:

Теорема 5. *Если верна Обобщённая Гипотеза Римана, то имеет место оценка*

$$\pi_\mathcal{N}(x) \ll \frac{x \ln\ln x}{(\ln x)^2}.$$

Чтобы доказывать верхние оценки подобного рода, необходимо найти какие-то ограничения, которым удовлетворяют простые числа Новака. Для этого рассмотрим простые делители первых 24 чисел вида $p-1$ с $p \in \mathcal{P}_{\mathcal{N}}$:

p	$p-1$	p	$p-1$	p	$p-1$
3	$\mathbf{2}$	41113	$\mathbf{2}^3 \cdot \mathbf{3}^2 \cdot \mathbf{571}$	174763	$\mathbf{2} \cdot \mathbf{3}^2 \cdot 7 \cdot \mathbf{19} \cdot 73$
19	$\mathbf{2} \cdot \mathbf{3}^2$	52489	$\mathbf{2}^3 \cdot \mathbf{3}^8$	196579	$\mathbf{2} \cdot \mathbf{3}^2 \cdot 67 \cdot \mathbf{163}$
163	$\mathbf{2} \cdot \mathbf{3}^4$	78787	$\mathbf{2} \cdot \mathbf{3}^3 \cdot \mathbf{1459}$	274081	$\mathbf{2}^5 \cdot \mathbf{3} \cdot 5 \cdot \mathbf{571}$
571	$\mathbf{2} \cdot \mathbf{3} \cdot 5 \cdot \mathbf{19}$	87211	$\mathbf{2} \cdot \mathbf{3}^3 \cdot 5 \cdot 17 \cdot \mathbf{19}$	370009	$\mathbf{2}^3 \cdot \mathbf{3}^4 \cdot \mathbf{571}$
1459	$\mathbf{2} \cdot \mathbf{3}^7$	135433	$\mathbf{2}^3 \cdot \mathbf{3}^4 \cdot 11 \cdot \mathbf{19}$	370387	$\mathbf{2} \cdot \mathbf{3}^3 \cdot \mathbf{19}^3$
8803	$\mathbf{2} \cdot \mathbf{3}^3 \cdot \mathbf{163}$	139483	$\mathbf{2} \cdot \mathbf{3}^5 \cdot 7 \cdot 41$	478243	$\mathbf{2} \cdot \mathbf{3}^2 \cdot \mathbf{163}^2$
9137	$\mathbf{2}^4 \cdot \mathbf{571}$	144667	$\mathbf{2} \cdot \mathbf{3}^4 \cdot \mathbf{19} \cdot 47$	760267	$\mathbf{2} \cdot \mathbf{3}^4 \cdot 13 \cdot \mathbf{19}^2$
17497	$\mathbf{2}^3 \cdot \mathbf{3}^7$	164617	$\mathbf{2}^3 \cdot \mathbf{3} \cdot \mathbf{19}^3$	941489	$\mathbf{2}^4 \cdot \mathbf{19}^2 \cdot \mathbf{163}$

Таблица 1: Факторизации $p-1$. Жирным выделены элементы $\{2\} \cup \mathcal{P}_{\mathcal{N}}$.

Данные Таблицы 1 позволяют высказать такое эвристическое предположение: для большинства $p \in \mathcal{P}_{\mathcal{N}}$ большинство простых делителей числа $p-1$ лежат в $\{2\} \cup \mathcal{P}_{\mathcal{N}}$.
Некоторое объяснение этому даёт Лемма 3. В самом деле, если Np — число Новака, то $p \mid 2^{Np}+1$ и, следовательно, $2^{2Np}-1$ делится на p, поэтому $\ell_2(p) \mid 2Np$. С другой стороны, если верна Обобщенная Гипотеза Римана, то для большинства простых чисел p число $\ell_2(p)$ является большим делителем числа $p-1$. Но все простые делители $2Np$ лежат в $\{2\} \cup \mathcal{P}_{\mathcal{N}}$, поэтому то же верно и для большинства простых делителей большинства чисел вида $p-1$. Для того, чтобы вывести из этого утверждения оценку для $\pi_{\mathcal{N}}(x)$, нам понадобится лемма о свободных мультипликативных подполугруппах в $\mathbb{N}$.

Лемма 8. *Пусть $\mathcal{Q}$ — множество простых чисел такое, что для некоторых положительных a и b выполнено равенство*

$$\pi_{\mathcal{Q}}(x) := |\mathcal{Q} \cap [1,x]| = \frac{ax}{\ln x} + O(\frac{x}{\ln^{1+b} x})$$

Пусть $\mathfrak{Q}$ — свободная подполугруппа в $\mathbb{N}$, порожденная $\mathcal{Q}$, то есть множество всех таких натуральных n, все простые делители которых лежат в $\mathcal{Q}$. Тогда

$$Q(x) := |\mathfrak{Q} \cap [1,x]| = C(\mathcal{Q}) x \ln^{a-1} x \left(1 + O\left(\frac{1}{\ln \ln^{\min(1,b)} x}\right)\right)$$

Доказательство этого факта легко следует из теоремы Бредихина (см. [P], с.135). □

Следствие 4. *В предположениях Леммы 8, имеем*

$$S(x,\mathfrak{Q}) := \sum_{\substack{n\in\mathfrak{Q}\\ n\le x}} \frac{1}{n} \gg \ln^a x$$

Доказательство Теоремы 5: Разобьем множество $\mathcal{P}_{\mathcal{N}}$ на два множества $\mathcal{R}$ и $\mathcal{Q}$. В $\mathcal{R}$ попадут те простые p из $\mathcal{P}_{\mathcal{N}}$, у которых $\ell_2(p) \le \frac{p\ln\ln p}{\ln p}$, а во второе все остальные. В силу Леммы 3, при условии истинности Обобщенной Гипотезы Римана, имеет место оценка

$$|\mathcal{R}\cap[1,x]| \ll \frac{x\ln\ln x}{\ln^2 x}$$

Для всех остальных чисел имеем $\ell_2(p)|p-1$, с другой стороны среди простых делителей $\ell_2(p)$ есть только простые числа Новака и 2. Поэтому любое $p\in\mathcal{Q}$ с $\sqrt{x} < p \le x$ обладает такими двумя свойствами: во-первых, для любого простого $q \le \sqrt{x}$, p не делится на q, а во-вторых, если нечётное простое $q\notin\mathcal{P}_{\mathcal{N}}$, но $p-1$ делится на q, то необходимо $q \le \frac{\ln x}{\ln\ln x}$. Действительно, q не делит $\ell_2(p)$, поскольку все нечётные простые делители $\ell_2(p)$ принадлежат $\mathcal{P}_{\mathcal{N}}$, стало быть, $p-1$ кратно $[q,\ell_2(p)] = q\ell_2(p)$. Поэтому $q \le \frac{p-1}{\ell_2(p)} \le \frac{\ln p}{\ln\ln p} \le \frac{\ln x}{\ln\ln x}$.
Итак, $|\mathcal{Q}\cap(\sqrt{x},x]| \le |A|$, где $\mathcal{A}$ — множество натуральных чисел, не превосходящих x, и не попадающих ни в один из $f(p)$ классов вычетов по модулю p. Здесь p пробегает все простые числа, не превосходящие $\sqrt{x}$. При этом, $f(p)=1$ если $p \le \frac{\ln x}{\ln\ln x}$ или $p\in\mathcal{P}_{\mathcal{N}}$, и $f(p)=2$ иначе.
В силу неравества Большого Решета, получаем

$$|\mathcal{Q}\cap[1,x]| \ll \sqrt{x} + \frac{x}{S},$$

где

$$S = \sum_{n\le\sqrt{x}} \mu^2(n) \prod_{p|n} \frac{f(p)}{p-f(p)}$$

Пусть $Q(x)$ означает подполугруппу, порожденную всему простыми, не лежащими в $\mathcal{P}_{\mathcal{N}}$ и простыми, не превосходящими $\frac{\ln x}{\ln\ln x}$, а $t(n)$ — количество делителей числа n, лежащих в $Q(x)$. Тогда легко видеть, что

$$S \ge \sum_{n\le\sqrt{x}} \frac{\mu^2(n)t(n)}{n} \gg \sum_{n\le\sqrt{x}} \frac{t(n)}{n}$$

С другой стороны,

$$\frac{t(n)}{n} = \sum_{\substack{mk=n\\ k\in Q(x)}} \frac{1}{km}$$

Поэтому выполнена оценка

$$S \gg \sum_{m \le x^{1/4}} \frac{1}{m} \sum_{\substack{k \le x^{1/4} \\ k \in Q(x)}} \frac{1}{k} \gg \ln x \sum_{\substack{k \le x^{1/4} \\ k \in Q(x)}} \frac{1}{k}$$

Кроме того,

$$\sum_{\substack{k \le x^{1/4} \\ k \in Q(x)}} \frac{1}{k} \gg \sum_{\substack{k \le x^{1/4} \\ k \in \overline{P_{\mathcal{N}}}}} \frac{1}{k} (L(x))^{-1},$$

где $L(x)$ есть сумма обратных величин всех натуральных чисел, у которых все простые делители не превосходят $\frac{\ln x}{\ln \ln x}$. Очевидно,

$$L(x) = \prod_{p \le \frac{\ln x}{\ln \ln x}} \frac{p}{p-1} \asymp \ln \ln x$$

Окончательно получаем

$$S \gg \frac{\ln x}{\ln \ln x} \sum_{\substack{k \le x^{1/4} \\ k \in \overline{P_{\mathcal{N}}}}} \frac{1}{k}$$

Таким образом,

$$\pi_{\mathcal{N}}(x) \ll \frac{x \ln \ln x}{\ln^2 x} + \frac{x \ln \ln x}{\ln x} \left(\sum_{\substack{k \le x^{1/4} \\ k \in \overline{P_{\mathcal{N}}}}} \frac{1}{k} \right)^{-1}$$

С другой стороны, если $p \in \mathcal{P}_{\mathcal{N}}$, то существует такое нечетное N, что $p | 2^N + 1$, поэтому -2 всегда квадратичный вычет по модулю p. Это значит, что сумма в левой части нашей оценки, согласно следствию из Леммы 8, по порядку хотя бы $\sqrt{\ln x}$, то есть

$$\pi_{\mathcal{N}}(x) \ll \frac{x \ln \ln x}{\ln^{3/2} x}$$

Из этого, в силу того же следствия, следует, что сумма по порядку хотя бы $\ln x$, а значит

$$\pi_{\mathcal{N}}(x) \ll \frac{x \ln \ln x}{\ln^2 x}$$

Тем самым, Теорема 5 доказана. □

5 Числа Новака-Кармайкла и некоторые гипотезы

Напомним, что натуральное число N называется *числом Кармайкла*, если для любого $a \in \mathbb{Z}$ с $(a, N) = 1$ выполнено $N|(a^{N-1} - 1)$. Хорошо известно, что имеет место следующий критерий:

Теорема (Корсельт, 1899)**.** *Натуральное число n является числом Кармайкла тогда и только тогда, когда оно бесквадратно и $(p-1)|(n-1)$ для любого простого $p|n$.*

В контексте нашей работы естественно также рассмотреть аналог чисел Кармайкла, т.е. такие натуральные N, что для любого целого a, взаимно простого с N, $a^N - 1$ делится на N. Будем называть такие числа *числами Новака-Кармайкла.* Легко понять, что для этих чисел имеет место критерий, аналогичный критерию Корсельта (интересно, что в этом случае пропадает требование бесквадратности):

Теорема 6. *Натуральное число n является числом Новака-Кармайкла тогда и только тогда, когда $(p-1)|n$ для любого простого $p|n$.*

Например, число 220 является числом Новака-Кармайкла, потому что делится на числа 2-1, 5-1 и 11-1.
Ясно, что все числа Новака-Кармайкла, кроме единицы, чётны. Интересно в связи с этим задаться таким вопросом: для каких чисел Новака N число $2N$ является числом Новака-Кармайкла? Оказывается, что простые делители таких чисел удовлетворяют весьма сильным ограничениям.

Теорема 7. *Пусть P_0 — множество всех простых чисел, сравнимых с 3 по модулю 8. Для положительного целого n определим множество P_n как множество всех простых чисел $p \in P_{n-1}$, таких, что все простые делители числа $\frac{p-1}{2}$ также лежат в P_{n-1}. Пусть $P_\infty = \cap_{n \geq 0} P_n$. Тогда верно утверждение: p — простой делитель числа Новака N, такого, что $2N$ — число Новака-Кармайкла, тогда и только тогда, когда $p \in P_\infty$.*

Доказательство. Будем доказывать наше утверждение по индукции. Для начала заметим, что $p \in P_0$: в самом деле, $\left(\frac{-2}{p}\right) = 1$, поэтому p сравнимо с 1 или 3 по модулю 8. Но с 1 оно сравнимо быть не может, потому что тогда, в силу нашего критерия, $8|(p-1)|2N$, что не так, т.к. N нечётно.
Предположим, что мы доказали для всех таких простых p, что $p \in P_n$. Тогда, в силу Теоремы 6, $(p-1)|2N$, то есть $\frac{p-1}{2}|N$, поэтому, в силу предположения, любой простой делитель числа $p-1$ также лежит в P_n. Тем самым, первая часть утверждения доказана.
Пусть теперь $p \in P_\infty$. Рассмотрим последовательность $a_0 = p$, $a_{n+1} = [a_n, p_{1n} - 1, p_{2n} - 1, \ldots]$, где $p_{1n}, p_{2n} \ldots$ — все простые делители числа a_n. Ясно, что эта последовательность стабилизируется. В самом деле, любой её элемент является делителем числа $p!$ и при этом последовательность неубывает. Пусть $A = \lim_{n\to\infty} a_n$. Ясно, что тогда, в силу Теоремы 6, A есть

число Новака-Кармайкла. С другой стороны, на каждом шаге мы брали НОК с некоторыми элементами P_∞, так как любые простые, давшие вклад в НОК, получались из числа p в результате многократного повторения операции «выбрать какой-нибудь простой делитель числа $\frac{p-1}{2}$». Поэтому число A имеет вид $2N$ для некоторого N, у которого все делители лежат в P_0. Поэтому -2 является квадратичным вычетом по модулю N. В силу нечётности N, из этого следует, что для некоторого нечётного m выполнено сравнение $m^2 \equiv -2 \pmod N$. В силу нечётности m, имеем $(m, 2N) = (m, A) = 1$. Поэтому $m^A \equiv 1 \pmod N$, а значит $-2^N = (-2)^N \equiv m^{2N} = m^A \equiv 1 \pmod N$. Таким образом, N является числом Новака. Что и требовалось доказать. □

Основываясь на Таблице 1, мы видим, что первые несколько элементов множества P_∞ таковы:

$$3, 19, 163, 1459, 8803, 17497, 52489, 78787, 164617, 370387 \ldots$$

Можно предположить, что P_∞ — очень редкое, но всё же бесконечное множество простых чисел.

Гипотеза 1. *Множество P_∞ бесконечно.*

Интересно было бы также выработать эвристику для определения порядка роста считающей функции множества P_∞. Кроме того, содержательным вопросом представляется доказательство бесконечности хотя бы каких-нибудь из множеств P_n с $n > 1$.

Список литературы

[GLPS] J. J. Alba González, F. Luca, C. Pomerance, and I. E. Shparlinski, On numbers n dividing the n-th term of a linear recurrence, Proc. Edinburgh Math. Soc., 55 (2012), 271–289.

[KaPoRV1] A.A. Karatsuba, Š. Porubský, M. Rokyta, Z.Vlášek, Nedožité sedmdesátiny Prof. RNDr. Břetislava Nováka, DrSc. (1938-2003), Pokroky matematiky, fyziky a astronomie, ročnik 53 (2008), č 1, 53-58

[KaPoRV2] A.A. Karatsuba, Š. Porubský, M. Rokyta, Z.Vlášek, Prof. RNDr. Břetislav Nov'ak, DrSc. (1938–2003) would be seventy, Mathematica Bohemica, 133 (2008), №2, 209–218

[KP] P. Kurlberg and C. Pomerance, On a problem of Arnold: the average multiplicative order of a given integer, Algebra and Number Theory, 7 (2013), 981–999.

[M] B. Michels, Zsigmondy's Theorem, users.ugent.be/~bmichels/files/zsigmondy_en.pdf

[P] А.Г.Постников, Введение в аналитическую теорию чисел, Издательство «Наука», Москва, 1971.

[Rot] A. Rotkiewicz, On the congruence $2^{n-2} \equiv 1 \pmod{n}$, Math. Comput., 43 (1984) 271-272; MR 85e:11005.